

**Cryptology: A didactical transposition into a grade 10
school mathematics classroom**

Kalvin Whittles

A thesis submitted in fulfillment of the requirements for the degree

Doctor of Philosophy

in

UN Mathematics Education

WESTERN CAPE

Department of Mathematics and Science Education

Faculty of Education

University of the Western Cape

Supervisors:

Professor Cyril Julie (University of the Western Cape, South Africa)

Professor Ole Einar Torkildsen (College of Volda, Norway)

Professor Trygve Breiteig (University College of Agder, Norway)

November 2007

Cryptology: A Didactical transposition into a grade 10 school mathematics classroom

Kalvin Whittles

KEYWORDS

South Africa

Grade 10

Didactical transposition

Realistic mathematics education

Cryptology

Design research

Teachability

Sense-making

Teaching experiment

New school mathematics



ABSTRACT

This study is an extension of a Master's study, entitled Realistic Mathematics Education and the strategies grade 8 learners develop for the solution of two simultaneous linear equations. The current study investigates how new content could be introduced into a school mathematics curriculum. The new content under discussion for this study is the topic of cryptology.

Two design research cycles were carried out. For the first design research cycle there were three teaching experiments with teachers, grade 10 learners and students as participants. Seven activities were developed for the second design research cycle which was worked through with grade 10 learners. All sessions for the second design research cycle were video taped. Important to the development of instructional materials was the development of a hypothetical learning trajectory about the learning and teaching of each activity.

A study of the literature, a historical and didactical phenomenological analysis of cryptology and the following of a course in number theory were done before instructional materials were developed for the research design cycles. The theoretical frameworks of realistic mathematics education, didactical transposition and workbench activity were used as analysis frameworks for the study.

The results of the study indicated that the way learners understood the content and the different ways in which they presented solutions augers well for the introduction of a specific new content strand, cryptology, into a new school mathematics curriculum. Furthermore, developed instruction materials should have links with current school mathematical topics in order to facilitate an easier passage for introducing new content. It is also important for developers of instructional materials to have a strong mathematical content knowledge for the design of instructional materials. A starting point for this content knowledge should be within mathematics. By way of a didactical transposition content of a

specific mathematics topic could undergo changes before ending up as content for school mathematics.

The extract from the *Sunday Times Magazine* (Figure 0) sets the scene for the introduction in chapter 1.



Figure 0 : Extract from *Sunday Times Magazine*

UNIVERSITY of the
WESTERN CAPE

DECLARATION

I declare that Cryptology: A didactical transposition into a grade 10 school mathematics classroom is my work, that it has not been submitted for any degree or examination in any other university and that all the sources I have used or quoted have been indicated and acknowledged as complete references.

Kalvin Whittles

November 2007

Signed:



ACKNOWLEDGEMENTS

Many people and institutions played a role in assisting me during the course of this study and I am grateful to them all.

- The schools who allowed me to work with their learners over these years to collect the data for this study.
- UWC for allowing me to work with teachers studying towards a B.Ed Honors degree.
- CPUT for the space to work with second year FET students studying towards a four-year teacher qualification.
- My wife and two sons for supporting me over these years and getting me going when things got difficult.
- My supervisors, Professors Cyril Julie, Ole-Einar Torkildsen and Trygve Breiteig for academic guidance and support during the time of research. Thanks Professor Julie for introducing me to secrecy and the topic of cryptology.
- Professor Roland Fray for his valuable input and helping me to make sense of the mathematics of cryptology.
- Professor Thomas Barr for his input on chapters one and four and for presenting me with a copy of his book, *Invitation to cryptology*.
- GRASSMATE for financial assistance for the duration of the study. Professors Øyvind Mikalsen and Cyril Julie for your leadership in chairing seminars of GRASSMATE.
- All the other supervisors on GRASSMATE who contributed by way of remarks and comments to bring this study to fruition.
- Two school mathematics teachers, the late Ronald Peffer (grade 10) and Wally van Graan (grade 7) for introducing me to the world of school mathematics.
- My current employer, Cape Peninsula University of Technology, for allowing me time off to do the data analysis for the study.
- God Almighty for granting strength, courage and grace to keep going in getting this study completed.

DEDICATION

This thesis is dedicated to my wife, Elvira Denise, my sons Nicólyn William and Alvin and my late parents, Moses Daniel (3 June 1917 – 2 October 1975) and Dora (5 July 1929 – 28 June 1993).



TABLE OF CONTENTS

KEYWORDS	i
ABSTRACT	ii
DECLARATION	iv
ACKNOWLEDGEMENTS	v
DEDICATION	vi
TABLE OF CONTENTS	vii
LIST OF TABLES	xvi
LIST OF FIGURES	xvii
LIST OF ACRONYMS	xix

CHAPTER 1 THE RESEARCH QUESTION AND STUDY

OVERVIEW	1
1.1 INTRODUCTION	1
1.2 BACKGROUND TO THE STUDY	1
1.3 THE RESEARCH QUESTIONS.....	2
1.3.1 Explaining the main research question	3
1.3.2 Explaining the subsidiary research questions	3
1.4 THEORETICAL FRAMEWORK	4
1.4.1 Realistic Mathematics Education (RME)	5
1.4.2 Didactical Transposition (DT)	5
1.4.3 Workbench Activity (WA).....	5
1.5 RESEARCH DESIGN	5
1.6 THESIS STRUCTURE AND OUTLINE.....	6

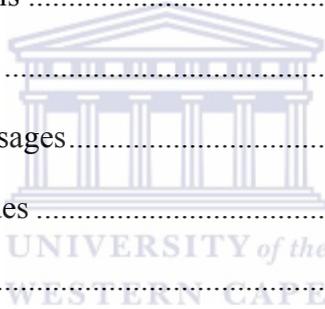
CHAPTER 2 THEORETICAL CONSIDERATIONS.....	10
2.1 INTRODUCTION	10
2.2 REALISTIC MATHEMATICS EDUCATION.....	10
2.2.1 Guided reinvention.....	12
2.2.2 Didactical phenomenology	12
2.3 DIDACTICAL TRANSPOSITION.....	14
2.3.1 Elementarization	15
2.3.2 Didactical engineering	15
2.4 WORKBENCH ACTIVITY	16
2.4.1 Practice.....	16
2.4.2 Dance of agency.....	18
2.4.3 Disciplinary agency.....	19
2.5 SUMMARY	21
CHAPTER 3 METHODOLOGY and RESEARCH DESIGN.....	22
2.1 INTRODUCTION	22
2.2 DESIGN RESEARCH	23
2.2.1 Characteristics	23
3.2.1.1 Cyclical nature of design research	24
3.2.1.2 Role of design	25
2.3 HYPOTHETICAL LEARNING TRAJECTORY (HLT).....	25
2.4 PREPARATIONS AND DESIGN PHASE.....	26
2.5 TEACHING EXPERIMENT PHASE	27
2.6 RETROSPECTIVE ANALYSIS PHASE	28
2.7 RELIABILITY AND VALIDITY	30
2.8 TEACHING EXPERIMENTS AND RESEARCH	
PARTICIPANTS	31
2.9 CONCLUSION	32

CHAPTER 4 LITERATURE REVIEW	33
4.1 INTRODUCTION	33
4.2 CRYPTOLOGY	33
4.3 TERMINOLOGY	34
4.4 CRYPTOGRAPHY	35
4.5 CRYPTANALYSIS	36
4.6 HISTORICAL BACKGROUND.....	38
4.6.1 Ancient uses	38
4.6.1.1 Birth of cryptology.....	38
4.6.1.2 Mesopotamia.....	39
4.6.1.3 Bible	39
4.6.1.4 Military context.....	40
4.6.1.5 Polybius.....	41
4.6.1.6 Iraq	42
4.6.1.7 Love and the occult.....	42
4.6.1.8 Yahmadi	43
4.6.1.9 Bacon	43
4.6.1.10 Nomenclator	43
4.6.1.11 Encyclopedia.....	44
4.6.1.12 Alberti	44
4.6.1.13 Trithemius	45
4.6.1.14 Belaso	47
4.6.1.15 Porta	47
4.6.1.16 Vigenère	49
4.6.1.17 Bacon vs Shakespeare.....	50
4.6.1.18 Jefferson	50
4.6.1.19 Electronic Communication.....	51
4.6.1.20 Wheatstone.....	52
4.6.1.21 Marconi	53
4.6.2 War World I	54
4.6.2.1 Austria.....	54
4.6.2.2 Russia	54
4.6.2.3 Britain.....	55
4.6.3 World War II.....	56
4.6.4 Modern Uses	59
4.7 OTHER RESEARCH INITIATIVES.....	63
4.7.1 Histo MAP project	63
4.7.1.1 Codes galore.....	63
4.7.1.2 Loads of codes	64

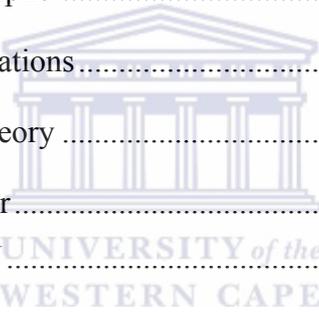
4.7.2	Washington MESA project	65
4.8	ANALYSIS	67

CHAPTER 5 HISTORICAL AND DIDACTICAL

	PHENOMENOLOGY OF CRYPTOLOGY	68
5.1	INTRODUCTION	68
5.2	PHENOMENOLOGY	69
5.3	HISTORICAL PHENOMENOLOGY OF CRYPTOLOGY	70
5.3.1	Bald message.....	71
5.3.2	A belt.....	71
5.3.3	Fire signals	72
5.3.4	Flag signals	72
5.3.5	Quilt code.....	72
5.3.6	Hobo messages.....	73
5.3.7	Sports codes.....	73
5.3.8	Pig Latin.....	73
5.4	DIDACTICAL PHENOMENOLOGY OF CRYPTOLOGY	74
5.4.1	Bald message.....	74
5.4.2	A belt.....	74
5.4.3	Substitution ciphers.....	74
5.4.4	Pig Latin.....	75
5.4.5	Discussion	75
5.5	CONCLUSION	76



CHAPTER 6 FIRST DESIGN RESEARCH CYCLE.....	77
6.1 INTRODUCTION	77
6.2 OUTLINE OF HYPOTHETICAL LEARNING TRAJECTORY.....	78
6.2.1 Teachers	78
6.2.2 Learners.....	79
6.2.3 Students.....	79
6.3 TEACHING MATERIALS	80
6.4 TEACHING EXPERIMENTS.....	81
6.4.1 Method	82
6.5 FEED-FORWARD ANALYSIS.....	86
CHAPTER 7 SECOND DESIGN RESEARCH CYCLE.....	88
7.1 INTRODUCTION	88
7.2 OUTLINE OF HYPOTHETICAL LEARNING TRAJECTORY.....	88
7.3 ACTIVITY 1	89
7.3.1 HLT for activity 1	89
7.3.2 Retrospective analysis.....	90
7.4 ACTIVITY 2.....	92
7.4.1 HLT for activity 2	92
7.5 ACTIVITY 3.....	94
7.5.1 HLT for activity 3	94
7.5.2 Retrospective analysis.....	94
7.6 ACTIVITY 4.....	97
7.6.1 HLT for activity 4	97
7.6.2 Retrospective analysis.....	98
7.7 ACTIVITY 5.....	99
7.7.1 HLT for activity 5	99
7.7.2 Retrospective analysis.....	100
7.8 ACTIVITY 6.....	103

7.8.1	HLT for activity 6	103
7.8.2	Retrospective analysis.....	104
7.9	ACTIVITY 7.....	104
7.9.1	HLT for activity 7	104
7.9.2	Retrospective analysis.....	105
7.10	OVERVIEW OF ACTIVITIES	105
7.11	RETROSPECTIVE ANALYSIS	106
7.11.1	Scytale.....	106
7.11.2	Alberti disk.....	107
7.11.3	Caesar cipher.....	107
7.11.4	Function cipher.....	108
7.11.5	Linear equations.....	108
7.11.6	Number theory	108
7.11.7	RSA cipher.....	109
7.12	CONCLUSION.....	109
		
CHAPTER 8 FINDINGS AND CONCLUSION.....		110
8.1	INTRODUCTION	110
8.2	ANSWER TO THE FIRST SUBSIDIARY RESEARCH QUESTION.....	110
8.3	ANSWER TO THE SECOND SUBSIDIARY RESEARCH QUESTION.....	113
8.4	ANSWER TO THE THIRD SUBSIDIARY RESEARCH QUESTION.....	115
8.4.1	Substitution as bridgehead	116
8.5	ANSWER TO THE MAIN RESEARCH QUESTION.....	118
8.6	REFLECTION AND DISCUSSION	119
8.6.1	Methodology	119
8.6.2	Theoretical framework.....	121

8.6.3	Literature review	121
8.7	LIMITATIONS OF THE STUDY	122
8.8	RECOMMENDATIONS	122
8.9	CONCLUSION	123
REFERENCES.....		124
APPENDIX A NOTES.....		130
APPENDIX B POSSIBLE PROJECTS FOR CRYPTOLOGY		131
APPENDIX C ALBERTI DISK: EXAMPLE		134
APPENDIX D1 RSA PUBLIC-KEY: EXPLANATION		135
APPENDIX D2 RSA PUBLIC-KEY: EXAMPLE.....		136
APPENDIX E FIRST DESIGN RESEARCH CYCLE (TITLE PAGE)		137
APPENDIX E1	FIRST TEACHING EXPERIMENT (TITLE PAGE).....	138
APPENDIX E2	UNIT 1: THE SPARTAN SCYTALE	139
APPENDIX E3	SPARTAN SCYTALE: ANSWER SHEET	140
APPENDIX E4	SECOND TEACHING EXPERIMENT (TITLE PAGE).....	141
APPENDIX E5	DECIPHERING AND READING OF MESSAGES	142
APPENDIX E6	DECIPHERING AND READING OF MESSAGES:	
	ANSWER SHEET	144
APPENDIX E7	THIRD TEACHING EXPERIMENT (TITLE PAGE)	145
APPENDIX E8	ALBERTI DISK	146
APPENDIX E9	ALBERTI DISK: ANSWER SHEET	147
APPENDIX F INVITATION FOR RESEARCH		148
APPENDIX G EPISODES FROM SECOND TEACHING		
	EXPERIMENT.....	149
APPENDIX H SECOND DESIGN RESEARCH CYCLE: ACTIVITIES		
	AFRIKAANS VERSION (FRONT PAGE).....	150
APPENDIX H1	CONTENTS	151
APPENDIX H2	INTRODUCTION	152
APPENDIX H3	TRANSPOSITION CIPHERS: OVERVIEW	153
APPENDIX H4	ACTIVITY 1: SPARTAN SCYTALE	154

APPENDIX H5 ALBERTI CIPHERS: OVERVIEW	156
APPENDIX H6 ACTIVITY 2: ALBERTI DISK.....	157
APPENDIX H7 ADDITIVE CIPHERS: OVERVIEW	159
APPENDIX H8 ACTIVITY 3: CAESAR CIPHER.....	160
APPENDIX H9 FUNCTION CIPHERS: OVERVIEW	161
APPENDIX H10 ACTIVITY 4: FUNCTION CIPHER.....	162
APPENDIX H11 AFFINE CIPHERS: OVERVIEW	163
APPENDIX H12 ACTIVITY 5: AFFINE CIPHER.....	164
APPENDIX H13 NUMBER THEORY: OVERVIEW	166
APPENDIX H14 ACTIVITY 6: NUMBER THEORY.....	167
APPENDIX H15 RSA CIPHER: OVERVIEW.....	170
APPENDIX H16 ACTIVITY 7: RSA CIPHER.....	171
APPENDIX I SECOND DESIGN RESEARCH CYCLE: ACTIVITIES	
ANSWERS (FRONT PAGE)	175
APPENDIX I1 CONTENTS.....	176
APPENDIX I2 INTRODUCTION	177
APPENDIX I3 ACTIVITY 1: SOLUTION.....	178
APPENDIX I4 ACTIVITY 2: SOLUTION.....	179
APPENDIX I5 ACTIVITY 3: SOLUTION.....	180
APPENDIX I6 ACTIVITY 4: SOLUTION.....	181
APPENDIX I7 ACTIVITY 5: SOLUTION.....	182
APPENDIX I8 ACTIVITY 6: SOLUTION.....	184
APPENDIX I9 ACTIVITY 7: SOLUTION.....	186
APPENDIX J SECOND DESIGN RESEARCH CYCLE: ACTIVITIES	
ENGLISH VERSION (FRONT PAGE)	188
APPENDIX J1 CONTENTS.....	189
APPENDIX J2 INTRODUCTION	190
APPENDIX J3 TRANSPOSITION CIPHERS: OVERVIEW	191
APPENDIX J4 ACTIVITY 1: SPARTAN SCYTALE	192
APPENDIX J5 ALBERTI CIPHERS: OVERVIEW.....	193
APPENDIX J6 ACTIVITY 2: ALBERTI DISK	194
APPENDIX J7 ADDITIVE CIPHERS: OVERVIEW	196

APPENDIX J8 ACTIVITY 3: CAESAR CIPHER	197
APPENDIX J9 FUNCTION CIPHERS: OVERVIEW	198
APPENDIX J10 ACTIVITY 4: FUNCTION CIPHER.....	199
APPENDIX J11 AFFINE CIPHERS: OVERVIEW.....	200
APPENDIX J12 ACTIVITY 5: AFFINE CIPHER	201
APPENDIX J13 NUMBER THEORY: OVERVIEW.....	203
APPENDIX J14 ACTIVITY 6: NUMBER THEORY	204
APPENDIX J15 RSA CIPHER: OVERVIEW	206
APPENDIX J16 ACTIVITY 7: RSA CIPHER	207
APPENDIX K TRANSLATION FOR FIGURE 3.5.....	211



LIST OF TABLES

Table 3.1 : First design research cycle	31
Table 4.1 : Example of a code	34
Table 4.2 : Cryptographic goals	36
Table 4.3 : Caesar alphabet	41
Table 4.4: Polybius square	41
Table 4.5: Example using Alberti's cipher wheel	45
Table 4.6: Trithemius' tableau	46
Table 4.7: Example using Trithemius' tableau	46
Table 4.8: Example of Belaso's work using the keyword <i>axis</i>	47
Table 4.9: Digraphic cipher	48
Table 4.10: Vigenère's autokey	49
Table 4.11: Example of Bacon's cipher	50
Table 4.12: Wheatstone's cipher using <i>Raymond</i> as keyword	52
Table 6.1: Group breakdown for teachers	82
Table 6.2: Group breakdown for learners	83
Table 6.3: Group breakdown for students	84
Table 7.1: Summary of seven activities	106
Table 8.1: Summary of first design research cycle	111
Table 8.2: HLT's alignment with LSS	114

LIST OF FIGURES

Figure 0 :	Extract from <i>Sunday Times Magazine</i>	iii
Figure 1.1 :	Thesis structure and outline (1, 2, 3 ... refer to chapters).....	6
Figure 1.2:	Impact of study on classroom practice.....	8
Figure 2.1 :	Theoretical considerations	21
Figure 3.1 :	Outline of research cycles	25
Figure 3.2 :	Example of an observation.....	28
Figure 4.1 :	Cryptosystem in cryptology	38
Figure 4.2:	Alberti's cipher wheel	44
Figure 4.3:	Enigma machine.....	57
Figure 6.1:	Time-line for first design research cycle.....	77
Figure 6.2:	Teacher's solution using columnar method	85
Figure 6.3:	Learner's solution using number of turns	85
Figure 6.4:	Learner's solution using columnar method.....	86
Figure 6.5:	Prepared message around batten	87
Figure 7.1:	Feed-forward from first to second design research cycle	88
Figure 7.2:	Transposition cipher activity.....	90
Figure 7.3:	Message on parchment around batten	90
Figure 7.4:	Transposition cipher activity: Solutions to problems 1.1 to 1.4 ...	91
Figure 7.5:	Transposition cipher activity: Description of turns.....	91
Figure 7.6:	Alberti's disk activity.....	92
Figure 7.7:	Alberti alphabet with cipher alphabets.....	93
Figure 7.8:	Alberti disk activity: Description of addition and subtraction.....	93
Figure 7.9:	Caesar cipher activity	94
Figure 7.10:	Caesar cipher activity: Solution to problem 3.....	95
Figure 7.11:	Caesar cipher activity: Description of values larger than 25	96
Figure 7.12:	Caesar cipher activity: Groups two's solution to problem 3.....	96
Figure 7.13:	Function cipher activity.....	97
Figure 7.14:	Function cipher activity: Substitution for x	98
Figure 7.15:	Function cipher activity: Solution for x and $f(x)$	98
Figure 7.16:	Function cipher activity: Solution to problem 1.4	99

Figure 7.17:	Affine cipher activity	100
Figure 7.18:	Affine cipher activity: Solution to problem 1	100
Figure 7.19:	Affine cipher activity: Solution to problem 2	101
Figure 7.20:	Affine cipher activity: Solution to problem 3 (group 3)	101
Figure 7.21:	Affine cipher activity: Solution to problem 3 (group 1)	102
Figure 7.22:	Affine cipher activity: Solution to problem 4	102
Figure 7.23:	Number theory activity	103
Figure 7.24:	Number theory activity: Solution to problem 2.1	104
Figure 7.25:	RSA cipher activity	105
Figure 7.26:	Scytale: Description of parchment	106
Figure 7.20:	Affine cipher activity: Solution to problem 3 (group 3)	116
Figure 7.22:	Affine cipher activity: Solution to problem 4	117
Figure 8.1:	Bridgehead as a link between known and new work	118
Figure 8.2:	Possible route for introducing new content.....	119



LIST OF ACRONYMS

OBE	Outcomes Based Education
TE	Teaching Experiment
RME	Realistic Mathematics Education
DT	Didactical Transposition
WA	Workbench Activity
GRASSMATE	Graduate Studies in Science, Mathematics and Technology Education
UWC	University of the Western Cape
ROSE	Relevance of Science Education
B.Ed	Bachelor of Education
FET	Further Education and Training
CPUT	Cape Peninsula University of Technology
MP	Mangle of Practice
STS	Science, Technology and Society
G10-C1	Grade 10 – First Cycle
G10-CII	Grade 10 – Second Cycle
T-CI	Teachers – First Cycle
ST-CI	Students – First Cycle
HLT	Hypothetical Learning Trajectory
TE1	First Teaching Experiment
TE2	Second Teaching Experiment
TE3	Third Teaching Experiment
WCED	Western Cape of Education Department
USA	United States of America
M or P	Plaintext
C	Ciphertext
$E_K(M)$	Encryption key of M the plaintext
$D_K(C)$	Decryption key of C the ciphertext
USMTC	United States Military Telegraph Corps
NBS	National Bureau of Standards

IBM	International Business Machines
DES	Data Encryption Standard
ATM	Automated Teller Machine
RSA	Rivest, Shamir and Adleman
PIN	Personal Identification Number
PEM	Privacy Enhanced Mail
PGP	Pretty Good Privacy
FBI	Federal Bureau of Investigation
NIST	National Institute of Standards and Technology
DSS	Digital Signature Standard
AES	Advanced Encryption Standard
EEC	Elliptic Curve Cryptography
Histo MAP	History of Mathematics and its Applications Project
COMAP	Consortium for Mathematics and its Applications Project
ZIP	Zonal Improvement Plan
ISBN	International Standard Book Number
MESA	Mathematics, Engineering, Science Achievement
NCTM	National Council for School Mathematics
DRC	Design Research Cycle
TE1 (T)-C1	First Teaching Experiment with Teachers in Cycle 1
TE2 (L)-C1	Second Teaching Experiment with Learners in Cycle 1
TE3 (S)-C1	Third Teaching Experiment with Students in Cycle 1
LSS	Learners' Solution Strategy

CHAPTER 1

THE RESEARCH QUESTION AND STUDY OVERVIEW

1.1 INTRODUCTION

For all of its existence humankind has always been intrigued by codes and secrets. On the one side is the ongoing urgency to develop codes to keep information secret, whilst others work hard at breaking codes to access secret information. This ongoing battle between code makers and code breakers is in essence civilization's secret history. Code makers (cryptographers) work under the topic of cryptography, whereas the work of code breakers (cryptanalysts) falls under cryptanalysis. Cryptography and cryptanalysis form the overall topic of cryptology.

These battles between cryptographers and cryptanalysts are interspersed over different spheres of life. Wars, countries, governments, businesses, computers and even ordinary people's lives are influenced by codes and secrets. An important element of codes and secrets is information. Man's search for the absolute code of secrecy ventured into new avenues of mathematics. In this way the use of big prime numbers were introduced to change information into a code. As our whole existence is built on information, the question is how the topic of cryptology encompassing both cryptography and cryptanalysis, could be introduced by mathematics educators into a school mathematics curriculum? This is one of the challenges this study tries to undertake.

1.2 BACKGROUND TO THE STUDY

In 2006 new curricula were introduced for all subjects in grade 10 in South Africa. The main aim of the new curricula was to break the shackles of the Apartheid past and to implement an Outcomes Based Education (OBE). This implied that learners had to show understanding of the content taught and be able to apply these competencies in different contexts.

More than ten years into our democracy, education in South Africa has undergone many changes and for school mathematics these changes have been drastic. Mathematics higher grade and standard grade (offered previously to grade 10 to 12 learners) were phased out and replaced with mathematics and mathematical literacy. Furthermore, all learners in grades 10 to 12 have to do one of the aforementioned subjects – this means as from 2006 all grade 10 learners will either do mathematics or mathematical literacy. School-going mathematics (mathematics or mathematical literacy) becomes compulsory for grade 10 to 12 learners. It is against this background that this study is undertaken.

1.3 THE RESEARCH QUESTIONS

The aim of this study is to investigate how new content could be introduced into a school mathematics curriculum and to develop an instructional theory for the teaching of a specific new content strand, cryptology. The main research question thus reads:

How could new content be introduced into school mathematics curricula?

UNIVERSITY of the
WESTERN CAPE

In order to obtain answers with respect to the overarching question stated above, the following interrelated subsidiary research questions are posed:

- *The question of teachability: How does one make the topic of cryptology teachable in school-going mathematics?*
- *The question of sense-making: How do learners make sense of the work on cryptology?*
- *The question of workbench activity: What sorts of activities will be generated by learners while working at the workbench?*

1.3.1 Explaining the main research question

How could new content be introduced into a school mathematics curriculum?

What follows is an explanation of the important constructs/words used in the main research question. They are explained and further references are given where these words are discussed in chapters within this study.

The main research question deals with the content of a topic for a school mathematics curriculum. The content identified is the topic of cryptology. In the main research question *how could* refers to a possible way that can be followed to introduce any content into a school mathematics curriculum. As mentioned before, *new content* is the topic of cryptology, which includes both cryptography and cryptanalysis. More information on cryptology can be found in chapters 3 and 4. *School mathematics curriculum* indicates the curriculum followed for mathematics in schools. The words *school mathematics* is used to indicate the mathematics or mathematical literacy that is done at school level.

1.3.2 Explaining the subsidiary research questions

How does one make the topic of cryptology teachable in school-going mathematics?

As the topic cryptology originates in the field of mathematics, the question addresses the form cryptology will have when introduced into a school mathematics classroom. These changes allude to the topic of cryptology undergoing a didactical transposition before ending up as a topic in a school mathematics classroom. Didactical transposition is captured as part of the theoretical framework discussed in chapter 2.

The word *teachable* refers to the content as developed to be presented by the teacher to learners of school mathematics. *Teachable*, not necessarily only refers

to the actual process of teaching, but could also refer to activities learners have to do on their own whilst the teacher acts as a facilitator in the class. *School-going mathematics* is the mathematics school-going learners do at school – also referred to as school mathematics and includes both mathematics and mathematical literacy.

How do learners make sense of the work on cryptology?

The use of the words *make sense* (*sense-making*) in the research question refers to the ways learners understand the work on cryptology. It also alludes to the ways and strategies they use whilst working on cryptological activities.

What sort of activities do learners engage with while working at the workbench?

Activities as used in the above research question include all the happenings as the learners work at the workbench. These happenings can include their actual writing, talking, gesturing and any other occurrences. *Workbench* is the place where learners or groups of learners work during the school mathematics sessions.

It is expected that designed activities on cryptology will be well received by participants. For this to happen, designers when designing activities on a new topic should take great care. It is recommended that they should have a thorough content knowledge of the topic concerned and designed activities should also consider the conceptual development of the participants.

1.4 THEORETICAL FRAMEWORK

Now that the research questions have been formulated and clarified, the question of the theoretical framework suitable for this study is addressed. Criteria to be considered for a useful theoretical framework are its relation to the research questions and its applicability to the design of instructional activities and to the interpretation and analysis of learners' observations (Drijvers, 2003:14).

In the following chapter the theoretical considerations best for this study are discussed. Of importance for this study is the development of instructional

materials for use in the teaching experiments (TE). Teaching experiment refers to each session with learners to work on activities. The frameworks used will be Realistic Mathematics Education (RME), Didactical Transposition (DT) and Workbench Activity (WA).

1.4.1 Realistic Mathematics Education (RME)

RME was developed in the Netherlands under the watchful eye of Freudenthal in the early 1970's. As a theory of mathematics education it offers a pedagogical and didactical philosophy for the teaching and learning, and on the design of instructional material for mathematics education. Theoretical issues from RME deemed suitable for this study will be used.

1.4.2 Didactical Transposition (DT)

Chevillard (1991, 1992) developed the theory of didactical transposition in the early 1980's. An important concept within didactical transposition is elementarization. Elementarization takes place with reference to the content of cryptology as it moves from its original sources or starting points in mathematics to the different points of teaching, namely a school mathematics classroom. Piloting of designed materials was done over two cycles. The first cycle, consisting of three different teaching experiments was done in one daily session, whilst the second cycle was done over a week with a unit consisting of seven activities.

1.4.3 Workbench Activity (WA)

Using the ideas of Pickering (1995) on the mangle of practice a framework is developed for the analysis of the goings-on or happenings at the workbench.

1.5 RESEARCH DESIGN

Whereas RME sets the scene for the overall study, design research serves as methodology as design forms an integral part of the research. Design in this context refers to the design of instructional materials for the teaching experiments.

A design research cycle has three phases:

- preparation and design phase;
- teaching experiment and
- retrospective analysis.

Design research, chosen as the preferred methodology is discussed in chapter 3. Teaching experiments are covered in chapters 6 and 7 and the retrospective analysis forms part of chapters 6, 7 and 8.

1.6 THESIS STRUCTURE AND OUTLINE

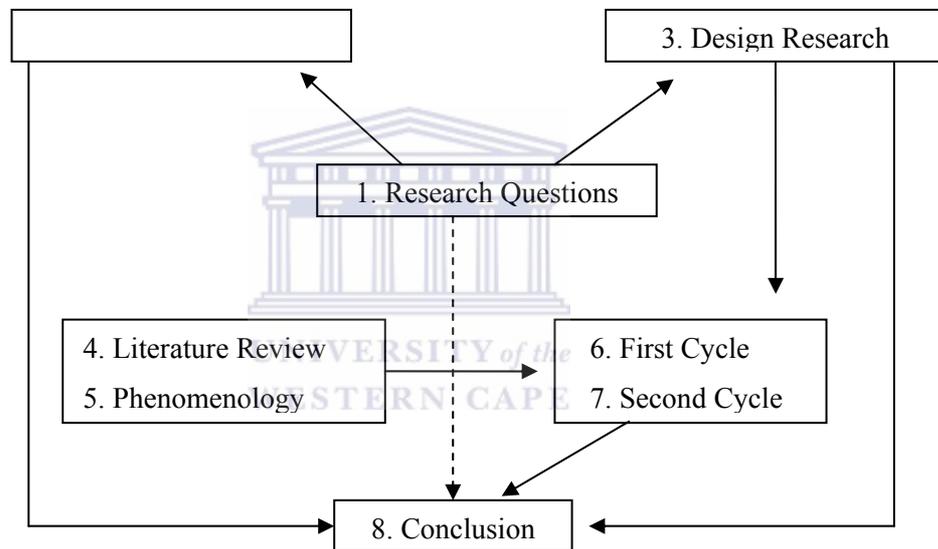


Figure 1.1 : Thesis structure and outline (1, 2, 3 ... refer to chapters)

Figure 1.1 gives an outline of the thesis. Chapter names are not given in full and only key words or abbreviations are used to indicate names for the respective chapters. The allocated numbers are in line with the chapter numbers of the thesis. For example, Chapter 1 is entitled the research question and study overview and is referred to as research questions in the figure. The research questions impact on the choice of theoretical frameworks for this study and are shortened to 1 Research Questions in Figure 1.1. The methodology of design research is an outcome of the theoretical framework and research questions and leads to the implementation phase of two cycles. From these two cycles are

drawn the conclusions for this research under the auspices of the stated research questions. Chapters 4 and 5, the literature review and historical and didactical phenomenology of cryptology, influence the materials developed for use in the research cycles.

1.7 CONTEXT FOR THE STUDY

This study was done under the auspices of the Graduate Studies in Science, Mathematics and Technology Education (GRASSMATE; see Appendix A, Note 1) initiative. GRASSMATE is a joint research initiative between the University of Bergen in Norway and the University of the Western Cape (UWC) in Cape Town. At a workshop held in 2000 (Julie & Mikalsen, 2000) academics from Norway and Sub-Saharan Africa gathered to set up this programme for doctoral research in Science, Mathematics and Technology Education to broaden the expertise for these disciplines in Sub-Saharan Africa. Another aim is to set up joint research initiatives or widen cooperative research between researchers from Norway and Sub-Saharan Africa. The Relevance of Science Education (ROSE) (Sjøberg, 2002) initiative is such an example.

Within the field of study, mathematics education, this study tries to address the dialectic between research and a school mathematics classroom. By way of design research as a methodology the study tries to do research on learning and teaching and its impact on classroom practice. The committee on learning research and educational practice (National Research Council, USA, 2004) highlights some of the barriers to research and practice:

- influence of research on educational practice is weak;
- educators generally do not look to research for guidance;
- language used by researchers is different from that of teachers and
- workload of teachers leaves them with little time to identify and read research.

Past research has at times managed to influence practice, albeit slowly and for the most part indirectly. The manner of influence is illustrated in figure 1.2 and is an adapted version of the one proposed by the committee (National Research Council, USA, 2004:7) and is an illustration of how this study could possibly have an impact on classroom practice:

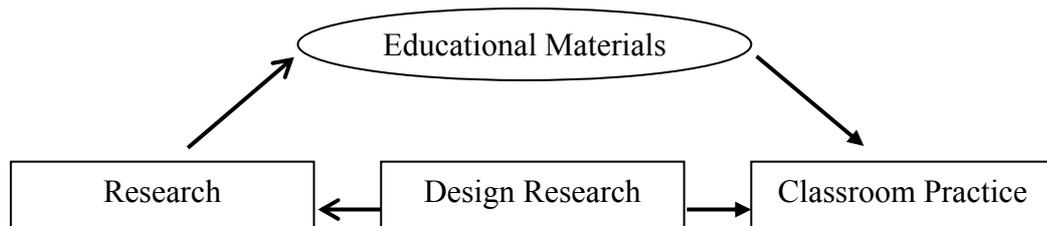


Figure 1.2: Impact of study on classroom practice

1.8 RESEARCH IMPLEMENTATION DECISIONS

What follows are some of the important decisions taken to give direction to the research questions. The two research cycles would be done with grade 10 learners from state schools in the Western Cape. These learners were to work in groups and at most two groups would be allowed. These teaching experiments with the learners would be video recorded with a camera focusing on the groups whilst working on instructional cryptological activities in a classroom. Learners would be allowed to make use of the available technology (scientific calculators) when doing calculations, but must at all times write out their solutions in full.

In a deviation from this decision, teaching experiments were also held with teachers of school mathematics and students in the second year of study towards a teacher's qualification. These were teachers enrolled for the Bachelor of Education (B.Ed) Honors degree course in mathematics education at the University of the Western Cape. Their teaching experiment was followed up with an exam question related to the work done in the teaching experiment. The students were all doing mathematics for teaching as one of their main subjects studying towards a Further Education and Training (FET) teacher's qualification at the Cape Peninsula University of Technology (CPUT) on the Wellington Campus. All of this is reported on in the first research cycle in chapter 6.

All teaching experiments were to be video recorded. If problems arose and no video recording was made, observations would be used in order to keep notes of the teaching experiment.

In the chapter that follows the theoretical frameworks used for this research are discussed.



CHAPTER 2

THEORETICAL CONSIDERATIONS

2.1 INTRODUCTION

Under scrutiny in this chapter are the theoretical frameworks for this study. In this regard, the study draws on different theoretical stances. The first theoretical position is informed by the theory of Realistic Mathematics Education (RME). RME developed in the Netherlands in the 1970's under Freudenthal (1973) and is an educational theory “that offers a pedagogical and didactical philosophy on mathematical learning and teaching as well as on designing instructional materials for mathematics education” (Bakker, 2004:5). This is in line with figure 1.2 in chapter one which captures what the thesis tries to achieve:

- To make the topic of cryptology teachable for grade 10 school mathematics learners and
- Design of instructional materials for the topic of cryptology.

Secondly, the study draws on the theory of didactical transpositions (DT) of the French mathematical didactical school. Inherent to the theory of didactical transpositions is the processes by which mathematical topics move from their sources of origin to various places of teaching (Julie, 2002:29). For this thesis it starts out as a topic in the field of mathematics and ends up as a topic for school teaching mathematics in a grade 10 classroom.

Thirdly, the study utilizes the theory of mangle of practice from the work of Pickering, entitled, Mangle of Practice (MP), to formulate a framework, called workbench mathematical activity and practices (WA) to evaluate the happenings or goings-on at the workbench

2.2 REALISTIC MATHEMATICS EDUCATION

The instruction theory of RME has made a considerable impact in the Netherlands over the past thirty years. Developed by Freudenthal in the early 1970's, this

theory was further developed under the auspices of the Freudenthal Institute. RME considers mathematics as a human (mental) activity (Freudenthal, 1973; Gravemeijer & Terwel, 2000). Teaching and learning within RME start with realistic or recognizable contexts. These realistic contexts are mathematized to lead to more formal relations and abstract structures (Van den Heuvel-Panhuizen, 1996).

Treffers (1987), however, distinguishes between horizontal and vertical mathematization. Horizontal mathematization is about changing contextual problems into a mathematical problem, whilst vertical mathematization involves taking mathematical problems to a higher level. Vertical mathematization thus opens up avenues for setting problems, which induce solutions at different mathematical levels (Freudenthal, 1991; Gravemeijer & Terwel, 2000). RME is not restricted to mathematical problems in realistic contexts only, but is open for developing formal mathematics by learners in any given context.

The three main underlying principles of RME are (Freudenthal, 1973, 1991):

- Guided reinvention;
- Didactical phenomenology and
- Emergent models.

These principles are drawn from Freudenthal's work, which emphasizes reinvention through progressive mathematization (Freudenthal, 1973, 1991). Through the process of mathematization learners develop informal solution strategies from experientially real situations (Gravemeijer & Doorman, 1999). RME allows researchers to use problems from realistic contexts that can lead to a wide variety of solution strategies. This was confirmed in a previous study where grade 8 learners worked on problems in a realistic context (Whittles, 1996).

