An Investigation into the Security of Machine Ciphers

By
Sarah Masood
2010-NUST-MS-CCS-21

Supervisor
Dr. Syed Ali Haider
Department of Computing

A thesis submitted in partial fulfillment of the requirements for the degree of Masters in Computer and Communication Security (MS CCS)

In
School of Electrical Engineering and Computer Science,
National University of Sciences and Technology (NUST),
Islamabad, Pakistan.

(August, 2014)

Approval

It is certified that the contents and form of the thesis entitled "**An Investigation into the Security of Machine Ciphers**" submitted by **Sarah Masood** have been found satisfactory for the requirement of the degree.

Advisor: **Dr. Syed Ali Haider**

Signature: ____________________

Date: ____________________

Committee Member 1: **Dr. Zahid Anwar**

Signature: ____________________
Date: ____________________

Committee Member 2: **Dr. Sohail Iqbal**

Signature: ____________________
Date: ____________________

Committee Member 3: **Mr. Waleed bin Shahid**

Signature: ____________________
Date: ____________________

Certificate of Originality

I hereby declare that this submission titled **An Investigation into the Security of Machine Ciphers** is my own work.To the best of my knowledge it contains no materials previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any degree or diploma at NUST SEECS or at any other educational institute, except where due acknowledgement has been made in the thesis. Any contribution made to the research by others, with whom I have worked at NUST SEECS or elsewhere, is explicitly acknowledged in the thesis.

I also declare that the intellectual content of this thesis is the product of my own work, except for the assistance from others in the project's design and conception or in style, presentation and linguistics which has been acknowledged. I also verified the originality of contents through plagiarism software.

Author Name: **Sarah Masood**
Signature: ____________________

Abstract

The history of classical ciphers is well documented with a lot of material available on their cryptanalysis. The modern ciphers are also being well researched. Due to the evolution of machine ciphers in a sensitive era involving the First and the Second World War, they are fairly less explored. Although publications are available on their analysis by experts, however, a lot of them are still kept confidential in the NSA archives. This thesis presents an insight of the two types of cipher machines, covering their operation and cryptanalysis under black-box conditions. Rotor is a scrambling device which gives rise to different permutations when rotated. A combination of rotors with varying rate of rotation owes to the security of rotor machines. The permutations produced by a rotor follow a pattern that is unique for a single rotor. This research presents an approach to mathematically link these patterns to recover the wiring of an unknown rotor. Given a stack of rotors with each rotor giving rise to a unique but related permutation, theory of permutations can be applied in a similar way to recover the unknown wiring. A one and a half rotor machine is designed as it presents the simplest model for a reciprocal rotor machine. A detailed account of the application of this technique to a one and a half rotor machine is given using only ciphertext. This approach is extended to a two and a half rotor machine. Finally, the method is applied to cryptanalyze the famous Enigma machine. Unlike the rotor machines, where the input is substituted by another alphabet based on its position in the plaintext, in pinwheel cipher the input is relatively shifted by an amount determined by the displacement count of lug cage at that position. The underlying plaintext exhibits certain properties as far as the frequency distribution of alphabets is concerned. The number of shift values vary depending on the complexity of the pinwheel cipher. The statistical properties of the underlying plaintext are utilized to divide the ciphertext into smaller number of groups in order to recover the pinwheels. As with the case of rotor machines, a small variant of the pinwheel cipher is first investigated. The approach is extended to a variant of M-209 cipher machine which has 6 wheels having lengths that are relatively prime. The techniques employed are compared with already known techniques and further areas of research are also highlighted.

Acknowledgment

It feel extremely blessed and owe my gratitude to a lot of people on this achievement. Firstly, I want to thank my mentor, Dr. Fauzan Mirza, for introducing me to Cryptology. When it comes to code-breaking, I think we share the same enthusiasm. I am grateful that he not only provided me the opportunity to explore the field that intrigued me, but also for his continuous support and motivation throughout the thesis phase. There were times when he believed in me, more so, than I did myself. His sense of patience and the effort that he took to make this research interesting for me deserves a lot of praise. I do not have enough words to thank him so all I can say is that I wish to pursue for PhD after this and InshAllah when the day comes, I know who I will be dedicating that dissertation to.

I am extremely grateful to Dr. Syed Ali Haider who is not only being a wonderful advisor but also a great person. I could not have asked for a better substitute after Dr. Fauzan left. His instant involvement in the work I had done, positive attitude, critique, and willingness to help was quite encouraging for me as a student and kept me focused.

I also want to acknowledge the efforts of my GEC members, Dr. Zahid Anwar and Dr. Sohail Iqbal; their valuable comments and feedback always provided me the opportunity to improve. Last but not least, I give it to the Principal, Dr. Arshad Ali and the HoD, Dr. Sharifullah Khan for facilitating me in every possible way due to which I was able to finish my thesis.