2.2.1 Guided reinvention

There is a consideration in mathematics education to view learning as a construction process. This contention was enforced by writings in RME (Treffers, 1987; Van den Heuvel-Panhuizen, 1996). Learning as a construction process is a principle of RME and is described as a reinvention process. Reinvention means that learners, up to a point, repeat the learning process of mankind (Freudenthal, 1983a, 1991). Freudenthal, however, pleads for a process of guided reconstruction.

Guided reinvention affords learners the opportunity to develop their own informal solution strategies that can lead them to the construction of solution procedures. In this way the reinvention process is guided by the teacher and the materials learners work on. For material development the teacher can look at the history of a topic in mathematics as a source of inspiration. This is done in the literature review and the historical and didactical phenomenology of cryptology in chapters 4 and 5 of this thesis.

The teacher also uses the informal solution strategies of learners solving experientially real problems for which standard solution procedures are not yet known, as starting points to lead to the formulation of procedures (Gravemeijer, 1994; Streefland, 1991). Using the process of progressive mathematization the teacher then uses all these to formulate a possible learning sequence or trajectory.

2.2.2 Didactical phenomenology

Freudenthal (1973) sees didactical phenomenology as the study of the relation between the phenomena that the mathematical concept represents and the concept itself. The focus is on how mathematical interpretations make phenomena accessible for reasoning and calculations. Didactical phenomenology has a design principle as it identifies possible instructional activities that could support individual or group discussions in which learners engage in progressive mathematization (Gravemeijer, 1994).

The aim of the phenomenological investigation is to create an environment wherein learners can work to reconstruct their informal solutions into sophisticated solutions when they work on experientially real problems (Gravemeijer, Cobb, Bowers & Whitenack, 2000). This principle of didactical phenomenology is applied in chapter 5 to the topic of cryptology.

2.2.3 Emergent models

The third principle of emergent models serves as a bridge between informal and formal knowledge in mathematics. The term model is used in a holistic way and refers to the situational and mathematical models developed by learners. In the first instance the model is a model of a situation that is known or familiar to learners. Secondly, the model becomes an entity of its own by the process of generalizing and formalizing. In this way the entity is used as a model for mathematical reasoning.

Gravemeijer (1994) identifies four models for learning and teaching:

- Situational;
- Referential;
- General and
- Formal.



For the situational level, situational knowledge and strategies are used within the context of the situation. Referential level refers to the situation described in the problem. General level is where the emphasis on mathematical strategies has preference over the context. Formal level of mathematics is where learners work with conventional mathematical procedures and notations.

The three principles of reinvention, didactical phenomenology and emergent models can be of service to the teacher in the development of hypothetical learning trajectories that can be investigated and revised during experiments in a school mathematics classroom. RME addresses both the collective mathematical

development of learners of school mathematics and of their mathematical learning as they participate in these teaching experiments.

2.3 DIDACTICAL TRANSPOSITION

A distinction is made in France between educational theory or pedagogy and the didactics of a subject. For example, the didactics of mathematics is regarded as the science of teaching and learning mathematics.

In simple terms, pedagogy is more general than didactics. The term pedagogy is generally used in terms of education and, according to Houssaye (Pepin, 1999:9), pedagogy includes general educational theory, such as socio-psychological theory. Didactics is, according to Henry (Pepin, 1999), "the study of phenomena of the teaching and learning in one discipline" which specifically includes not only the teaching but also the learning of the subject. Thus, the term pedagogy is used in a much broader sense and not specialized on one subject, whereas didactics refers almost immediately to the teaching and learning of a specific subject.

Robert (Pepin, 1999:11) explains didactics as follows:

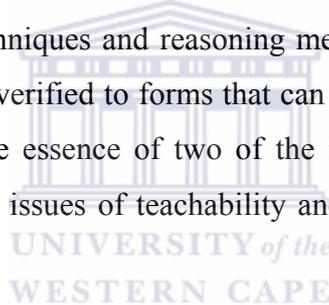
One of the ambitions of didactics is to try to specify in the most scientific way the real possibilities for manoeuvre for all ... teaching in the class by analyzing the functioning of the totality of the system and its components, and then to develop and study certain choices which are regarded to be optimal in the sense of general and individualized classroom management

Didactics of mathematics is aimed at the preparation of mathematics for learners. The theoretical framework of didactical transposition serves as an overarching theory to do so. Chevallard developed the theory of didactical transposition in the early 1980's (Chevallard, 1991, 1992). In the first part of the next section, there is an attempt to show how the theoretical framework shapes the process of preparing mathematics for teachers and learners. This will be done by way of elementarization of knowledge. This section concludes with a discussion of didactical engineering that serves to make the framework operational (Artigue, 1994:27).

Didactical transposition within the scope of the thesis implies the movement of knowledge from an institution of knowledge production to an institution where teachers teach learners. Knowledge refers to the topic of cryptology. Institution of knowledge is referred to as sources by Julie (2002) and it can take on different forms. For this study it refers to the non-exam course on number theory that was followed at the mathematics department of UWC, the literature review and historical and didactical phenomenology of cryptology and consultations with supervisors. Targets as referred to by Julie (2002) are in the context of this study, a grade 10 school mathematics classroom.

2.3.1 Elementarization

Fey's (1994:15) exposition of elementarization as the "translation of mathematical concepts, principles, techniques and reasoning methods from the forms in which they are discovered and verified to forms that can be learned by a broad audience of students" captures the essence of two of the interrelated subsidiary research questions addressing the issues of teachability and sense-making with respect to cryptology.



Elementarization impacts on the content of cryptology as it moves from the different sources to the point of delivery, a school mathematics classroom.

2.3.2 Didactical engineering

Didactical engineering emerged within the field of didactics. According to Chevillard (1991) didactical engineering addresses two fundamental issues:

- Dealing with the complexities of the phenomena in research method and practice;
- The relationship between research and action in the educational setup.

The term engineering draws an analogy between the development, design and implementation work in mathematics education and the work of a civil engineer.

The use of didactical engineering within the framework of this study refers to the teacher who designs mathematical material for implementation and evaluation in a school mathematics classroom.

Figure 2.1 outlines the route cryptology as a mathematics topic takes to end up as a topic for teaching in a school mathematics classroom. Also given are the different aspects that influenced cryptology, the source, in its didactical transposition to end up as a school mathematics topic.

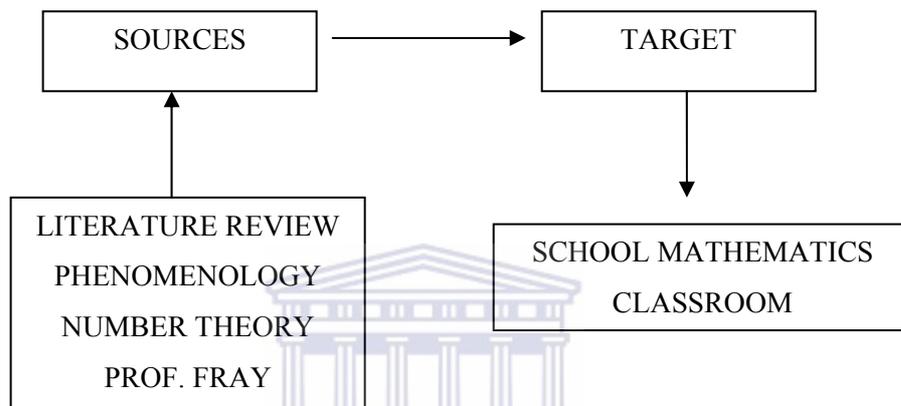


Figure 2.1 : Movement of cryptology from sources to target

2.4 WORKBENCH ACTIVITY

The discussion of the theoretical framework for the goings-on at the workbench serves as a basis for the interpretation of data. Although referred to as workbench activity the description workbench mathematical activity and practices is more appropriate as it captures the essence of the framework. What now follows is an exposition of the main ideas within this framework.

2.4.1 Practice

Pickering (1995) gives an outline of how he sees practice. He refers to it as “a general analysis of scientific practice, which [he] calls the mangle, and some pointers as to how it might be extended toward an understanding of the reciprocal production of science, technology and society (STS)” (1995:1). This notion of practice was informed by the following concerns:

- The production of new knowledge in science;
- Transformation of material and
- Social dimension of science.

However, the abiding concern was with scientific practice, which has to be understood as the work of cultural extension. The use of culture in this context refers to the made things in science, in which are included “skills and social relations, machines and instruments, as well as scientific facts and theories” (Pickering, 1995:3). Cultural extension can further be understood as the scientific practice where human, non-human and material agency temporally emerges in practice. Pickering uses ‘captures’ to refer to the things that come out of the mangle and frames when he speaks of “the theories that are generated as a result of the mangle and subsequently go back into the mangle.” “Disciplined human agency and captured material agency are, as I say, constitutively intertwined; they are interactively stabilized” (Pickering, 1995:17).

To make sense of the relationships of material and social aspects, Pickering (1995) uses the real time dialectics of resistance and accommodation and this is the main thrust of the mangle of practice. This dialectic is referred to as the mangle. In working towards a cultural extension, a breakdown, or obstacles, may occur thus a failure to derive certain associations. These problems or obstacles are the resistances and this is where the mangle goes into action and the dialectic starts (Pickering, 1994:115).

In response to resistance there is a search for accommodation. Accommodation refers to new ways, changes or the use of new directions for cultural extension. Examples could be a machine that works, a new instrument, new knowledge or a new interpretation. These examples mentioned are explorations of “transformed cultural elements” (Pickering, 1994:112). The conflict between resistance and accommodation leads to a new “genuinely emergent process that gives structure to the extension of scientific culture in the actual process of scientific research” (Pickering, 1994:112).

When Pickering refers to real-time he means cultural extensions as it happens in time. It is not the retrospective approaches that look backward from some vantage point of cultural extension to explain practice in terms of what transpires at the vantage point (Pickering, 1995:3). The next section looks at the happenings in the mangle and the concepts used to describe what transpires in the mangle.

2.4.2 Dance of agency

Agency is a term that is used to describe the actions when humans act upon the world. These actions of humans on the world are referred to as human agency. Agency is not restricted to humans and we also get material agency. Whereas human agency is restricted to the body, material agency is agency performed by machines or non-humans.

In the world we live in, humans and non-humans are forever doing something and this is why agency is important. Pickering (1995:6) describes it as follows:

One can start from the idea that the world is filled, not in the first instance, with facts and observations, but with agency. The world I want to say, is continually doing things, that bear upon us not as observation statements upon disembodied intellects but as forces upon material beings.

All these doings and agencies capture Pickering's notion of science as a performative idiom. According to him the representational theories of science distorts science by thinking of practice as ideal. "The representational idiom cast science as, above all, an activity that seeks to represent nature, to produce knowledge that maps, mirrors, or corresponds to how the world really is" (Pickering, 1995:5).

The world is depicted as permeated by action and not just full of facts and observations. In order to make better sense of the world we have to discard the representational idiom and rather focus on how human and machines interact:

The performative idiom that I seek to develop thus subverts the black-and –white distinctions of humanism/antihumanism and moves into a posthumanist space, a space in which the human actors are still there but now inextricably entangled with the non-human, no longer at the center of the action and calling the shots (Pickering, 1995:26).

In the performative idiom, the performances of human and material agency are highlighted. In all this the human and material agency are intertwined. The humans start by constructing some new machine. They then go into a passive mode to monitor and observe the performance of the machine to see what will evolve. During this period of human passivity, material agency manifests itself. When the actions from the material agency are not satisfactory, a reversal in roles takes place. The human now becomes active and the machine assumes a passive role.

There is forever a switch from human performance and material passivity on the one side to human passivity and material performance on the other. This is called the dance of agency, seen asymmetrically from the human side. The dance of agency takes the form of dialectic between resistance and accommodation. Pickering also uses tuning as a metaphor to describe the dance of agency.

2.4.3 Disciplinary agency

The analysis of conceptual practice is informed by the following concerns:

- Cultural practices are disciplined and machinelike.
- Practice, as cultural extension is in essence a process of open-ended modelling.
- Modelling takes place in a realm of cultural multiplicity and leads to the production of associations between diverse cultural elements (Pickering, 1995:114).

Conceptual practice is informed by what transpires at the workbench. This means all the happenings at the workbench are included. All the work of human agency is based on prior learning and is now put to use in the working at the workbench.

Conceptual systems, then, hang together with specific disciplined patterns of human agency, particular routinized ways of connecting marks and symbols with one another. Such disciplines – acquired in training and refined in use – carry human conceptual practices along, as it were, independently of individual wishes and intents (Pickering, 1995:115).

The human is, during this process, passive in disciplined conceptual practice. This passivity of the human is referred to as disciplinary agency. What it means is that the human is passive, but in the actual working, the work leads the way in being active.

Pickering (1995) identifies three stages in the analysis of conceptual practice. In the first called bridging, a bridgehead is utilized to build a connection between the work at hand and work already known. This bridgehead is now used to “convey” or copy work from the old system for use in the new work system. This is called transcription. Filling is now used to complete the new work system which means what is at hand is used without clear guidance from the old work system.

The concepts bridging, transcription and filling which is central to the analysis of conceptual practice also connect to the idea of dance of agency. Bridging and filling are activities of choice and discretion, related to the intentionality of human agency. As there is choice or discretion involved, the actions of bridging and filling are called free moves. During these activities the human agency is active and the disciplinary agency passive. Transcription, however, is the activity where the disciplinary agency asserts itself and where the human agency is passive. When this occurs, transcriptions are then disciplined forced moves.

The activities, bridging, transcription and filling bring out the alternating roles of human agency and disciplinary agency. On the human side there is an interconnection of free and forced moves in practice. On the side of the disciplinary agency there is at first a passivity, which is then followed by activity.

This reversal of roles leads to resistance, which later is followed by accommodation, opening up the dialectics of resistance and accommodation.

Figure 2.2 outlines the concepts of bridging, transcription and filling used for analysis of conceptual practice as discussed above.

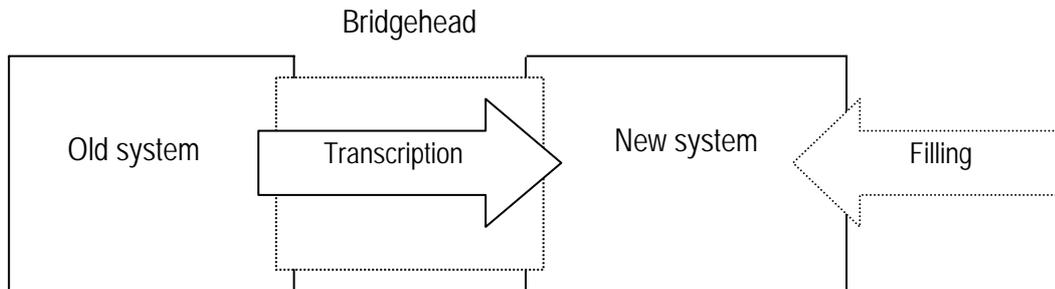


Figure 2.1 : Analysis of conceptual practice

2.5 SUMMARY

Figure 2.3 tries to capture the discussion for the theoretical considerations for this study.

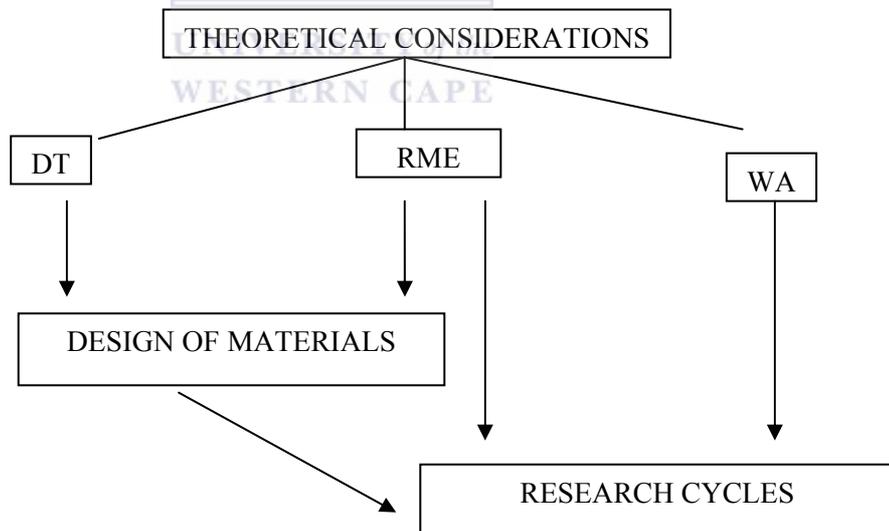


Figure 2.1 : Theoretical considerations

The theoretical frameworks of RME and DT impact on the development of instructional materials for the research cycles. For the analysis of what transpires in the research cycles the frameworks of RME and WA are utilized. In the next chapter the methodology and research design comes under scrutiny.

CHAPTER 3

METHODOLOGY and RESEARCH DESIGN

2.1 INTRODUCTION

The purpose of this study is to investigate how new content could be introduced into a school mathematics curriculum and how it contributed to develop an instruction theory for the teaching of cryptology as a school-going mathematics topic. This instruction theory encapsulates the three interrelated subsidiary research questions on the teachability and sense-making of cryptology and the happenings at the workbench.

In the research for this thesis teaching experiments were used. For these experiments instructional activities were developed. Secondly, the research focused on the analysis of learners' school-going mathematics learning and strategies, which informed the second subsidiary research question on the issue of sense-making, on how learners understand and internalize the content on cryptology. As these two aspects occur in the social setting of a school mathematics classroom, the interactions that occur in this setting informs the third research question on the activities that occur at the workbench between learners and the content they work on.

The issues thus under scrutiny in this thesis involve instructional development and classroom-based research (see figure 1.2 in chapter 1). An important aspect of instructional development is the issue of design. As such the methodology falls under the general heading of design research as the best approach to answer the research questions. Research that includes both instructional development and classroom-based research is also given a general heading of developmental research, also called design research. Kortland (2001:10) highlights three issues in his exposition of developmental research:

- Cyclical process of reflection on content and the teaching and learning process;

- Small-scale curriculum development and teacher preparation and
- Classroom research of the interaction of the teaching and learning processes.

This thesis captures elements of Kortland's (2001) exposition of developmental research with respect to the cyclical nature, curriculum development and classroom research. The overall study falls under the general heading of design research as developed within the Freudenthal Institute in the Netherlands. Design research and the way it contributes to the study are discussed in the next section.

2.2 DESIGN RESEARCH

Many authors (Freudenthal, 1991; Brown 1992; Gravemeijer, 1993, 1994, 1998; Treffers, 1993; Leijnse, 1995; van den Akker, 1999; Gravemeijer & Cobb, 2001; Edelson, 2002; Drijvers, 2003; Bakker, 2004) have over the years discussed and contributed to design research as a methodology. It started out as developmental research and is the preferred research method mostly used by the Freudenthal Institute to develop mathematics education in line with Freudenthal's (1973) view of mathematics as a human activity. Bakker (2004:37) refers to this link between the two when he refers to it as design research, which he likens to developmental research. For this study there will be no differentiation between design research and developmental research.

2.2.1 Characteristics

Design research or developmental research aims to change education, in this instance mathematics education. Gravemeijer (2001:43) warns that the aim of this research method is not to prove that some innovative approach is better than some other approach, but "to offer a grounded theory on how the proposed innovative approach works." Furthermore, the research methodology of design research aims at developing instructional materials and tries to make sense of how the teaching and learning works (Research Advisory Committee, 1996). The strategy of design then plays an important part in this process for developing and fine-tuning theories.

Although authors (van den Akker, 1999; Edlson, 2002; Freudenthal, 1991; Gravemeijer, 1991, 1993, 1994, 1998; Gravemeijer & Cobb, 2001; Treffers, 1993) may have different takes on how they view design research there is consensus on two main points: the cyclical nature of design research and the design of instructional activities.

The next section addresses the characteristics of the cyclical nature of design research and the design of instructional activities important for this study.

3.2.1.1 Cyclical nature of design research

Design research is cyclical in nature. A design research study consists of research cycles in which thought experiments and teaching experiments alternate. Furthermore we distinguish between macro and micro research cycles. Macro research cycles indicate the teaching experiments and micro research cycles refer to the lessons. According to Gravemeijer (1993, 1994) the cycles lead to a cumulative effect of small steps in which teaching experiments provide 'feed forward' for the next thought experiments and teaching experiments.

Design research or the macro-cycles consist of three phases:

- Preparation and design phase;
- Teaching experiments and
- Retrospective analysis.

For this study two macro design research cycles were carried out. These cycles were carried out with grade 10 learners (in the 15 – 17 age groups) and they are indicated as G10-CI and G10-CII respectively (see Appendix A, Note 2). Within the first cycle three teaching experiments (TE 1, TE 2 and TE3) with teachers (TE 1), learners (TE 2) and students (TE 3) were carried out. Figure 3.1 outlines the research cycles within this study.

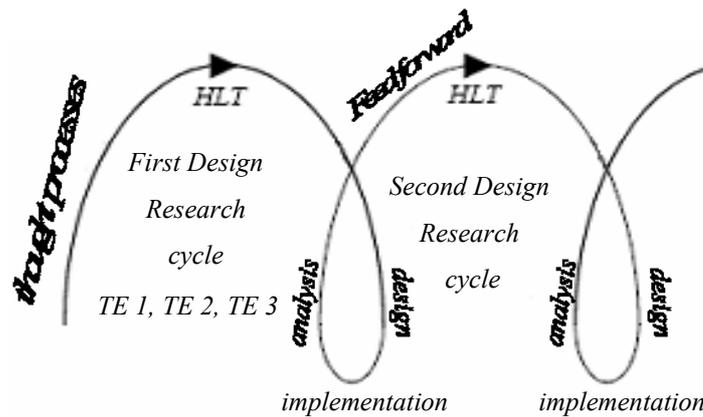


Figure 3.1 : Outline of research cycles

3.2.1.2 Role of design

Of importance within the role of design of instructional activities, is the development of a learning trajectory. The learning trajectory becomes tangible in these instructional activities (Gravemeijer, 1994). In order for the teaching experiments to be carried out, instructional activities must be designed. Edelson (2002:107) underscores the design of learner instructional activities as important to the researcher:

... design research explicitly exploits the design process as an opportunity to advance the researchers' understanding of teaching, learning, and educational systems.

An important part of this study is the development of instructional materials for learners of school-going mathematics. According to Gravemeijer (1994:108) "curricula are developed to change education, to introduce new content or new goals, or to teach the existing curriculum according to new insights." For this thesis the focus is on new content with cryptology as the topic to be taught.

2.3 HYPOTHETICAL LEARNING TRAJECTORY (HLT)

The HLT is a useful instrument for use in all three phases of design research. As part of the first phase of preliminary design we have the development of a HLT and the design of instructional activities. The HLT developed as an extension of

the thought experiment of Freudenthal. It was Simon (1995:136), however, who defined the HLT for the first time:

The hypothetical learning trajectory is made up of three components: the learning goal that defines the direction, the learning activities, and the hypothetical learning process – a prediction of how the students' thinking and understanding will evolve in the context of the learning activities.

The learner instructional activities are aimed at eliciting productive mental activities from learners and with it come the designer's description of why the activities should work and what mental development is expected. Helpful to the designer of the instructional activities is a strong knowledge of the teaching topic, previous experience and the chosen repertoire of activities and representations (Drijvers, 2003). In the context of this thesis the literature review (chapter 4), the historical and didactical phenomenology of cryptology (chapter 5) and the number theory course (see Appendix A, Note 3) contributed in building the domain specific knowledge of the researcher.

Teaching experiments in a research cycle will be followed by an analysis, the HLT will be changed and adapted and will 'feed forward' into teaching experiments towards a next research cycle.

2.4 PREPARATIONS AND DESIGN PHASE

In preparing for this phase it is important that the topic of cryptology be studied first. This affords the design researcher the opportunity to use and access all relevant materials to gain insights and practical experience when working through the topic for the teaching and designing of instructional materials. For the thesis chapters four and five on the literature review and the historical and didactical phenomenology of cryptology respectively, as well as the course followed in number theory, served as a domain to extract the relevant theoretical knowledge.

In the first phase instructional activities were developed for grade 10 learners, teachers and students. These activities were presented to supervisors and

professor Fray (see Appendix A, Note 3), an expert on cryptology, for their input and comments. The final choice of activities was made based on their potential role in the HLT. The first HLT reflected on prior acquired school mathematics knowledge and how learners would make use of strategies based on the basic mathematical operations of addition and subtraction. Another inspiration was the scytale as a starting context to introduce learners to a transposition cipher.

2.5 TEACHING EXPERIMENT PHASE

The teaching experiment phase of the design research cycle is aimed at taking the developed instructional activities into a classroom to be worked on by participants. Steffe (Steffe & Thompson, 2000) developed the phrase '*teaching experiment*'. According to Lehrer and Schauble (2001) researchers take what is best for the situation. Bakker (2004:42) rephrases it as follows: researchers "use activities and types of instruction that seem most appropriate at that moment according to the HLT". There is thus an ongoing reflection on the happenings in a lesson and this can lead to changes for the next lesson.

In the first design phase varied means of data collection were used. For the teaching experiment with the teachers, the following data was collected: teachers' written work, observations and field notes. In the teaching experiment with the learners the following data was collected: learners' written work, field notes and a video recording. During the teaching experiment for the students the following data was collected: field notes and students' written work. The time allocation for each lesson was about 45 minutes.

The following are excerpts from different teaching experiments to show what is meant by observations (figure 3.2), field notes (figure 3.3) and written work (figure 3.4) by the participants.

analysis the HLT is compared with the participant's learning. Based on the analysis, the research questions are answered. The main sources of data for the analysis were field notes, observations and solutions of the teachers and students. For the learners it was their written work observations, field notes and video recordings.

All the written work of the participants was considered for analysis. With respect to the video recordings a selection was made based on the relevance of the episode to the research questions. The video recordings were first transcribed. Part of the transcription recordings involved the translation of conversations from Afrikaans into English. At first the transcription was done in the language of conversation, Afrikaans, and afterwards translated into English. Transcripts were thus repeatedly read and reread for clarity. This also applied to watching the video recording.

A transcript from a video clip follows in figure 3.5. It is an excerpt from the second research design cycle with grade 10 learners. It was part of an introduction to the second activity on the Alberti cipher (see Appendix H4). The summary that was made on the white board (in Afrikaans) is given in figure 3.5 (for English version see Appendix K).

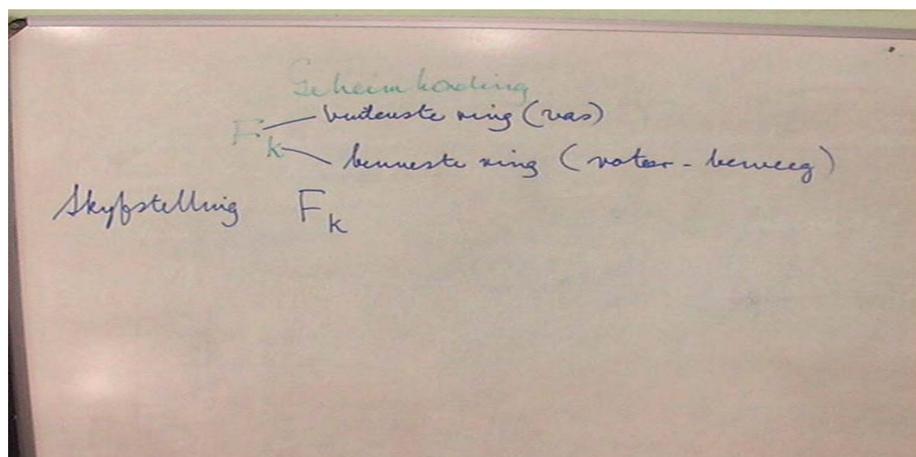
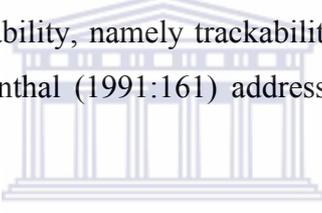


Figure 3.5 : Transcript from video clip

2.7 RELIABILITY AND VALIDITY

This section reflects on the reliability and validity of the research methodology. For this discussion the issues of internal and external reliability and validity is addressed. Internal reliability focuses on the reliability within the research project, especially the data collection methods used. The previous section covered the data collection methods and how it contributes to answer the research questions. Credibility was established because the three supervisors reviewed observations of all work.

External reliability addresses the issue of replicability, which means “that the conclusions of the study depend on the subjects and conditions and not on the researcher” (Bakker, 2004:46). The research must be reported in such a way that it clearly shows how the research was done and how the conclusions were derived – the criterion for replicability, namely trackability (Gravemeijer & Cobb, 2001) is thus ensured. Freudenthal (1991:161) addresses the need for trackability as follows:



Developmental research means: experiencing the cyclic process of development and research so consciously, and reporting on it so candidly that it justifies itself, and that this experience can be transmitted to others to become like their own experience.

Internal validity is about the quality of the data collection and the sensible reasoning that has led to the conclusions of this study. Various methods of data collection were used to ensure internal validity of this study. Generated conjectures were tested against:

- Video recordings;
- Written work from participants;
- Field notes and observations;
- Talk and gestures from participants;
- Different teaching experiments with teachers, learners and students and
- Succession of two design research cycles.

External validity refers to the generalizability of the results. Of concern is how we generalize the results for this specific context in order to be applicable to another context. The results must be presented in such a way that others can adjust it to their situations.

2.8 TEACHING EXPERIMENTS AND RESEARCH PARTICIPANTS

This study was done over two design research cycles. For the first research cycle we had three teaching experiments with teachers, learners and students respectively. An outline of the first research cycle is given below reporting on the teaching experiments (TE1, TE2 and TE3), target groups, number of groups, data collection methods used, conversation language used and topic covered. The number of participants for each teaching experiment is given in brackets with the number of groups.

FIRST DESIGN RESEARCH CYCLE			
Teaching Experiment	TE1	TE2	TE3
Target Group	Teachers	Learners	Students
Number of Groups	3 (13)	2 (6)	4 (8)
Video Recording	No	Yes	No
Observations	Yes	Yes	Yes
Field Notes	Yes	Yes	Yes
Written Work	Yes	Yes	Yes
Conversation Language	English	Afrikaans	Afrikaans
Topic	Scytale	Scytale	Alberti Disk

Table 3.1 : First design research cycle

All teachers were students at UWC studying towards a B.Ed Honors degree. They did the courses for mathematics for teaching and mathematics education. The teaching experiment was part of their mathematics for teaching course. The learners were in grade 10 and fall in the 14 – 16 age groups. They come from a

state school in Wellington, near Cape Town. The students referred to were all in their second year of study towards a school mathematics teacher qualification for the FET phase of CPUT at the Wellington campus. FET caters for learners in grades 10 to 12.

The second design cycle was only done with grade 10 learners and all the data collection methods mentioned above, were again utilized. For examples of an instructional activity worked on by the participants, see Appendixes E and H.

2.9 CONCLUSION

This chapter is a discussion of the research methodology and data collection methods for the study. The next chapter reports on the literature review for the topic of cryptology.



CHAPTER 4

LITERATURE REVIEW

FEW FALSE IDEAS have more firmly gripped the minds of so many intelligent men than the one that, if they just tried, they could invent a cipher that no one could break. (Kahn, 1996:763)

4.1 INTRODUCTION

This chapter aims to give a historical background to the development of cryptology as a mathematics topic. At first the mathematical underpinnings of cryptology are considered. Secondly, the focus shifts to two research initiatives that were introduced in the United States of America (USA) to develop activities on cryptology for use in high school mathematics classrooms. An outcome of this chapter is the identification of different projects on cryptology for school mathematics – see Appendix B.

4.2 CRYPTOLOGY

The word cryptology has its origins in ancient Greek. Cryptology is derived from the Greek words *kryptos*, meaning hidden, and *logos*, meaning word. The field of cryptology has two subdivisions, namely cryptography and cryptanalysis. So whenever the word cryptology is used in this thesis, it refers to cryptography, cryptanalysis, and the interaction between them (Barr, 2002:2; see Appendix A, Note 4). Cryptology is also known as the study of code.

Cryptology has a social dimension because of the human being's need to communicate. Kahn (1996:752) summarizes it as follows:

Cryptology is, by definition, a social activity, and so it may be examined from a sociological point of view. It is secret communication, and communication is perhaps man's most complex and varied activity. It encompasses not just words but gestures, facial expressions, tone of voice, even silence.

Over the years people have used secret messages. The need for secret communication has occurred in especially diplomatic, military, financial and

electronic affairs. With the increased use of electronic communication it has become essential to safeguard these communications by introducing secrecy measures. Therefore there is great interest in ways of making messages sent to another person or institution more secure.

Before moving on to a discussion of cryptography and cryptanalysis the terminology used in these discussions will be clarified. The terms cipher, key, code, plaintext, ciphertext, encoding or enciphering and decoding or deciphering will come under scrutiny in the following section.

4.3 TERMINOLOGY

The word cipher comes from the Hebrew word, *sapher*, which means number. Ciphers employ a key or a rule, which specifies the arrangement to be used to change a message into secret form. A cipher can be seen as a form of substitution. One or more letters or numbers substitutes a letter or letters of the alphabet. A code on the other hand, consists of words, phrases or letters with the codewords replacing plaintext elements. Table 4.1 below is an example of what a code might look like:

TEXT	CODEWORD
Place	1234
Encode	098
Refer to	97

Table 4.1 : Example of a code

The key specifies the arrangement or rule to be followed to change a message. Sometimes the key consists of a word (keyword) or a phrase (keyphrase) or a number (keynumber). Plaintext refers to the message that will be changed into secret form. The process of changing the legible text, also called the plaintext, into an intelligible form is called enciphering or encoding. The reverse process, that is changing the intelligible text, also called the ciphertext, into plaintext, is called deciphering or decoding. The secret form of the message is called the ciphertext.

Kahn (1996: xvii) distinguishes between decipher or decode and cryptanalyze. Decipher or decode is used to indicate that the key is known to the person working on changing the secret message into plaintext form. Cryptanalyze, on the other hand, is used if the key for changing the secret message into its plaintext form is unknown.

4.4 CRYPTOGRAPHY

The aim of cryptography is to allow two parties A and B to communicate in such a way that C, a listener, intruder or opponent, is not able to understand what is being said. When defining cryptography, most authors (Barr, 2002; Rosen, 2005; Stinson, 1995; Beutelspacher, 1994) focus on cryptography as a discipline to keep communications private. For Kahn (1996: xv) the methods of cryptography “do not conceal the presence of a secret message but render it unintelligible to outsiders by various transformations of the plaintext.”

Menezes (1997:4) goes a step further and defines cryptography as "the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication." All the issues mentioned by Menezes (1997) are concerned with information security. Table 4.2 summarizes what Menezes (1997:4) describes as the cryptographic goals:

GOAL	SERVICE	DESCRIPTION
Confidentiality	To make the content of information only available to authorized users	Secrecy is synonymous with confidentiality and privacy. Numerous approaches for providing confidentiality exist. Some include physical protection by using mathematical algorithms, which render data unintelligible.
Data Integrity	Looks at the unauthorized alteration of data	For data to be secure, it is important to be able to detect data manipulation by unauthorized users. Methods of data manipulation include insertion, deletion and substitution.
Entity Authentication	The need for identification	This applies to both the sender and receiver. They should be able to identify each other.
Data Authentication	The need for identification	It must be possible to authenticate information with respect to origin, date of origin, data content, etc.
Non-repudiation	Is a means achieved through cryptographic methods, which prevents an individual or entity from denying having performed a certain action related to data.	Whenever disputes arise, there must be ways of resolving it. Whenever authorization was given and the person denies that it was given, a procedure allowing a third party to resolve the issue is needed.

Table 4.2 : Cryptographic goals

A fundamental aim of cryptography is to address these five areas in both theory and practice.

The use of the key plays an important role in cryptography to render a plaintext message unintelligible. For a message to be hidden from prying eyes, a key is used to make it secure. This key takes on different forms. Examples of keys used in sending messages in history include battens (scytals), linear equations and shifting of letters. The importance of keeping the key secret is summarized by the Kerchoffs' principle, paraphrased below (Barr, 2002:52; Singh, 1999:12):

Don't underestimate the enemy. The idea is not to keep the encryption and decryption algorithm secret. The main idea is to keep the key itself secret.

4.5 CRYPTANALYSIS

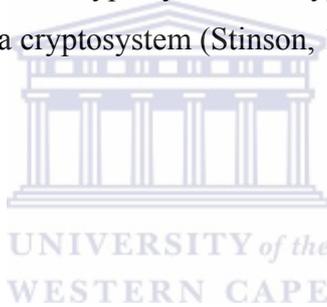
Cryptanalysis is the process of converting a received message from ciphertext into plaintext without key information. It is sometimes also referred to as

codebreaking. Whereas cryptography is theoretical and abstract, cryptanalysis is empirical and concrete.

The person involved with breaking the ciphertext (secret message) is called a cryptanalyst. The Arabs were one of the first nations to record their methods of cryptanalysis (Kahn, 1996:93). They used cryptanalysis for the first time to break the monoalphabetic substitution cipher (Singh, 1999:15). A monoalphabetic substitution cipher is where only one alphabet cipher is used. Another early example of cryptanalysis is from the Bible in Daniel chapter 5 where Daniel interprets the dream of Belshazzar.

The process of changing a plaintext message into ciphertext and then back into plaintext is referred to as the cryptosystem in cryptology. The following can be described as elements of a cryptosystem (Stinson, 1995:1):

- Plaintexts;
- Ciphertexts;
- Possible keys;
- Encryption rule and decryption rule.



Within this cryptosystem it is important to distinguish between secret-key cryptography and public-key cryptography. Conventional or secret key cryptography, also known as symmetric cryptography uses a single secret key for both encryption and decryption. Conversely, public-key cryptography, also known as asymmetric cryptography, uses a pair of keys – a public key and a private key. The private key is kept secret, while the public key is known.

Based on the discussion above, figure 4.1 gives a summary of how the topic of cryptology is constituted.

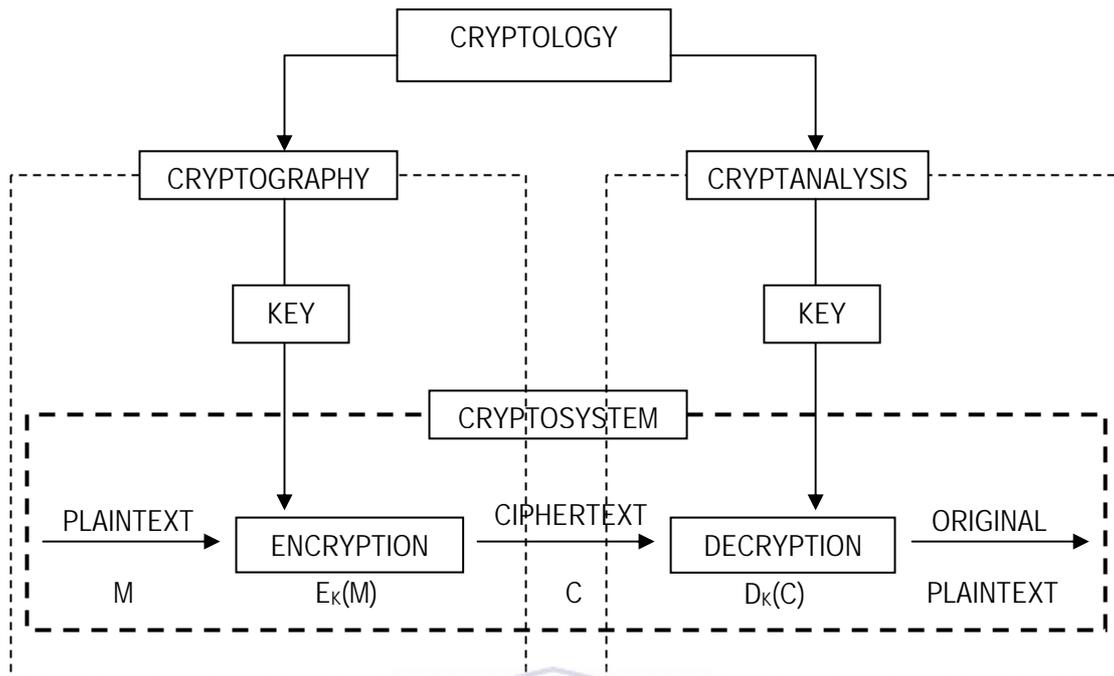


Figure 4.1 : Cryptosystem in cryptology

4.6 HISTORICAL BACKGROUND

In the historical background of cryptology, we'll focus on persons, events and issues deemed to represent some of the highlights in the development of cryptology. This discussion will be done under the following headings: Ancient uses, World War I, World War II and Modern uses. The aim of the discussion is to look for suitable examples to form part of activities on cryptology for a school-going mathematics curriculum.

4.6.1 Ancient uses

The period coined ancient uses of cryptology stretches from the birth of cryptology in 1900 B.C. up to the introduction of the radio in 1895. Events included in this era span various countries, people, books and inscriptions.

4.6.1.1 Birth of cryptology

The birth of the history of cryptology can be traced back to Menet Khufu (1900 B.C.), a small town near the Nile River in Egypt. It was common practice to have inscriptions on gravestones. Such an inscription was done in the rock of the tomb

for a nobleman, Khnumhotep II (Kahn, 1996:71). There was a deviation in the writing as some unusual hieroglyphic symbols were used in place of ordinary letters from the actual alphabet. This was not a form of secret writing, but a way of transforming writing, that is, “substituting unusual symbols for those ordinarily used in writing” (Barr, 2002:3).

4.6.1.2 Mesopotamia

The people in Mesopotamia took an interest in the Egyptian’s work on cryptology and went a step further. In 1500 B.C. an encrypted formula for pottery glaze was developed (Kahn, 1996:75). The tablet containing the formula was about 7.5 x 5 cm (3 x 2 inches) in size and was found on the banks of the Tigris River. On the tablet special signs were used to which different meanings could be attached. It meant that signs were substituted for the ordinary letters of the alphabet.

4.6.1.3 Bible

Not even the Bible escaped the world of cryptology. In the book of Jeremiah 25:26 and Jeremiah 51:41 in the Old Testament Sheshach is used as a cryptogram for Babylon. There is nothing secretive about this as Sheshach is openly substituted for Babylon (Satinover, 1997:90) in Jeremiah 51:41:”How Sheshach will be captured, the boast of the whole earth seized! What a horror Babylon will be amongst the nations!” (Disciple’s Study Bible, 1988:969).

In a second example of substitution in Jeremiah 51:1, Leb Kamai is a cryptogram for Chaldea, that is, Babylonia (Satinover, 1997:997). " ... See, I will stir up the spirit of a destroyer against Babylon and the people of Leb Kamai. In a similar way are names or words substituted by numbers, referred to as the *gematria*. For example in the book of Revelations the number of “the beast” is given as 666.

This is an example of a letter-substitution code called *atbash*, where the first letter in the Hebrew alphabet (aleph) is replaced by the last (tav) and the second letter (bet) by the second-to-last letter (shin) and so on. This is the equivalent of $a \leftrightarrow z$, $b \leftrightarrow y$, $c \leftrightarrow x$, ... for the Roman alphabet. This method of substitution was also

referred to as the permutation of letters and an image thereof is found in Luke 13:30 (Disciple's Study Bible, 1988:1292) where it reads: "Indeed there are those who are last who will be first, and first who will be last."

4.6.1.4 Military context

Cryptology was for the first time used in a military context with the introduction of the scytale (pronounced si'-ta-lee) about 500 B.C. in Sparta (Kahn, 1996:82). The scytale is a wooden batten that was carried in the belt around a soldier's waist. An ingenious way was developed to use the belt and scytale to encrypt and decrypt messages.

The belt was turned around the scytale and a letter of the message written on each turn of the belt. After completion of the message, the belt was unwound and the message became scrambled. The person carrying the message wore the belt and on handing it over to the concerned party, the belt was again wrapped around a scytale of the same size as the previous one, thus unscrambling the message

This introduction of secrecy into the military realm spilled over to India and around 300 B.C. Kautilya wrote a book called, *Artha-śāstra* (Kahn, 1996:74). In it Kautilya made a plea to the officers in charge of espionage to conceal assignments to their spies by way of secret writing. Furthermore, he presented various ways of cryptanalysis to the Indian Intelligence in order to break codes, thus allowing them access to intelligence reports written in code.

In 50 B.C. Julius Caesar, ruler of Rome used different ways of concealing his military communications, because of betrayal in his ranks. The first method he used was to shift every letter of the alphabet three places – also called the Caesar alphabet (Kahn, 1996:84). This meant every *a* in a plaintext message changed into a *D* for the ciphertext and every *b* into an *E* (see table 4.3), etc.

Caesar Alphabet													
PLAINTEXT	a	b	c	d	e	f	g	h	i	j	k	l	m
CIPHERTEXT	D	E	F	G	H	I	J	K	L	M	N	O	P
PLAINTEXT	n	o	p	q	r	s	t	u	v	w	x	y	z
CIPHERTEXT	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Table 4.3 : Caesar alphabet

The plaintext message *I am Caesar* enciphers to the ciphertext: *ldpfdhvdu*

In addition, he also used language to strengthen his encryption, replacing Latin letters with Greek letters. His scribe, Tyro, also used a form of short hand to replace words in communications (Laffin, 1964:28).

4.6.1.5 Polybius

In 205 B.C. Polybius, a Greek writer, formally used numbers substitutes for the letters of the alphabet. This was done by way of a 5x5 table, now referred to as the Polybius checkerboard or Polybius square (I and J were in one cell). Adapted for the Roman alphabet, it looked as follows (see Table 4.4):

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	IJ	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Table 4.4: Polybius square

Letters from the alphabet were now converted to numbers. From this table the values for A and S will be 11 and 43 respectively (row value followed by column value). The word *table* encodes to *4411123115*.

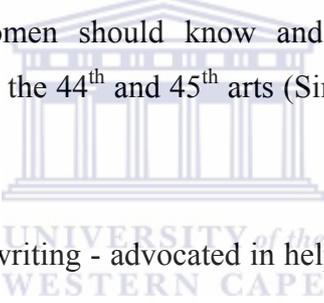
4.6.1.6 Iraq

In ancient Uruk (about 130 B.C.), now called Iraq, it was popular for writers to change their names into numbers (Kahn, 1996:76). This was not done to hide anything, but by way of amusing the readers by their writings.

4.6.1.7 Love and the occult

In 200 A.D. a manuscript, the Leiden Papyrus (Kahn, 1996:91) was discovered at Thebes. This manuscript contained recipes on how to make unusual potions. Portions of these recipes were enciphered. Examples listed include how to make a man love a woman and how to give a man an incurable disease.

In what seemed to be a deviation from the ordinary, Vātsyāyana (in the year 400 A.D.) in his book on erotics, *Kāma-sūtra*, “lists secret writing as one of the 64 arts, or yogas, that women should know and practice” (Kahn, 1996: 74). According to Vātsyāyana the 44th and 45th arts (Singh, 1999:9) that people should know and practice are:

- 
- The art of secret writing - advocated in helping women conceal the details of their affairs.
 - The art of speaking by changing the form of the word.

The period A.D. 500 to 1500 was a quiet stage in cryptology in Western civilization. Kahn (1996:91) ascribed this to the fact that people likened cryptology to the black arts and the occult. Another contributing factor was the confusion of cryptology with the Jewish kabbalah. The Jewish kabbalah referred to a way of life or religion.

Even in modern everyday life this perception of cryptology as mystified and related to the occult is enforced. Some book dealers list books on cryptology under occult. Could this also be the reason why the USA used the code name MAGIC for deciphering intercepted Japanese messages?

4.6.1.8 Yahmadi

This did not mean that nothing took place on the development side with respect to cryptology in other countries. In 725, Abu Yahmadi, compiler of the first Arab dictionary (al-Kadi, 1992; Thinkquest, 2002:2), wrote up his solution for a Byzantine cryptographic puzzle written in Greek. To solve the puzzle he assumed that the puzzle began with "In the name of God", and from this he worked out the rest. Abū Bakr Ahmad ben ‘Alī ben Washiyya an-Nabatī, a scholar, published cipher alphabets in 855 that were used for encrypted communication (Kahn, 1996:93).

4.6.1.9 Bacon

Different forms of representing messages were used during the Dark Ages (500-1400). For example, around 1226, political documents in circulation in Venice contained crosses and dots instead of ordinary words, thus trying to keep information about sensitive political information secret. It was however, Roger Bacon, an English monk, who brought some light into this period in the Western world. He wrote the first book on Cryptology in 1250, entitled *Epistle on the Secret Works of Art and the Nullity of Magic* (Singh, 1999:26-27). In the book he described seven ways for keeping messages secret. William Romain Newbold, an American, worked on the writings of Bacon to analyze it. After his death a colleague, Roland Grubb Kent, continued his work and in 1928 the book, *Cipher of Roger Bacon* was published (Kahn, 1996:868).

4.6.1.10 Nomenclator

In 1400 nomenclators, also referred to as codebooks, came into being (Barr, 2002:6). It showed how letters, words and phrases could be changed into code. A second part included the reverse where it showed how codes translate back into ordinary language. A phonebook is an example of a nomenclator where the phone number serves as a code next to the name and address of the individual on the left.

4.6.1.11 Encyclopedia

The Arabs continued their work on cryptology and the Arabic Encyclopedia of 14 volumes, *Subh al-a 'sha*, completed in 1412, contained a section on cryptology (Kahn, 1996:95). The two-part section included writings on symbolic actions, allusions, invisible inks and cryptology.

4.6.1.12 Alberti

Kahn (1996:125) refers to Leon Battista Alberti (1404-1472) as the "Father of Western Cryptology". Alberti wrote on cryptanalysis and developed a difficult system of encipherment and encoding. The cipher wheel (see figure 4.2) he developed, used the first polyalphabetic substitution, where different substitution alphabets were used for different parts of a message (Kahn, 1996:128). A polyalphabetic substitution is where two or more cipher alphabets are employed in an agreed upon prearranged pattern. The outer ring was fixed and consisted of 24 cells with the capital letters (H, J, K, U, W and Y omitted). The inner free spinning wheel contained lowercase letters.

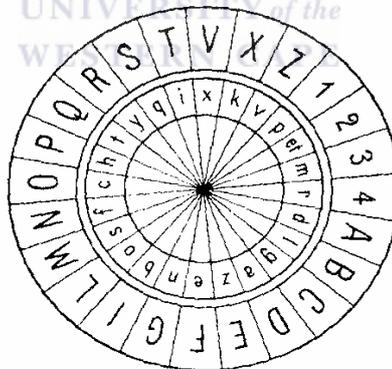


Figure 4.2: Alberti's cipher wheel

For sending a message, the two parties had to agree on a starting point for the inner wheel. Alberti usually chose *k* as the setting for the inner ring. The inner wheel (small letters) could revolve around the axis whilst the outer wheel (capital letters) was fixed. For example, the message *Alberti was an Italian*, is now enciphered with *k* the setting on the inner ring and F, V, Q and M the settings on the outer ring aligned with *k* for the respective words in the message.

Table 4.5 shows the disk alignment and the enciphered words for the message – see Appendix C:

PLAIN WORD	DISK ALIGNMENT	ENCIPHERED WORD
ALBERTI	Fk	tetyxaep
W*AS	Vk	kkli
AN	Qk	eq
ITALIAN	Mk	ilxisv

Table 4.5: Example using Alberti’s cipher wheel

*A double V was substituted for W. So W encoded to kk (Barr, 2002:8)

The ciphertext could also be summarized as:

F e e t y x a t p V k k l i Q v e M m b q r m q l

F, V, Q and M indicate the disk alignment with k for the respective words in the message.



The Alberti disk could also be combined with codes where certain numbers are exchanged for words. This implied that a codebook had to be available that included these codes. For the example that follows, the correspondents had a nomenclator available in which the code for 14 was FAMILY and the code for JUNE was 24. The ciphertext *X x b q b i R c y f d a Z n s p m* (k is still the setting on the inner ring) deciphers as *VISITING 14 IN 24*. With the use of the nomenclator it changes to *VISITING FAMILY IN JUNE*.

4.6.1.13 Trithemius

Johannes Trithemius, a German monk, took polyalphabetic substitution a step further. His work culminated in the first printed book on cryptology, entitled *Polygraphia*, in 1518. He used a different alphabet to encode each letter in a word. This was by way of Trithemius' tableau, also called “tabula recta” (Kahn, 1996:136) which looked as follows (see table 4.6).

a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	N
a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	1 st
b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	2 nd
c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	3 rd
.
z	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	23 rd
w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	24 th

Table 4.6: Trithemius' tableau

The basic tenet that underlies Trithemius' system was the use of normal alphabets in various positions as the cipher alphabet. It has to be noted that the letters j and v were omitted from the alphabets leaving only 24 letters in the alphabet. For enciphering j and v the letters, k and w were used. His encipherment rule was very simple. The first letter of a message was enciphered with the first alphabet, the second letter with the second and so on. The 25th letter was again enciphered with the first alphabet and so it continued.

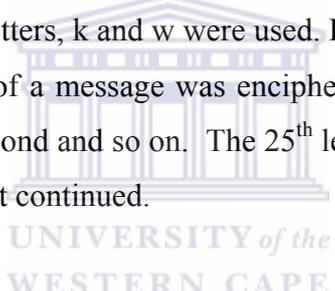


Table 4.7 gives the ciphertext for the plaintext message *Mathematics is fun*.

PLAINTEXT	CIPHERTEXT
MATHEMATICS IS FUN	MBXLIRGBRMDUKTEG

Table 4.7: Example using Trithemius' tableau

The second *M* in the word *MATHEMATICS* is the 6th letter of the message. To get the corresponding letter for the ciphertext, we go to the 6th alphabet starting with *f*, go to *m* in the first, the alphabet (N) in row 1 and read off the corresponding value underneath *m* in the 6th row, which is *r*.

The difference from that of Alberti was that Trithemius used a new alphabet for every letter, starting again from the first alphabet for the 25th letter.

4.6.1.14 Belaso

Giovan Batista Belaso, a nobleman from Brescia, extended the work of Alberti and Trithemius by introducing a keyword, or a countersign as he called it, in 1553 (Kahn, 1996:137). The keyword had to be written above the plaintext and continuously repeated for each letter in the plaintext. For the message, *My name is Giovan Belaso*; we use the keyword *axis*. Table 4.8 gives the solution for the above message. Each letter of the keyword denotes the starting letter for the alphabet from table 4.6.

KEYWORD	a	x	i	s	a	x	i	s	a	x	i	s	a	x	i	s	a	x	i	s
PLAINTEXT	m	y	n	a	m	e	i	s	g	i	o	v	a	n	b	e	l	a	s	o
CIPHERTEXT	m	s	x	s	m	a	r	l	g	e	y	r	a	i	k	y	l	x	b	g

Table 4.8: Example of Belaso’s work using the keyword *axis*

To obtain the first cipherletter for the plaintext letter *m*, we use the alphabet listed as normal (N) and read off the corresponding value in the 1st alphabet starting with a. M is now enciphered with *m*. For the second letter *y*, the alphabet starting with x will be used to determine the cipher letter. This work paved the way for the eventual formulation of the concept of polyalphabetic substitution.

4.6.1.15 Porta

Giovanni Battista Porta, born in Naples in 1535, was instrumental in introducing us to the first known form of the digraphic cipher (Barr, 2002:10; Kahn, 1996:144). A digraphic cipher is one in which special symbols are used to represent pairs of letters. Table 4.9 is an example of a Porta table (Laffin, 1964:39). We use this table to work out an example.

Key word: CHIEF

Message: Porta is from Naples

Each letter from the keyword has to be part of one of the two letters from the key in table 4.9. To encipher *p* we use the alphabet from C (in CD, see line CD in table 4.9) and see which letter is on top or below *p*. That means *p* changes into *d*.

For the second letter, o changes into e from alphabet H (in GH). The ciphertext for the message is: *deiiy ui ogdy dufwqi*

KEY	PLAINTEXT/CIPHERTEXT												
AB	a	b	c	d	e	f	g	h	i	j	k	l	m
	n	o	p	q	r	s	t	u	v	w	x	y	z
CD	a	b	c	d	e	f	g	h	i	j	k	l	m
	z	n	o	p	q	r	s	t	u	v	w	x	y
EF	a	b	c	d	e	f	g	h	i	j	k	l	m
	y	z	n	o	p	q	r	s	t	u	v	w	x
GH	a	b	c	d	e	f	g	h	i	j	k	l	m
	x	y	z	n	o	p	q	r	s	t	u	v	w
IJ	a	b	c	d	e	f	g	h	i	j	k	l	m
	w	x	y	z	n	o	p	q	r	s	t	u	v
KL	a	b	c	d	e	f	g	h	i	j	k	l	m
	v	w	x	y	z	n	o	p	q	r	s	t	u
MN	a	b	c	d	e	f	g	h	i	j	k	l	m
	u	v	w	x	y	z	n	o	p	q	r	s	t
OP	a	b	c	d	e	f	g	h	i	j	k	l	m
	t	u	v	w	x	y	z	n	o	p	q	r	s
QR	a	b	c	d	e	f	g	h	i	j	k	l	m
	s	t	u	v	w	x	y	z	n	o	p	q	r
ST	a	b	c	d	e	f	g	h	i	j	k	l	m
	r	s	t	u	v	w	x	y	z	n	o	p	q
UV	a	b	c	d	e	f	g	h	i	j	k	l	m
	q	r	s	t	u	v	w	x	y	z	n	o	p
WX	a	b	c	d	e	f	g	h	i	j	k	l	m
	p	q	r	s	t	u	v	w	x	y	z	n	o
YZ	a	b	c	d	e	f	g	h	i	j	k	l	m
	o	p	q	r	s	t	u	v	w	x	y	z	n

Table 4.9: Digraphic cipher

This same idea of the digraphic cipher was later used by Lester Hill to introduce the Hill cipher in 1929 (Sinkov, 1996). The unpublished M. Ed mini-dissertation (Whittles, 1996), entitled *The strategies that grade 8 learners develop for the*

solution of two linear, simultaneous equations, is an extension of this digraphic cipher.

4.6.1.16 Vigenère

Blaise de Vigenère, a Frenchman, wrote a book entitled *Traicté des Chiffres* in 1585 (Kahn, 1996:146). This was done after he made a study of the works of Alberti, Trithemius and Belaso. He made use of a one-letter autokey that was extended by the message itself. This was applied to his table, also referred to as the Vigenère square (see Table 4.10).

	A	B	C	D	E	V	W	X	Y	Z
A	A	B	C	D	E	V	W	X	Y	Z
B	B	C	D	E	F	W	X	Y	Z	A
C	C	D	E	F	G	X	Y	Z	A	B
D	D	E	F	G	H	Y	Z	A	B	C
E	E	F	G	H	I	Z	A	B	C	D
.
.
.
.
V	V	W	X	Y	Z	P	R	S	T	U
W	W	X	Y	Z	A	Q	S	T	U	V
X	X	Y	Z	A	B	R	T	U	V	W
Y	Y	Z	A	B	C	S	U	V	W	X
Z	Z	A	B	C	D	T	V	W	X	Y

Table 4.10: Vigenère’s autokey

We now look at an example to illustrate Vigenère’s autokey. Sender and receiver decide on a predetermined letter to use as first letter (*M* for our example) of the autokey. Letters from the message now follow the letter *M* from the autokey to complete the autokey.

Plaintext: THIS IS A CIPHER

Autokey: MTHI SI S ACIPHE

To find the ciphertext for the first letter the T from the plaintext indicates the column and the M from the autokey indicates the row. T is now enciphered with the corresponding letter from the above-mentioned column and row, namely F. For the second letter, we proceed to column H and row T, changing H into Z. The full ciphertext message is: *fapa aa s ckxwlv*

4.6.1.17 Bacon vs Shakespeare

During these developments of the cryptology field, many authors showed a keen interest in these happenings. Francis Bacon was a keen cryptologist and developed a cipher in 1623 by using the letters a and b in different combinations for all the letters of the alphabet (Laffin, 1964:46).

A aaaaa	B aaaab	C aaaba	D aaabb	E aabaa	F aabab	G aabba	H aabbb
IJ abaaa	K abaab	L ababa	M ababb	N abbaa	O abbab	P abbba	Q abbbb
R baaaa	S baaab	T baabb	UV baabb	W babaa	X babab	Y babba	Z babbb

Table 4.11: Example of Bacon’s cipher

This substitution method was very laborious. At this stage a debate ensued over who the real author of the Shakespearean works was. Different authors came up with proofs to show who the real author was. The explanation from Booth is listed as an example.

Bt with the motion of all elements,
Courses as swift as thought in every power,
And gives to every power a double power.

Using the underlined letters (B, C, A, o and n) which spells out Bacon, he deduced that Bacon was the author of the play. This argument was soon discarded.

4.6.1.18 Jefferson

During the 1790’s Thomas Jefferson, the third president of the United States, joined the cryptology fray and invented what he called the “wheel cypher” (Kahn,

1996:192). It was generally accepted that if the President presented his invention to the secretary of state of that time, James Madison, it would enable the USA's communication to withstand all the cryptologic attacks of those times. His work was however lost and only found in 1922 and reworked for use by the USA navy in World War II.

4.6.1.19 Electronic Communication

Communication is a vital source in keeping people up to date. Within cryptology it is important to ensure that messaging, if intercepted, is not prone to being read by those who intercepted the message. This is why the advent of the telegraph was so important for cryptology. We share Barr's view when he states that "the invention of the telegraph marks one of the most significant turning points in communication security" (2002:17). The first recorded use of the telegraph was in 1753 when sender and receiver communicated over a distance by way of 26 cables, each cable denoting a letter of the alphabet (Singh, 1999:60).

The telegraph is associated with Samuel F.B. Morse who used the Morse code (containing mainly dots and dashes) to send the message "What hath God wrought!" in 1844 (Kahn, 1996:189). What made the use of the telegraph more significant was the use of previously developed methods to send messages. These methods included:

- Monoalphabetic substitution.
- Polyalphabetic ciphers.
- Codebooks or nomenclators

Another method used was *route ciphers*. The United States Military Telegraph Corps (USMTC) made use of word transpositions and added words of no importance to messages to confuse potential cryptanalysts when sending messages during the Civil war of 1861-1865, (Barr, 2002:18).

The telegraph also opened the field of cryptology to error correcting codes. Friedman discusses this when he states that codes are constructed in a way enabling receivers to identify and fix parts of a message that were corrupted during transmission (Barr, 2002:19)

4.6.1.20 Wheatstone

Although Morse is seen as the father of the telegraph, it was Charles Wheatstone and William Forhergill Cooke whose electric telegraph was used in 1839 to send messages between railway stations in West Drayton and Paddington over a distance of 29 km in England (Singh, 1999:60). Wheatstone was also instrumental in developing the Wheatstone-Playfair cipher in 1854. Lyon Playfair was deputy speaker of the House of Commons, postmaster general and president of the British Association for the advancement of science (Kahn, 1996:198). The Wheatstone-Playfair cipher is a digraphic cipher and was used by the British forces in the Boer War and World War I.

The cipher is a 5 x 5 matrix that contained the letters of the alphabet with the letters IJ in one cell. A keyword can also be used to start the matrix and the rest of the cells are then filled with the missing letters not included in the keyword. For our example below, we use the name Raymond as keyword.

R	A	Y	M	O
N	D	B	C	E
F	G	H	IJ	K
L	P	Q	S	T
U	V	W	X	Z

Table 4.12: Wheatstone’s cipher using *Raymond* as keyword

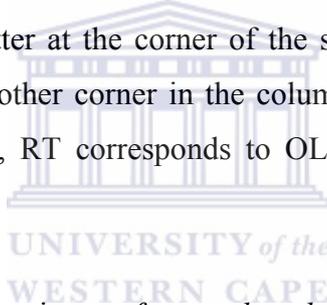
We now want to encipher the message, ALL GOOD STARTS WITH LOVE. Start out by grouping the message into letter pairs. If a pair consist of a double pair (OO in the example,) insert an X to break it up. When the message consists

of an uneven number of letters, an X or a null is added. The message now becomes:

AL LG OX OD ST AR TS WI TH LO VE

The following rules are applied for enciphering:

1. When a pair of letters is in the same row, the ciphertext pair is the two letters to the right of each letter. For instance, RY changes to AM, HI corresponds to IK, and WZ changes to XU (stay in the same row).
2. If a pair of letters appears in the same column, the letters beneath it, following the same rules as for the rows, replace them. For instance RL changes to NU, HW corresponds to QY and TO changes to ZE.
3. For a pair of letters at the corners of a rectangle or a square the first letter enciphers with the letter at the corner of the same row and the second letter with the letter at the other corner in the column to complete the rectangle or square. For instance, RT corresponds to OL, BJ enciphers as CH and SD changes to PC.



The full ciphertext message is: *rp pf mz ae tl ya lt xh qk tr zd*

4.6.1.21 Marconi

Although the invention of the telegraph was considered a breakthrough for use as a source for secure communication, the introduction of the radio in 1895 surpassed this. The work of Guglielmo Marconi, an Italian physicist who worked on electrical circuits, resulted in the first radio (Singh, 1999:101). Whereas the telegraph needed wires to be set up between two communicating partners, wires were not needed for the radio.

With the radio also came the situation that more and more messages were intercepted, thus meaning that the emphasis of cryptology also had to make a shift. While the focus on the ancient development of cryptology fell on writing messages in different ways in order to keep it secret, it was now important to

develop measures to analyze these intercepted messages. This meant that with war looming, the art of cryptanalysis came into being.

4.6.2 War World I

With the increase in the number of codes and ciphers by 1900, all the nations were obsessed with the idea of secret writing. The access to radio made it incumbent on them to increase the difficulty level of their ciphers. With prospects of war more evident, nations were eager to lay their hands on the codes and secret messages of their foes.

4.6.2.1 Austria

Vienna was the place where the actual action started. Colonel Alfred Redl, an Austrian, betrayed his country's secrets to Russia (Laffin, 1964:103). In the early days of World War I, Russia defeated the Austrian army. Behind the battle lines of war, another war was raging. The war of cryptologists - hard at work to decipher captured and intercepted messages. However, sometimes a bit of luck (to others a disaster) was also needed to help those behind the scene workers.



4.6.2.2 Russia

In 1914, Russia was at war with Germany. The Russian armies were operating in Galicia and they were cut off by road and rail and had to communicate by radio. The Russians knew the Germans had access to their old ciphers, so they developed a new one. They still communicated by using the old ciphers when sending messages that were of lesser importance and no value. When it seemed that war was inevitable, they communicated by using the new cipher. This is where their problems arose. The only copy of the cipher was in the hands of General Zhilinsky and he gave it to General Rennenkampf, commander of the First Army (Esposito, 1964:142). The First Army sent the received message to the Second Army under the command of General Samsonov (Esposito, 1964:142), who did not know about the new cipher and was unable to decipher the message.

In order to communicate with the First Army they resorted to the old cipher to establish communications. Nevertheless, the First Army had, on request of General Jilinsky, destroyed all old ciphers. Communication became impossible between the two armies and they started communicating in plaintext (Russian). The German General Paul von Hindenburg could not believe his luck when he received an intercepted message reading: *I am halting temporarily and cannot link with you as my supplies trains have not arrived* (Laffin, 1964:107). This is all what von Hindenburg needed and his armies dealt the Russian armies a comprehensive defeat at the battle of Tannenberg (Laffin, 1964:107) - all because of the Russia's incompetent cryptologists.

Ironically, the Russians actually played a big role in the eventual defeat of Germany. In addition, in 1914, a German cruiser, the Magdeburg ran aground in fog in the Russian Baltic Sea. The captain ordered an officer to dump their code books in the sea. It was then that Russian warships opened fire, sinking the cruiser and killing all aboard. Upon picking up the bodies, they came across the German officer, still with the lead covers of the codebooks in his hands. Russian divers recovered the codebooks and they were rushed to the British Admiralty in London.

4.6.2.3 Britain

The British Admiralty had a special department, called Room 40, where a crack team of the top brains assembled to work on captured documents and messages in order to decipher them. Room 40 was the headquarters of the Royal Navy's cryptologic section, under the command of Admiral Reginald Hall (Laffin, 1964:108).

The British also played an instrumental role in the war against Germany and in getting the USA to become involved in the war. Besides the code books received from the Russians, the act to cut Germany's underwater communication cables and the events that followed changed the course of World War I. This forced the Germans to use British cables for their communications and this is how a German

communication, called the Zimmermann telegram, was intercepted. Arthur Zimmermann was the German minister of foreign affairs. In the telegram, Zimmermann asked Mexico to invade the USA, thus keeping the USA away from the war zone in Europe. The Germans promised to support Mexico in the war and would repay them by handing over the three states of Texas, New Mexico and Arizona.

Reverend Montgomery took charge of deciphering the telegram at Room 40 and with the help of Nigel de Grey, they worked on a solution (Singh, 1999:112). Woodrow Wilson, the US president at that time, used this information to get the USA to change their position on the war. A copy of the deciphered message was presented to the USA and the British published articles crediting the USA as the solvers of the encrypted telegram. The USA had no option but to enter the war and together with the French and British troops succeeded in finally winning the war against Germany.

4.6.3 World War II

Many feats, unknown to the public, played an important role in changing the course of the war. Although not all feats were war related, some cryptologic events in this era paved the way for forging the field of cryptology. The Germans took their mistakes of World War I to heart and developed the Enigma cipher machine. Arthur Scherbius, a German inventor, developed the Enigma machine. He deemed the cryptologic systems used in World War I as inadequate and wanted to develop a machine that exploited the technology of the 20th century (Singh, 1999:127; Gilbert, 1989:39).

Scherbius's Enigma machine was an electrical application of Alberti's cipher disk. It consisted of three parts, keyboard, scrambler and lampboard. For every letter typed on the keyboard, the scrambler rotated once, while the lampboard lit up indicating the encrypted letter (see figure 4.2), (Singh, 1999:139).



Figure 4.3: Enigma machine

Two documents published by the British on how they gained access to German World War I communications, forced the Germans to accept the Enigma as their official encrypting cipher for World War II. As the Enigma was available on the commercial market, newer versions were developed with more wires and different scrambler settings. Cryptologists from different countries were all working hard to understand how the Germans employed Enigma to encipher German communications between their troops. The developments in the next section try to show how a joint Anglo-French effort succeeded in doing this.

Poland fearing an invasion from Germany showed an interest in these messages. The British and French could not make any headway in deciphering these messages and "it was above all a Pole, Marian Rejewski, helped by material obtained by a French secret agent, Asché, who made the crucial breakthrough in Poland before the war" (Gilbert, 1989:39). Although Rejewski played a big role in deciphering messages sent by Enigma, it did not help Poland in the war against Germany. The turning point for breaking Enigma came on 4 September 1939, when the Government Code and Cypher School asked Alan Turing to work at Bletchley (Singh, 1999:169). He worked feverishly on German intercepted messages and employed the strategies used by Rejewski in order to break

Enigma. What made their task more difficult was the fact that the Germans used different codes for different operations. Some of these codes were intercepted and this helped the cryptanalysts in eventually breaking Enigma. David Kahn describes the work of Turing and others in breaking Enigma and their decoding of other intercepted messages as follows (Kahn, 1980:639):

It saved lives. Not only Allied and Russian lives but, by shortening the war, German, Italian and Japanese lives as well. Some people alive after World Wars I and II might not have been but for these solutions. That is the debt that the world owes to the codebreakers; that is the crowning human value of their triumphs.

This work was further recognized with the release of the film, *Enigma*, in 2002.

Besides breaking Enigma, intercepted Italian and Japanese messages were also broken. This work, done under the code name Ultra, gave the allied troops the advantage when they invaded Europe. Sir Harry Hinsley paid the following tribute (Singh, 1999:187) to the cryptologists: “the war, instead of finishing in 1945, would have ended in 1948 had the Government Code and Cypher School not been able to read the Enigma cyphers and produce the Ultra intelligence.”

With the British and other allied partners’ attack on Enigma, the USA had a similar battle with respect to breaking the Japanese cipher, known as Purple. The Purple cipher machine was a modified version of the Germans Enigma cipher machine. This did not mean that the British and Americans did not have cipher machines of their own. The British used the Typex (Type X) cipher machine for their army and airforce, while the Americans used the SIGABA (or M-143-C) cipher machine (Singh, 1999:192). The ciphers of these machines, both more sophisticated than Enigma, were never broken during the war.

A Russian born American scientist, William Friedman, achieved the breaking of Purple. Working with Frank Rowlett, Solomon Kullback and Abraham Sinkov, they achieved the Purple solution that led to the triumph of World War II (Kahn,

1996:385-386). Elizebeth, Friedman's wife, was also an ardent cryptologist and worked with him on some of his projects.

The Arabs' use of their language and linguistics to set up keys to encipher and decipher messages were taken up by the Americans and used as a means to conceal messages. They used the language spoken by the Navajo tribe as a communication medium between their troops. The idea was to use the Navajos as radio operators to translate messages from their spoken language, Navajo, into English. These Navajos became known as the code talkers. Although the Japanese broke the American Air Force code, they failed to break the Navajo code (Singh, 1999:201). The Navajos contribution to the war was finally recognized when the U.S. Government named August 14 the "National Navajo Code Talkers Day" (Singh, 1999:201). Further recognition was given with the release of the film *The Windtalkers*, based on a true story from World War II. The tagline to advertise the movie, *The Navajo Has The Code. Protect The Code At All Costs* is quite fitting.

The work done by Friedman and others during World War II paved the way for the further development of cryptology.

4.6.4 Modern Uses

The era of World War II was followed by the introduction of the information era. In 1949 Claude Shannon, a researcher at Bell Laboratories, took "*the mathematical approach to all kinds of information that could be handled electronically*" (Barr, 2002:25) to new heights. Linking information theory to the mathematics of language and cryptology, he developed the Shannon theorem on information capacity. Submitting the languages of English and French to statistical analysis and coming up with ways in which they could be simulated, the concept of perfect security in a cryptosystem was clarified. In essence, it means that it is "impossible for an adversary who knows the cipher algorithm in use to do any better than pure guesswork at deciphering intercepts" (Barr, 2002:25-26).

With the increase in information and technology there was an upsurge in the use of computers in industry and commerce. Because of the increase in transmission of data by electronic means, this meant security became a risk. In 1975, the National Bureau of Standards (NBS) in the USA gathered proposals for a uniform method of encrypting non-military data. International Business Machine's (IBM) proposed Lucifer-system was modified and culminated in Data Encryption Standard (DES) by NBS in 1977 (Barr, 2002:26). Although not widely accepted, "it is routinely used by banks all over the world to protect electronic funds transfers such as automatic teller machine (ATM) and credit card transactions" (Barr, 2002:26).

Martin Hellman and Whitfield Diffie, influenced by the work of Ralph Merkle (Diffie and Hellman, 1976), worked together to come up with a solution for the distribution of the cipher key in a cryptosystem. They developed what is known as an asymmetric key in 1976 where the enciphering key and deciphering key are different. All previous systems up to then used symmetric keys, meaning the decrypting key is the opposite or inverse of the encrypting key. Let's look at the analogy of padlocks to explain their basic idea. Both persons A and B receive identical boxes (each containing the common key) each locked with two padlocks. One padlock can be opened by A and the other by B. On receiving the boxes they open their padlocks and interchange boxes again. Persons A and B now use their keys to open the remaining padlock and retrieve the secret key for communication. Clipping the padlock closed is likened to encrypting, but for decryption, you need the actual key to the padlock. The trio of Hellman, Whitfield and Merkle had difficulties translating their work into reality.

Ronald Rivest, Adi Shamir and Leonard Adleman took up this challenge to make an asymmetric cipher a reality. Their system, called RSA (Rivest, Shamir and Adleman) became the most important breakthrough in cryptology (Singh, 1999:274). The RSA system rests on the premise that it is difficult to factor a big integer into prime factors. Moreover, in this lies the security of their public-key method. The following is a discussion of an example of how the RSA system

works (see Appendices D1 and D2). Choose any two prime numbers p and q . Multiply the two prime numbers to equal a new number N . This number N is now becomes the encryption key and is known to all. The values of p and q are the private keys and are known only to the sender, who uses these values to decrypt messages. Although all can use the encryption values to send messages, they don't have the keys p and q for decrypting the message.

The mathematical underpinnings of the RSA method were developed in the eighteenth century by Fermat and Euler and are contained in many books on number theory with applications in cryptography (Jackson, 1987; Koblitz, 1994; Kumanduri & Romero, 1998; Rosen, 1985; Stinson, 1995).

With the advent of the computer age, information secrecy moved to automated teller machines, cellular telephones, World Wide Web search engines and smart cards. Public-key cryptology was applied on secure Web pages in order to ensure safe credit card transactions over the Internet. Individuals use personal identification numbers (PIN's) for authentication at ATM's. An increase in e-mail usage has necessitated ways of keeping mail from prying eyes. Currently e-mail users have access to packages as Privacy Enhanced Mail (PEM) and Pretty Good Privacy (PGP) to safeguard their mail from unauthorized readers. Both these packages use public-key cryptology for key exchange and digital signature generation (Barr, 2002:29). For both the RSA and public-key cryptology for research and applications, the attention fell on cryptographic protocols. This is in line with the table outline adapted from Menezes (1996) in table 4.2. Phil Zimmermann, who was instrumental in developing PGP, was under scrutiny from the Federal Bureau of Investigation (FBI) (Singh, 1999:314). The FBI tried to stop the distribution of PGP, as it would enable other countries to safeguard their mail from being compromised.

With an increase in electronic commerce, it was necessary to set up a uniform standard for signing nonclassified documents. With this in mind, the National Institute of Standards and Technology (NIST) developed the Digital Signature

Standard (DSS) in 1994 (Barr, 2002:30). In 1997, NIST set up plans to have DES replaced by the Advanced Encryption Standard (AES) (Barr, 2002:30). They called for submissions and set the following requirements (Barr, 2002:30):

- It should use symmetric (secret-key) cryptography;
- It should be a block cipher and
- It should operate on 128-bit blocks of plaintext and allow for three sizes of key: 128-, 192-, and 256-bit.