Sarah Masood

Dedicated to my loving parents for going out of the way in every matter that entrusts my happiness

…and to my sister, Kiran, for providing a great sibling support!

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Evolution of Cryptography

Cryptography has undergone tremendous evolution over time with the primary purpose of providing confidentiality to sensitive information and for data privacy. With the advancement in technology and increasing demand of security, pen and paper ciphers were gradually replaced with machine ciphers and this trend shifted to digital ciphers in the 70's. The advancement of cipher technology through history is closely followed by the development of code-breaking technology. The nations skilled in cryptanalysis enjoyed a huge advantage on the battlefield which led to a direct impact on the course of history [1].

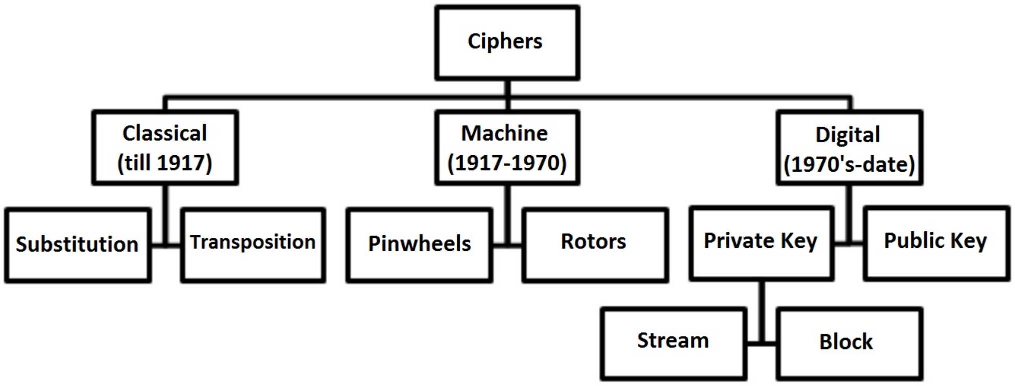


Figure 1.1: Hierarchical Representation of Ages of Cryptography

1.2 Motivation

1.2.1 Historical Perspective

Cipher machines, despite going out of use, still attract a lot of researchers who are into the social and technical aspects of historical cryptography. With the advent of the First World War, and the induction of capable mathematicians and cryptanalysts into military and intelligence departments, the pen and paper techniques were rendered impractical. It was then when the need for strong and resilient cryptosystems was truly realized. A variety of mechanical and electromechanical stream ciphers were invented which allowed the military to carry out secret communication. Among the famous cipher machines include the Enigma, M-209, M-94, SIGABA, PURPLE and NeMa. Details of their history and operation can be easily found online. Enigma machine was used by the Germans during World War II. It suffered a bad fate and was broken by the Polish, and later by the British and Americans. M-209 and SIGABA was used by the American forces. Japanese used the PURPLE machine while NeMa was used by the Swiss. William Friedman, Solomon Kullback, Marian Rejewski, and Alan Turing are some of the famous cryptanalysts of this era.

In the early 70s, the spread of digital computers rendered these machines obsolete and their use and production was ultimately discontinued. They were succeeded first by shift registers and then block ciphers. The machine ciphers have now become valuable collectable items for those having interest in cryptology.

1.2.2 Relative lack of Literature

Detailed studies have been carried out on various classical ciphers and their cryptanalysis. The techniques employed are thoroughly discussed and well documented. Likewise, the evolving modern ciphers are also cryptanalyzed with new techniques being regularly developed and published. A substantial amount of material can be found to analyze any system from these two periods. However, a similar exercise for machine ciphers would yield considerably fewer publications.

The reason for this is that classical ciphers were used in World War I, and they were also broken. Subsequently, the ciphers that were designed and used for military purpose were not pencil-and-paper based; they were essentially mechanical or electrical-mechanical devices. Furthermore, any analysis of their security was classified as top secret. Hence, there was an effective *"black hole"* of knowledge concerning these systems until the 1970's, when some analysis was published (by hobbyists). Detailed analysis of these systems remained classified for decades, even after digital ciphers and computers were widely used, and machine ciphers were practically obsolete.

The NSA website keeps a list of documents declassified at various times and released to National Archives and Records Administration (NARA) [2] . However, there is still a lot of secret research that exists. The documents available at the National Archives are mostly only for study purposes and can not be duplicated or distributed, hence limiting their availability. An index of papers published in the NSA Technical Journal (from 1956-1980) was declassified and published online, and papers are listed in this which directly concern cryptanalysis of machine ciphers [3]; however, many of those papers are still classified and modern cryptology research has changed direction entirely, with very little or no research published on machine ciphers. For example, Military Cryptanalysis was published in six volumes between 1957 and 1977. Its last two volumes are still classified. Of these, volume 6 is based on the solution of cipher machines. Another excellent example to illustrate the significance of this problem is that a report on the cryptographic security of the Hebern Cipher Machine written by William Friedman in 1935, titled *"Analysis of a Mechanico-Electrical Cryptograph"* is still not available in un-redacted form; this paper is available in the US National Archives, but it is heavily redacted, so that most of the interesting analysis of this machine is not public. In 1978, James Reeds, Dennis Ritchie and Robert Morris submitted a paper to Cryptologia titled *"The Hagelin Cipher Machine (M-209): Cryptanalysis from Ciphertext Alone"*, however, it was never published due to the nature of cryptanalytic technique applied [4].

1.2.3 Genetic Approach to Cryptanalysis

With the arrival of digital computers, and knowledge on operation of cipher machines made open, most of the solutions later published outside the military circle were based on genetic algorithms which required the use of a computing machine to solve these ciphers. While known mathematical techniques were employed, little research was done to invent new ones. Solutions for unknown internal settings of machines were mostly based on use of optimization algorithms such as hill-climbing and maximum-likelihood estimation (MLE).

1.3 Objective

The main objective for doing this thesis is to understand the mechanism and evolution of cryptology in the time span between classical ciphers (whose weaknesses are well known and documented) and modern digital ciphers (where most of current cryptology research is focused). The reason behind this is to obtain a better understanding of how the evolution of machine ciphers affected modern cryptology, and to also understand their weaknesses. Machine ciphers are investigated to learn what types of attacks they are susceptible to under different assumptions. Published work can be found on analysis of these machines with known internal settings, hence we have focused our research on the case when nothing is known about the cipher machine except its working or principle of operation.

1.4 Contribution

This objective defined is achieved by studying a few variations of some well-known machine ciphers, and analyzing these systems with respect to various mathematical techniques including algebraic and statistical. For rotor-based machines, a mathematical technique is devised and first applied to a one-and-a half rotor machine. The approach is then extended to cryptanalyze a two-and-a-half rotor machine and finally the Enigma cipher machine. A more statistical approach is used to cryptanalyze pinwheel ciphers. Starting from a two pinwheel machine, the technique is used to analyze a four pinwheel cipher and finally the M-209 cipher machine which contains six pinwheels. Hence, this thesis presents a fairly thorough compilation of different machine ciphers and describes some fundamental design mechanisms and weakness of such systems.

1.5 Thesis Overview

This thesis is divided into two sections presenting separate study on two kinds of cipher machines. Section 1 covers chapters from 2 till 8, while the second section includes chapters from 9 to 13. Chapter 2 sheds light on background knowledge required to understand rotor operation and reciprocal alphabets. Chapter 3 covers the literature review and chapters 4 and 5 describe the proposed methodology to attack a reciprocal rotor-based cryptosystem. Chapters 6 till 8 describe the implementation of proposed technique to a one-and-a-half rotor machine, a two-and-a-half rotor machine and finally the Enigma cipher machine. In section 2, chapter 9 discusses the operation of pinwheel ciphers in general while chapter 10 covers the literature review. The attack methodology is described in chapter 10 while the implementation examples are presented in chapter 11 and 12. Chapter 13 describes the implementation of proposed methodology to M-209 cipher machine. Results and comparison with existing literature is presented in chapter 14. Finally, the conclusion is given in chapter 15.

Chapter 2

Background on Rotor Machines

Rotor is an electro-mechanical component capable of rotation and is the basic building block of rotor-based cryptosystems.

2.1 Rotor Mechanics

2.1.1 Rotor Construction

Rotor is an alphabetical disk with electrical contacts on both sides. The internal wiring of the rotor connects the input contacts to a set of different output contacts on the other side. The electrical interface is thus responsible for encryption. The outer circumference has toothed edges which interact with the geared mechanism inside the rotor assembly; hence, causing the rotor to turn. In 2.1, the inner dark gray ring contains the electrical contacts arranged in a ring and wired to the other side. The outer ring has toothed edges to allow rotation about the central hole [5].