In 2000 NIST decided that Joan Daemen of Proton World International and Vincent Rijmen of Katholieke Universiteit Leuven should be the team to develop the AES (Barr, 2002:31).

With all the activity on the cryptological front openings occurred for number theory to become more applicable. More and more textbooks on number theory venture into the field of cryptology. Number theory has a prominent role in various cryptologic protocols. This has resulted in the development of Fiat-Shamir protocol (Barr, 2002:31).

With the opportunities in number theory, research into the elliptic curve cryptography (ECC) started. Neal Koblitz and Victor Miller proposed EEC in 1985(Barr, 2002:31). EEC is based on mathematics with algebraic abstractions on certain types of geometric curves.

The basic idea behind encryption is to come up with an encryption system that will withstand all attacks, even from a quantum computer. While quantum theory is the basis for a computer that could break all current ciphers, “it is also at the heart of a new unbreakable cipher called *quantum cryptography*” (Singh, 1999:332). Whenever this is achieved, it will mean the end of the battle between codemakers and codebreakers. Will governments allow this to happen?

4.7 OTHER RESEARCH INITIATIVES

4.7.1 Histo MAP project

Two books, *Codes Galore* (Malkevitch *et al.*, 1993) and *Loads of Codes* (Malkevitch & Froelich, 1993), were developed by Histo MAP (The History of Mathematics and its Applications Project), which was funded by the National Science Foundation. Histo MAP was developed under the auspices of the Consortium for Mathematics and its Applications Project (COMAP). COMAP is a non-profit corporation engaged in research and curriculum development in mathematics education.

The goal of Histo MAP is to develop, through a group of users and developers, a system of instructional modules for students of high school mathematics, which combined historical anecdotes and mathematical applications. *Codes Galore*, was the first in the COMAP's historical module series. Its aim was to give students insight into the many codes that influenced their daily lives. *Load of Codes* on the other hand, puts more emphasis on the protection of information and the compression of data.

4.7.1.1 Codes galore

The module, *Codes Galore*, gives students insight into the different codes that they come across in their daily lives. It begins with the secret codes used in World War I and ends with the error-correcting codes of a compact disc (CD). The mathematics used in both secret codes and error-correcting, are examined in detail. The historical section gives an explanation of how codes originated and the people who were influential in developing them. In essence, this module concentrates on the correction and tracking issues of codes.

This module consists of two chapters divided into sections, highlighting different topics. In chapter one, the following are covered in the respective sections:

- Introduction;
- Secret Codes;
- ZIP Codes;
- ISBN Codes and
- Bank Identification Codes.

Chapter two includes the following:

- Introduction;
- What is a Channel?
- Error Correcting Codes;
- Linear Codes;
- Check Digits and
- Applications.



An appendix follows the two chapters, giving explanations and listing worked out examples. In the following section lessons are presented with activities for the students to work through. The module concludes with a teacher's guide including answers and comments on the lessons for the students.

4.7.1.2 Loads of codes

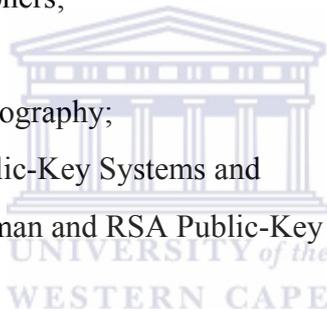
This module looks at codes used in a variety of contexts. Its main concern is the framework mathematics brings for seeing the uses of the word code in the different phrases (secret codes, product code, ZIP codes, genetic codes and other phrases), what they have in common and how they differ.

When contemplating codes what comes to mind is that it is used to conceal. Historically, it has been important to hide sensitive information of political or military nature from the enemy. Currently one might be more interested in hiding information about the transactions between the bank and an individual or between two banks.

The issue of product codes and ZIP codes are different, as they are public knowledge. For example, a supermarket can use information about its products, represented in the form of bar codes, in order to keep track of how much of a product has been sold in a given week, while at the same time sending the customer through the checkout line faster. It is important that the information being stored, transmitted or communicated is accurate. Codes can thus be used to hide, track, protect, or compress data. This module concentrates on codes to hide and compress data.

Chapter one, entitled *Protecting Information*, contains the following sections:

- Introduction;
- Hiding Information;
- Transposition Ciphers;
- Hill Codes;
- Public-Key Cryptography;
- Protection in Public-Key Systems and
- The Merkle-Hellman and RSA Public-Key Systems



In chapter two, entitled *Loads of Data*, the following sections are included:

- Compressing Data;
- Statistical Properties of English Text;
- Prefixes;
- Huffman Codes and
- Conclusion.

The sections that follow chapter two are the same as the explanation given in the outline for module one.

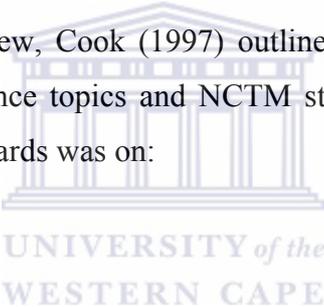
4.7.2 Washington MESA project

The Washington MESA (Mathematics, Engineering, Science Achievement) project aims to introduce classroom materials that facilitate links between classroom and real-world mathematics and science (Cook, 1997). This was done

by way of instructional modules created and field-tested by the Washington MESA project. For the project staff members of MESA and teachers worked with scientists, mathematicians and engineers to develop modules. This culminated in the module, *Secret Codes*.

The module, *Secret Codes*, was piloted in the middle grades of high schools in Seattle, Spokane, Tacoma, Toppenish and Yakima, Washington. This was all done under the auspices of the University of Washington. The module included seven activities based on the reform philosophies recommended by the National Council of Teachers of Mathematics' (NCTM) *Curriculum and Evaluation Standards for School Mathematics* and the American Association for the Advancement of Science's *Project 2061* (Cook, 1997).

In the conceptual overview, Cook (1997) outlines the links of *Secret Codes* to mathematics topics, science topics and NCTM standards. The emphasis of the NCTM Curriculum standards was on:

- 
- Problem Solving;
 - Communication;
 - Reasoning and
 - Mathematical Connections.

For the NCTM teaching standards the focus was on:

- Worthwhile tasks;
- Teacher's Role;
- Enhancement Tools and
- Learning Environment.

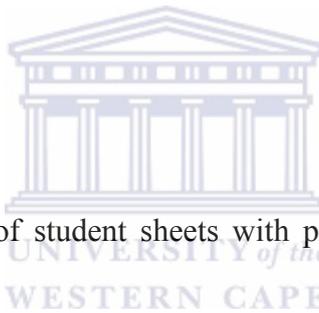
Of the seven activities, six are for the students and one for the family. The aim of the activities was to introduce students to the different types of ciphers. These ciphers included:

- Additive Ciphers;
- Modular Arithmetic;

- Multiplicative Shifts;
- Prime Numbers;
- Affine Ciphers and
- Vigenère Ciphers.

The family activity was a combination of the above mentioned activities aimed at getting the family as a whole to work on the problems. Every activity was introduced with an overview, followed by background information and ways of presenting the activity. So each MESA module focused on different topics, but had links with the following:

- Career;
- Writing;
- History;
- Interest and
- Technology.



Each activity consisted of student sheets with problems that had to be worked through by the students.

4.8 ANALYSIS

The discussion of the literature review opens up a rich context for the development of activities for school mathematics teaching and the formulation of school mathematics projects – see Appendix B. For these activities, a background of number theory becomes helpful. This is because most of the solutions when cryptanalyzing, are set against the background of number theory. The following chapter, entitled historical and didactical phenomenological study of secret messages, will help for further preparing the ground for developing instructional activities.

CHAPTER 5
HISTORICAL AND DIDACTICAL PHENOMENOLOGY OF
CRYPTOLOGY

Concealment, codes, and other types of ingenious communication.
(Butler & Keeney, 2001)

5.1 INTRODUCTION

An important aspect of this study is the development of instructional materials on cryptology for grade 10 learners of school going mathematics. This becomes even more important within the context of the main research question:

How could new content be introduced into school mathematics curriculum?

In order to get a grip on the topic to be taught, there needs to be understanding of the main concepts within the topic as well as a historical and didactical phenomenology thereof in order to make statements with respect to the teaching and learning of the topic of cryptology.

The previous chapter, entitled literature review, gave a broad overview of the historical development of cryptology. Working through the literature review gave some insights into the links between history and education, which opens up different learning trajectories with respect to cryptology. On developing these learning trajectories, the aim is that learners somehow reinvent, in a guided way, the mathematical concepts (Freudenthal, 1973 & 1991).

The young learner recapitulates the learning process of mankind, though in a modified way. He repeats history not as it actually happened but as it would have happened if people in the past would have known something like what we do know now. It is revised and improved version of the historical learning process that young learners recapitulate. ‘Ought to recapitulate’ – we should say. In fact we have not understood the past well enough to give them this chance to recapitulate it. (Freudenthal, 1983b:1696)

In order to make sense or understand concepts within a mathematical topic, it is useful to look at its history. Freudenthal (1883b) and Stanton (2001) support the notion that studying the history of a topic is good for teaching that topic. This is aimed at determining what motivated its emergence and shaped its development. The mathematics and Dutch historian, Dijksterhuis (1990), is of the opinion that learners come to grips with history at a higher speed. Problems that current learners of school-going mathematics encounter resemble problems that generations before them experienced. With this in mind, I will look for historical contexts that open up avenues for cryptological notions and to look for some of the conceptual obstacles that mathematicians and users of mathematics encountered.

5.2 PHENOMENOLOGY

Phenomenology can be described as an objective inquiry into the logic of essences and meanings of trying to make sense of a topic. This objective enquiry can take on different forms. Possible forms are a theory of abstraction, deep psychological description or an analysis of consciousness (Thévenaz, 1962:37). Phenomenological analysis means approaching the study object, the phenomenon, as free as possible from conceptual presuppositions. The aim of phenomenological research is to obtain insights into the essential structures of these phenomena based on mental examples supplied by experience or imagination and by a systematic variation of these examples in the imagination.

Freudenthal, however, goes a step further. Freudenthal (1983a) describes a method of studying relations between mathematics, history and education. Freudenthal distinguishes between *phenomena* and *concepts*. Phenomena refers to that we want to understand, make sense of, or structure, while concepts are the thought processes that organize these phenomena. Based on this, he defines phenomenology as follows (Freudenthal, 1983a: 28-29):

Phenomenology of a mathematical concept, a mathematical structure, or a mathematical idea means, in my terminology, describing this noumena in its relation to the phainomena of which it is the means of

organizing, indicating which phenomena it is created to organize, and to which it can be extended, how it acts upon these phenomena as a means of organizing, and with what power over these phenomena it endows us. If in this relation of noumenon and phenomenon I stress the didactical element, that is, if I pay attention to how the relation is acquired in a learning-teaching process, I speak of didactical phenomenology of this noumenon. (...) if “is ... in a learning-teaching process” is replaced by “was ... in history”, it is historical phenomenology.

Within the context of this study, historical phenomenology and didactical phenomenology have to be clarified. Historical phenomenology is the study or probing of historical contexts wherein certain mathematical concepts are present in order to make sense of why and how they came up in these contexts. Didactical phenomenology, on the other hand, is the study of relationships “between the mathematical concepts and the phenomena in which they arise with respect to the process of teaching and learning these concepts and their applications” (Bakker, 2003).

This brings us to the aim of this chapter: to make a study of cryptology from two stances i.e. from a historical and didactical stance. What follows is a historical phenomenology of cryptology. The chosen examples are organized chronologically and are by no means exhaustive. This will be followed by a didactical phenomenology of the same examples. The didactical phenomenology will be further informed by field-testing developed materials on cryptology with teachers of school-teaching mathematics, learners of school-going mathematics and second year students in the further and education phase (FET) studying towards a teacher’s qualification with mathematics for teaching as one of their main subjects.

5.3 HISTORICAL PHENOMENOLOGY OF CRYPTOLOGY

A historical study of secret messages is not an easy process. When people write about history, it is usually with respect to men/women or books, and rarely with respect to concepts. A second problem could be that the topic of secret messages is not an established one that stands on its own in mathematics. The historical

phenomenology of secret messages will therefore look at examples within different contexts in which it was used. Therefore, what follows is rather an exposition of how secret messages were used in war, communication and other contexts.

5.3.1 Bald message

Herodotus (Singh, 1999:3-5) in 'The Histories' chronicled one of the earliest conveyances of a secret message. Singh (1999) relates how Histiaieus, governor of Miletus, and an enemy of the Persian ruler, Darius, secretly communicated with Aristagoras. Histiaieus shaved off the hair on his messenger's head and tattooed a message on his scalp. After a few weeks, the hair on the messenger's head grew back on, covering the message. The messenger was sent to Aristagoras to deliver the message. He had no problems in crossing Persian enemy lines. On arrival before Aristagoras he said: "Master, shave my head." This was done and the secret message revealed.

The message on the baldhead was kept secret by allowing the hair to grow back on, thus covering the message. The hair that grew back on the head ensured encoding of the message.

5.3.2 A belt

Lysander (Laffin, 1964:29-30), a Spartan General, and his troops were away from home, Greece, for quite a while. Their allies in the war, Persia, remained behind to safeguard Greece against their common enemies. On his arrival at the war front, a messenger was asked to appear before Lysander. On asking the messenger what his business was, he could not say. Lysander then saw the broad leather belt around the messenger's waist. Under scrutiny, Lysander found different letters branded into the belt. He took the belt and wrapped it around the long wooden baton he carried with him.

In so doing, the scrambled letters aligned into legible words and sentences. The message thus uncovered informed him of a possible uprising in Greece by

Pharnabazus from Persia. Lysander went back to Greece and crushed the rebellion.

5.3.3 Fire signals

Aeschylus, a dramatist, related the story that the fall of Troy (Butler and Keeney, 2001:22) in 1084 BC was news so important, that it had to be relayed to Queen Clytemnesta in Argos. The problem was that she was about 805 kilometers away.

Before the Queen left for Argos, it was agreed that a visible fire would indicate a good outcome. The Greeks arranged for fires to be lit on nine hills about 72 kilometers apart. Different fire teams gathered on the respective hills and on noticing the fire 72 kilometers back, lit their own to notify the next fire team. This, being the first recorded use of long-range communication, took about 11 minutes to travel the length of Greece.

5.3.4 Flag signals

During the 1800's fleets of ships communicated with each other by way of flags. This innovative way of communication was used by the British, hoisting flags whose graphic designs, lines, shapes and colors all of which had their own specific meaning.

During the battle of Trafalgar between the British and French forces, Horatio Nelson's use of a new signal system proved decisive in winning the war. After much consultation with his flag lieutenant, Mr. Pesco, the following message was sent using seven flags: "England expects that every man will do his duty" (Butler & Keeney, 2001:38). The message inspired the British to a victory over the French troops.

5.3.5 Quilt code

The quilt code was developed by slaves in America to indicate escape routes to Canada. According to Tobin & Dobard (1998), the designs each conveyed a different instruction. Although the slaves could follow the instructions given on

these quilts (hanged on washing lines), outsiders and even slave owners could not make sense of it.

5.3.6 Hobo messages

As the economic depression increased in the 1930's, more and more people lost their jobs and became wanderers. In their wanderings, they often used signs, marks and symbols on sidewalks, houses, towns and cities to communicate different meanings. Only hobos understood this secret language of symbols.

5.3.7 Sports codes

Signs by way of number calls, hands and fingers are a prominent feature of sports' games. Any game on a baseball field is rife with hand signals. Rugby players, for example, use numbers to indicate a code for finding a lineout jumper when throwing in a ball at a lineout.

5.3.8 Pig Latin

Pig Latin was developed by children as a way to keep their communication secret or confidential. If two children communicated, they used Pig Latin to keep their communication secret from a third party. The Pig Latin system works as follows:

- Words that start with a vowel (A, E, I, O, U) have “way” appended to the end of the word;
- Words that start with a consonant have all consonant letters up to the first vowel moved to the end of the word and “ay” appended at the back and
- ‘Y’ is counted as a vowel in this context.

The sentence “*Please pass me the yellow spoon*” changes to “*Easeplay asspay emay ethay ellowyay oonspay*” in Pig Latin.

5.4 DIDACTICAL PHENOMENOLOGY OF CRYPTOLOGY

The discussion on didactical phenomenology of secret messages is informed by the cryptosystem within cryptology (see figure 4.1 in Chapter 4) in order to identify the type of cipher and keys used to encrypt and decrypt messages.

5.4.1 Bald message

For this message, both the enciphering and deciphering keys are shaving of the hair. As the original message remained the same (as inscribed on the head), there were no changes in the plaintext message. The bald message is an example of a plain cipher or a null cipher, as the message did not undergo any changes. The person carrying the message serves as the code as well.

5.4.2 A belt

For the belt episode, the wooden baton, acts both as enciphering as well as deciphering key. Turning the belt around the wooden baton also extended the keys to include a certain number of turns for both instances. An outcome of the turns was that the original message was scrambled on the belt after it was unwound from the baton. This is an example of a transposition cipher, meaning the ciphertext contained the same letters as in the plaintext, but in different positions.

5.4.3 Substitution ciphers

Under substitution ciphers are included the fire, flag, quilt, hobo and sport messages. They all have in common the fact that symbols in whatever form have been used to indicate different things. For example, the fire was a symbol of good news, whereas the designs on the flag denoted different words. In the case of the quilts and hobo messages, patterns and markings translated into a language only to be understood by the people concerned. Concerning the sports codes, these signs and signals were there to indicate the play that was about to take place. This was aimed at keeping the opposition guessing.

For the examples listed under substitution ciphers the symbols, patterns, fires, etc indicate the encryption keys, while the decryption key was the translation of these into a plain message or an action.

5.4.4 Pig Latin

Pig Latin is a simple form of a transposition cipher where letters in a word change position. The adding of the “*ay*” or “*way*” at the back is an example of a null cipher. A null cipher is an example of a cipher that does not change a word or its form. This is one of the first examples in history where two ciphers were used.

5.4.5 Discussion

The examples listed above, show how difficult it is to make implicit aspects of cryptology explicit. Although Lysander thought of the shaving of the hair to inscribe a message on the head and later allowing the hair to grow back on to cover the same message as a way of keeping it secret, this will not be a good example to use for teaching. Both the encoding and decoding keys are the same and the message itself did not undergo any changes.

The observation that the oldest historical examples had to do with secrecy, gives rise to the question: *Is secrecy a good starting point for the teaching and learning of cryptology?* The answer is yes. Cryptology has as its aim secrecy or confidentiality. The historical examples show messages had elements important to cryptology. Some of these elements are the encoding key, decoding key and the different types of ciphers.

Another observation from history is that the idea was to keep messages or communications secret. This alludes to the importance of the key in encoding messages. The more difficult the key, the more difficult it will be to decode the message.

For the teaching and learning of cryptology, the historical examples needed changes or revision. First, most learners have an idea what secrecy is, but deal

with it in situations at play. Secondly, not all the historical contexts are suitable for instruction. How many learners would be interested in deciphering flag signals or hobo messages? The example of the belt is an appealing context to start the teaching of cryptology. It has elements of a practical activity as well as introducing a transposition cipher.

What the examples of history open up is the introduction of different ways of communication to keep messages secret. In all these messages, the way of hiding the message, namely the key, was a central concept. For the teaching and learning of cryptology, it seems it would be best to introduce the topic of cryptology by way of secrecy and furthermore to introduce learners to the different ciphers in order to render messages intelligible.

5.5 CONCLUSION

What the chapter set out to do was to show how some of the concepts important to cryptology started back in history. Although only a few of these concepts were discussed, it shows the importance of historical phenomenology for the designing of instructional material. Furthermore, the examples gave a starting point for the teaching and learning of cryptology. These insights gained thus far will be used to discern about a didactical phenomenology and to develop a hypothetical learning trajectory for the teaching and learning of cryptology in two research cycles. The next chapter reports on the first research cycle of data collection for the teaching and learning of cryptology.

CHAPTER 6

FIRST DESIGN RESEARCH CYCLE

6.1 INTRODUCTION

This chapter reports on the first design research cycle of the data collection. As reported in previous chapters, this study consists of two design research cycles (DRC). CI and CII indicating the first and second cycles respectively denote these cycles. The cycles with the learners are indicated as G10-CI and G10-CII, where G10 is used to indicate grade 10.

Teaching experiments are denoted by TE1, TE2 and TE3 to indicate the number of experiments that took place. (TE1) T – C1 refers to the teachers (T) in the first experiment (TE1) of the first design research cycle (C1), whereas (TE3) S - C1 indicates the students (S) in the third experiment (TE3) of the first design research cycle (C1). Figure 6.1 outlines the time-line (see Appendix A, Note 5) for the teaching experiments in the first design research cycle.

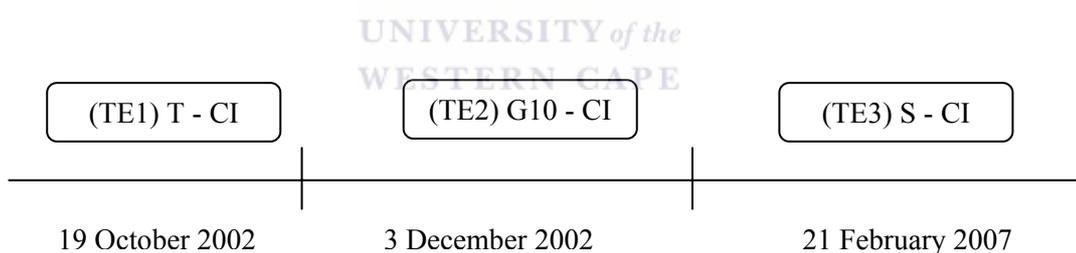


Figure 6.1: Time-line for first design research cycle

In the first part of the chapter we describe the development of the hypothetical learning trajectory (HLT), which is informed by the literature review, and the historical and didactical phenomenology of cryptology discussed in chapters four and five. Secondly, the instructional activities developed for the first design research cycle is discussed. Thirdly follows a description of the respective teaching experiments. The chapter concludes with a feed-forward analysis for the second design research cycle.

6.2 OUTLINE OF HYPOTHETICAL LEARNING TRAJECTORY

The main focus of the instructional materials was to introduce participants to the different types of ciphers in cryptology. As a starting point the context of the Spartan scytale was used to introduce the transposition (scrambled) cipher to teachers and learners. For the students the Alberti disk was deemed a suitable activity to introduce the cipher concept of cryptology. This meant two types of ciphers were piloted as part of the first design research cycle.

As the participants for the first design research included teachers, learners and students, the discussion of the HLT will be done with respect to the different participants.

6.2.1 Teachers

Starting out the activity as a practical one with cutting of paper as a scroll for turning around a batten will be intimidating to teachers. It could mean that some of them might lose interest because they don't see the mathematics in it. As identified earlier, understanding how the cryptosystem within cryptology works is central to the development of the HLT. The reification of the enciphering and deciphering by way of a key or a rule was seen to be important for the conceptual development thereof.

Assuming that the scytale was a relevant context to introduce the transposition cipher the assumption is that teachers' prior knowledge will enable them to deal with the calculations at hand. Their understanding of the working of the inverse processes in mathematics for teaching will enable them to make the translation from enciphering to deciphering messages. Guidance given by way of the questions will allow them to easily make the connection between enciphering and deciphering to build on how the key (number of turns around the batten) works in the cryptosystem.

6.2.2 Learners

When the teaching experiment was done with the grade 10 learners, they were still part of the old school mathematics curriculum for grade 10. Although they followed an OBE curriculum up to grade 9 the implementation date for the new OBE curriculum for grade 10 was 2006. These learners thus had exposure to activities within the OBE mode.

This background is important as it gives credence to starting the instructional material for learners with a practical hands-on activity. Although the nature of the practical activity could be intimidating to teachers, it could have the opposite effect for the learners. This might allow them to be interested and to keep them working in order to solve the problems.

It is further assumed that learners will relate the number of turns around the batten to the total number of letters in the message. From this they will divide the total of numbers by the number of turns in order to decipher the message - at times it could be possible if the number of turns is a divisor of the total number of letters in the message. In so doing the connection between the forms of the message while turned around the batten and when unwrapped from the batten won't make sense to them. The essence of understanding of the inverse to decipher a message will thus be missed.

It is further conjectured that learners will solve problems by using informal methods and not necessarily use the formal mathematical methods that the teachers might use.

6.2.3 Students

As the students were new to me I did not have an idea of the mathematics they did at CPUT. However, for entrance to the course they all had to have a grade 12 qualification in school mathematics. When revisiting and rereading the literature review, it came to me that the Alberti disk could be a suitable context to introduce one of the different types of ciphers for the cryptosystem.

The following assumptions were made with respect to how the students would proceed when working through the instructional activity. They would use the given Alberti alphabet and use the mathematical principle of counting forward (adding on) or counting backwards (subtraction) to determine corresponding values for enciphering or deciphering messages. There were not many mathematical calculations to be done so it was required of the students to give a description of how they solved the respective problems. It was assumed that their descriptions would capture the words of addition or subtraction between the numbers of 0 and 25 as listed in the Alberti alphabet. At no stage would it be expected that students would know that even values bigger than 25 or smaller than 0 (negative whole numbers) could be determined from the Alberti alphabet.

6.3 TEACHING MATERIALS

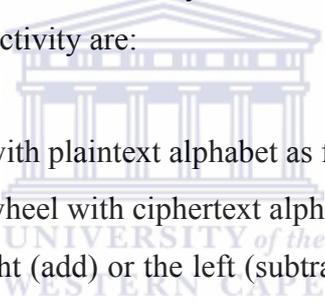
This section reports on how the HLT of the cipher impacts on activities for the teaching materials. Teaching materials are also referred to as instructional activities in the text. For the first design research cycle instructional materials were developed for teachers, learners and students. Developed instructional materials for the teachers were done in English, whilst those for the learners and students were developed in Afrikaans.

For the (TE1) T – C1 (see Appendix E2) and (TE2) G10-CI (see Appendix E5) the teaching activity on the scytale was introduced by a short introduction. The aim of the scytale activity was to introduce the participants to the transposition cipher. As previously mentioned the scytale activity had a practical nature as it aimed to attract learners' attention and also to direct them through the activity to the techniques of enciphering and deciphering of messages within a realistic context. The key issues at heart of the scytale activity could be summarized as follows:

- Number of turns;
- One letter to a turn, moving to the right and continuing below;
- Writing down of the form of the message from the turns;

- Writing down of the scrambled message in the form it appears after taking the scroll off the batten;
- Making an inference about the message in its original form, around the batten and when taken from the batten;
- Using the knowledge gained by working through the previous steps to rewrite a scrambled message into its original forms irrespective of whether the number of turns around the batten is known or unknown.

The Alberti disk activity for the (TE3) S - C1 (see Appendix E8) was done as part of the didactics of mathematics lessons with students of CPUT. The aim of the Alberti disk was to introduce students to the addition or subtraction cipher within the cryptosystem. This introduction was important as it had leanings towards an introduction to the use of number theory in an informal way. The key aspects at work in the Alberti disk activity are:

- 
- The outer wheel with plaintext alphabet as fixed;
 - Revolving inner wheel with ciphertext alphabet;
 - Moving to the right (add) or the left (subtract) to determine corresponding letters from the deciphering or enciphering wheels;
 - Making inferences about letters if their values fall outside the given values for an alphabet.

The next section reports on the different teaching experiments of the first design research cycle.

6.4 TEACHING EXPERIMENTS

The aim of the three teaching experiments with teachers, learners and students was to investigate how the developed HLT would play out in the respective classrooms and whether they would enable the participants to understand the enciphering and deciphering processes within the cryptosystem.

In the first part of this discussion we discuss how the teaching experiments were carried out, the break down of the different participants with respect to gender for the respective groups as well the setting where the teaching experiments occurred. This discussion is done under the general heading of method.

6.4.1 Method

The teaching experiment for the teachers was held on the UWC premises in a lecture hall. Professor Julie, lecturer for the B.Ed honors course, was present at the teaching experiment. As already mentioned in chapter 3 (see field notes in figure 3.3) no video recording was made for this session. The researcher and professor Julie made observations and field notes. After a short introduction on the instructional activity, the teachers worked at the activity on the scytale. Where problems arose a general explanation was given to elucidate matters. All the written work was handed in after completion of the session, which lasted for about 1 hour.

The breakdown for the number of groups and gender in the teaching experiment with the teachers is given in the table that follows.

TEACHING EXPERIMENT WITH TEACHERS			
GROUPS	MALE	FEMALE	TOTAL
1	3	3	6
2	3	4	7
TOTAL	6	7	13

Table 6.1: Group breakdown for teachers

For the teaching experiment with the learners, the learners came to the UWC campus after completion of their final exams in grade 10. The learners gathered with the researcher in the local physics laboratory where the video recording was to be made. Although the learners' parents gave their consent for participation in the teaching experiment (see Appendix F), learners were again briefed on the aim of the teaching experiment and how it would be reported on in the thesis.

The practical nature of the teaching experiment was enhanced with the learners having to act out the roles of sender, receiver and interceptor of messages. With this the ideas of enciphering and deciphering were captured. A video recording was made and observations and field notes were taken. The same presentation style as described for the teachers above was adopted. Sometimes it was necessary for the researcher to engage with members in a group to clarify certain aspects or to give direction. This session lasted for about 45 minutes.

Table 6.2 outlines the gender and number of groups for this teaching experiment with the learners.

TEACHING EXPERIMENT WITH LEARNERS			
GROUPS	MALE	FEMALE	TOTAL
1	1	2	3
2	0	3	3
TOTAL	1	5	6

Table 6.2: Group breakdown for learners

In the last teaching experiment for the first research design cycle students from the Cape Peninsula University of Technology acted as participants. These students were in their second year of studies for the teacher's qualification in the FET phase. They all did mathematics for teaching and the didactics of mathematics as part of their course towards a teaching qualification. The teaching experiment was done during normal class time for a mathematics didactics lecture of 45 minutes in a lecture room on the Wellington campus.

The breakdown for the number of groups and gender (see also figure 3.2 in chapter 3) in the teaching experiment with the students is given in the table below.

TEACHING EXPERIMENT WITH STUDENTS			
GROUPS	MALE	FEMALE	TOTAL
1	0	2	2
2	0	2	2
3	0	2	2
4	2	0	2
TOTAL	2	6	8

Table 6.3: Group breakdown for students

In the following part of the discussion of the teaching experiment we focus on the experiences and happenings (6.4.2) of the teaching experiments.

6.4.2 Experiences

In this section follows a description of the experiences and happenings during the teaching experiments with the teachers, learners and students. This discussion is informed by the observations, field notes, written work and video recording.

The teachers started out slowly so as to familiarize themselves with the description given for the activity on the scytale. The choice of the number of turns to be used around the batten was problematic. Their understanding was that the size of the batten or the total number of letters in the message determined the number of turns – this discussion took place with one of the groups (taken from observations):

Researcher: Do you understand the issue on the number of turns?

Teacher 1: Still working on it ...

Teacher 2: Can we decide on the number of turns?

Researcher: Yes, but what is important here?

Teacher1: Number of letters in the message, size of the batten.

Teacher3: No, one letter per turn, going right and going on below.

(Gesturing with the fingers)

The following extract from the written work shows how they went about deciphering the message by using the columnar method (first 8 and then 6).

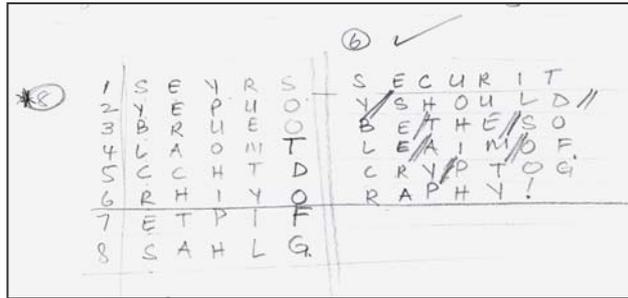


Figure 6.2: Teacher’s solution using columnar method

The same concern about the number of turns and the total number of letters was captured by learners in a group in their explanation of how they actually solved the problem. Translated, their explanation (Afrikaans version in figure 6.2) says the following:

Counted actual letters, 21 in total
 Divided by 3 = 7

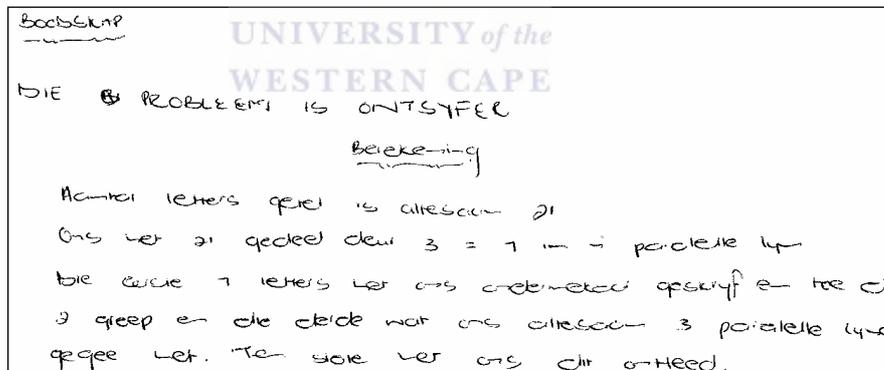
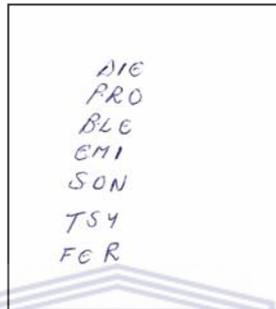


Figure 6.3: Learner’s solution using number of turns

The learners on the other hand started out more enthusiastically after reading through the introduction. A point of concern to one group was how to proceed with the deciphering of the message. The following extract, from an episode from the video recording, captures how they decided to approach this concern – translated from Afrikaans into English (see Appendix G episode 2 for Afrikaans version; L1: Learner 1 and L2: Learner 2).

- L1: I'll try 5 turns; you try 6 and so on ...Instead of us working on the same turns.
L2: *How many turns?*
L1: Take 5 or should we try 6? It's not going to work 2, 4, 6, ...Is it not 7? It won't *work*.

An outcome of their choice on working with three turns is given below. It is important to note that they worked with three columns, writing the first seven letters of the scrambled message as the first column.



DIE
PRO
BLE
EM1
SON
TSY
FER

Figure 6.4: Learner's solution using columnar method

6.5 FEED-FORWARD ANALYSIS

In the previous part of this chapter we reflected on the happenings and experiences of the first design research cycle in order to formulate a feed-forward for the second design research cycle. For the feed-forward to have credence on the follow-up research cycle there had to be a reflection on all the aspects of the teaching experiments of the first design research cycle.

The first issue concerned the understanding of enciphering and deciphering of messages and making sense of how the cryptosystem worked in cryptology. It was expected that the scytale activity, because of its realistic context, could help in establishing the processes of enciphering and deciphering. This was not always the case and it was difficult for the teachers and learners to deduce from their calculations how to proceed to decipher a scrambled message. On the issue of the language used in the teaching experiments it is important that it should be reader friendly in order for learners to follow easily. The way questions were formulated could also help in this regard.

The feed-forward for the HLT addressed the introduction to the scytale and the Alberti disk to introduce participants to a transposition and addition cipher. Results from the first teaching experiment suggested that the scytale activity be kept as an introduction and the questions be rephrased in order to lead participants to come to grips with the processes of enciphering and deciphering. A question with a message on a parchment turned around a scytale could also be included. It was concluded that the scytale is a meaningful and realistic context for the participants to start off with.

A possible question in this regard could be:

Around the batten we have a prepared message on a parchment.

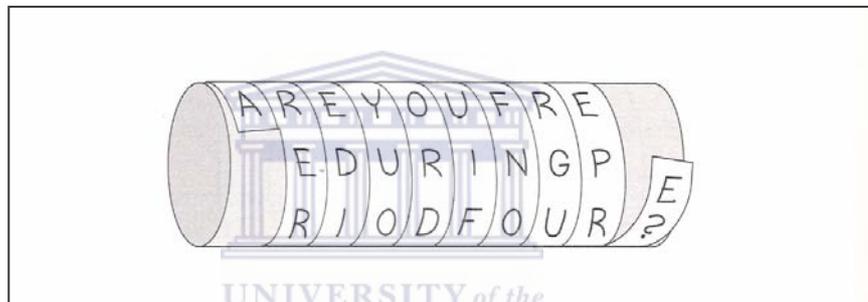


Figure 6.5: Prepared message around batten

1. How many turns do we have for the parchment around the batten?
2. Write down the message that was send.
3. Write down the message, as it appears wrapped around the batten.
4. Write down the form the message will have on the parchment after being unwrapped from the batten.

Results from the Alberti disk teaching experiment suggested that the activity be kept and included as part of the instructional materials. It is evident from the feed-forward analysis of the instructional activities that learners needed more practice in the different types of ciphers. In this way they could get more practice in applying their problem solving techniques. There was also a need to select the instructional activities in such a way as to show the varied use of cryptology in the field of school mathematics.

CHAPTER 7

SECOND DESIGN RESEARCH CYCLE

7.1 INTRODUCTION

This chapter reports on the second design research cycle, which was carried out with grade 10 learners. This second design research cycle with the grade 10 learners is denoted by G10 – CII. The outline followed for chapter six will also be used for chapter seven, but instead of a feed-forward analysis, the HLT for each of the seven activities is followed by a retrospective analysis. Figure 7.1 outlines the route from the first design research cycle and its three teaching experiments with the teachers, learners and students and how the feed-forward impacts on the second design research cycle (G10 – CII).

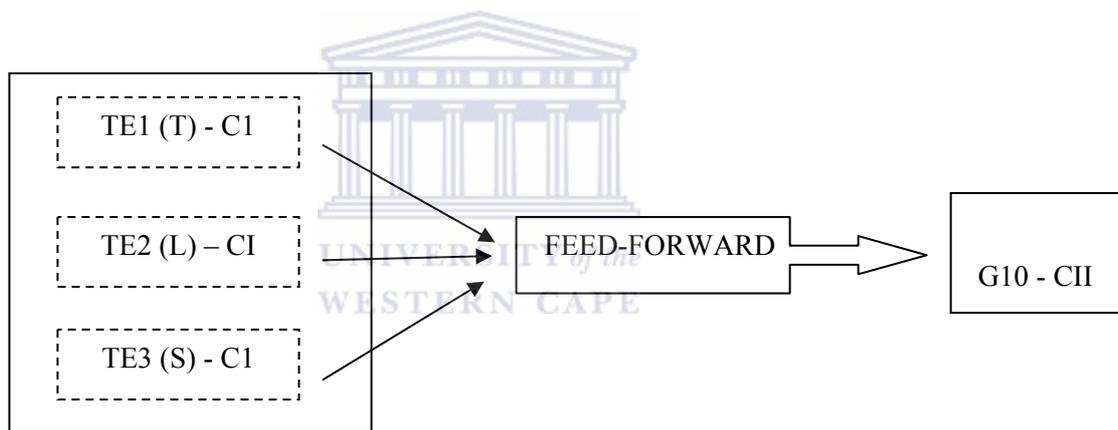


Figure 7.1: Feed-forward from first to second design research cycle

7.2 OUTLINE OF HYPOTHETICAL LEARNING TRAJECTORY

This section describes the points of departure for the HLT for the G10-CII design research and compares it with learners' actual learning. As seven activities were developed for the second design research cycle, the discussion of the HLT and the retrospective analysis were done for each activity. All seven activities for the second design cycle are included under Appendix H (Afrikaans version) and Appendix J (English version).