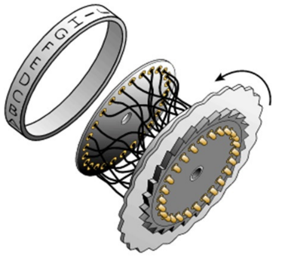


Figure 2.1: A Disassembled Generic Rotor

2.2 Rotor Mathematics

2.2.1 Rotor Encryption

For a fixed position, a rotor produces monoalphabetic ciphertext. When the rotor is turned, the wiring remains the same but the relative position of the incoming letter is changed, which results in producing a different cipher alphabet each time [6]. Figure 2.2 shows the mechanics of a single rotor having an alphabet size of 6 whose permutation is denoted in cycle notation as (EBA)(CFD). After each turn the ciphertext mapping changes and is recorded in a table. Cycles are formed between consecutive rows of permutations and have the same distribution of cycle lengths. Table 14.1 which is derived from a rotor exhibits certain mathematical properties that are useful in cryptanalysis. These properties will be discussed in detail in Chapter 5.

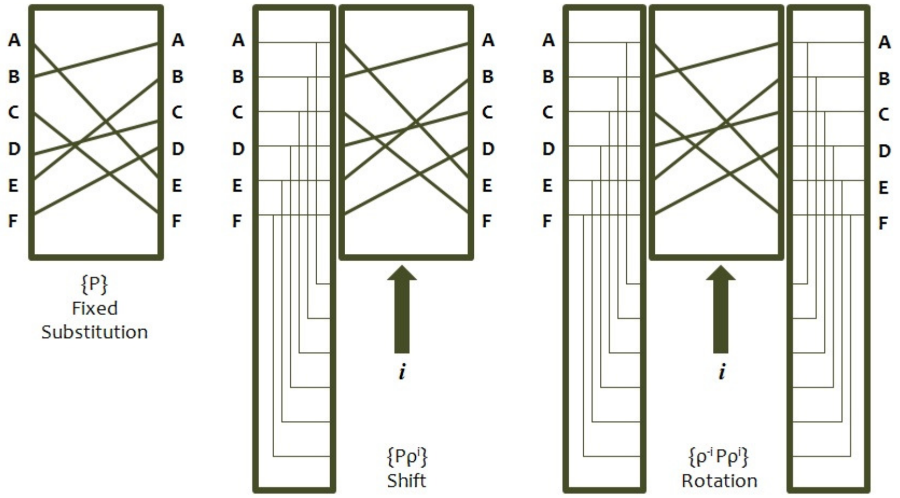


Figure 2.2: Mechanics of Rotor; Fixed, Shifted and Rotated Alphabets

Table 2.1: Rotor Table for a 6 Alphabet Rotor

Ciphertext	Plaintext						
A	E	A	F	C	B	D	
B	F	E	B	A	C	D	
C	D	A	F	B	C	E	
D	F	E	A	B	D	C	
E	D	F	A	C	B	E	
F	E F	F	B	A	D	C	[0.5ex] height

Rotor encryption is a substitution function which involves the current state of the rotor. Let X = (ABCDEF) be the 6 letter alphabet and R be the fixed substitution function of rotor. This is a one-to-one function from X to X and is assumed to be R = (EAFCBD). If i is the current state of the rotor, then the output function Y is represented by 2.1

$$Y_i = Xp^i Rp^{-i} \tag{2.1}$$

where p^i is the circular shift which is represented by modulo6 addition (in this case). If i=2 is the initial state of the rotor, then the input string 'DEAF' is encrypted to

'BDDC'. The step-by-step procedure is tabulated and given in Table 2.2

Table 2.2: Encryption Example for a 6 Alphabet Rotor Machine

X	:	i	p^i	R	p^{-i}	:	Y
D	:	2	F	D	B	:	B
E	:	3	B	A	D	:	D
A	:	4	E	B	D	:	D
F	:	5	E	B	C	:	C

The decryption equation (2.2 is similar to encryption except that it requires the inverse of rotor R.

$$X = Y_i p^i R^{-1} p^{-i} \tag{2.2}$$

The inverse of rotor R is R^{-1} = (BEDFAC). The decryption process is demonstated using the same encrypted string from previous example. The results are given in Table 2.3

Table 2.3: Decryption Example for a 6 Alphabet Rotor Machine

Y_i	:	i	p^i	R^{-1}	p^{-i}	:	X
B	:	2	D	F	D	:	D
D	:	3	A	B	E	:	E
D	:	4	B	E	A	:	A
C	:	5	B	E	F	:	F

2.2.2 Multi-Rotor Cryptosystems

Although a single rotor is capable of generating a multitude of substitution alphabets, however, its security is only limited due its short period which is equal to the alphabet size of the rotor. If we consider a rotor of size 26, it will only be secure enough to send messages of lengths less than 26. One of the reasons why classical ciphers were rendered obsolete was due to their short period and hence low security. After the First World War, the trend in cryptography took a big shift. Cryptographic machines were developed to automate the process of encryption and to render the old cryptanalytic techniques useless by having practically large key space. A combination of rotors with varying rate of rotation owes to the security of rotor machines.

To maximize the period, all rotors are not turned simultaneously. Most of the rotor machines involved the movement of one rotor at every state. The next rotor turned only after a complete rotation of the previous rotor, or once in between as in the case of Enigma cipher machine. With this rotation scheme, the period of the cipher machine was equal to the Nth power of 26 where N was equal to the number of rotors employed in the cryptosystem. Hence, the maximum period of the multi-rotor system shown in Figure 2.3 is 26^3.

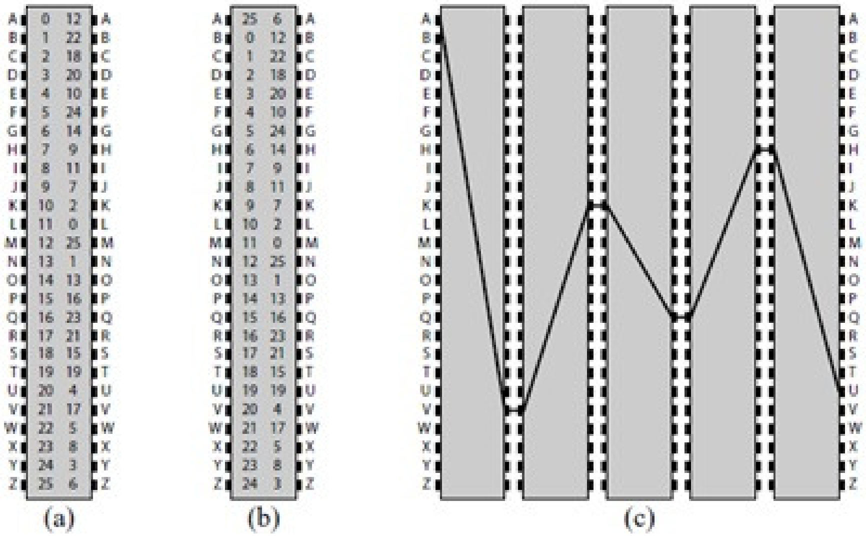


Figure 2.3: Multiple Rotor Cryptosystem (Current Path)

2.3 Friedman Squares

The alphabets produced by a single rotor in its various starting positions can be represented in the form of a table similar to a Vigenere Table. Such a table, for a rotor, is called a Friedman Square [7]. Table 3.1 shows a Friedman square generated by a rotor.

This table like the Vigenere or the Beaufort table also has regularity, although, it is less obvious. A Vigenere table consists of standard shifted alphabets running across its rows. In a rotor table, shifted standard alphabets run across the diagonal. For polyalphabetic ciphers, in which secondary alphabets are produced by shifting mixed-alphabet slides, a powerful cryptanalytic technique called "symmetry of position" is used.

2.3.1 Properties of Friedman Squares

2.3.1.1 Symmetry of Position

Consider the first four rows of a shift cipher which uses mixed alphabets.

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

Symmetry of position can be used in this case to recover the mixed cipher sequence. Assume that we know A and B are mapped onto V and D in one position and to O and H in the other. This suggests that V and D are separated by the same distance as O and H in the mixed sequence. Moreover, this displacement is equal to the distance between A and B which is 1. This technique is called symmetry of position.

Table 2.4: A Friedman Square

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

In rotor machine, the same principle can be applied but it requires a little modification. Since the rotor moves by one position between the alphabets, therefore, this rotation has to be compensated in the analysis. Hence, the comparison would be between A and B in first position which after one turn will be translated to Z and A. From Table

2.3.1.2 Frequency Analysis

A rotor produces a stream of polyalphabetically enciphered text. We will turn our focus to one element in the first row (*say M*). Table 3.1 maps M onto Z in this position. The subsequent encryptions which run down this diagonal are given in Table 2.5.

If some plaintext is encrypted using this rotor and the ciphertext is arranged in 26 columns then each column consists of monoalphabetically enciphered text. If we take the frequency count of letter Z in the column which corresponds to position A of the rotor, the count of letter Y in the next column, the count of letter X in the column after that and so on, then the distribution sampled in this manner will be monoalphabetic and will have an index of coincidence equal to 0.066. Although each column can be evaluated separately but for shorter messages, the frequency distribution is rather flat.

Table 2.5: A Diagonal from Friedman Square

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

If the aforementioned process is carried out using all alphabets, then we will have 26 monoalphabetic distributions. These distributions can be combined by adding proper shift to give one monoalphabetic distribution which can be evaluated using frequency analysis [8].