Important to the development of the HLT was the notion of enciphering and deciphering and some of the different types of ciphers within cryptology. All the experiences discussed under 6.4.2 together with the feed-forward analysis in 6.5 in chapter six impacted on the HLT.

7.3 ACTIVITY 1

Activity 1 was aimed at introducing the important concepts of enciphering and deciphering of messages by way of the transposition cipher. This was a practical hands-on activity of the scytale cipher where learners used materials to make sense of how these messages were developed and sent in the past.

As found in the previous experiments in the first design research cycle with the learners and teachers it would not be easy for learners to decipher the transposition cipher. This was why more questions were added on the number of turns and learners also had to explain how they went about deciphering the message.

7.3.1 HLT for activity 1

From the previous teaching experiment it was found that the scytale activity was a good starting point to introduce the HLT. As the number of turns was crucial in order to make sense of the transposition cipher for the scytale activity, a question on the number of turns around the batten was included for this activity. The previous experiment with the teachers and learners had shown that this question would be helpful in building a sense of the concepts enciphering and deciphering within the cryptosystem.

Figure 7.2 outlines the relationship of concepts within the scytale activity.

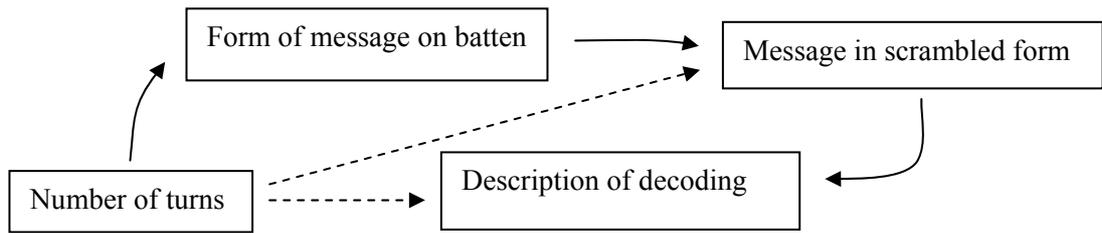


Figure 7.2: Transposition cipher activity

The number of turns around the batten influenced the form of the plaintext message on the parchment wrapped around the batten. When the parchment was removed a scrambled form of the message was displayed. In order to decode a message in scrambled form it was important to make a decision on the possible number of turns that were used for the parchment around the batten.

7.3.2 Retrospective analysis

A short introduction was given to learners with respect to the background for the activity. The chosen example where an already prepared message was turned around a batten (see figure 7.3 below) played a role in helping them to see how these messages were prepared in the context of the Spartan war and the importance of the number of turns was also highlighted.

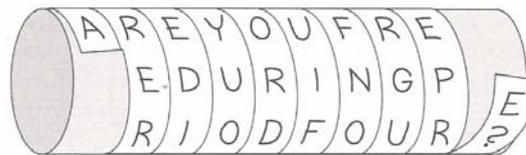


Figure 7.3: Message on parchment around batten

In figure 7.4 the solution of group one for 1.1 to 1.4 is given. Their solution showed they understood the problem. Of interest was the way they presented their solution for the scrambled message on the parchment after being unwrapped from the batten.

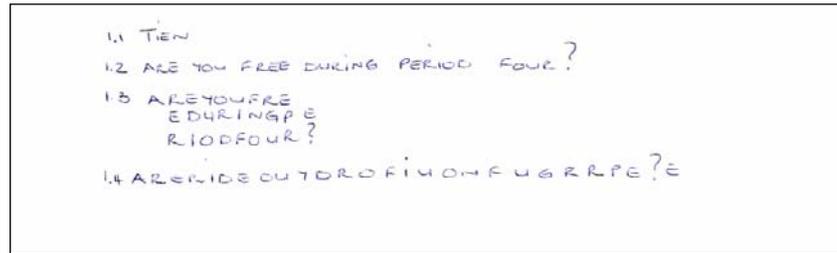


Figure 7.4: Transposition cipher activity: Solutions to problems 1.1 to 1.4

Whilst the accepted start for each part of a message was with the letter in the top row for each column on the batten, they actually started with the bottom letter for each column. The solutions given below illustrate this deviation:

Intended solution: A RER EDI YUO ORD UIF FNO RGU EPR E?

Group's solution: A RER IDE OUY DRO FIU ONF UGR RPE ?E

The misunderstanding occurred because there was only one letter on the first turn. If there had been more letters on the first turn (first column) it could possibly have lead them to see that the top row of the message starts out each turn's part of the message on the parchment when unwrapped from the batten.

In the problem where the group had to describe how they went about decoding the scrambled message the word turns was not used, but the wording of their description indicated that they referred to the number of turns. Part of their explanation (Afrikaans in figure 7.5) is given below:

We encircled every third letter and read it. Every third letter refers to three turns.

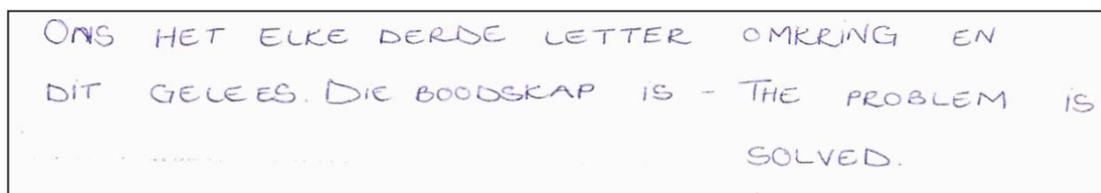


Figure 7.5: Transposition cipher activity: Description of turns

Besides the representation of the solution for 1.3 it can be concluded that the learners' solution was aligned with the HLT for the transposition cipher.

7.4 ACTIVITY 2

In order to build on the work done with the scytale as a practical activity the Alberti disk cipher was included as a further practical activity. It was only on working out an example for the literature review on the Alberti disk that its use as a follow-up activity for the scytale was seen. The first design research cycle with the students confirmed this and thus it was included as part of the second design research cycle for the learners.

7.4.1 HLT for activity 2

The Alberti disk alignment or setting showed the relationship between letters from the plaintext and ciphertext alphabets. In this way learners were introduced to different types of plain and cipher text alphabets to read off letters for messages. The expectation was that learners would make use of counting forward or backwards to encipher or decipher messages. Figure 7.6 outlines the important concepts for the Alberti disk activity.

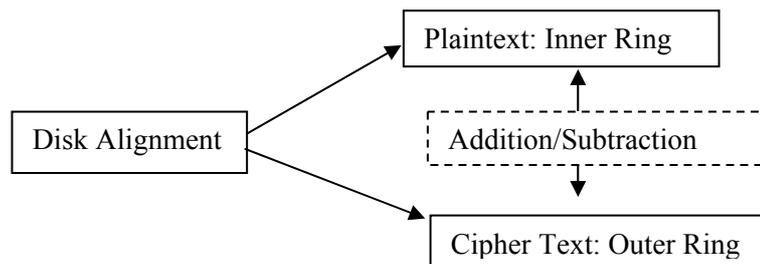


Figure 7.6: Alberti's disk activity

7.4.2 Retrospective analysis

Work by the groups on the Alberti cipher proceeded well. Group one used the given alphabet (figure 7.7) to indicate the four cipher alphabets for the disk settings Fk, Vk, Ok and Mk

e	A	n	B	a	b	C	ä	o	D	z	c	E	e	F	n	c	G	b	h	I	o	t	L	s	y	M	F	g	N	c	i	O	h																													
t	s	y	f	g	c	i	h	x	e	k	y	v	q	p	i	e	t	x	y	m	k	r	v	d	P	x	P	t	k	Q	u	v	R	g	p	S	i	e	T	x	m	V	t	r	X	v	d	Z	p	l	I	e	t	y	2	m	a	3	r	z	4	d
l	e	g	m	a	r	z	d	e	l	n	g	b	a	o	z	s	e	y	f	n	c	b	h	o																																						

Figure 7.7: Alberti alphabet with cipher alphabets

For their explanation of how they read off the respective cipher texts for the different disk settings the following words were used by group three (Afrikaans in figure 7.8):

- 3.1 For Fk we counted 6 from the left
- 3.2 For Vk we counted 1 backwards from the left
- 3.3 For Qk we counted 6 from the right
- 3.4 For Mk we counted 10 from the right

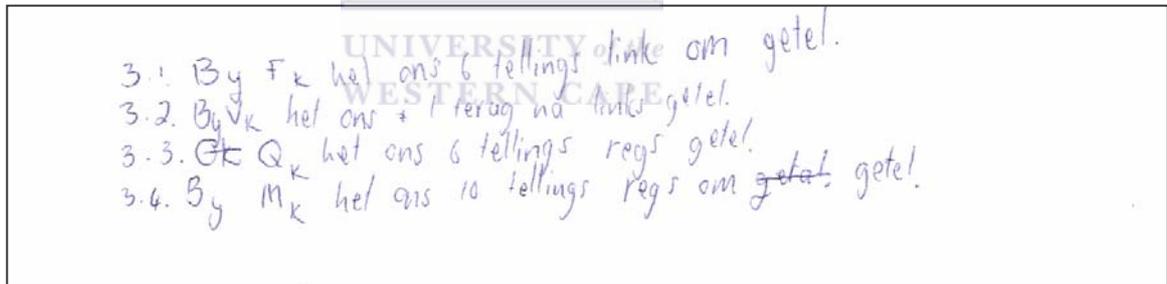


Figure 7.8: Alberti disk activity: Description of addition and subtraction

The listed HLT for the Alberti cipher was confirmed in the words of group three. The group used the words *right* and *left* to describe the respective forward and backwards counting to determine the ciphertext messages.

7.5 ACTIVITY 3

Activity 3 focused on the shifting of numbers a certain number of positions. Starting with a shift of three to introduce the Caesar cipher this later extended to numbers within the range for the ordinary alphabet of 26 numbers. The inverse process was also introduced for the deciphering of messages.

7.5.1 HLT for activity 3

Learners would be able to read off the number values for the respective letters of the alphabet. The expectation was that learners would go about the activity by adding numbers and substituting values to determine the total value for a certain shift. It's contended that they would be able to understand that minus three was needed to determine the plaintext message when using the Caesar cipher for the deciphering of messages. Where the shift key was not known it was expected of groups to each work on different substitution keys, thus substituting with values of 1, 2, 3, etc until a understandable readable plaintext message was formed.

As negative values would be encountered, it was envisaged that learners would determine the corresponding alphabet letters for negative values by counting backwards starting with the last letter in the alphabet. The corresponding letter for -1 would then be Z. Figure 7.9 outlines the concepts important to the Caesar cipher.

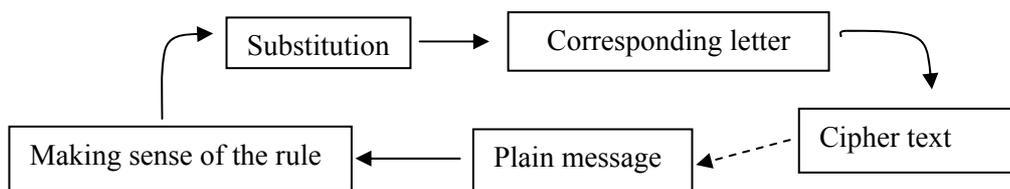


Figure 7.9: Caesar cipher activity

7.5.2 Retrospective analysis

The first part of the Caesar cipher activity did not produce any difficulties for the groups. At first some groups used addition of 3 for the decoding of a ciphertext message. After a general remark to the groups about the decoding process as the

inverse of the encoding, they used subtraction of 3 to determine the plaintext message.

For problem 3 all groups used the same method to start their solution. Instead of the group working on one rule at a time, each learner in the group worked on a different rule to determine the plaintext message. In one group one learner worked with numbers less than 10, whilst the other learner used numbers larger than 10.

When confronted with negative numbers groups utilized different strategies to translate the negative number into a letter from the alphabet. Group three (figure 7.10) used the counting backwards method to change negative values into alphabet letters.

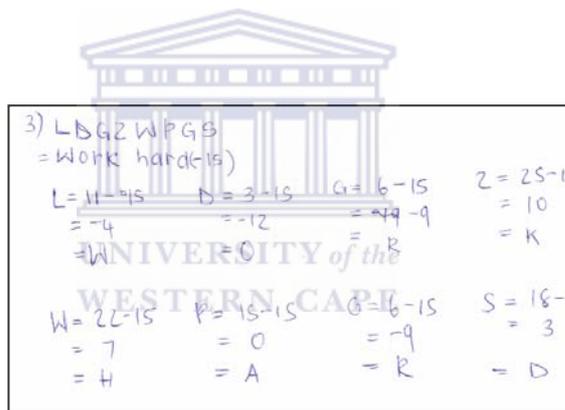


Figure 7.10: Caesar cipher activity: Solution to problem 3

In their response to the question *What happens if the value used in the rule is larger than 25?* they continued in a similar manner by using the counting forward method. This is confirmed in their description given in figure 7.11, with the translation below:

If the number is larger than 25 we start again with A.

As die getal groter as 25 is dan begin jy by A.

Figure 7.11: Caesar cipher activity: Description of values larger than 25

Groups one and two on the other hand made use of addition of 26 (figure 7.12) to change negative values into positive values to get the respective alphabet letters. They also used subtraction of 26 to convert numbers from 26 onwards into values of 0 up to 25. Group two even wrote out an explanation for the addition of 26:

To change a negative into a positive add 26.

LETTER + 15 LDGZ WPGS

(L) (E) (W) (A) $26 - 26 = 0$ (A)

$11 - 15 = -4 + 26 = 22$ (O) (B) $27 - 26 = 1$ (B)

(D) (M) (R) om 'n negatief na 'n

$3 - 15 = -12 + 26 = 14$ (R) LE VERANDER TEL 26

(G) (I) (K) (X)

$6 - 15 = -9 + 26 = 17$

(Z) (K) UNIVERSITY of the

$25 - 15 = 10$ WESTERN CAPE

(W) (N) WORK HARD.

$22 - 15 = 7$

P A

$15 - 15 = 0$ R

(I) (A) (Z) = 17

Figure 7.12: Caesar cipher activity: Groups two's solution to problem 3

Work of group three with the counting backwards and forward confirmed the HLT, whilst the solution strategies of groups one and two with the addition and subtraction of 26 showed an understanding (unknowingly) of the congruent modulo 26 concept.

7.6 ACTIVITY 4

In activity 4 notation of the function concept was introduced. It started off distinguishing between $f(x)$ (cipher alphabet) and x (plaintext alphabet) by having to read off corresponding values for these two notational forms. There was also an introduction to the null cipher where the values for $f(x)$ and x were the same. The null cipher concept was however, not further explored. The activity concluded with the substitution of values based on the relationship between $f(x)$ and x and further extended into a linear equation in two unknown where the values for the unknowns had to be determined.

7.6.1 HLT for activity 4

Learners would have difficulty in distinguishing the difference between $f(x)$ and x and it was expected that this would be the case for this activity. Furthermore it would be difficult for them relating x to the plaintext form of the alphabet and $f(x)$ to the ciphertext form of the alphabet. In no way would it be possible for them to identify the neutral cipher or null cipher.

The expectation was that $f(x) = x$ would not lead them to deduce that the plaintext and ciphertext alphabets are the same. Learners would have difficulty in deriving the linear equation, as they would not know how to set up the equations needed when substituting letters with their denoted number values. Figure 7.13 outlines the main features of this activity.

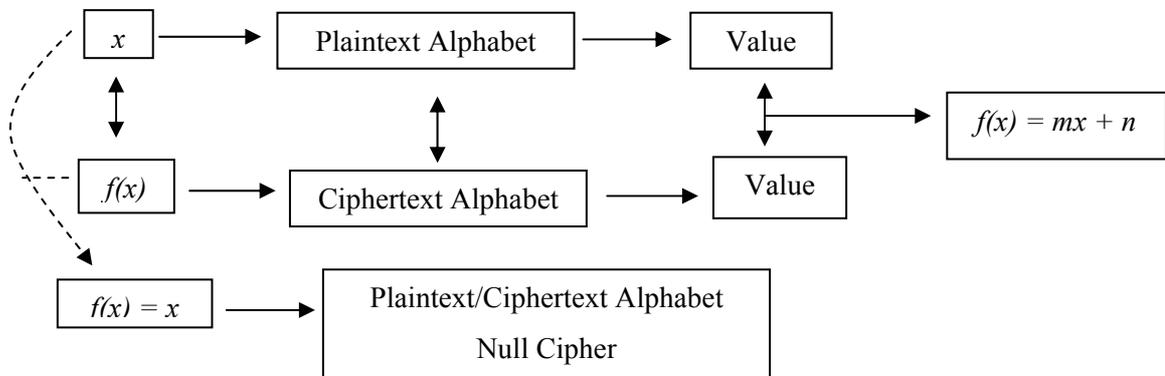


Figure 7.13: Function cipher activity

7.6.2 Retrospective analysis

Learners had difficulties in distinguishing between $f(x)$ and x as was hypothesized in 7.6.1. This meant that more than one explanation had to be made to explain it. This led to them being unsure about x and $f(x)$ denoting the plaintext and ciphertext respectively.

Figures 7.14 and 7.15 show the difficulties one of the groups had in deriving the linear equations in order to determine the values for the two unknowns. Instead of substituting 9 as a value for $mx + n$, it was substituted as a value for x (figure 7.14).

$$f(1) = 9$$

$$f(x) = mx + n$$

Figure 7.14: Function cipher activity: Substitution for x

Later on they rectified their mistake but had problems with the multiplication of m by 3 (figure 7.15):

$$f(1) = m(1) + n = 9$$

$$m + n = 9$$

$$f(3) = 23$$

$$f(x) = m x + n$$

$$f(3) = m(3) + n = 23$$

$$= m + n = 23$$

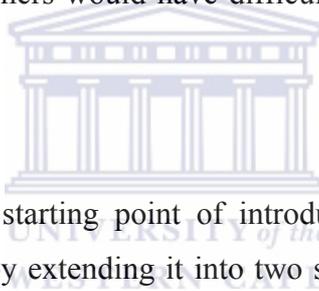
Figure 7.15: Function cipher activity: Solution for x and $f(x)$

Only group three was able to set up and determine values for the two unknowns from the two simultaneous equations in two unknowns (figure 7.16).

$$\begin{aligned}
 f(A) &= C \\
 f\left(\frac{0}{26}\right) &= m\left(\frac{0}{26}\right) + n = 2 \\
 &= 0 + n = 2 \\
 &= n = 2 \\
 \\
 f(B) &= E \\
 f\left(\frac{1}{26}\right) &= m\left(\frac{1}{26}\right) + n = 4 \\
 &= m + 2 = 4 \\
 &= m = 4 - 2 \\
 &= m = 2 \\
 \\
 f(C) &= G \\
 f\left(\frac{2}{26}\right) &= m\left(\frac{2}{26}\right) + n = 6 \\
 &= 2m + 2 = 6 \\
 &= 2m = 6 - 2 \\
 &= 2m = 4 \\
 &= m = 4 \div 2 \\
 &= m = 2 \\
 \\
 f(D) &= I \\
 f\left(\frac{3}{26}\right) &= m\left(\frac{3}{26}\right) + n = 8 \\
 &= 3m + 2 = 8 \\
 &= 3m = 8 - 2 \\
 &= 3m = 6 \\
 &= m = 6 \div 3 \\
 &= m = 2 \\
 \\
 f(E) &= K \\
 f\left(\frac{4}{26}\right) &= m\left(\frac{4}{26}\right) + n = 10 \\
 &= 4m + 2 = 10 \\
 &= 4m = 10 - 2 \\
 &= 4m = 8 \\
 &= m = 8 \div 4 \\
 &= m = 2 \\
 \\
 f(F) &= M \\
 f\left(\frac{5}{26}\right) &= m\left(\frac{5}{26}\right) + n = 12 \\
 &= 5m + 2 = 12 \\
 &= 5m = 12 - 2 \\
 &= 5m = 10 \\
 &= m = 10 \div 5 \\
 &= m = 2 \\
 \\
 f(G) &= O \\
 f\left(\frac{6}{26}\right) &= m\left(\frac{6}{26}\right) + n = 14 \\
 &= 6m + 2 = 14 \\
 &= 6m = 14 - 2 \\
 &= 6m = 12 \\
 &= m = 12 \div 6 \\
 &= m = 2 \\
 \\
 f(H) &= Q \\
 f\left(\frac{7}{26}\right) &= m\left(\frac{7}{26}\right) + n = 16 \\
 &= 7m + 2 = 16 \\
 &= 7m = 16 - 2 \\
 &= 7m = 14 \\
 &= m = 14 \div 7 \\
 &= m = 2 \\
 \\
 f(I) &= S \\
 f\left(\frac{8}{26}\right) &= m\left(\frac{8}{26}\right) + n = 18 \\
 &= 8m + 2 = 18 \\
 &= 8m = 18 - 2 \\
 &= 8m = 16 \\
 &= m = 16 \div 8 \\
 &= m = 2 \\
 \\
 f(J) &= U \\
 f\left(\frac{9}{26}\right) &= m\left(\frac{9}{26}\right) + n = 20 \\
 &= 9m + 2 = 20 \\
 &= 9m = 20 - 2 \\
 &= 9m = 18 \\
 &= m = 18 \div 9 \\
 &= m = 2 \\
 \\
 f(K) &= W \\
 f\left(\frac{10}{26}\right) &= m\left(\frac{10}{26}\right) + n = 22 \\
 &= 10m + 2 = 22 \\
 &= 10m = 22 - 2 \\
 &= 10m = 20 \\
 &= m = 20 \div 10 \\
 &= m = 2 \\
 \\
 f(L) &= Y \\
 f\left(\frac{11}{26}\right) &= m\left(\frac{11}{26}\right) + n = 24 \\
 &= 11m + 2 = 24 \\
 &= 11m = 24 - 2 \\
 &= 11m = 22 \\
 &= m = 22 \div 11 \\
 &= m = 2 \\
 \\
 f(M) &= A \\
 f\left(\frac{12}{26}\right) &= m\left(\frac{12}{26}\right) + n = 26 \\
 &= 12m + 2 = 26 \\
 &= 12m = 26 - 2 \\
 &= 12m = 24 \\
 &= m = 24 \div 12 \\
 &= m = 2 \\
 \\
 f(N) &= C \\
 f\left(\frac{13}{26}\right) &= m\left(\frac{13}{26}\right) + n = 28 \\
 &= 13m + 2 = 28 \\
 &= 13m = 28 - 2 \\
 &= 13m = 26 \\
 &= m = 26 \div 13 \\
 &= m = 2 \\
 \\
 f(O) &= E \\
 f\left(\frac{14}{26}\right) &= m\left(\frac{14}{26}\right) + n = 30 \\
 &= 14m + 2 = 30 \\
 &= 14m = 30 - 2 \\
 &= 14m = 28 \\
 &= m = 28 \div 14 \\
 &= m = 2 \\
 \\
 f(P) &= G \\
 f\left(\frac{15}{26}\right) &= m\left(\frac{15}{26}\right) + n = 32 \\
 &= 15m + 2 = 32 \\
 &= 15m = 32 - 2 \\
 &= 15m = 30 \\
 &= m = 30 \div 15 \\
 &= m = 2 \\
 \\
 f(Q) &= I \\
 f\left(\frac{16}{26}\right) &= m\left(\frac{16}{26}\right) + n = 34 \\
 &= 16m + 2 = 34 \\
 &= 16m = 34 - 2 \\
 &= 16m = 32 \\
 &= m = 32 \div 16 \\
 &= m = 2 \\
 \\
 f(R) &= K \\
 f\left(\frac{17}{26}\right) &= m\left(\frac{17}{26}\right) + n = 36 \\
 &= 17m + 2 = 36 \\
 &= 17m = 36 - 2 \\
 &= 17m = 34 \\
 &= m = 34 \div 17 \\
 &= m = 2 \\
 \\
 f(S) &= M \\
 f\left(\frac{18}{26}\right) &= m\left(\frac{18}{26}\right) + n = 38 \\
 &= 18m + 2 = 38 \\
 &= 18m = 38 - 2 \\
 &= 18m = 36 \\
 &= m = 36 \div 18 \\
 &= m = 2 \\
 \\
 f(T) &= O \\
 f\left(\frac{19}{26}\right) &= m\left(\frac{19}{26}\right) + n = 40 \\
 &= 19m + 2 = 40 \\
 &= 19m = 40 - 2 \\
 &= 19m = 38 \\
 &= m = 38 \div 19 \\
 &= m = 2 \\
 \\
 f(U) &= Q \\
 f\left(\frac{20}{26}\right) &= m\left(\frac{20}{26}\right) + n = 42 \\
 &= 20m + 2 = 42 \\
 &= 20m = 42 - 2 \\
 &= 20m = 40 \\
 &= m = 40 \div 20 \\
 &= m = 2 \\
 \\
 f(V) &= S \\
 f\left(\frac{21}{26}\right) &= m\left(\frac{21}{26}\right) + n = 44 \\
 &= 21m + 2 = 44 \\
 &= 21m = 44 - 2 \\
 &= 21m = 42 \\
 &= m = 42 \div 21 \\
 &= m = 2 \\
 \\
 f(W) &= U \\
 f\left(\frac{22}{26}\right) &= m\left(\frac{22}{26}\right) + n = 46 \\
 &= 22m + 2 = 46 \\
 &= 22m = 46 - 2 \\
 &= 22m = 44 \\
 &= m = 44 \div 22 \\
 &= m = 2 \\
 \\
 f(X) &= W \\
 f\left(\frac{23}{26}\right) &= m\left(\frac{23}{26}\right) + n = 48 \\
 &= 23m + 2 = 48 \\
 &= 23m = 48 - 2 \\
 &= 23m = 46 \\
 &= m = 46 \div 23 \\
 &= m = 2 \\
 \\
 f(Y) &= Y \\
 f\left(\frac{24}{26}\right) &= m\left(\frac{24}{26}\right) + n = 50 \\
 &= 24m + 2 = 50 \\
 &= 24m = 50 - 2 \\
 &= 24m = 48 \\
 &= m = 48 \div 24 \\
 &= m = 2 \\
 \\
 f(Z) &= A \\
 f\left(\frac{25}{26}\right) &= m\left(\frac{25}{26}\right) + n = 52 \\
 &= 25m + 2 = 52 \\
 &= 25m = 52 - 2 \\
 &= 25m = 50 \\
 &= m = 50 \div 25 \\
 &= m = 2 \\
 \\
 f(0) &= C \\
 f\left(\frac{26}{26}\right) &= m\left(\frac{26}{26}\right) + n = 54 \\
 &= 26m + 2 = 54 \\
 &= 26m = 54 - 2 \\
 &= 26m = 52 \\
 &= m = 52 \div 26 \\
 &= m = 2 \\
 \\
 f(x) &= 7x + 2
 \end{aligned}$$

Figure 7.16: Function cipher activity: Solution to problem 1.4

The stated HLT that learners would have difficulties was confirmed in the work from two of the groups.



7.7 ACTIVITY 5

Activity 5 built on the starting point of introducing a linear equation in two unknowns in activity 4 by extending it into two simultaneous linear equations in two unknowns. In the first part the emphasis was on enciphering by way of substitution using two rules. The second part focused on deciphering where the values for two unknowns had to be determined after deriving two simultaneous equations in two unknowns.

7.7.1 HLT for activity 5

In solving problems on activity 5 it was contended that learners would use informal solution strategies. This could be by way of substitution of values for the respective unknowns and not using the more formal method of elimination of an unknown to determine values for the respective unknowns. They would not have any difficulties in enciphering messages using the two rules but may encounter problems when having to determine the values for the two unknowns from the two simultaneous linear equations. Figure 7.17 is a summary of what this activity tries to capture and plots a relationship of workings in this activity.

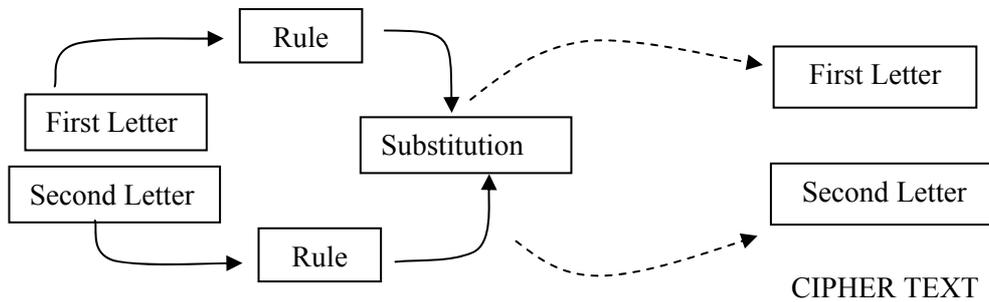


Figure 7.17: Affine cipher activity

7.7.2 Retrospective analysis

The groups did not have any problems in substituting using the two rules to determine the enciphered letters from the plaintext pair of letters. Whereas groups one and two again employed subtraction of 26 as in 7.5.2, group three also employed their method of 7.5.2 of counting backwards and forward as a solution strategy. Group one’s work is captured in figure 7.18 (solution for problem 1) and group three’s work is contained in figure 7.19 (solution for problem 2).

UNIVERSITY of the
WESTERN CAPE

$P : 3(15) + 17 = 62 - 26 - 26 = 10 = K$
 $R : 4(15) + 3(17) = 111 - 26 - 26 - 26 - 26 - 7 = H$ $PR \rightarrow KH$

$I : 3(8) + 18 = 40 - 26 = 14 = O$
 $S : 4(8) + 3(18) = 86 - 26 - 26 - 26 = 8 = I$ $IS \rightarrow OI$

$O : 3(14) + 13 = 55 - 26 - 26 = 3 = D$ $ON \rightarrow DR$
 $N : 4(14) + 3(13) = 95 - 26 - 26 - 26 = 17 = R$

$\beta : 3(1) + 17 = 20 = U$
 $R : 4(1) + 3(17) = 55 - 26 - 26 = 3 = D$ $BR \rightarrow UD$

$E : 3(4) + 0 = 12 = M$
 $A : 4(4) + 3(0) = 16 = Q$ $EA \rightarrow MQ$

$K : 3(10) + 10 = 40 - 26 = 14 = O$ $KK \rightarrow OS$
 $K : 4(10) + 3(10) = 70 - 26 - 26 = 18 = S$

Geheime Taal = KH O I DR U O M Q O S

Figure 7.18: Affine cipher activity: Solution to problem 1

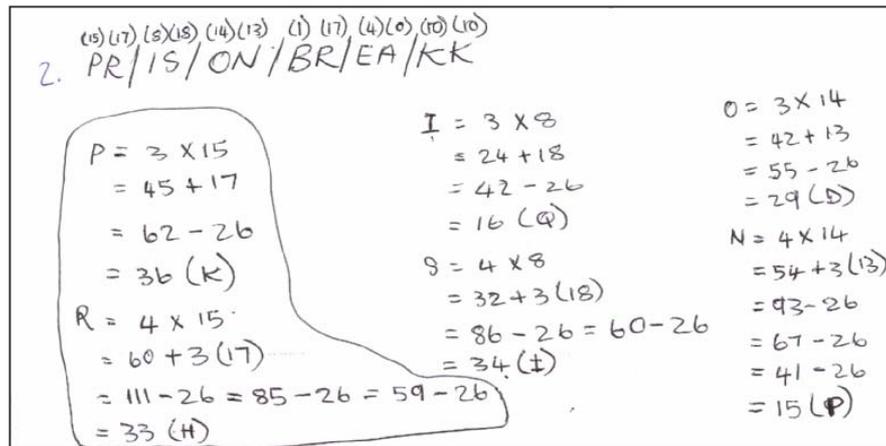


Figure 7.19: Affine cipher activity: Solution to problem 2

Group three again showed their understanding of solving these types as was also shown in 7.6.2 (figure 7.15). It appears as if this group had a stronger school mathematical content grounding. Their solution strategy employed for problem 3 in shown figure 7.20:

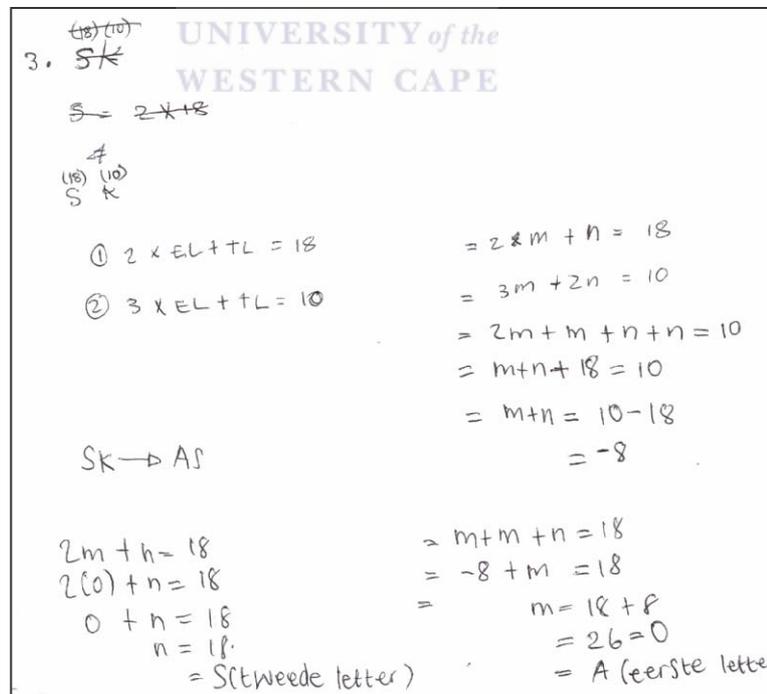


Figure 7.20: Affine cipher activity: Solution to problem 3 (group 3)

Group one wrote down the values for the simultaneous linear equations and used the values for A (0) and S (18) to see if these values satisfied the two equations. Their solution method is given in figure 7.21.

$$\textcircled{3} \text{ \â } \text{Reel } \textcircled{1} : 2xEL + TL = 18 \text{ S}$$

$$\text{Reel } \textcircled{2} : 3xEL + 2xTL = 10 \text{ K}$$

$$A \text{ EL} = 0 \times 0 + 18 = 18 \text{ S}$$

$$S \text{ TL} = 3 \times 0 + 2 \times 18 = 36 + 26 = 10 \text{ K}$$

$$18 - 10 = 8$$

$$EL = 0 - 0 = 0$$

$$TW = 36 - 18 = 18$$

$$0 + 18 =$$

Figure 7.21: Affine cipher activity: Solution to problem 3 (group 1)

Groups one and two had problems in solving problem 4. This was not the case for group three and their workings again showed their stronger school mathematical content knowledge. Their solution for the deciphering of the problem is given below:

$$EL + 2x + TL = 11$$

$$EL + TL = 10$$

$$M + 2N = 1$$

$$M + N = 10$$

$$M + N + N = 1$$

$$= 10 + N = 1$$

$$= N = -9 + 26$$

$$= 17 (R)$$

$$m + 12 = 10$$

$$m = 10 - 12$$

$$m = -2 + 26$$

$$m = 19 (T)$$

$$= T$$

Die ander waarde is op dieselfde manier gedoen.

Figure 7.22: Affine cipher activity: Solution to problem 4

Although the group did not work out the problem in full they were able to solve the problem in full. The remark *the other values were determined in the same way* indicates how they went about to solve the rest of the problem.

7.8 ACTIVITY 6

Activity 6 aimed to introduce learners to workings of number theory with respect to the congruent modulo concept. It later extended into the solution of simple linear equations in number theory. The congruence modulo concept was explained by using the remainder principle, which should be known to learners when determining factors of a number.

7.8.1 HLT for activity 6

Relating the remainder principle to the congruence modulo concept would help learners to build an understanding of this concept in number theory. Learners would easily make the connection between the remainder and the congruence modulo concept. They would however not be able to extend it into a general linear form of $ax + k$, where a indicated the congruence modulo number, k the remainder and x the different positive integer values that can be substituted to determine corresponding congruence modulo numbers. Applying the aforementioned explanation to example 1.1 meant $9 \equiv 5 \equiv 1 \equiv 17 \pmod{4}$ could be extended into $4x + 1$ to determine equivalent values. They would be able to use the congruent modulo value to get a multiple to solve the linear equations in number theory. Figure 7.23 outlined the relationship between the concepts introduced by the activity on number theory.

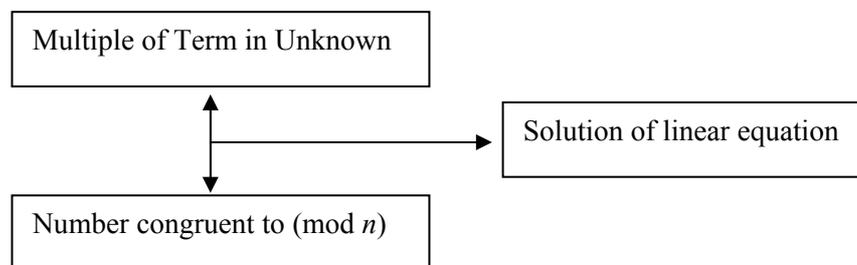
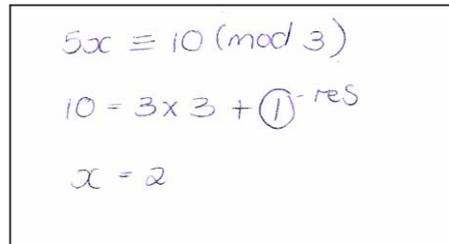


Figure 7.23: Number theory activity

7.8.2 Retrospective analysis

Solutions from the three groups showed that they understood the congruence modulo concept. All the groups were able to substitute values congruent to the respective modulo values. For the solution of the linear equation they (group 1) could see that they needed a multiple of 5 for the solution of $5x \equiv 1(\text{mod}3)$:



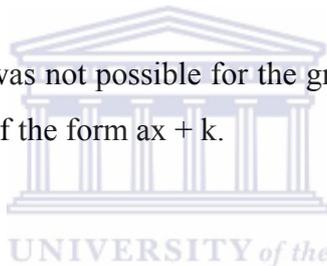
$$5x \equiv 10 \pmod{3}$$

$$10 = 3 \times 3 + \textcircled{1} \text{ - res}$$

$$x = 2$$

Figure 7.24: Number theory activity: Solution to problem 2.1

As stated in the HLT it was not possible for the groups to develop a general form of the linear expression of the form $ax + k$.



7.9 ACTIVITY 7

An application of the RSA cipher was included as a follow-up on activity 6 and as an extension of the number theory started in activity 6. Developed by Rivest, Shamir and Adleman (Barr, 2000) the cipher was aimed at making it as difficult as possible to break a message if encrypted with the RSA cipher. Knowledge of number theory and prime numbers were needed to understand the workings of the RSA cipher.