2.4 Reciprocal Alphabets

2.4.1 Reflecting Rotors

Reflecting rotors belong to a special class of rotors called *"reflectors"*. A reflecting rotor is defined by an involution function which is its own inverse. Reflector gives the property of reciprocity to the machine. It brought flexibility to the use of cipher machines as there was no need to have a separate mode for encryption and decryption. Enigma is a famous cipher machine that employed a reflecting rotor.

Consider a reflecting rotor of size 6 denoted as Q = (EDFBAC). Using the same string "DEAF" as given in Section 2.2 and a rotor starting position of i=2, the ciphertext is given in Table 2.6

The decryption process is similar to encryption as Q^{-1} = Q.

Table 2.6: Rotor Table for a Reflector

X	:	i	p^i	Q	p^{-i}	:	Y
D	:	2	F	C	A	:	A
E	:	3	B	D	A	:	A
A	:	4	E	A	C	:	C
F	:	5	E	A	A	:	A

Although the use of a reflecting component brings flexibility, however, it reduces the period of a cipher from its theoretical maximum value. The total number of permutations for a rotor of length N is N! which includes the possibilities where a letter can be mapped onto itself. Reflectors reduce this number and the total permutations in this case are given by a special permutation used in combinatorial mathematics called *"derangements"* which is denoted by *!N*. The relation between a factorial and derangement is given in Equation 2.3.

$$!N = \frac{N!}{e}, \quad whereN > 1 \tag{2.3}$$

Hence, the total permutations are almost reduced by a factor of 3. This reduction can be overcome by an added rotor in the assembly. However, the restrictions on the encrypted output can make the analysis easier with a known plaintext attack since some of the positions will be ruled out.

2.4.2 Analyzing Reciprocal Alphabets

As the name implies, reciprocal alphabet is an alphabet whose mapping is an involution function. For example, if $A_p = B_c$ then it also requires that $B_p = A_c$. The subscripts p and c stand for plaintext and ciphertext values respectively.

The cycle notation of these permutations consist of a product of 13 disjoint cycles.

Let us consider reciprocal alphabets given in Table **??**:

If chains are constructed between the letters of sequence 1 and 2, then a new permutation is derived:

```
(LBOZSPH)(WANTEFG)(MRY)(IXJ)(QV)(DK)(U)(C)
```

Theorem: *If two permutations of the same degree consist only of disjoint transpositions, then their product contains an even number of disjoint cycles of the same length.*

There exists a relationship between these chains which will become apparent if these chains are written out such that the corresponding plaintext letter is written underneath the respective cipher values in sequences 1 and 2. This is shown in Table 2.8

Table 2.8: Reciprocal Alphabets and Differential Cryptanalysis

LBOZSPHL	WANTEFGW	MRYM	IXJI	QVQ	DKD	UU	CC
AWGFETN	BLHPSZO	IXJ	MYR	DK	QV	C	U

As observed, this process generates a pair for each chain within its set. As the chain progresses, the letters in its pair appear in the reverse order. Hence, if the chains between two cipher sequences are available they can be superimposed to recover the plaintext-ciphertext relations of alphabets 1 and 2. This approach is akin to *Differential Cryptanalysis*.

```
P :  LBOZSPH   WANTEFG   MRY   IXJ   QV   DK   U   C
C1:  AWGFETN   BLHPSZO   IJX   MYR   DK   QV   C   U

P :  LBOZSPH   WANTEFG   MRY   IXJ   QV   DK   U   C
C2:  NAWGFET   OBLHPSZ   XIJ   RMY   KD   VQ   C   U
```

Chapter 3

Literature Review on Rotor Machines

This chapter describes the related research work done on analyzing rotor machines in general. The different approaches used to cryptanalyze Enigma machine are also particularly discussed. Since each paper involves a different approach to cryptanalysis, hence, they are discussed separately.

3.1 Application of the Theory of Permutations in Breaking the Enigma Cipher

The first break into the Enigma Machine was carried out by Marian Rejewski who wrote this paper describing his approach [9]. The instruction manual and operating procedures on Enigma cipher was delivered to Rejewski by a German spy using which he derived a system of equations for the machine. He also related the corresponding equivalent letters in the message key to derive the three product permutations which consisted of paired chains. Using probable message keys he was able to recover the plain-cipher relationship for 6 consecutive positions. The system of equations derived contained a number of variables and could not be solved directly. By getting his hands on a leaked copy of the key settings, he was able to eliminate the effect of plugboard and reduce the number of variables in his system of equations. The equations were than solved simultaneously to recover the fast rotor. Since the rotor positions were changed on a daily basis, hence, he was able to recover all the rotors when they appeared in the fast rotor position [10]. Another notable contribution is the design of cryptologic bomb or the cyclometer which was made to recover the daily settings of the keys. Based on the same principle of cycle factorization, it consisted of an assembly of drums which could be arranged in any order and set against any starting position. They were used to calculate the length and number of cycles in the characteristic and to prepare a lookup table. Depending on the nature of cycles, the rotor order of the machines could be recovered [11]. Once the rotor order is determined, all messages for that day could be deciphered. On average around 80 messages were sent out each day. All this work was done prior to the invention of

British Bombe [12].

3.2 The Black Chamber: A Column how the British broke Enigma

Cipher A. Deavours gives a brief account on the functionality of the Bombe and gives an example to explain how it works [13]. Alan Turing designed the first Bombe along with Gordon Welchman who improved its efficiency by introducing the diagonal board. The high speed *"Bombes"* were constructed to aid in the process of deciphering messages by recovering the internal machines settings - the rotor order and the ring settings, and the external settings namely the message key and one plugboard setting. The purpose of Bombe was not to provide a complete solution but to reduce the number of assumptions to a manageable count.The design principle of British Bombe was different from the Polish Cryptologic Bomb. The underlying principle of the Bombes was based on using cribs which are probable words and are assumed to have occured in the ciphertext. Since Enigma was a reciprocal cipher machine, hence, many positions for the crib were automatically rejected which showed contradiction. To test a crib against a piece of ciphertext, loops were examined between the plain-cipher pairs. A menu was produced for wiring up the bomb to test the crib against ciphertext. Longer cribs and more number of loops resulted in decreased false alarms and reduced search space which could be readily analyzed [14].

3.3 Ananlysis of the Hebern Cryptograph

Cipher A. Deavours described the isomorphic property of rotor machines by using a prototype of Hebern machine as an example. Assuming that the movement of the rotors is regular, Deavours described the effect of such a movement on the cryptogram produced. If the starting position of the fast rotor is the same at the beginning of two equal plaintexts, then the resulting cryptograms are isomorphic in nature and ciphertexts corresponding to equivalent plaintext are called isomorphs. The following isomorphs have been obtained using a 3 rotor machine. The left-most rotor is the fast rotor [15].

Table 3.1: Isomorphs produced by an Enigma Machine

		Starting Position
Plaintext :	CRYPTOLOGY	
	UEIRDFAFNI	DPL
Ciphertext :	TQGSUYOYHG	DML
	ZEXIPHRHQX	DMG

An example cryptogram is solved using this principle. He described the probability of occurrence of various length isomorphs in the ciphertext and also solved a cryptogram using this principle. Isomorphs play a crucial role in the placement of probable plaintext.

3.4 Ciphertext-Only Cryptanalysis of Enigma

In this paper [16], James J. Gillogly presents a ciphertext only attack to recover the internal settings of an Enigma Machine namely the rotor order and ring settings. Additionally, the message key and plugboard is also recovered. Longer messages are solved using a different approach than short messages. For longer messages, all possible rotor combinations are tried and for each order, the message is decrypted using all possible starting positions. Rotor orders and positions corresponding to high Index of Coincidence values are stored. All possible ring settings are applied on each rotor one by one to maximize the Index of Coincidence. The recovered rotor settings are then used to decipher the message. For few connections on the plugboard, all combinations involving two letters are tried and a trigraph score is kept to find the plug settings. The success rate of the proposed technique is close to 80%. It is inferred that for shorter messages, the ring setting of the fast rotor and the message key can be recovered using 2^{64} tests, where as with 26^5 tests both ring settings can be recovered at once. An improved technique to solve messages encrypted using more cables in the plugboard is given in the paper titled *"Applying statistical language recognition techniques in the Ciphertext-Only Cryptanalysis of Enigma"* in which Heidi Williams has designed an effective statistical test to identify bigrams and unigrams in ciphertext [17].

3.5 File Security and UNIX Crypt Command

Crypt is an obsolete file encryption program in UNIX [18]. The command operates on blocks of 256 characters called cryptoblocks using a function similar to one-and-a-half rotor machine. If p_{ij} and c_{ij} are the *i-th* plaintext and ciphertext characters in *j-th* cryptoblock, then they are related by Equation 3.1.

$$c_{ij} = R^{-1}[S[R[i + p_{ij}] + j] - i \tag{3.1}$$

The addition and subtraction functions are performed using modulo256 operator. The corresponding notation using cyclic shift C_i and C_j is given in Equation **??**

$$c_{ij} = C^{-i}R^{-1}C^{-j}SC^{j}RC^{i}p_{ij} \tag{3.2}$$

$$c_{ij} = C^{-i}A_jC^{i}p_{ij} \tag{3.3}$$

where A_j is self-inverse.