7.9.1 HLT for activity 7

The RSA cipher built on different rules for its application. It was expected of learners not to have problems as they only had to follow the rules and do the necessary substitutions. In this regard determining the value of E (used for enciphering) could be difficult if there was a lack of understanding of the factor concept. Also calculating the value of D (used for deciphering) might give difficulty because of the way it is defined ($E \times D - 1$ to be a multiple of A). Figure 7.25 outlines links in the solution for the RSA activity.

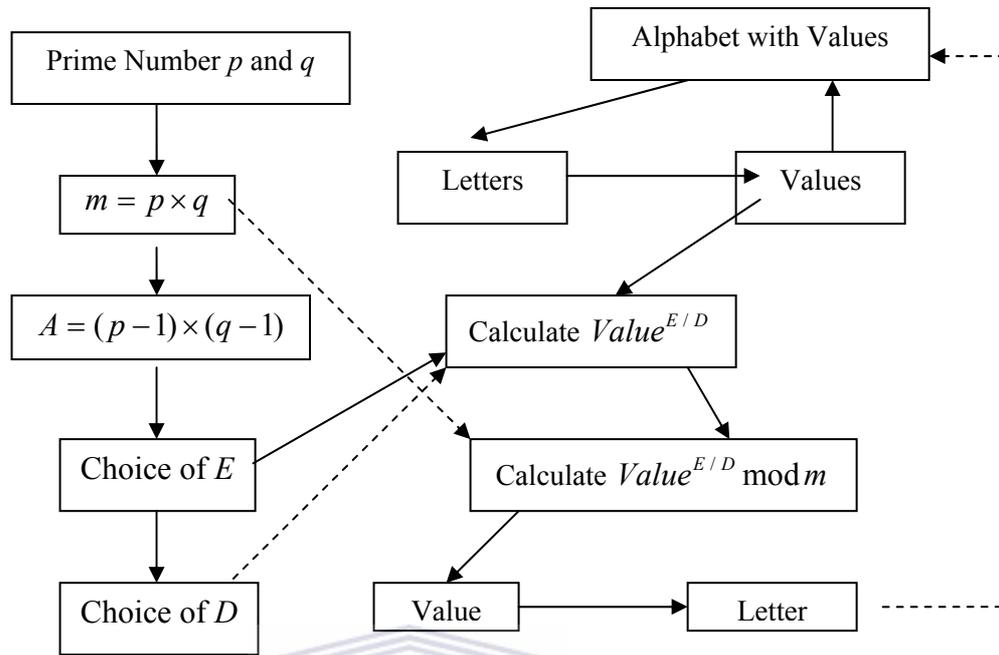


Figure 7.25: RSA cipher activity

7.9.2 Retrospective analysis

During implementation it was decided to do only the enciphering part of the problem. The specific guidelines outlining what should be done, together with the given values for the respective unknowns in the example, contributed to learners being able to easily do the enciphering part of the problem.

7.10 OVERVIEW OF ACTIVITIES

Activities for the second design research cycle were introduced in 7.3 to 7.9 above. Table 7.1 outlines a summary of the seven activities by highlighting the concepts important to each activity.

ACTIVITY	TOPIC	CONCEPTS
1	Scytale	Transposition, number of turns
2	Alberti disk	Addition, subtraction
3	Caesar cipher	Substitution
4	Function cipher	$f(x)$, x , substitution, linear equation
5	Affine cipher	Substitution, addition, subtraction, multiplication, division, solving of 2 simultaneous linear equations
6	Introduction to number theory	Remainder theorem, factors, congruence, modulus
7	RSA cipher	Prime numbers, exponents, remainder theorem

Table 7.1: Summary of seven activities

7.11 RETROSPECTIVE ANALYSIS

Retrospective analysis of the seven developed activities for the second design research cycle with the learners would focus on problems experienced with the evidence and suggestions on a feed-forward for a next phase of implementation.

7.11.1 Scytale

It is important to be consistent with the use of terminology. In the Afrikaans version the use of batten, cylindrical rod, and parchment could be confusing for learners. In the answer to 3.2 where an explanation was needed on how they went about to solve the problem, learners from group one responded (figure 7.26) as follows: *We turned the message around the parchment and it was clear.*

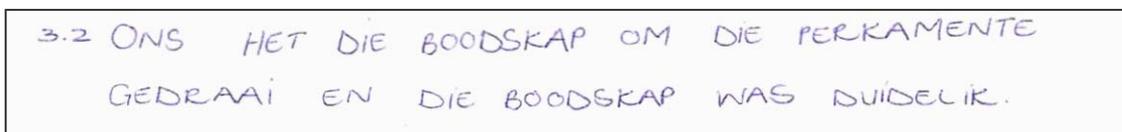


Figure 7.26: Scytale: Description of parchment

Translated it meant *we turned the message around the parchment and the message was clear.* Parchment in their context was seen to be the same as batten. In order to remove confusion terminology should be clearly defined. The questions for the

activity could remain the same but a question could be added on battens of different diameters.

The solution given below by a group in 7.3.2 could also be addressed in a next phase.

Intended solution: A RER EDI YUO ORD UIF FNO RGU EPR E?

Group's solution: A RER IDE OUY DRO FIU ONF UGR RPE ?E

One way could be by having more than one letter on the first turn so to show that the top row of letters started out each column of letters.

7.11.2 Alberti disk

There were no problems with this activity. Whereas the scytale activity had a long explanation, the explanation for the Alberti disk was much shorter. The uncertainty with respect to what each ring depicted was addressed in the description where it was stated that the outer ring is used to read off the plaintext alphabet, whilst the inner ring denoted the ciphertext alphabet.



7.11.3 Caesar cipher

Learners did not encounter any problems with this activity. The first question for enciphering the message *This is a shift three cipher* is too long and could be shortened. It was found that the second problem where the message *ZHKDSHWRUN* had to be deciphered that the plaintext message *WEHAPETORK* was not a clear English plaintext message. Although this is acceptable it is not recommended. The plaintext message was supposed to be *WE HAVE WORK* meaning that the cipher text message should have been *ZHKDYZRUN*.

A similar problem was encountered with question three but it was changed during the teaching experiment. The given cipher text of *WRGSLDGZEPOH* was changed into *LDGZWPGS* which decipheres to *WORK HARD*. This is one of the advantages of a developmental study, which changes can be made for developed activities during the course of a teaching experiment.

7.11.4 Function cipher

Function notation was new to learners and as such much more explanation than usual was needed. Question four was difficult for learners to conceptualize and could be preceded by questions that could help them to make sense of the question. Examples of such questions could be:

- Given $f(x) = 2x + 1$. Show that $f(B) = D$.
- If $f(x) = 3x + 4$, determine $f(R)$.
- Determine the replacement letter for x for $f(x) = V$ if $f(x) = 4x + 1$.

These questions would possibly contribute to help learners to understand question four better. Learners also had difficulties in calculating the values for m and n in question four. In one group the value allocated for x was also seen as the value for $mx + n$ (see figure 7.14).

7.11.5 Linear equations

For the enciphering in questions one and two learners did not have any difficulties in doing the substitutions to get the respective letters for the cipher text alphabet. One group applied previously acquired knowledge from the function cipher and was able to solve questions three and four. There seemed to be a difference in the school mathematical content knowledge of groups as was shown in the solutions of group three against those of the other two groups.

7.11.6 Number theory

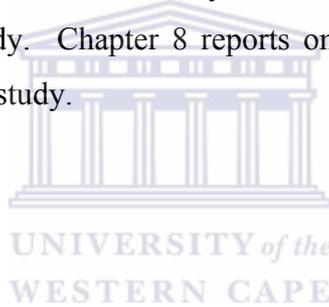
It was not easy for learners to translate the given definition under the introduction into the number values given in the example. So more examples were worked through to see how the given numbers fit the definition. Solutions from the learners showed that although it was all new to them, they could cope with the work. Even the question where there was no possible solution was recognized and that $5k + 1$, for k an element of the positive integers can never deliver a number divisible by 15. It is recommended that this activity stay as is.

7.11.7 RSA cipher

The activity on the enciphering of the RSA cipher as a follow-up on the congruence modulus activity did not give any problems and the learners easily did the calculations. It should be kept as an introductory activity as the mathematics of the RSA cipher and the deciphering part should be kept as part of the activity.

7.12 CONCLUSION

The discussions on the HLT and the retrospective analysis for each activity together with the overview and retrospective analysis of the developed activities will now be used to answer the research questions. We will further reflect on the conjectured HLT's, the work of the learners as a response to the HLT, the literature review and on the suitability of the methodology and theoretical frameworks for this study. Chapter 8 reports on these matters, limitations and recommendations of the study.



CHAPTER 8

FINDINGS AND CONCLUSION

8.1 INTRODUCTION

The main aim of the research was to investigate how new content could be introduced into a school mathematics curriculum. In order to answer the research question this study has to make statements with respect to the teachability and sense-making of cryptology as a school mathematics topic. Teachability and sense-making are captured as part of the two subsidiary research questions. A third subsidiary question on the happenings further informs the main research question. The significance of this present research lies in the opening of avenues for new school mathematics topics and how it could be introduced and taught by teachers of school teaching mathematics and learnt by learners doing school-going mathematics.

The chapter starts out with a discussion of findings based on the analysis of the data in chapters 6 and 7 for the three respective subsidiary research questions. These findings discussed for the three subsidiary research questions will be utilized to answer the main research question. All the data collected were considered for this analysis. This is followed by a reflection on the methodology and theoretical frameworks utilized for this study as well as a reflection on the literature review. The chapter concludes with the limitations of the study and recommendations for future research.

8.2 ANSWER TO THE FIRST SUBSIDIARY RESEARCH QUESTION

For the first subsidiary research question the issue of teachability of cryptology comes under scrutiny. Teachability within the context of the study refers to the issues of design of teaching materials and how the designed materials impacted on the learning of the topic of cryptology by learners.

The study was developmental in nature and there were two design research cycles. For the first design cycle materials there were three teaching experiments. These

teaching experiments were piloted with high school teachers of school mathematics, learners doing school mathematics and students in their second year of studying towards a teacher’s qualification in school mathematics. Table 8.1 (see also table 3.1 in chapter 3) outlines the respective topics covered for cryptology that were done with the three groups as part of the first research design cycle.

GROUP	ACTIVITY
Teachers	Transposition Cipher
Learners	Transposition Cipher
Students	Alberti Disk Cipher

Table 8.1: Summary of first design research cycle

For the second research design cycle booklets with the activities in Afrikaans and English (Appendices H and J) consisting of seven instructional activities with their solutions (Appendix I) were developed. Table 7.1 in chapter 7 outlined the activities used for the second design research cycle.

Reasons for the choice of said activities were based on the literature review (chapter 4), the didactical and phenomenological discussion of cryptology in chapter 5 and the formulation of a HLT. All learners in grade 10 have been exposed to outcomes based education. One of the tenets of this educational system is to allow learners to take charge of their own learning and as such they are exposed to working on practical activities in the classroom. The scytale activity (transposition cipher) chosen has practical elements and is in line with outcomes based education.

Materials designed for the first research design cycle was a culmination of a developmental process that started out in the field of mathematics. Following a course on number theory presented by professor Fray (see Appendix A. Note 3) led to a deepening of the mathematical content knowledge of cryptology. Developed materials were presented to supervisors and professor Fray for their input and comments and the necessary revisions were made where needed.

Findings with respect to the design of instructional activities are evaluated against tenets discussed as part of design research in chapter 3.

The development of a HLT and instructional materials were closely related as the HLT guided the instructional activities. Choices made in the development of instructional activities also impacted on the HLT. In coming up with findings for the design of materials it was found that the development of a HLT impacted positively on the development of instructional activities as the designer had to think through the possible ways learners would work in solving these activities. The challenge was to develop instructional activities so as to align learners' cognitive development with the outcomes of the HLT.

Another challenge was to link instructional materials on cryptology to existing known school mathematics topics. This is important to bring out relationships between different mathematical topics so as not to see any topic as a stand alone within the discipline, mathematics. This is a challenge for designers of instructional materials of school mathematics.

Use of the design principle, guided reinvention, was useful in rethinking the development of mathematical concepts from a given problem setup. This was one of the challenges within the scope of this thesis. Working through the literature review and coming up with choices to find suitable contexts to develop the concepts important to cryptology were a daunting task. Guided reinvention, together with the historical and didactical phenomenology of the topic, presented helped in this regard.

What this study found is that the principles of design research and the historical and didactical phenomenology of a topic presented the designer with tools to develop activities well thought through and aligned to the conceptual development of learners. Instructional activities developed on the basis of these mentioned principles were well received by participants in the different experiments and it augers well for the teachability of the topic, cryptology.

The main findings for the development of materials for the topic of cryptology are now presented. An extensive literature review to trace the development of the topic over a period of time was a useful starting point. Extending the literature review into a historical and didactical phenomenological exegesis of cryptology gave insights to the learning and teaching of the topic. The HLT was a useful tool for this exposition as it developed grounds for the design of instructional materials. Giving the activities a realistic flavor was also helpful as a context for the learners. Designers should be careful in their phrasing of questions so as not to confuse participants. There could also be guiding questions preparing the grounds for the main questions. A deep conceptual knowledge of the topic is important for the development of instructional material in order to link the topic to other content strands of school mathematics.

8.3 ANSWER TO THE SECOND SUBSIDIARY RESEARCH QUESTION

In this part of the findings for the second subsidiary research question on the sense-making of cryptology, the issue of learning comes under scrutiny. Learning here refers to the ways learners came to understand the topic and the way they expressed their understanding and learning in their respective solutions. Only certain solutions will be selected to highlight different ways in which learners made sense of the instructional activities. A detailed discussion is included as part of the retrospective analysis in chapter 7 (see 7.3 – 7.9), so only highlights will be given for this section.

The issue of sense-making was further applied to see in what way solution strategies developed by learners were in line with the conjectured HLT or if there was a deviation and in which direction it was. An upward direction (LSS above HLT) with a full line between HLT and LSS was an example of where the learners' solution strategy (LSS) was above expectations set out in the HLT. For other instances a dotted line between the HLT and LSS was used. This is important because it has implications for the formulation of HLT's and the design of activities for a third design research cycle.

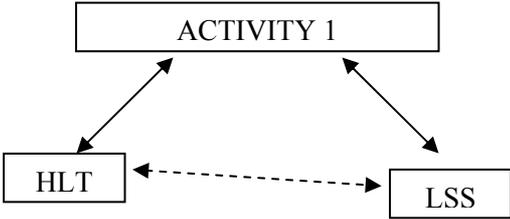
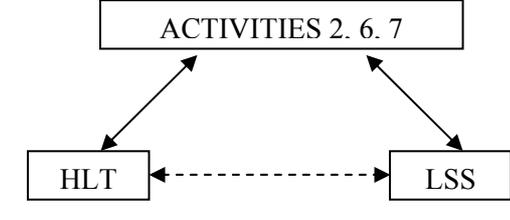
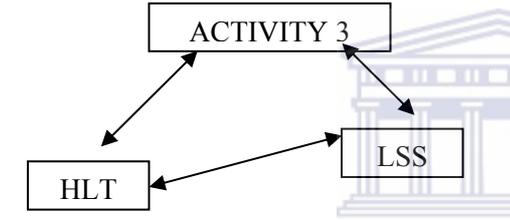
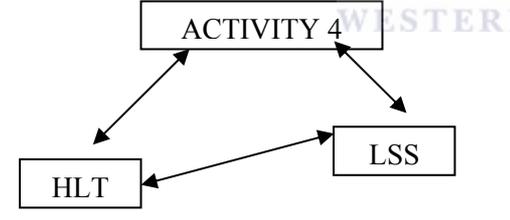
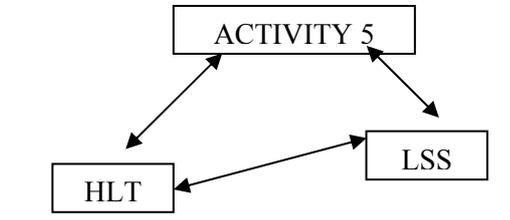
Drawing and Activity	Description
	<p>The slight deviation downwards was because of the way learners presented their solution for the message on the parchment when unwrapped from the batten (see 7.3.2).</p>
	<p>There were no deviation from the stated HLT and work from learners confirmed the HLT.</p>
	<p>Deviation from the conjectured HLT because of the use of addition of 26 to change a negative value into a positive value and subtraction of 26 to change from 26 onwards into values from 0 to 25 (see discussion of 7.5.2).</p>
	<p>Use of functional notation to determine the rule applied for linear equation to translate value for x into $f(x)$ (see discussion of 7.6.2).</p>
	<p>Use of two rules for two unknowns to set up two simultaneous linear equations in two unknowns and determine the values for the two unknowns (see discussion of 7.7.2).</p>

Table 8.2: HLT's alignment with LSS

Remarks made by learners after completion of the second design research cycle need to be mentioned. *The first two problems were easy but it became more*

difficult as it progressed. The two research cycles have shown that it is possible for learners to solve these problems. Solutions developed for these activities showed it was possible for learners to work out these problems. The work of group three has to be mentioned - it appeared that they had a strong school mathematical content grounding and this became important when working on activities of a new school mathematics topic.

Solution strategies developed by learners as discussed in 7.3-7.9 with the summary on its alignment with the stated HLT in table 8.2 indicate that they developed an understanding and that they did make sense of the instructional materials on cryptology.

8.4 ANSWER TO THE THIRD SUBSIDIARY RESEARCH QUESTION

The third subsidiary research question reflected on the happenings at the workbench. For this section the findings concentrate on learner-learner engagement and instructional material-learner engagement in the groups. Groups worked well together as they were known to each other. Engagement with respect to the work division was argued about and generally accepted. This came to the fore in the discussion of the retrospective analysis in 7.5.1.

Despite the remark concerning the progressive difficulty of problems, work by the groups had shown that there was a place for the topic of cryptology in school mathematics. Some of the solution strategies developed by group three indicate that a strong school mathematical content knowledge could be beneficial when working on a topic of school mathematics.

The theoretical framework, called workbench activity, was further utilized to evaluate what transpired at the workbench. For this discussion the focus was on the solutions learners developed for activities of the second design research cycle. Examples for the discussion were drawn from solutions presented for activity 5 on the affine cipher (see figures 7.20 and 7.22) as part of 7.7.2 in chapter 7.

8.4.1 Substitution as bridgehead

Pickering (1995) describes bridging as the development of a bridgehead to establish a link between the work at hand and work already known. For the Caesar activity and the start of the affine activity, letters were substituted with different number values as set out in a table for the letters of the alphabet. Work from participants in the groups showed they knew how to substitute a letter with its allocated value. This was confirmed in their work on the Caesar activity (see figures 7.10 and 7.12); the function activity (see figures 7.14, 7.15 and 7.16) and the affine activity (see figures 7.18 and 7.19).

In their solution to problem 3 of the affine cipher, group 3 utilized another form of substitution to solve the problem. Their solution captured in figure 7.20 given below, was used for this discussion.

Handwritten solution for an affine cipher problem. The work is contained within a rectangular frame with a faint watermark of a classical building and the text 'UNIVERSITY of the WESTERN CAPE' in the background.

At the top left, it says '3. SK' with '(18) (10)' written above it. Below this, the equation $S \rightarrow 2x + 18$ is written.

Below the equation, the letters 'S' and 'K' are listed with '(18)' and '(10)' written above them respectively.

Two equations are listed on the left side:

$$\textcircled{1} 2 \times EL + TL = 18$$

$$\textcircled{2} 3 \times EL + TL = 10$$

On the right side, a series of equations are shown:

$$= 2m + n = 18$$

$$= 3m + 2n = 10$$

$$= 2m + m + n + n = 10$$

$$= m + n + 18 = 10$$

$$= m + n = 10 - 18$$

$$= -8$$

Below these equations, the substitution $SK \rightarrow AP$ is written.

At the bottom left, a series of equations are shown:

$$2m + n = 18$$

$$2(0) + n = 18$$

$$0 + n = 18$$

$$n = 18$$

Below these, it says '= S (tweede letter)'.

At the bottom right, a series of equations are shown:

$$= m + m + n = 18$$

$$= -8 + m = 18$$

$$= m = 18 + 8$$

$$= 26 = 0$$

Below these, it says '= A (eerste letter)'.

Figure 7.20: Affine cipher activity: Solution to problem 3 (group 3)

The terms of $3m$ and $2n$ of the second equation were changed into $2m + m$ and $n + n$ respectively. The group did the changing of $3m$ and $2n$ by way of choice and is an example of a free move as described in the dance of agency. These free moves

are also referred to as filling. In this way $2m + n$ could be substituted with the value of 18 and it was now possible to derive a value for $m + n$. The substitution of a single letter with its number value (known work), now led to the substitution of two letters with a number value (work at hand). $2m + n = 18$ is seen as the first substitution bridgehead and $m + n = -8$ as the second substitution bridgehead.

The same substitution method was now utilized for solving problem 4 of the affine cipher (see figure 7.22 below).

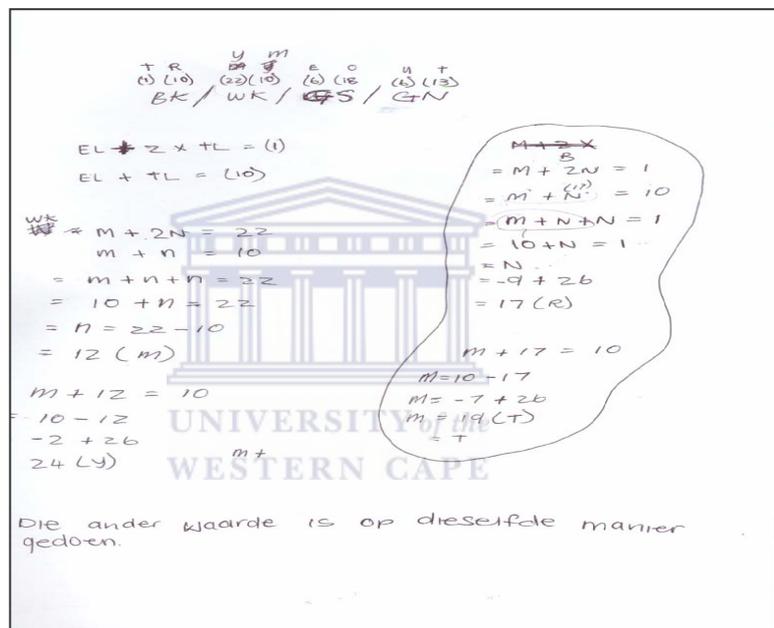


Figure 7.22: Affine cipher activity: Solution to problem 4

Only one substitution bridgehead ($m + n = 10$) was used to solve the problem. As the method was now known it was not a free move, but became an example of a forced move, which is called transcription. Figure 8.1 outlines the link between the work at hand and work already known.

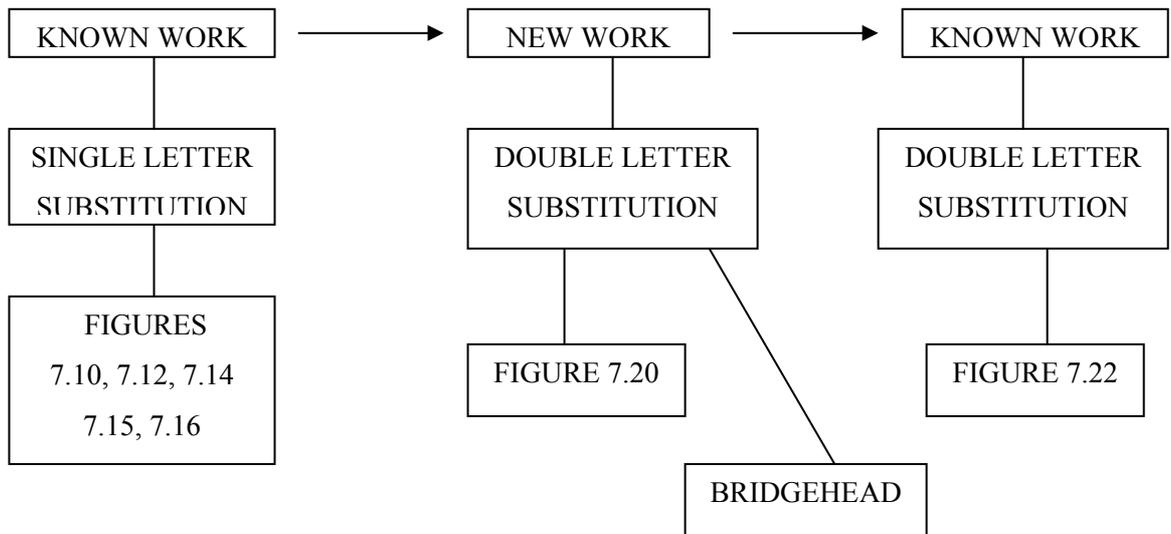


Figure 8.1: Bridgehead as a link between known and new work

Although learners in their respective groups did not know the content of cryptology the focus of the affine cipher activity on two simultaneous linear equations was a contributing factor in coming up with a solution strategy. The development of the double substitution bridgehead for the solution in figure 7.20 was then changed to a single bridgehead for the solution in 7.22.

8.5 ANSWER TO THE MAIN RESEARCH QUESTION

The main research question speaks to the issue of how new content could be introduced into a school mathematics curriculum. All the above discussions on the findings for the three subsidiary research questions should be seen as part of the answer to the main research question. For the answer to the main research question the focus is on the route the study took before it ended up as instructional material in a school mathematics classroom. This is important because it makes statements about how we see mathematics and how it undergoes changes before it ends up as school mathematics.

As mentioned in the study the starting point in mathematics was a course on number theory that ventured into cryptology. This was important as it gave insights into the mathematics behind number theory, prime numbers, pseudo prime numbers and the Euclidean theorem. The literature review on cryptology

complemented the formal course on number theory as it gave breadth to the depth gained from doing the course.

In doing the chapter on the historical and didactical phenomenology of cryptology the way was paved for the development of instructional material and the conjectured HLT was a positive contributing factor in the design process. The cyclical nature of the design phase together with the feed-forward and retrospective analysis was important to this phase. Figure 8.2 outlines a possible route for the study on how new content could be introduced into a school mathematics curriculum.

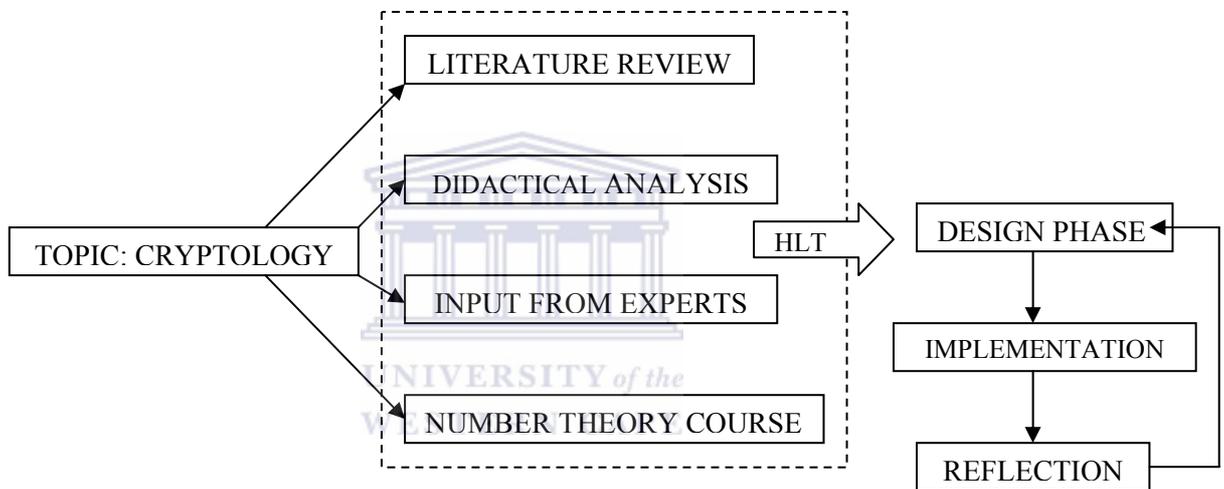


Figure 8.2: Possible route for introducing new content

8.6 REFLECTION AND DISCUSSION

The following section looks at the methodology and theoretical frameworks used for this study. This section concludes with a reflection on the literature review.

8.6.1 Methodology

Design research was utilized as methodology for this study. In reflecting on the methodology the features highlighted by Cobb, Confrey, et al (2003) as important to all forms of design research will be used as a framework. The present study is then evaluated against these features.

One of the features of design research is to develop theories about learning and the means needed to design support for that learning. Although the thesis did not develop a theory about the teaching of a new topic, it makes statements about the learning of the topic and the design of instructional activities that were piloted as two design research cycles. The discussion on the teachability and sense-making of the topic under 8.2 and 8.3 could be seen as a possible instruction theory for the topic.

A second feature is the interventionist nature of design research. This was done under the experiences (6.4), feed-forward analysis (6.5) in chapter 6 and the reflective analysis for the seven activities in chapter 7. A third feature of design research is the prospective and reflective components. The prospective part of design research was covered with the formulation of a HLT for each activity whilst the reflective part was captured in the feed-forward analysis for the first design research cycle and the reflective analysis of the second design research cycle.

A fourth feature of design research is its cyclical nature and this was an important part of the thesis with the development of instructional materials for the first design research cycle and the revision of these materials after implementation in three teaching experiments. This was followed by a second design cycle with seven activities, which was followed with an analysis with recommendations for a third design research cycle. From the aforementioned discussion with the four features of design research as guideline it can be concluded that the methodology was suitable within the context of this study.

The main finding with respect to design research was that it afforded the researcher to make the best possible decisions within the constraints of the design context. Furthermore decisions on the prospected HLT paved the way for learning about the teaching and learning of cryptology. The video recordings afforded opportunities to observe the consequences of these decisions. Edelson (2002:112) summarized it as follows:

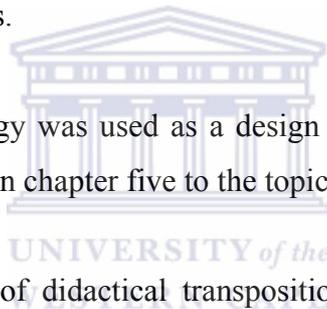
That is, the goal of ordinary design is to use the lessons embodied in a design procedure, problem analysis, and design solution to create a successful design product. Design research retains that goal but adds an additional one, the goal of developing useful, generalizable theories. The opportunity that designs offers for theory development is the possibility of using the lessons learned in constructing design procedures, problem analysis, and design solutions to develop useful theories.

8.6.2 Theoretical framework

Chapter two introduced the theoretical frameworks for this study. The following heuristics important to RME were utilized in this study:

- Guided reinvention;
- Didactical phenomenology and
- Emergent models.

Didactical phenomenology was used as a design principle and was discussed in chapter two and applied in chapter five to the topic of cryptology.



The second framework of didactical transposition was applied to the topic of cryptology to elementarize content as it moved from its different sources until it ended up at its target. Target here referred to a grade 10 school mathematics classroom.

Although the two aforementioned frameworks contributed to the outcomes of the study, the theoretical framework, entitled workbench activity, encapsulating the work of Pickering (1995), did not contribute much to the study. This could be seen as one of the limitations of the study.

8.6.3 Literature review

As stated in chapter 4, the literature review is in no way exhaustive. In the latter part of chapter 4 there was not much discussion on other research initiatives (see 4.7) and it is expected of readers to consult the references in this regard. Although

examples are given for certain ciphers, it would have been more ideal if each discussion of a cipher could be followed by an example.

8.7 LIMITATIONS OF THE STUDY

The first design research cycle of three teaching experiments consisted of only one activity. Perhaps it should have been a full set of activities as developed for the second design research cycle. The fact that the researcher was the facilitator for the two design cycles could be seen as a limitation. Further limitations were highlighted in the reflection on the methodology (8.6.1), theoretical frameworks (8.6.2) and literature review (8.6.3).

8.8 RECOMMENDATIONS

A third design research cycle is recommended. The changes suggested in the respective retrospective analyses could be implemented for this phase. Currently schools have an option to write three school mathematics question papers (the third question paper is optional) for the grade 10 to 12 school mathematics curriculum. A third design research cycle could be done by teaching the topic of cryptology for one period per week at a school and to follow it up with an exam which could then form part of the third school mathematics paper.

As the thesis focused on the design of materials the role of the teacher was not in the foreground. In a third design research cycle teachers could also be participants in a teaching experiment to enable them to teach the activities in teaching experiments with learners for a third design research cycle.

As mentioned in 8.6.3 the issue about the limitations of the literature review could be addressed by developing a reader for the topic. Work done on the literature review (chapter 4) and the historical and didactical phenomenology of cryptology (chapter 5) could be used as a starting point for this reader. Examples for the different ciphers could then be included as well as activities for a proposed third design research cycle. The possible projects identified as part of Appendix B could also be included as part of this reader.

8.9 CONCLUSION

We currently live in an information age and it is important that school mathematics explore topics within information. Cryptology as a topic could be able to do so. In order to succeed as a topic within school mathematics, teachers should be well trained to teach the topic. As cryptology has links to different fields of mathematics, for example number theory, it is important for the training to build a sound mathematical knowledge thereof.

Singh's concerns that a third world war would be fought on the information front should be taken seriously. As human beings we should be concerned with our privacy and the way we work with information. Introducing cryptology as a school mathematics topic could be a start to address these concerns.



REFERENCES

- Al-Kadi, I.A. (1992). The origins of cryptology: The Arab contributions. *Cryptologia*, **16**(2), 97-126.
- Artigue, M. (1994). Didactical engineering as a framework for the conception of teaching products. In R. Biehler, R.W. Scholtz, R. Strässer & B. Winkelmann (Eds.), *Didactics of mathematics as a scientific discipline* (pp. 27-39). Dordrecht: Kluwer Academic Publishers.
- Bakker, A. (2000). Historical and didactical phenomenology of average values. In Proceedings of the Conference, *History and Epistemology in mathematical Education*, Belgium.
- Bakker, A. (2003). The Early History of Average Values and Implications for Education. *Journal of Statistics Education* [Online], **11**(1).
www.amstat.org/publications/jse/v11n1/bakker.html
- Bakker, A. (2004). Historical and didactical phenomenology of average values. In Proceedings of the Conference, *History and Epistemology in mathematical Education*, Belgium.
- Barr, T.H. (2002). *Invitation to cryptology*. Upper Saddle River, New Jersey: Prentice Hall.
- Beutelspacher, A. (1994). *Cryptology*. Washington DC: The Mathematical Association of America, (Incorporated).
- Brown, A.L. (1992). Design experiments: Theoretical and methodological challenges in creating complex interventions in classroom settings. *Journal of the Learning Sciences*, **2**(2), 141-178.
- Butler, W., & Keeney, L.D. (2001). *Secret messages*. London: Simon & Schuster.
- Chevellard, Y. (1991). *La transposition didactique* (2nd ed.). Grenoble, France: La Pensée Sauvage.
- Chevellard, Y. (1992). Concepts fondamentaux de la transposition didactique: Perspectives apportées par une perspective anthropologique. *Recherches en Didactique des Mathématiques*, **12**(1), 73-112.
- Cobb, P., Confrey, J., diSessa, A. A., Lehrer, R., & Schauble, L. (2003). Design experiments in educational research. *Educational Researcher*, **32**(1), 9-13.
- Cook, N. (1997). *Secret codes: Real-world mathematics through science*. Palo Alto: Dale Seymour Publications.

REFERENCES

- Diffie, W. & Hellman, M.E. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, **22**(6), 644-654.
- Dijksterhuis, E.J. (1990). *Clio's stiefkind*. Amsterdam: Bert Bakker.
- Disciple's study Bible. (1988). Nashville: Holman Bible Publishers.
- Drijvers, P. (2003). *Learning algebra in a computer algebra environment: Design research on the understanding of the concept of parameter*. Utrecht, the Netherlands: CD Bèta Press.
- Edelson, D.C. (2002). Design research: What we learn when we engage in design. *Journal of the Learning Sciences*, **11**(1), 105-121.
- Esposito, V.J. (1964). *A concise history of World War I*. London: Pall Mall Press.
- Fey, J.T. (1994). Eclectic approaches to elementarization: Cases of curriculum construction in the United States. In R. Biehler, R.W. Scholtz, R. Strässer & B. Winkelmann (Eds.), *Didactics of mathematics as a scientific discipline* (pp. 15-26). Dordrecht: Kluwer Academic Publishers.
- Freudenthal, H. (1973). *Mathematics as an educational task*. Dordrecht, the Netherlands: Reidel.
- Freudenthal, H. (1983a). *Didactical phenomenology of mathematical structures*. Dordrecht, the Netherlands: Reidel.
- Freudenthal, H. (1983b). The implicit philosophy of mathematics: History and education. In *Proceedings of the International Congress of Mathematicians* (pp. 1695-1709). Warsaw and Amsterdam: Polish Scientific Publishers and Elsevier Science Publishers.
- Freudenthal, H. (1991). *Revisiting mathematics education, China lectures*. Dordrecht, the Netherlands: Kluwer Academic Publishers.
- Gilbert, M. (1989). *Second world war*. London: George Weidenfeld and Nicolson Ltd.
- Gravemeijer, K.P.E. (1993). Ontwikkelingsonderzoek als basis voor theorievorming [Design research as a basis for theory building]. In R. de Jong & M. Wijers (Eds.), *Ontwikkelingsonderzoek, theorie en praktijk* (pp. 17-34) [Design research, theory and practice]. Utrecht, Netherlands: Freudenthal Instituut.
- Gravemeijer, K.P.E. (1994). *Developing realistic mathematics education*. (Dissertation). Utrecht: CD Bèta Press.

REFERENCES

- Gravemeijer, K.P.E. (1998). *Developmental research as a research method*. Utrecht: CD Bèta Press.
- Kilpatrick & A. Sierpiska (Eds.), *Mathematics education as a research domain: A search for identity* (pp. 277-295). Dordrecht, Netherlands: Kluwer Academic Publishers.
- Gravemeijer, K.P.E. (2001). Developmental research, a course in elementary data analysis as an example. In Lin, F.L. (Ed.) *Common sense in mathematics education* (pp. 43-68). Proceedings of the Netherlands and Taiwan Conference on Mathematics Education.
- Gravemeijer, K.P.E. & Cobb, P. (2001). *Designing classroom-learning environments that support mathematical learning*. Paper presented at the Symposium 'Design experiments, or engineering prototypes of interactive learning environments in science and mathematics', at the American Educational Research Association (AERA), Seattle, USA.
- Gravemeijer, K.P.E., Cobb, P., Bowers, J., & Whitenack, J. (2000). Symbolizing, modeling, and instructional design. In P. Cobb, E. Yackel & K. McClain (Eds.), *Symbolizing and communicating in mathematics classrooms: Perspectives on discourse, tools and instructional design* (pp. 225-273). Mahwah, NJ: Lawrence Erlbaum Associates.
- Gravemeijer, K.P.E. & Doorman M. (1999) Context problems in Realistic Mathematics Education: A calculus course as an example, *Educational Studies in Mathematics* **39**(1), 111-129.
- Gravemeijer, K.P.E. & Terwel, J. (2000). Hans Freudenthal: A mathematician on didactics and curriculum theory. *Journal of Curriculum Studies* **32**(6), 777-796.
- <http://library.thinkquest.org/28005/flashed/timemachine/timeline.shtml>
(14/04/2002)
- Jackson, T.H. (1987). *From number theory to secret codes*. Bristol: Adam Hilger.
- Julie, C., & Mikalsen, Ø. (2000). Workshop on International Collaboration in Science and Mathematics Education. Department of Applied Education. University of Bergen. 20-24 November.
- Julie, C. (2002). The Activity System of School-Teaching Mathematics and Mathematical Modelling. *For the Learning of Mathematics*. **22**(3), 29-37.
- Kahn, D. (1980). Codebreaking in World Wars I and II: The major successes and failures, their causes and their effects. *The Historical Journal*. **23**(3), 617-639.