Two attacks are described in the paper. The known plaintext attack involves recovery of A_j. Plaintext and corresponding ciphertexts are related to evaluate A_j. The unknown plaintext attack involves using probable plaintext and finding its placement in ciphertext that gives rise to no contradictions. Finally a ciphertext only attack is described which is based on the statistics of underlying text to partially recover A_j which is further evaluated using a technique called *knitting* that relates A_j with A_{j+1}. A secure design for the scheme is described by replacing the shift i with $f(i)$ which is equivalent to irregular rotor movement.

3.6 The Cryptanalysis of a Three Rotor Machine Using a Genetic Algorithm

This paper [19] presents a three rotor machine with an odometer-like regular stepping mechanism. The rotors are completely unknown. A Genetic Algorithm is designed to recover the fast rotor. Starting with a GA population of 50 mappings for the third rotor, in each selection the mutation function involves randomly swapping two rotor wirings and shifting a randomly selected substring of rotor wiring to a random position. During the merging process, the new solution is added to the pool if it has a better fit than the worst member of the pool. Different ciphertext lengths are used to draw conclusions. Having recovered the fast rotor, the remaining system is periodic with shift of 26x26 = 676.

3.7 Bulldozer: A Cribless Rapid Analytical Machine (RAM)

The breaking of Enigma cipher relied heavily on the use of cribs which were used in combination with *Bombes* and *Rapid Analytical Machines (RAMs).* Lee A. Gladwin describes a machine called Bulldozer which was designed to break Enigma keys without the use of cribs but it came around late when Enigma Machines were going obsolete. Like any other RAM, the purpose of *Bulldozer* was also to reduce the search space for solution to the cipher. The hypothetical machine *(Statistical Grenade)* was designed to break the Enigma cipher for which the starting positions were unknown, while the other variables were assumed to be known. Bulldozer or Statistical Bomb was designed to target Enigma Machines which had no plugboard or for which the plugboard was known such that its effect could be removed. The Statistical Bombe stopped when the results approached a rough monoalphabetic distribution [20].

Chapter 4

Attack Methodology for Rotor-based Machines

This chapter provides an in-depth knowledge on analyzing reciprocal alphabets and rotor tables. The properties of such cryptosystems are discussed in detail with the aid of examples and techniques are developed which will be used in later chapters during cryptanalysis.

4.1 Recovery of Diagonal Sequence

4.1.1 Derivation using Principle of Superposition

So far we have learnt that a rotor table consists of non-repeating alphabets in each row and shifted standard alphabets along its diagonal.

Let us take the first six rows of the rotor table given in Table 2.4

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

As we did with the reciprocal alphabets, similar chains are created between consecutive rows of this table.

Table 4.1: Chains formed using a Friedman Square

```
1-2: (HUFLQBMDEJNZTWYKAS)(XGPRVO)(I)(C)
2-3: (GTEKPALCDIMYSVXJZR)(UNWFOQ)(H)(B)
3-4: (QFSDJOZKBCHLXRUWIY)(TMVENP)(G)(A)
```

New chains can be constructed using the available chains in table 4.1. From the chains already given, 1-3 and 2-4 can be constructed. The elements derived from the common middle row are omitted. For example, (1-(2-2)-3) shows that the factor of second row is eliminated to construct 1-3.

```
1-3: H(U)N(Z)R(V)X(G)T(W)F(L)C(C)D(E)K(A)L(Q)U(F)O(X)J
     (N)W(Y)S(H)H, B(M)Y(K)P(R)G(P)A(S)V(O)Q(B), M(D)I,
     E(J)Z(T),
1-3: (HNRXTFCDKLUOJWS)(BYPGAVQ)(MI)(EZ)
```

Similarly, the chain 2-4 is derived from (2-(3-3)-4)

```
2-4: (GMQWSEBCJKTNIVR)(UPAXOFZ)(HL)(YD)
```

It is observed that pairs of consecutive rows or rows separated by same shift value give rise to chains that match in terms of length. This property is exhibited by all rotors and rotor assemblies that involve the movement of only one rotor between these consecutive rows. The reason for the existence of this property is the diagonal sequence which monoalphabetically relates pairs of letters which occur in consecutive columns. If we study the Rotor Tableau, we will notice that every pair of vertical letters has a corresponding monoalphabetically related pair situated diagonally to the left. Hence, the corresponding pairs of HU, UF and FL in 2-3 are GT, TE and EK.

The chains can be superimposed correctly to recover the diagonal sequence. If a minimum of three such chains are available then the diagonal sequence can be uniquely determined.

Instead, if we are given only the chains in table 4.1, there are a number of ways in which they can be superimposed. The correct superposition between consecutive chains will result in the recovery of diagonal sequence. Let us assume the chains in 1-2 ans 2-3 are superimposed as $\frac{I}{B}$