REFERENCES

- Kahn, D. (1996). *The code breakers: The story of secret writing*. New York: The Macmillan Company.
- Koblitz, N. (1994). *A course in number theory and cryptography*. Heidelberg: Springer-Verlag.
- Kortland, J. (2001). *A problem posing approach to teaching decision making about the waste issue*. Utrecht: CD Bèta Press. (PhD thesis).
- Kumanduri, R., & Romero, C. (1998). *Number theory with computer applications*. Upper Saddle River, New Jersey: Prentice Hall.
- Laffin, J. (1964). *Codes and ciphers*. New York: Abelard-Schuman Limited.
- Laitman, M. (27/02/2002) <http://www.kabbalah.info>
- Lehner, R., & Scauble, L. (2001). Accounting for contingency in design experiments. Paper presented at AERA, Seattle, WA.
- Leijnse, P.L. (1995). 'Developmental research' as a way to an empirically based 'didactical structure' of science. *Science Education*, **79**, 189-199.
- Malkevitch, J., & Froelich, G. (1993). *Loads of codes*. Lexington: COMAP, Inc.
- Malkevitch, J., Froelich, G., & Froelich, D. (1993). *Codes galore*. Lexington: COMAP, Inc.
- Menezes, A., van Oorschot, P., & Vanstone, S. (1997). *Handbook of applied cryptography*. Boca Raton, Florida: CRC Press, Inc.
- National Research Council. (2004). *How people learn: Bridging research and practice*. Washington, DC: National Academy Press.
- Pepin, B. (1999). Existing models of knowledge in teaching: Developing an understanding of the Anglo/American, the French and the German scene. *TNTEE Publications*, **2**(1), 49-65.
- Pickering, A. (1994). Objectivity and the Mangle of Practice. *Rethinking Objectivity*. Ed. Alan Megill. Durham: Duke UP, 109-125.
- Pickering, A. (1995). *The Mangle of Practice: Time, Agency, and Science*. Chicago: University of Chicago Press.
- Rechin & Wilder. (2004). Crock. *Sunday Times Magazine*, Sunday 25 April 2004.

REFERENCES

- Research Advisory Committee of the National Council of Teachers of Mathematics. (1996). Justification and reform. *Journal for Research in Mathematics Education*, **27**(5), 516-520.
- Rosen, K.H. (2005). *Elementary number theory and its applications*. New York: Addison Wesley.
- Satinover, J. (1997). *The truth behind the Bible code*. London: Sidgwick & Jackson.
- Scøberg, S. (2002). *Science for the children? Report from the science and scientists-project* (Vol. 1/2002). Oslo: Department of teacher education and school development, University of Oslo.
- Simon, M.A. (1995). Reconstructing mathematics pedagogy from a constructive perspective. *Journal for Research in Mathematics Education*, **26**(2), 114-145.
- Singh, S. (1999). *The code book: The science of secrecy from ancient Egypt to quantum cryptography*. New York: Anchor Books.
- Sinkov, A. (1996). *Elementary cryptanalysis: A mathematical approach*. Washington DC: The Mathematics Association of America, (Incorporated).
- Stanton, J.M. (2001). Galton, Pearson, and the Peas: A brief history of linear regression for statistic instructors, *Journal of Statistics Education* [Online], **9**(3). (www.amstat.org/publications/jse/v9n3/stanton.html)
- Steffe, L.P., & Thompson, P.W. (2000). Teaching experiments methodology: Underlying principles and essential elements. In R. Lesh & A.E. Kelly (Eds.), *Research design in mathematics and science education* (pp. 267-307). Hillside, NJ: Erlbaum Associates.
- Stinson, D.R. (1995). *Cryptography: Theory and practice*. Boca Raton, Florida: CRC Press, Incorporated.
- Streefland, L. (1991). *Fractions in realistic mathematics education: A paradigm of developmental research*. Dordrecht, the Netherlands: Kluwer Academic Publishers.
- Thévenaz, P. (1962). *What is phenomenology and other essays*. Edited and translated by J..M. Edie. London: Merlin Press.
- Tobin, J., & Dobard, R. (1998). *Hidden in plain view: The secret story of quilts and the underground railroad*. New York: Doubleday.
- Treffers, A. (1987). *Three dimensions: A model of goal and theory description in mathematics instruction – The Wiskobas Project*. Dordrecht, the Netherlands: Reidel.

REFERENCES

- Treffers, A. (1993). Ontwikkelingsonderzoek in eerste aanzet [Design research as a first step]. In R. de Jong & M. Wijers (Eds.), *Ontwikkelingsonderzoek, theorie en praktijk* [Design research, theory and practice] (pp. 35-58). Utrecht, the Netherlands: Freudenthal Instituut.
- Van den Akker, J. (1999). Principles and methods of development research. In J. van den Akker, R. M. Branch, K. Gustafson, N. Nieveen & T. Plomp (Eds.), *Design approaches and tools in education and training* (pp. 1-14). Boston, Dordrecht: Kluwer Academic Publishers.
- Van den Heuvel-Panhuizen, M. (1996). *Assessment and realistic mathematics education*. Utrecht, the Netherlands: CD Bèta Press.
- Whittles, K. (1996). *Realistic mathematics education and the strategies grade 8 learners develop for the solution of two linear simultaneous equations*. Unpublished Master's Dissertation. Bellville: University of the Western Cape.



APPENDIX A

NOTES

NOTE 1

GRASSMATE was sponsored by the Norwegian Agency for Development (NORAD) through the Norwegian Committee for Development Research and Education (NUFU). Professors C. Julie (University of the Western Cape, South Africa) and Ø. Mikalsen (University of Bergen, Norway) chaired proceedings of GRASSMATE.

NOTE 2

These learners were from two high schools in Wellington near Cape Town in South Africa.

NOTE 3

Professor R. Fray, head of the Mathematics Department, taught the course on number theory, with the book, *Number theory with computer applications* as prescribed book.

NOTE 4

Professor T.H. Barr was a staff member of Rhodes College in Michigan State, USA. He is author of the book, *Invitation to cryptology*, which was developed as a course, *Science of secret writing*, he taught to students at the college. He presented me with a desk copy of his book after I made contact with him via the internet. Contact was made because of a common interest in the topic of cryptology. He also gave valuable input on the thesis for chapters 1 and 4.

NOTE 5

The discrepancy in the dates is due to work commitments of the researcher when he returned to his full-time work as a Deputy Principal of a high school in Wellington, South Africa. During 2002 the researcher had a stint of working at UWC on a part-time basis. In January 2007 the researcher started in a new post at the Cape Peninsula University of Technology: Wellington Campus (Education Faculty).

APPENDIX B

POSSIBLE PROJECTS FOR CRYPTOLOGY

It is required of learners in the different grades at high school in South Africa to do projects. This was also identified as a problem for mathematics teachers at school level. This could be one way of introducing learners to cryptology and afford teachers the opportunity to learn and interact with the content of cryptology. In this way they could build on their knowledge base of cryptology and build up a resource base for the teaching of the topic at a later stage.

Possible projects topics

1. Simon Singh contends in his book, *The Code Book* (1999), that World War III will be fought on the information front. Discuss this statement with respect to:
 - 1.1. World War I
 - 1.2. World War II(Could be asked as two different projects)
2. Discuss the ancient uses of cryptology
3. Terminology plays an important role in cryptology. Name and clarify the terminology that forms part of cryptology as well as how the cryptosystem is structured.
4. Discuss and give examples to explain the following types of ciphers:
 - 4.1. Caesar
 - 4.2. Substitution
 - 4.3. Additive
 - 4.4. Transposition
 - 4.5. Monoalphabetic
 - 4.6. Polyalphabetic
 - 4.7. Symmetric
 - 4.8. Asymmetric
5. Discuss the contributions of William and Elizabeth Friedman to the development of cryptology.

6. Cipher machines were utilised for encryption and decryption purposes during World War II. Discuss the workings of the different cipher machines that were developed by countries during the war.
7. The Zimmermann telegram changed the course of World War II. Discuss this issue with respect to secrecy and solving intercepted messages.
8. The Germans thought Enigma to be unsolvable. Critically discuss this statement.
9. It is argued that the Enigma cipher machine is an extension of the Alberti Disk. Discuss the relationship between the two machines highlighting the structural design and working of the machines.
10. Name and discuss the role of the persons involved in breaking the Enigma code.
11. The movie, Enigma, tries to depict the happenings around Enigma. Critically discuss the merits/demerits of the movie.
12. Name and discuss the role of the persons involved in breaking the Purple code.
13. Discuss the cryptanalysis involved in solving messages encrypted with the Vigenère table.
14. Different persons played important roles in establishing and developing cryptology as a topic. Choose one person, highlighting his/her role and contributions towards achieving this.
15. The lesbian and gay issue is under scrutiny in our society. Discuss this issue with respect to the life of Alan Turing, highlighting his studies, his work and his eventual death.
16. Women in cryptology: The case of Elizebeth Friedman.
17. Discuss the uses of cryptology in our daily lives.
18. Cryptology opened avenues for number theory to drop its shackles for not having any applications in real life. Discuss this issue with respect to public-key cryptography.
19. Language played a major role in World War II between the USA and Japan. Discuss the role of the Navajos in this regard.

20. The movie, *The Windtalkers*, tries to show the role the Navajo tribe played in World War II. How true a reflection is the movie of the Navajo's contribution to the war?
21. Discuss the working of the ADFGVX cipher. Use the cipher to encrypt the message: MATHS COULD BE FUN
(The other ciphers could also be covered with similar types of questions)
22. Discuss the modern uses of cryptology.



APPENDIX C

ALBERTI DISK: EXAMPLE

For the Alberti alphabet, the letters *H, K, Y, J, U and W* are left out. The outer wheel which is fixed denotes the plaintext. The inner revolving wheel indicates the ciphertext.

For disk alignment F_k , the corresponding alignment for the alphabet will be as follows:

A	B	C	D	E	F	G	I	L	M	N	O
<i>t</i>	<i>y</i>	<i>q</i>	<i>i</i>	<i>x</i>	<i>k</i>	<i>v</i>	<i>p</i>	<i>et</i>	<i>m</i>	<i>r</i>	<i>d</i>
P	Q	R	S	T	V	X	Z	1	2	3	4
<i>l</i>	<i>g</i>	<i>a</i>	<i>z</i>	<i>e</i>	<i>n</i>	<i>b</i>	<i>o</i>	<i>s</i>	<i>f</i>	<i>c</i>	<i>h</i>

The alphabet alignments for V_k , Q_k and M_k are given below:

<i>V_k</i>											
A	B	C	D	E	F	G	I	L	M	N	O
<i>l</i>	<i>g</i>	<i>a</i>	<i>z</i>	<i>e</i>	<i>n</i>	<i>b</i>	<i>o</i>	<i>s</i>	<i>f</i>	<i>c</i>	<i>h</i>
P	Q	R	S	T	V	X	Z	1	2	3	4
<i>t</i>	<i>y</i>	<i>q</i>	<i>i</i>	<i>x</i>	<i>k</i>	<i>v</i>	<i>p</i>	<i>et</i>	<i>m</i>	<i>r</i>	<i>d</i>

<i>Q_k</i>											
A	B	C	D	E	F	G	I	L	M	N	O
<i>e</i>	<i>n</i>	<i>b</i>	<i>o</i>	<i>s</i>	<i>f</i>	<i>c</i>	<i>h</i>	<i>t</i>	<i>y</i>	<i>q</i>	<i>i</i>
P	Q	R	S	T	V	X	Z	1	2	3	4
<i>x</i>	<i>k</i>	<i>v</i>	<i>p</i>	<i>et</i>	<i>m</i>	<i>r</i>	<i>d</i>	<i>e</i>	<i>g</i>	<i>a</i>	<i>z</i>

<i>M_k</i>											
A	B	C	D	E	F	G	I	L	M	N	O
<i>s</i>	<i>f</i>	<i>c</i>	<i>h</i>	<i>t</i>	<i>y</i>	<i>q</i>	<i>i</i>	<i>x</i>	<i>k</i>	<i>v</i>	<i>p</i>
P	Q	R	S	T	V	X	Z	1	2	3	4
<i>et</i>	<i>m</i>	<i>r</i>	<i>d</i>	<i>l</i>	<i>g</i>	<i>a</i>	<i>z</i>	<i>e</i>	<i>n</i>	<i>b</i>	<i>o</i>

APPENDIX D1

RSA PUBLIC-KEY: EXPLANATION

Choose any two prime numbers p and q :

$$p = 17 \text{ and } q = 23$$

Determine m where $m = p \times q$:

$$m = 17 \times 23 = 391$$

Determine n where $n = (p - 1)(q - 1)$:

$$n = (17 - 1)(23 - 1) = 16 \times 22 = 352$$

Next, select another number e , a public key, which is relatively prime to $n = 352 = 2^5 \cdot 11$

(relatively prime: 1 as the only common divisor)

$$e = 29$$

Now determine the inverse d of e modulo 391 by the extended Euclidean algorithm:

$$352 = 12 \times 29 + 4$$

$$29 = 7 \times 4 + 1$$

Now, by working backwards, we get:

$$\begin{aligned} 1 &= 29 - 7 \times 4 \\ &= 29 - 7(352 - 12 \times 29) \\ &= 85 \times 29 - 7 \times 352 \end{aligned}$$

Now write down the value for d :

$$d \equiv 85 \pmod{391}$$

The values for $n = 352$ and the exponent $e = 29$ is published for all to know and the values for d , p and q are kept secret.

APPENDIX D2

RSA PUBLIC-KEY: EXAMPLE

For a message to be send we use the rule:

$$x = 24 \times (\text{First Letter}) + \text{Second Letter}$$

The following values are used for the respective letters of the alphabet:

<i>a</i>	<i>b</i>	<i>c</i>	<i>d</i>	<i>e</i>	<i>f</i>	<i>g</i>	<i>h</i>	<i>i</i>	<i>j</i>	<i>k</i>	<i>l</i>	<i>m</i>
<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>	<i>6</i>	<i>7</i>	<i>8</i>	<i>9</i>	<i>10</i>	<i>11</i>	<i>12</i>	<i>13</i>
<i>n</i>	<i>o</i>	<i>p</i>	<i>q</i>	<i>r</i>	<i>s</i>	<i>t</i>	<i>u</i>	<i>v</i>	<i>w</i>	<i>x</i>	<i>y</i>	<i>z</i>
<i>14</i>	<i>15</i>	<i>16</i>	<i>17</i>	<i>18</i>	<i>19</i>	<i>20</i>	<i>21</i>	<i>22</i>	<i>23</i>	<i>24</i>	<i>25</i>	<i>26</i>

We want to send the following message: *HE*

The value for x now becomes: $x = 24 \times 8 + 5 = 197$

This value of 197 is enciphered by calculating:

$$\begin{aligned}
 y &= x^e \equiv 197^{29} \\
 &\equiv 147 \pmod{391}
 \end{aligned}$$

We need to decipher *147* by calculating $y^{85} \text{MOD } 391$

$$\begin{aligned}
 y^{64} &\equiv 147^{85} \\
 &\equiv (147^{27})^3 \cdot 147^4 \\
 &\equiv 284^3 \cdot 259 \\
 &\equiv 351 \cdot 259 \\
 &\equiv 197 \pmod{391}
 \end{aligned}$$

The corresponding values for the two letters are now calculated by dividing 24 into 197:

$$197 = 8 \times 24 + 5$$

The values 8 and 5 lead to us to the letters *HE*.

APPENDIX E
FIRST DESIGN RESEARCH CYCLE (TITLE PAGE)

FIRST DESIGN RESEARCH CYCLE



UNIVERSITY *of the*
WESTERN CAPE

TOPIC: CRYPTOLOGY

ACTIVITIES

APPENDIX E1
FIRST TEACHING EXPERIMENT (TITLE PAGE)

FIRST TEACHING EXPERIMENT



TOPIC: SPARTAN SCYTALE

PARTICIPANTS: TEACHERS

APPENDIX E2
UNIT 1: THE SPARTAN SCYTALE

INTRODUCTION

The Spartan government sent messages to its generals on the war front in the following way. Sender and receiver each had a cylindrical rod, called a *scytale* (pronounced si'-ta-lee), of exactly the same radius. The sender wrapped a narrow strip of parchment around the rod (see figure), then wrote a message line by line parallel to the rod's axis. Successive letters went on successive turns of the parchment. Then a messenger carried the strip and handed it over to the intended receiver.

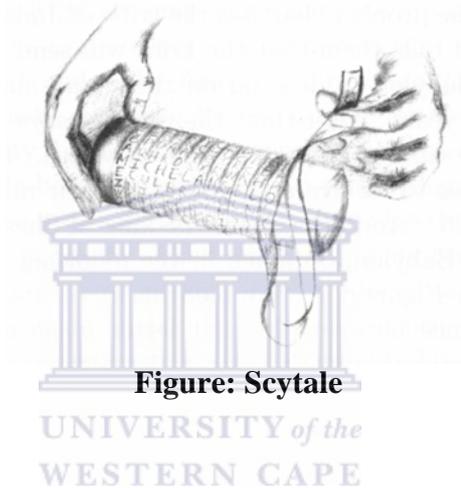


Figure: Scytale

GROUP 1

1. GROUP AS SENDER

Use the available materials and prepare your strip of parchment. You want to send the message:

A SECRET IS USEFUL TODAY

to group 2. Follow the descriptions in the introduction above and prepare the message for the messenger to take to group 2.

2. GROUP AS RECEIVER

Unscramble the received message and write down the original message from group 2.

3. GROUP AS RECEIVER

What is the message corresponding to the following sequence of letters, which was obtained using a scytale?

SYBLCRESEERACHTAYPUOHIPHRUEMTYILSOO!TDOFG

APPENDIX E3
SPARTAN SCYTALE: ANSWER SHEET

The answers to problems 1 and 2 depend on the number of turns chosen around the batten.

SOLUTION TO PROBLEM NUMBER 3

First Solution

Write down S

Start with Y (next to S above) and then count 6 letters, ending in E. Write down E.

Start with S (next to E above) and count six letters, ending in C. Write down C.

Start with H (next to C) and count six letters, ending in U. Write down U.

Proceed in this manner

Answer: SECURTIY SHOULD BE THE SOLE AIM OF CRYPTOGRAPHY!



Second Solution

Break the message down as follows:

/ SYBLCR / ESEERA / CHTAYP / UOHIPH / RUEMTY / ILSOO! / TDOFG /

Now write down in columnar form:

S	E	C	U	R	I	T
Y	S	H	O	U	L	D
B	E	T	H	E	S	O
L	E	A	I	M	O	F
C	R	Y	P	T	O	G
R	A	P	H	Y	!	

Answer: SECURTIY SHOULD BE THE SOLE AIM OF CRYPTOGRAPHY!

APPENDIX E4
SECOND TEACHING EXPERIMENT (TITLE PAGE)

SECOND TEACHING EXPERIMENT



TOPIC: SPARTAN SCYTALE

PARTICIPANTS: LEARNERS (AFRIKAANS)

APPENDIX E5

DECIPHERING AND READING OF MESSAGES

ONTSYFERING EN LEES VAN BOODSKAPPE

INLEIDING

Om geheimhouding te verseker, het die Spartaanse regering probeer om boodskappe so te skryf, dat indien dit onderskep sou word, dit moeilik ontsyfer sou word. Boodskappe is as volg deur die regering aan bevelvoerders op die oorlogsfront gestuur. Beide sender en ontvanger het 'n silindriese staf gehad. Om die staf is 'n dun strook perkament gedraai. Die sender het dan die boodskap in parallele rye op die strook geskryf, een letter per draai. Vooraf is besluit hoeveel draaie vir die skryfwerk benodig sal word.



Figuur: Staf met strook perkament omgedraai

GROEP 2

1. GROEP AS SENDER

Gebruik die beskikbare materiaal en berei jou strook perkament voor. Die volgende boodskap moet aan groep 1 gestuur word:

ONS HET JUL BOODSKAP GELEES

Volg die verduideliking in die inleiding hierbo en berei die boodskap voor.

- 1.1 Skryf die boodskap op die perkament neer terwyl dit om die staaf gedraai is.
- 1.2 Skryf die boodskap neer soos dit voorkom op die perkament nadat dit afgedraai is.
- 1.3 Neem nou die boodskap (perkament) na groep 1 om te ontsyfer.

3. GROEP AS ONTVANGER

Ontsyfer en skryf neer die boodskap ontvang van groep 1.

3. GROEP AS ONDERSKEPPER

Die volgende boodskap wat ook met 'n staf voorberei is, is deur 'n lid in jul groep onderskep. Probeer nou vasstel wat die oorspronklike boodskap is. Wys alle berekeninge.

DPBESTFIRLMOSEEOEINYR



APPENDIX E6

DECIPHERING AND READING OF MESSAGES: ANSWER SHEET

ONTSYFERING EN LEES VAN BOODSKAPPE: ANTWOORDBLAD

Probleme 1 en 2 se oplossings word deur die aantal draai om die staf bepaal.

OPLOSSING VIR PROBLEEM 3

Eerste Oplossing

Skryf die letter D neer.

Begin met die volgende letter P en tel sewe letters. Eindig in I. Skryf nou I neer.

Begin met R (langs I) en tel dan sewe letters. Eindig in E. Skryf nou E neer.

Herhaal die prosedure vir die res van die letters.

Antwoord: DIE PROBLEEM IS ONTSYFER

UNIVERSITY of the
WESTERN CAPE

Tweede Oplossing

Paar die letters van die boodskap as volg af:

/ DPBESTF / IRLMOSE / EOEINYR /

Skryf afgebakende letters in kolomvorm:

D	I	E
P	R	O
B	L	E
E	M	I
S	O	N
T	S	Y
F	E	R

Antwoord: DIE PROBLEEM IS ONTSYFER

APPENDIX E7
THIRD TEACHING EXPERIMENT (TITLE PAGE)

THIRD TEACHING EXPERIMENT

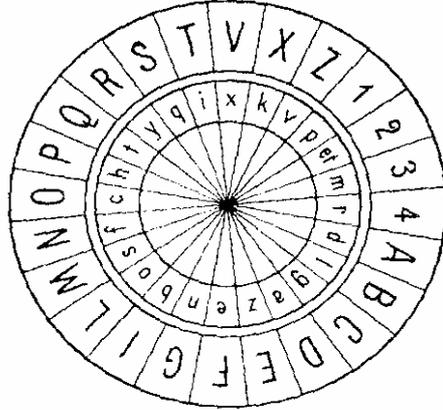


TOPIC: ALBERTI CIPHER

PARTICIPANTS: STUDENTS (AFRIKAANS)

**APPENDIX E8
ALBERTI DISK**

ALBERTI SKYF



SKYFSTELLING: Fk

Voltooi nou die Alberti Alfabet

A	B	C	D	E	F	G	I	L	M	N	O
P	Q	R	S	T	V	X	Z	1	2	3	4

Gebruik die Alberti skyf en wys hoe die volgende boodskap verander:

ALBERTI WAS AN ITALIAN

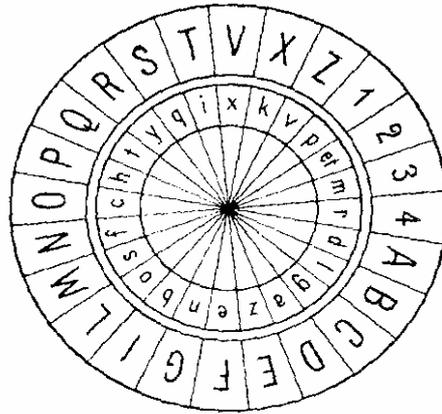
WOORD	SKYFSTELLING	NUWE WOORD
ALBERTI	Fk	
W*AS	Vk	
AN	Qk	
ITALIAN	Mk	

***W word met 'n Dubbel V vervang**

(WYS ALLE BEREKENINGE)

APPENDIX E9
ALBERTI DISK: ANSWER SHEET

ALBERTI SKYF: ANTWOORDBLAD



SKYFSTELLING: Fk

Voltooi nou die Alberti Alfabet

A	B	C	D	E	F	G	I	L	M	N	O
<i>t</i>	<i>y</i>	<i>q</i>	<i>i</i>	<i>x</i>	<i>k</i>	<i>v</i>	<i>p</i>	<i>et</i>	<i>m</i>	<i>r</i>	<i>d</i>
P	Q	R	S	T	V	X	Z	1	2	3	4
<i>l</i>	<i>g</i>	<i>a</i>	<i>z</i>	<i>e</i>	<i>n</i>	<i>b</i>	<i>o</i>	<i>s</i>	<i>f</i>	<i>c</i>	<i>h</i>

Gebruik die Alberti skyf en wys hoe die volgende boodskap verander:

ALBERTI WAS AN ITALIAN

WOORD	SKYFSTELLING	NUWE WOORD
ALBERTI	Fk	<i>tetyxaep</i>
W*AS	Vk	<i>kkli</i>
AN	Qk	<i>eg</i>
ITALIAN	Mk	<i>ilxisiv</i>

***W word met 'n Dubbel V vervang**

(WYS ALLE BEREKENINGE)

APPENDIX F
INVITATION FOR RESEARCH

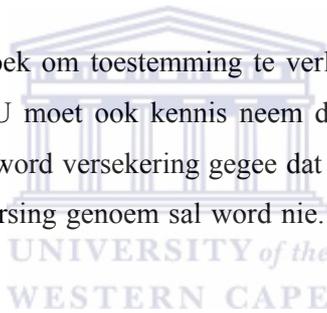
23 SEPTEMBER 2002

Geagte Ouer

NAVORSING: UITNODIGING

Die ondergetekende is tans besig met navorsing onder die vaandel van die Universiteit van Wes-Kaapland vir 'n doktorsale studie. Die navorsing het ten doel om te kyk hoe nuwe inhoud in 'n skool wiskunde kurrikulum ingevoer kan word. Vir die doel word graad 10 leerders wat wiskunde as skoolvak het, benodig om aan die navorsing deel te neem.

Graag wens ons u te versoek om toestemming te verleen vir u seun/dogter om aan die navorsing deel te neem. U moet ook kennis neem dat video opnames van die sessies geneem sal word. Verder word versekering gegee dat u seun/dogter se naam onder geen omstandighede in die navorsing genoem sal word nie. As u enige navrae het, kan u my by 0825542284 kontak.



Geliewe dan ook die strokie hieronder te voltooi ten einde u besluit oor die navorsing aan ons deur te gee.

.....

K. Whittles

ANTWOORDSTROKIE

Hiermee bevestig ek (Naam en Van) dat ek kennis neem van die inhoud van die skrywe en dat ek toestemming/nie toestemming verleen vir deelname van my seun/dogter aan die navorsing. (Skrap die onderstreepte gedeelte wat nie van toepassing is nie)

Geteken te(plek) op (datum)

.....

(Handtekening)

APPENDIX G

EPISODES FROM SECOND TEACHING EXPERIMENT

NOTATION USED

Researcher: R

Group 1: G1

Learner 1: L1

Episode 1: Afrikaans version

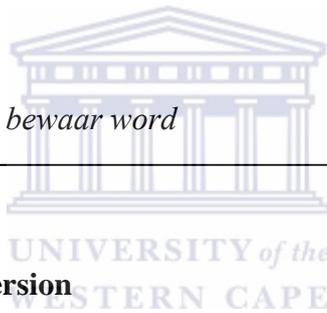
R: *Goed wat is die boodskap?*

L1G1: *Ons het julle boodskap gekry.*

R: *Is dit julle boodskap?*

L2G1: *Ja ...*

L1G1: *Ja, Geheime moet bewaar word*



Episode 2: Afrikaans version

L1G2: *Ek draai 5, jy draai 6 ens. As wat ons almal nou op 1 ding werk*

L2G2: *Hoeveel draaie?*

L1G2: *Vat 5, of moet ons 6 probeer? Gaan nie werk nie. 2, 4 6, ...Is dit nie 7 nie? Dit gaan nie werk nie*

APPENDIX H
SECOND DESIGN RESEARCH CYCLE: ACTIVITIES
AFRIKAANS VERSION (FRONT PAGE)

SECOND DESIGN RESEARCH CYCLE

TOPIC: CRYPTOLOGY



ACTIVITIES

AFRIKAANS VERSION

APPENDIX H1 CONTENTS

INTRODUCTION

ACTIVITY 1: OVERVIEW

ACTIVITY 1: EXAMPLE

ACTIVITY 2: OVERVIEW

ACTIVITY 2: EXAMPLE

ACTIVITY 3: OVERVIEW

ACTIVITY 3: EXAMPLE

ACTIVITY 4: OVERVIEW

ACTIVITY 4: EXAMPLE

ACTIVITY 5: OVERVIEW

ACTIVITY 5: EXAMPLE

ACTIVITY 6: OVERVIEW

ACTIVITY 6: EXAMPLE

ACTIVITY 7: OVERVIEW

ACTIVITY 7: EXAMPLE



APPENDIX H2

INTRODUCTION

The activity booklet for learners consists of seven activities. One of the aims of the activities is to introduce learners to some of the ciphers within the topic of cryptology. A further aim is to introduce learners to the workings of enciphering (encoding) and deciphering (decoding). In this way they get exposure to the how the cryptosystem within cryptology works. There is also an introduction to number theory and the solution of simple equations with modular mathematics. The booklet concludes with an activity on the RSA cipher.

Each activity tries to explore one specific cipher in cryptology and at times it extends into various directions of number theory and some related school mathematics topics. There will be no formal teaching during these sessions. It is expected that learners develop the required knowledge needed and use previously acquired knowledge to work out the examples. Where problems come up, there could be input by the researcher. This will be done by way of remarks or comments to facilitate them getting going again.

WESTERN CAPE

All sessions will be video recorded and observations and field notes will be kept where necessary. Each activity is introduced by a short overview to explain what the activity is all about. An activity is planned to be completed in the space of 45 minutes. More time will be allowed if needed. Learners are allowed to work in groups. Each group is expected to hand in their work at the end of the 45-minute session. All calculations (written work) must be shown on the given pages. Learners will be allowed to use their scientific calculators.

It is important to note that the booklet is aimed at grade 10 learners. The implementation for the second design research cycle will only be done with these learners. Activities are drawn up in Afrikaans, but most of the messages used in the examples are written in English.

APPENDIX H3

TRANSPOSITION CIPHERS: OVERVIEW

ACTIVITY 1

TRANSPOSITION CIPHERS

OVERVIEW

Learners are introduced to transposition ciphers of the sort in which letters in a word change positions. Working in groups they explore the Scytale, a batten that was carried by soldiers in the Persian-Greece war in 1200. They use a given batten and paper to construct a message to see how the apparatus was utilised during this war. Groups then interchange their respective messages to decode the other group's message. They then have to use the insights and knowledge gained to decipher a given message. Their solution must include an explanation of how they actually decoded the message.

APPENDIX H4
ACTIVITY 1: SPARTAN SCYTALE

AKTIWITEIT 1

INLEIDING

Om geheimhouding te verseker, het die Spartaanse regering probeer om boodskappe so te skryf, dat indien dit onderskep sou word, dit moeilik ontsyfer sou word. Boodskappe is as volg deur die regering aan bevelvoerders op die oorlogsfront gestuur. Beide sender en ontvanger het 'n silindriese staf gehad. Om die staf is 'n dun strook perkament gedraai. Die sender het dan die boodskap in parallele rye op die strook geskryf, een letter per draai. Vooraf is besluit hoeveel draaie vir die skryfwerk benodig sal word.

1. Hieronder volg 'n boodskap om 'n staf.



- 1.1 Hoeveel draaie is daar vir die perkament om die staf?
- 1.2 Wat is die boodskap wat gestuur word?
- 1.3 Skryf die boodskap neer soos dit sal voorkom op die perkament om die staf gedraai.
- 1.4 Skryf die boodskap neer soos dit sal voorkom op die perkament nadat dit van die staf afgedraai is.

2. GROEP AS SENDER

Gebruik die beskikbare materiaal en berei jou strook perkament voor. Die volgende boodskap moet aan 'n groep gestuur word:

WE GOT YOUR MESSAGE (groep 1 en 3)

READ THIS MESSAGE (groep 2 en 4)

Volg die verduideliking in die inleiding hierbo en berei die boodskap voor.

2.1 Skryf die boodskap soos dit voorkom op die perkament neer terwyl dit om die staaf gedraai is.

2.2 Skryf die boodskap neer soos dit voorkom op die perkament nadat dit afgedraai is.

2.3 Neem nou die boodskap (perkament) na 'n groep (1 ↔2; 3 ↔4) om te ontsyfer.

3. GROEP AS ONTVANGER

3.1 Ontsyfer en skryf die boodskap ontvang van ander groep neer.

3.2 Beskryf hoe julle te werk gegaan het om die boodskap te kry.

4. GROEP AS ONDERSKEPPER

4.1 Die volgende boodskap wat ook met 'n ander staf voorberei is, is deur 'n lid in jul groep onderskep. Probeer nou vasstel wat die oorspronklike boodskap is. Wys alle berekeninge.

TBSHLOEELPMVRIE OSD

4.2 Beskryf hoe julle te werk gegaan het om die boodskap te ontsyfer.

APPENDIX H5
ALBERTI CIPHERS: OVERVIEW

ACTIVITY
2

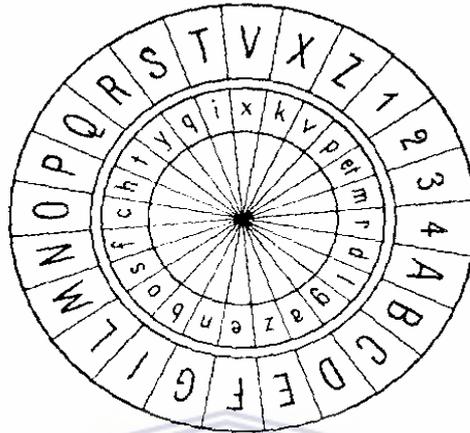
ALBERTI
CIPHERS

OVERVIEW

Activity 2 introduces learners to an Alberti cipher aided by an Alberti Disk. An Alberti disk introduces the addition or subtraction cipher. This is aimed at introducing learners to this cipher to further enhance the workings of enciphering and deciphering of messages

APPENDIX H6
ACTIVITY 2: ALBERTI DISK

AKTIWITEIT 2



ALBERTISKYF

Die buitenste ring (met die Hoofletters is vas en kan nie beweeg nie). Die ring stel voor die alfabet vir die aflees van letters vir gewone boodskappe

Die binneste ring (met die klein letters kan roteer) beweeg om die as. Die ring stel voor die alfabet vir die aflees van ooreenstemmende letters vir geheime boodskappe.

1. SKYFSTELLING: *Fk*

Voltooi nou die Alberti Alfabet

A	B	C	D	E	F	G	I	L	M	N	O
					k						
P	Q	R	S	T	V	X	Z	1	2	3	4

2. Gebruik die Alberti skyf en wys hoe die volgende boodskap verander met die gegewe skyfstelling:

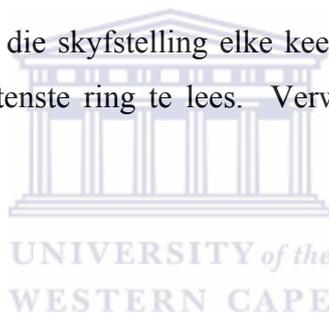
ALBERTI WAS AN ITALIAN

WOORD	SKYFSTELLING	NUWE WOORD
ALBERTI	Fk	
W*AS	Vk	
AN	Qk	
ITALIAN	Mk	

***W word met 'n Dubbel V vervang**

3. Verduidelik nou hoe die skyfstelling elke keer gebruik is om die veranderde letters vanaf die buitenste ring te lees. Verwys na elke skyfstelling hierbo gebruik.

- 3.1 Fk
- 3.2 Vk
- 3.3 Qk
- 3.4 Mk



APPENDIX H7
ADDITIVE CIPHERS: OVERVIEW

ACTIVITY
3

**ADDITIVE
CIPHERS**

OVERVIEW

Additive ciphers are an introduction to the shifting of letters of the alphabet a certain number of positions. The activity is introduced with the Caesar cipher (shift 3). Examples include bigger shifts and later conclude with the decoding of messages given the shift and when the shift is not given. The aim of the activity is to introduce working with numbers outside of the ordinary alphabet number values.

APPENDIX H8
ACTIVITY 3: CAESAR CIPHER

AKTIWITEIT 3

Gaius Julius Caesar (100 B.C. – 44 B.C.) was ‘n generaal en ‘n politikus van Rome. Om boodskappe aan sy troepe op die slagveld geheim te hou is A met D, B met E, C met F, ...ens vervang. Hy het dus die reël *LETTER* + 3 gebruik om ‘n gewone boodskap in geheime taal te omskep.

<i>Letter</i>	A	B	C	D	E	F	G	H	I	J	K	L	M
<i>Waarde</i>	0	1	2	3	4	5	6	7	8	9	10	11	12
<i>Letter</i>	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
<i>Waarde</i>	13	14	15	16	17	18	19	20	21	22	23	24	25

Gebruik die tabel hierbo en werk die volgende voorbeelde uit.

1. Wys hoe die boodskap hieronder verander met Caesar se reël.

Boodskap: THIS IS A SHIFT THREE CIPHER

Reël: *LETTER* + 3

2. Die volgende boodskap is met die Caesar reël verander. Probeer om nou die oorspronklike boodskap te bepaal.

Geheime Boodskap: ZHKDSHWRUN

3. Die boodskap WRGSLDGZEPHO is deur jou groep onderskep . Dit word vasgestel dat die boodskap met Reël: *LETTER* + ? verander is. Probeer om nou die oorspronklike boodskap te bepaal.

4. Verduidelik nou die voordele/nadele tussen die Caesar reël en die reël wat in 3 gebruik is om boodskappe geheim te hou. Wat gebeur as die getal groter as 25 is?

APPENDIX H9
FUNCTION CIPHERS: OVERVIEW

ACTIVITY
4

FUNCTION
CIPHERS

OVERVIEW

The function is an important concept within school mathematics. This activity introduces enciphering and deciphering by way of functional notation. An important extension here is the introduction of the null cipher where no changes occur when enciphering or deciphering.

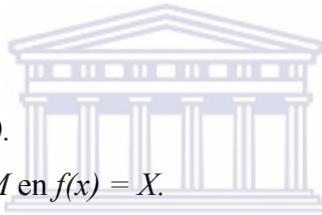
APPENDIX H10
ACTIVITY 4: FUNCTION CIPHER

AKTIWITEIT 4

In tabel 1 hieronder word die letter waardes vir x en $f(x)$ gegee:

x	A	B	C	D	E	F	G	H	I	J	K	L	M
$f(x)$	C	J	Q	X	E	L	S	Z	G	W	U	B	I
x	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$f(x)$	P	W	D	K	R	Y	F	M	T	A	H	O	V

Tabel 1



1.1 Evalueer $f(B)$ en $f(T)$.

1.2 Bepaal x vir $f(x) = M$ en $f(x) = X$.

1.3 Vir watter waarde(s) van x is $f(x) = x$?

1.4 In tabel 2 hieronder word die waardes vir die onderskeie letters van die alfabet aangegee. As $f(x)$ hierbo gegee word: $f(x) = mx + n$, waar m en n positiewe getalle is, bepaal die waardes van m en n om die reël te kry om te wys hoe elke letter vir x in $f(x)$ verander.

x	A	B	C	D	E	F	G	H	I	J	K	L	M
Vx	0	1	2	3	4	5	6	7	8	9	10	11	12
x	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Vx	13	14	15	16	17	18	19	20	21	22	23	24	25

Tabel 2

APPENDIX H11
AFFINE CIPHERS: OVERVIEW

ACTIVITY
5

AFFINE
CIPHERS

OVERVIEW

Affine ciphers use two mathematical operations, namely multiplication and addition. The key or rule takes the form $ax + b$, where a , b can take on any positive value. The work on multiplicative ciphers is applied for formulating linear equation examples with respect to two unknowns. Examples on decoding conclude the activity.

APPENDIX H12
ACTIVITY 5: AFFINE CIPHER

AKTIWITEIT 5

<i>Letter</i>	A	B	C	D	E	F	G	H	I	J	K	L	M
<i>Waarde</i>	0	1	2	3	4	5	6	7	8	9	10	11	12
<i>Letter</i>	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
<i>Waarde</i>	13	14	15	16	17	18	19	20	21	22	23	24	25

Vir al die toepassings wat volg, word die tabel hierbo gebruik om die waarde vir elke letter van die alfabet af te lees. Die volgende reëls word deurlopend op al die probleme hieronder toegepas:

- (A) Paar elke twee letters af tot aan die einde van die boodskap.
- (B) Indien 'n boodskap uit 'n onewe aantal letters bestaan, word die laaste letter herhaal ten einde 'n paar te vorm
- (C) Die eerste letter in 'n paar word na verwys as die *Eerste Letter* en die tweede letter in 'n paar as die *Tweede Letter*.

1. Om 'n boodskap in geheime taal te omskep word die volgende in plek gekry om elke letter van 'n paar te verander:

Reël vir verandering van eerste letter in paar:

$$2 \times \textit{Eerste Letter} + \textit{Tweede Letter}$$

Reël vir verandering van tweede letter in paar:

$$\textit{Eerste Letter} + \textit{Tweede Letter}$$

Die boodskap wat ons wil verander is: *MATHS IS FUN*

- 1.1 Gebruik die twee reëls en wys hoe *MA* in *YM* verander.

- 1.2 Bepaal die res van die kodeerde boodskap

2. Gebruik die volgende reëls om *PRISON BREAK* in geheime taal te skryf.

Reël vir verandering van eerste letter in paar:

$$3 \times \textit{Eerste Letter} + \textit{Tweede Letter}$$

Reël vir verandering van tweede letter in paar:

$$4 \times \textit{Eerste Letter} + 3 \times \textit{Tweede Letter}$$

3. 'n Boodskap in gewone taal het verander na *SK* met die reëls.

Reël vir verandering van eerste letter in paar:

$$2 \times \textit{Eerste Letter} + \textit{Tweede Letter}$$

Reël vir verandering van tweede letter in paar:

$$3 \times \textit{Eerste Letter} + 2 \times \textit{Tweede Letter}$$

Wys nou dat die oorspronklike boodskap *AS* was.

4. 'n Boodskap in gewone taal het verander na *BKWKGSGN* met die volgende reëls:

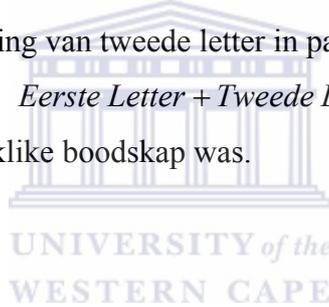
Reël vir verandering van eerste letter in paar:

$$\textit{Eerste Letter} + 2 \times \textit{Tweede Letter}$$

Reël vir verandering van tweede letter in paar:

$$\textit{Eerste Letter} + \textit{Tweede Letter}$$

Bepaal wat die oorspronklike boodskap was.



APPENDIX H13
NUMBER THEORY: OVERVIEW

ACTIVITY

6

NUMBER THEORY

OVERVIEW

Up to now learners unknowingly used number theory to solve problems. They are introduced to solve problems of the type $ax \equiv 1 \pmod{b}$ where a and b are positive numbers. This will be helpful for the last activity where an example of the RSA cipher is introduced.

APPENDIX H14
ACTIVITY 6: NUMBER THEORY

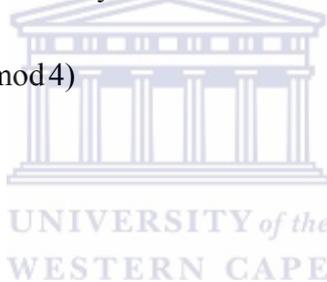
AKTIWITEIT 6

INLEIDING

Twee integers a en b is *kongruent*(mod n) indien $a \equiv b(\text{mod } n)$. Dit beteken a en b het dieselfde res as dit deur n gedeel word. Byvoorbeeld $25 \equiv 13 \equiv 1(\text{mod } 6)$.

1. Voltooi nou die volgende. Wys elke keer wat die res is.

1.1 $9 \equiv \dots \equiv \dots \equiv \dots(\text{mod } 4)$



1.2 $17 \equiv \dots \equiv \dots \equiv \dots(\text{mod } 3)$

1.3 $29 \equiv \dots \equiv \dots \equiv \dots(\text{mod } 12)$

2. Los nou vervolgens die volgende vergelykings op. Wys alle berekeninge.

2.1 $5x \equiv 1(\text{mod}3)$

2.2 $3x \equiv 1(\text{mod}7)$



2.3 $5x \equiv 1(\text{mod}15)$

$$2.4 \quad 2x \equiv 3 \pmod{11}$$

$$2.5 \quad 2x \equiv -1 \pmod{13}$$



$$2.6 \quad 3x \equiv -2 \pmod{4}$$

APPENDIX H15
RSA CIPHER: OVERVIEW

ACTIVITY
7

RSA CIPHER

OVERVIEW

Activity 7 introduces the workings of the RSA cipher. Furthermore, learners work with number theory introduced in Activity 6. Work for number theory focuses on determining the remainder on division by a certain number.

UNIVERSITY of the
WESTERN CAPE

APPENDIX H16
ACTIVITY 7: RSA CIPHER
AKTIWITEIT 7

Die RSA is deur die persone Rivest, Shamir en Adleman ontwikkel. Hul doelwit was om dit so moeilik moontlik te maak vir persone om hul boodskappe te ontsyfer. Vir die doel het hulle die volgende reëls saamgestel:

No	Reël	Voorbeeld
1.	Kies enige twee priemgetalle p en q	$p = 2$ en $q = 5$
2.	Stel $m = p \times q$	$m = 2 \times 5 = 10$
3.	Stel $A = ((p - 1) \times (q - 1))$	$A = 1 \times 4 = 4$
4.	Kies 'n getal E , kleiner as A en wat geen faktore gemeen het met A nie	$E = 3$
5.	Vind 'n getal D sodat $(E \times D) - 1$ 'n veelvoud van A is	$D = 7$
<p><i>$E (= 3)$ en $m (= 10)$ is die waardes wat aan almal bekend is.</i></p> <p><i>E word gebruik om 'n gewone boodskap in geheime taal te omskep (enkodeer).</i></p> <p><i>m word gebruik as mod 10 en word met deling gebruik om die res te vind.</i></p> <p><i>$D (= 7)$ word gebruik om die geheime boodskap terug in sy oorspronklike vorm te kry. D se waarde is nie aan almal bekend nie.</i></p>		

1. Die RSA word nou gebruik om die boodskap *DOOR* te omskep in geheime taal.

Ons gebruik die volgende verkorte alfabet met hul onderskeie waardes.

Letter	A	D	E	H	N	O	R	S	T
Waarde	1	2	3	4	5	6	7	8	9

Omskrywing	Berekeninge
Skryf die boodskap neer	
Skryf nou elke letter se waarde neer	
Verhef nou elke waarde tot die mag van $E (= 3)$	
Bereken die waardes hierbo vir $\text{mod } m (= 10)$	
Skryf nou die ooreenstemmende letters vir die waardes neer	
Die woord <i>DOOR</i> verander dus in	

Berekeninge:

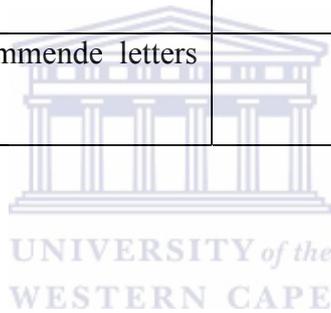
2. Om die geheime boodskap in sy oorspronklike vorm terug te skryf word as volg te

werk gegaan. Ons gebruik die geheime boodskap hierbo verkry om te wys hoe dit

weer in *DOOR* verander

Omskrywing	Berekeninge
Skryf die geheime boodskap neer	
Skryf nou elke letter se waarde neer	
Verhef nou elke waarde tot die mag van $D (= 7)$	
Bereken die waardes hierbo vir $\text{mod } m (= 10)$	
Skryf nou die ooreenstemmende letters vir die waardes neer	

Berekeninge:



3. Doen die volgende voorbeeld. Gebruik dieselfde waardes van D en m .

Geheime Boodskap	Oorspronklike Boodskap
$NRDT$	

Berekeninge:



APPENDIX I
SECOND DESIGN RESEARCH CYCLE: ACTIVITIES
ANSWERS (FRONT PAGE)

SECOND DESIGN RESEARCH CYCLE

TOPIC: CRYPTOLOGY



ACTIVITIES: ANSWERS

APPENDIX I1

CONTENTS

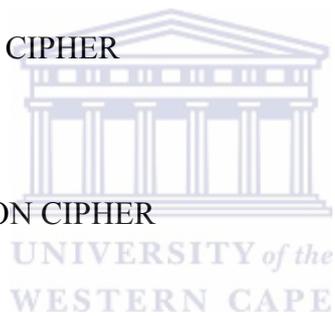
INTRODUCTION

ACTIVITY 1: SPARTAN SCYTALE

ACTIVITY 2: ALBERTI DISK

ACTIVITY 3: CAESAR CIPHER

ACTIVITY 4: FUNCTION CIPHER



ACTIVITY 5: AFFINE CIPHER

ACTIVITY 6: NUMBER THEORY

ACTIVITY 7: RSA CIPHER

APPENDIX I2

INTRODUCTION

This booklet entitled *Activities: Answers* for the second design research cycle for the topic of cryptology captures possible solutions for the seven activities. The aim is to show a possible solution to an activity and these solutions are not in any way exhaustive. It is not an aim to venture in difficult mathematical procedures that are unknown to readers, but to show how even persons without some school mathematical background could also do these examples. Although the activities are in Afrikaans, the outline and solutions for the respective seven activities are in English.



APPENDIX I3
ACTIVITY 1: SOLUTION

1.1 10 Turns

1.2 ARE YOU FREE DURING PERIOD FOUR?

1.3 ARE YOU FRE
EDURING PE
RIOD FOUR?

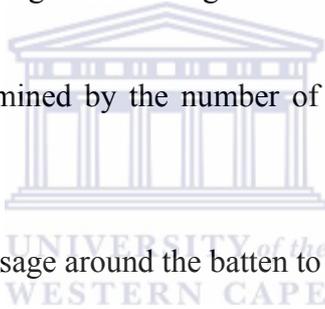
1.4 A RER EDI YUO ORD UIF FNO EPR E?

Could possibly be also given as a single row.

2. Answer will be determined by the number of turns chosen by the respective groups.

3. Turn the received message around the batten to get the original message.

4. THE PROBLEM IS SOLVED



APPENDIX I4
ACTIVITY 2: SOLUTION

1. DISK ALIGNMENT: *Fk*

A	B	C	D	E	F	G	I	L	M	N	O
<i>t</i>	<i>y</i>	<i>q</i>	<i>i</i>	<i>x</i>	<i>k</i>	<i>v</i>	<i>p</i>	<i>et</i>	<i>m</i>	<i>r</i>	<i>d</i>
P	Q	R	S	T	V	X	Z	1	2	3	4
<i>l</i>	<i>g</i>	<i>a</i>	<i>z</i>	<i>e</i>	<i>n</i>	<i>b</i>	<i>o</i>	<i>s</i>	<i>f</i>	<i>c</i>	<i>h</i>

2.

WORD	DISK ALIGNMENT	NEW WORD
ALBERTI	Fk	<i>tetyxaep</i>
W*AS	Vk	<i>kkli</i>
AN	Qk	<i>eg</i>
ITALIAN	Mk	<i>ilsxisv</i>

3.5 Fk: Count 13 places backwards OR Count 11 places forward ($13 + 11 = 24$)

3.6 Vk: Count 1 places backwards OR Count 23 places forward ($1 + 23 = 24$)

3.7 Qk: Count 5 places backwards OR Count 19 places forward ($5 + 19 = 24$)

3.8 Mk: Count 9 places backwards OR Count 15 places forward ($9 + 15 = 24$)

APPENDIX I5
ACTIVITY 3: SOLUTION

5. WKLV LV D VKLIW WKUHH FLSKHU

6. Use the inverse process of -3 ($+3$): WE HAVE TO WORK

7. *Letter* + 15 WORK HARD

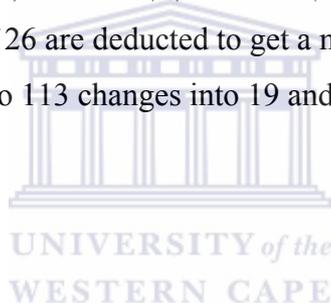
8. Caesar: Easier to get the message. With *Letter* + ? it takes longer

For numbers larger than 25 we count on as follows to show how 25 changes into 0, 26 into 1, etc.

$26 \rightarrow 0$ (A); $27 \rightarrow 1$ (B); $28 \rightarrow 2$ (C); $29 \rightarrow 3$ (D); ...

It means multiples of 26 are deducted to get a number value between 0 and 25.

$113 - 4 \times 26 = 19$. So 113 changes into 19 and is substituted with the letter T.



APPENDIX I6
ACTIVITY 4: SOLUTION

1.5 $f(B) = J$ en $f(T) = F$.

1.6 $f(U) = M$ en $f(D) = X$.

1.7 $f(E) = E$; $f(R) = R$

1.4

$$f(x) = mx + n$$

$$f(A) = C$$

$$f(0) = 2$$

$$m(0) + n = 2$$

$$n = 2$$

$$f(B) = J$$

$$f(1) = 9$$

$$m(1) + n = 9$$

$$m + n = 9$$

$$m + 2 = 9$$

$$m = 7$$

$$f(x) = 7x + 2$$



APPENDIX I7
ACTIVITY 5: SOLUTION

<i>Letter</i>	A	B	C	D	E	F	G	H	I	J	K	L	M
<i>Waarde</i>	0	1	2	3	4	5	6	7	8	9	10	11	12
<i>Letter</i>	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
<i>Waarde</i>	13	14	15	16	17	18	19	20	21	22	23	24	25

MA TH SI SF UN

1.3 M of MA $\rightarrow 2(12) + 0 = 24 \rightarrow Y$; A of MA $\rightarrow 12 + 0 = 12 \rightarrow M$

1.4 T of TH $\rightarrow 2(19) + 12 = 50 = 24 \rightarrow Y$; H of TH $\rightarrow 19 + 12 = 31 = 5 \rightarrow F$

S of SI $\rightarrow 2(18) + 8 = 44 = 19 \rightarrow T$; I of SI $\rightarrow 18 + 8 = 26 = 0 \rightarrow A$

S of SF $\rightarrow 2(18) + 5 = 41 = 15 \rightarrow P$; F of SF $\rightarrow 18 + 5 = 23 \rightarrow X$

U of UN $\rightarrow 2(20) + 13 = 53 = 1 \rightarrow B$; N of UN $\rightarrow 20 + 13 = 33 = 7 \rightarrow H$

MATHS IS FUN \rightarrow YMYFTAPXBH

2.

PR IS ON BR EA KK

P of PR $\rightarrow 3(15) + 17 = 62 = 10 \rightarrow K$; R of PR $\rightarrow 4(15) + 3(17) = 111 = 7 \rightarrow H$

I of IS $\rightarrow 3(8) + 18 = 42 = 16 \rightarrow Q$; S of IS $\rightarrow 4(8) + 3(18) = 86 = 8 \rightarrow I$

O of ON $\rightarrow 3(14) + 13 = 55 = 1 \rightarrow B$; N of ON $\rightarrow 4(14) + 3(13) = 95 = 17 \rightarrow R$

B of BR $\rightarrow 3(1) + 17 = 20 \rightarrow U$; R of BR $\rightarrow 4(1) + 3(17) = 55 = 3 \rightarrow D$

E of EA $\rightarrow 3(4) + 0 = 12 \rightarrow M$; A of EA $\rightarrow 4(4) + 3(0) = 16 \rightarrow Q$

K of KK $\rightarrow 3(10) + 10 = 40 = 14 \rightarrow O$; K of KK $\rightarrow 4(10) + 3(10) = 18 \rightarrow S$

PRISON BREAK \rightarrow KHQIBRUDMQOS

3.

$$2 \times \text{Eerste Letter} + \text{Tweede Letter} = S = 18$$

$$3 \times \text{Eerste Letter} + 2 \times \text{Tweede Letter} = K = 10$$

$$3 \times \text{Eerste Letter} + 2 \times \text{Tweede Letter} = 10 \text{ now becomes}$$

$$\text{Eerste Letter} + \text{Tweede Letter} + 18 = 10$$

$$\text{Eerste Letter} + \text{Tweede Letter} = -8 = 18$$

$$2 \times \text{Eerste Letter} + \text{Tweede Letter} = S = 18 \text{ now becomes}$$

$$\text{Eerste Letter} + 18 = 18$$

$$\text{Eerste Letter} = 0 = A$$

$$\text{Tweede Letter} = 18 = S$$

4.

BK WK GS GN

$$\text{Eerste Letter} + 2 \times \text{Tweede Letter} = B = 1$$

$$\text{Eerste Letter} + \text{Tweede Letter} = K = 10$$

$$\text{Tweede Letter} + 10 = 1$$

$$\text{Tweede Letter} = -9 = 17 = R$$

$$\text{Eerste Letter} = -7 = 19 = T$$

Similarly $WK \rightarrow YM$; $GS \rightarrow EO$; $GN \rightarrow UT$

$BKWKGS GN \rightarrow TRY ME OUT$



UNIVERSITY of the
WESTERN CAPE

APPENDIX I8
ACTIVITY 6: SOLUTION

1.1 $9 \equiv 1 \equiv 5 \equiv 13 \pmod{4}$. Takes the form of $1 + 4k, k \in \{0;1;2;3;\dots\}$

1.2 $17 \equiv 2 \equiv 5 \equiv 8 \pmod{3}$. Takes the form of $2 + 3k, k \in \{0;1;2;3;\dots\}$

1.3 $29 \equiv 5 \equiv 17 \equiv 41 \pmod{12}$. Takes the form of $5 + 12k, k \in \{0;1;2;3;\dots\}$

2.1 $5x \equiv 1 \pmod{3}$. Takes the form of $1 + 3k, k \in \{0;1;2;3;\dots\}$

$$5x \equiv 1 \equiv 10 \pmod{3} \quad 1 + 3(3) = 10$$

$$x \equiv 2$$

2.2 $3x \equiv 1 \pmod{7}$. Takes the form of $1 + 7k, k \in \{0;1;2;3;\dots\}$

$$3x \equiv 1 \equiv 15 \pmod{7} \quad 1 + 7(2) = 15$$

$$x \equiv 5$$

2.3 $5x \equiv 1 \pmod{15}$. Takes the form of $1 + 15k, k \in \{0;1;2;3;\dots\}$

No solution as $1 + 15k, k \in \{0;1;2;3;\dots\}$ cannot be a multiple of because of the addition of 1

2.4 $2x \equiv 3 \pmod{11}$. Takes the form of $3 + 11k, k \in \{0;1;2;3;\dots\}$

$$2x \equiv 3 \equiv 36 \pmod{11} \quad 3 + 11(3) = 36$$

$$x \equiv 18$$

2.5 $2x \equiv -1 \pmod{13}$. Takes the form of $-1 + 13k, k \in \{0;1;2;3;\dots\}$

$$2x \equiv -1 \equiv 12 \pmod{13} \quad -1 + 13(1) = 12$$

$$x \equiv 6$$

2.6 $3x \equiv -2 \pmod{4}$. Takes the form of $-2 + 4k, k \in \{0;1;2;3;\dots\}$

$$3x \equiv -2 \equiv 6 \pmod{4} \quad -2 + 4(2) = 6$$

$$x \equiv 2$$



APPENDIX I9
ACTIVITY 7: SOLUTION

1.

Omskrywing	Berekeninge
Skryf die boodskap neer	DOOR
Skryf nou elke letter se waarde neer	D = 2; O = 6; O = 6; R = 7
Verhef nou elke waarde tot die mag van $E (= 3)$	$2^3 = 8$; $6^3 = 216$; $6^3 = 216$; $7^3 = 343$
Bereken die waardes hierbo vir $\text{mod } m (= 10)$	8 6 6 3
Skryf nou die ooreenstemmende letters vir die waardes neer	S O O E
Die word DOOR verander dus in	SOOE

2.

Omskrywing	Berekeninge
Skryf die geheime boodskap neer	SOOE
Skryf nou elke letter se waarde neer	8 6 6 3
Verhef nou elke waarde tot die mag van $D (= 7)$	$8^7 = 2097152$; $6^7 = 279936$; $6^7 = 279936$; $3^7 = 2187$
Bereken die waardes hierbo vir $\text{mod } m (= 10)$	2 6 6 7
Skryf nou die ooreenstemmende letters vir die waardes neer	DOOR

3.

Omskrywing	Berekeninge
Skryf die geheime boodskap neer	$NRDT$
Skryf nou elke letter se waarde neer	5 7 2 9
Verhef nou elke waarde tot die mag van $D (= 7)$	$5^7 = 78125$; $7^7 = 823543$; $2^7 = 128$; $9^7 = 4782969$
Bereken die waardes hierbo vir $\text{mod } m (= 10)$	5 3 8 9
Skryf nou die ooreenstemmende letters vir die waardes neer	NEST

4. A cryptanalyst with an understanding of the RSA will attempt to find factors for m . With m known it is possible to compute $A = (p - 1)(q - 1)$. It has been conjectured that breaking the RSA is equivalent to factoring m . For the RSA cryptosystem to be secure, it is necessary that $m = p \times q$ must be large enough that factoring it will be computationally infeasible. Current factoring algorithms are able to factor numbers having up to 130 decimal digits. To be on the safe side choose p and q such that each have at least 100 digits – then m will have 200 digits.

APPENDIX J
SECOND DESIGN RESEARCH CYCLE: ACTIVITIES
ENGLISH VERSION (FRONT PAGE)

SECOND DESIGN RESEARCH CYCLE

TOPIC: CRYPTOLOGY



ACTIVITIES

ENGLISH VERSION

APPENDIX J1

CONTENTS

INTRODUCTION

ACTIVITY 1: TRANSPOSITION CIPHERS: OVERVIEW

ACTIVITY 1: SPARTAN SCYTALE

ACTIVITY 2: ALBERTI CIPHERS: OVERVIEW

ACTIVITY 2: ALBERTI DISK

ACTIVITY 3: ADDITIVE CIPHERS: OVERVIEW

ACTIVITY 3: CAESAR CIPHER

ACTIVITY 4: FUNCTION CIPHERS: OVERVIEW

ACTIVITY 4: FUNCTION CIPHER

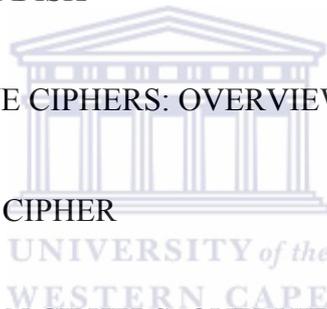
ACTIVITY 5: AFFINE CIPHERS: OVERVIEW

ACTIVITY 5: AFFINE CIPHER

ACTIVITY 6: NUMBER THEORY: OVERVIEW

ACTIVITY 6: NUMBER THEORY

ACTIVITY 7: RSA CIPHER: OVERVIEW



ACTIVITY 7: RSA CIPHER

APPENDIX J2 **INTRODUCTION**

The activity booklet for learners consists of seven activities. One of the aims of the activities is to introduce learners to some of the ciphers within the topic of cryptology. A further aim is to introduce learners to the workings of enciphering (encoding) and deciphering (decoding). In this way they get exposure to the how the cryptosystem within cryptology works. There is also an introduction to number theory and the solution of simple equations with modular mathematics. The booklet concludes with an activity on the RSA cipher.

Each activity tries to explore one specific cipher in cryptology and at times it extends into various directions of number theory and some related school mathematics topics. There will be no formal teaching during these sessions. It is expected that learners develop the required knowledge needed and use previously acquired knowledge to work out the examples. Where problems come up, there could be input by the researcher. This will be done by way of remarks or comments to facilitate them getting going again.

All sessions will be video recorded and observations and field notes will be kept where necessary. Each activity is introduced by a short overview to explain what the activity is all about. An activity is planned to be completed in the space of 45 minutes. More time will be allowed if needed. Learners are allowed to work in groups. Each group is expected to hand in their work at the end of the 45-minute session. All calculations (written work) must be shown on the given pages. Learners will be allowed to use their scientific calculators.

It is important to note that the booklet is aimed at grade 10 learners. The implementation for the second design research cycle will only be done with these learners. Messages used in the activities were kept short and where possible relevant within the experiences of learners.

APPENDIX J3
TRANSPOSITION CIPHERS: OVERVIEW

ACTIVITY

1

**TRANSPOSITION
CIPHERS**

OVERVIEW

Learners are introduced to transposition ciphers of the sort in which letters in a word change positions. Working in groups they explore the Scytale, a batten that was carried by soldiers in the Persian-Greece war in 1200. They use a given batten and paper to construct a message to see how the apparatus was utilised during this war. Groups then interchange their respective messages to decode the other group's message. They then have to use the insights and knowledge gained to decipher a given message. Their solution must include an explanation of how they actually decoded the message.

APPENDIX J4

ACTIVITY 1: SPARTAN SCYTALE

INTRODUCTION

The Spartan government sent messages to its generals on the war front in the following way. Sender and receiver each had a cylindrical rod (batten), called a *scytale* (pronounced *si'-ta-lee*), of exactly the same radius. The sender wrapped a narrow strip of parchment around the batten (see figure below), then wrote a message line by line parallel to the batten's axis. Successive letters went on successive turns of the parchment. A messenger then carried the strip of parchment and handed it over to the intended receiver.

1. Around the batten we have a message prepared on a parchment.



- 1.1 How many turns do we have for the parchment around the batten?
- 1.2 Write down the message that was send.
- 1.3 Write down the message, as it appears wrapped around the batten.
- 1.5 Write down the form the message will have on the parchment after being unwrapped from the batten.

APPENDIX J5
ALBERTI CIPHERS: OVERVIEW

ACTIVITY
2

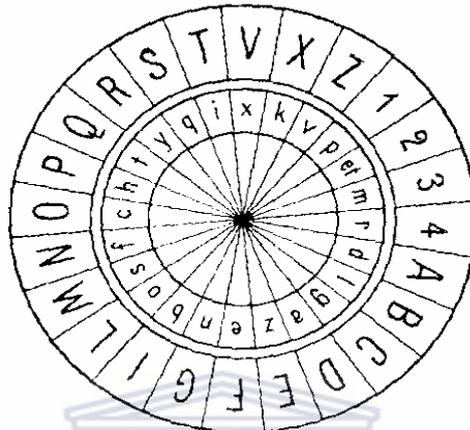
ALBERTI
CIPHERS

OVERVIEW

Activity 2 introduces learners to an Alberti cipher aided by an Alberti Disk. An Alberti disk introduces the addition or subtraction cipher. This is aimed at introducing learners to this cipher to further enhance the workings of enciphering and deciphering of messages by way of problems in a practical context.

APPENDIX J6
ACTIVITY 2: ALBERTI DISK

ALBERTI DISK



The outer ring of the disk (Capital letters) is fixed and can't turn. This ring contains the letters for the plaintext alphabet.

The inner ring (small letters) can rotate around the axis. This ring indicates corresponding letters for secret messages.

1. DISK ALIGNMENT: ***Fk***

Complete the Alberti Alphabet

A	B	C	D	E	F	G	I	L	M	N	O
					k						
P	Q	R	S	T	V	X	Z	1	2	3	4

2. Use the Alberti disk and show how the words in the following message change for the respective disk alignments:

ALBERTI WAS AN ITALIAN

WORD	DISK ALIGNMENT	SECRET WORD
ALBERTI	Fk	
W*AS	Vk	
AN	Qk	
ITALIAN	Mk	

***W is replaced by Double V**

3. Now explain how you went about to read letters from the inner ring for each disk alignment.

- 3.9 Fk
- 3.10 Vk
- 3.11 Qk
- 3.12 Mk



APPENDIX J7
ADDITIVE CIPHERS: OVERVIEW

ACTIVITY
3

**ADDITIVE
CIPHERS**

OVERVIEW

Additive ciphers are an introduction to the shifting of letters of the alphabet a certain number of positions. The activity is introduced with the Caesar cipher (shift 3). Examples include bigger shifts and later conclude with the decoding of messages given the shift and when the shift is not given. The aim of the activity is to introduce working with numbers outside of the ordinary alphabet number values.

APPENDIX J8
ACTIVITY 3: CAESAR CIPHER

Gaius Julius Caesar (100 B.C. – 44 B.C.) was a general and politician from Rome. In order to keep messages to his troops secret he changed A into D, B into E, C into F, etc. He thus employed the rule *LETTER* + 3 to change a plaintext message into a secret message.

<i>Letter</i>	A	B	C	D	E	F	G	H	I	J	K	L	M
<i>Value</i>	0	1	2	3	4	5	6	7	8	9	10	11	12
<i>Letter</i>	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
<i>Value</i>	13	14	15	16	17	18	19	20	21	22	23	24	25

Use the table above for the following examples

9. Show how the message below will change with Caesar's rule.

Message: THIS IS A SHIFT THREE CIPHER

Rule: *LETTER* + 3

10. A message prepared with Caesar's rule changed into the following secret message. Determine the original message.

Secret Message: ZHKDYHWRZRUN

11. The message LDGZWPGS was intercepted by your group. On investigation it was found that a Rule: *LETTER* + ? was employed to change the message. Determine the plaintext message.

12. Now explain the advantages/disadvantages between Caesar's rule and the rule used in 3 to render a message intelligible. What happens if the value used in the rule is larger than 25?

APPENDIX J9
FUNCTION CIPHERS: OVERVIEW

ACTIVITY

4

**FUNCTION
CIPHERS**

OVERVIEW

The function is an important concept within school mathematics. This activity introduces enciphering and deciphering by way of functional notation. An important extension here is the introduction of the null cipher where no changes occur when enciphering or deciphering.

APPENDIX J10
ACTIVITY 4: FUNCTION CIPHER

In table 1 below the values for x and $f(x)$ is given.

X	A	B	C	D	E	F	G	H	I	J	K	L	M
$f(x)$	C	J	Q	X	E	L	S	Z	G	W	U	B	I
x	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$f(x)$	P	W	D	K	R	Y	F	M	T	A	H	O	V

Table 1

1.8 Evaluate $f(B)$ and $f(T)$.

1.9 Determine x for $f(x) = M$ en $f(x) = X$.

1.10 For which value(s) of x is $f(x) = x$?

1.11 In table 2 below values for the respective letters of the alphabet are given.

$F(x)$ used in table 1 is given as: $f(x) = m x + n$, with m and n positive numbers. Now determine the values for m and n to establish the rule employed to change x into $f(x)$ for table 1.

X	A	B	C	D	E	F	G	H	I	J	K	L	M
V_x	0	1	2	3	4	5	6	7	8	9	10	11	12
x	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
V_x	13	14	15	16	17	18	19	20	21	22	23	24	25

V : Value

Table 2

APPENDIX J11
AFFINE CIPHERS: OVERVIEW

ACTIVITY
5

**AFFINE
CIPHERS**

OVERVIEW

Affine ciphers use two mathematical operations, namely multiplication and addition. The key or rule takes the form $ax + b$, where a , b can take on any positive value. The work on multiplicative ciphers is applied for formulating linear equation examples with respect to two unknowns. Examples on decoding conclude the activity.

APPENDIX J12
ACTIVITY 5: AFFINE CIPHER

<i>Letter</i>	A	B	C	D	E	F	G	H	I	J	K	L	M
<i>Value</i>	0	1	2	3	4	5	6	7	8	9	10	11	12
<i>Letter</i>	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
<i>Value</i>	13	14	15	16	17	18	19	20	21	22	23	24	25

The given table with values for the letters of the alphabet is used for all the examples that follow. The following general rules apply to all problems.

- (A) Pair off letters in a message in two's.
- (B) If a message contains an uneven number of letters, the last letter in the message is repeated to ensure two letters per pair.
- (C) The first letter of a pair is referred to as *First Letter* and the second letter of a pair as the *Second Letter*.

1. To change a plaintext message into a secret form the following rules were used to change each letter of a pair:

Rule for changing the first letter of a pair:

$$2 \times \text{First Letter} + \text{Second Letter}$$

Rule for changing the second letter of a pair:

$$\text{First Letter} + \text{Second Letter}$$

Plaintext message: *MATHS IS FUN*

- 1.5 Use the two rules to show how *MA* changes into *YM*.

- 1.6 Determine the remainder of the secret message.

2. Use the given rules below to determine the secret message for *PRISON BREAK*.

Rule for changing the first letter of a pair:

$$3 \times \text{First Letter} + \text{Second Letter}$$

Rule for changing the second letter of a pair:

$$4 \times \text{First Letter} + 3 \times \text{Second Letter}$$

3. A plaintext message changed into the secret form of *SK* with the rules below:

Rule for changing the first letter of a pair:

$$2 \times \textit{First Letter} + \textit{Second Letter}$$

Rule for changing the second letter of a pair:

$$3 \times \textit{First Letter} + 2 \times \textit{Second Letter}$$

Show that the plaintext message was *AS*.

4. A plaintext message changed into *BKWKGSGN* with the use of the following rules:

Rule for changing the first letter of a pair:

$$\textit{First Letter} + 2 \times \textit{Second Letter}$$

Rule for changing the second letter of a pair:

$$\textit{First Letter} + \textit{Second Letter}$$

Determine the plaintext message.



APPENDIX J13
NUMBER THEORY: OVERVIEW

ACTIVITY
6

NUMBER THEORY

OVERVIEW

Up to now learners unknowingly used number theory to solve problems. They are introduced to solve problems of the type $ax \equiv 1 \pmod{b}$ where a and b are positive numbers. This will be helpful for the last activity where an example of the RSA cipher is introduced.

APPENDIX J14
ACTIVITY 6: NUMBER THEORY

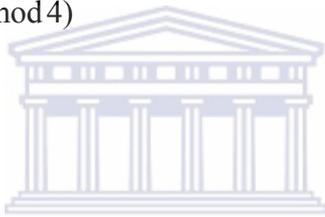
INTRODUCTION

Two integers a and b is said to be *congruent*(mod n) if $a \equiv b(\text{mod } n)$. It means a and b will have the same remainder on division by n . For example:

$$25 \equiv 13 \equiv 1(\text{mod } 6).$$

1. Complete the following. Show the remainder for each case.

1.1 $9 \equiv \dots \equiv \dots \equiv \dots(\text{mod } 4)$



UNIVERSITY of the
WESTERN CAPE

1.2 $17 \equiv \dots \equiv \dots \equiv \dots(\text{mod } 3)$

1.3 $29 \equiv \dots \equiv \dots \equiv \dots(\text{mod } 12)$

2. Now solve each of the following equations. Show all calculations.

2.1 $5x \equiv 1 \pmod{3}$

2.2 $3x \equiv 1 \pmod{7}$

2.3 $5x \equiv 1 \pmod{15}$

2.4 $2x \equiv 3 \pmod{11}$

2.5 $2x \equiv -1 \pmod{13}$

2.6 $3x \equiv -2 \pmod{4}$



APPENDIX J15
RSA CIPHER: OVERVIEW

ACTIVITY
7

RSA CIPHER

OVERVIEW

Activity 7 introduces the workings of the RSA cipher. Furthermore, learners work with number theory introduced in Activity 6. Work for number theory focuses on determining the remainder on division by a certain number.

UNIVERSITY of the
WESTERN CAPE

APPENDIX J16
ACTIVITY 7: RSA CIPHER

The RSA was developed by Rivest, Shamir and Adleman. Their main aim was to make it as difficult possible for persons to decipher a secret message. In order to do so, they established the following rules:

Nr	Rule	Example
1.	Choose any two prime numbers p en q	$p = 2$ en $q = 5$
2.	Let $m = p \times q$	$m = 2 \times 5 = 10$
3.	Let $A = ((p - 1) \times (q - 1))$	$A = 1 \times 4 = 4$
4.	Choose a number E , smaller than A with no factors common with A	$E = 3$
5.	Find a number D such that $(E \times D) - 1$ is a multiple of A	$D = 7$
<p>$E (= 3)$ and $m (= 10)$ are the values known to the public</p> <p>E is the value used to encode a plaintext message into a secret message</p> <p>m is the value used with <i>mod 10</i> to determine the remainder on division by 10</p> <p>$D (= 7)$ is used to decode a secret message into a plaintext message</p> <p>The value of D is not known to all.</p>		

1. The RSA cipher is now used to change the word *DOOR* into a secret message. We use a shortened version of an alphabet of letters with their respective values.

Letter	A	D	E	H	N	O	R	S	T
Value	1	2	3	4	5	6	7	8	9

Description	Calculations
Write down the plaintext message	
Write down the values for the letters	
Raise each value to the power of E $E (= 3)$	
Determine the values calculated for $\text{mod } m (= 10)$	
Write down the corresponding letters for the calculated values	
The word DOOR thus changes into	

Calculations:

2. In order to get the plaintext message from a secret message the following is recommended. We use the secret message obtained from the word DOOR to show how it changes back into DOOR.

Description	Calculations
Write down the secret message	
Write down the corresponding values for each letter	
Raise each value to the power of $D (= 7)$	
Determine the values above for $\text{mod } m (= 10)$	
Write down the corresponding letters for the respective values	

Calculations:



3. Do the following example. Use the same values for D en m as above.

Secret Message	Plaintext Message
<i>NRDT</i>	

Calculations:

4. Now discuss the following: How can the RSA cipher be used to make it so difficult possible for a person to decipher an intercepted message although the values of E and m are known.



APPENDIX K
TRANSLATION FOR FIGURE 3.5

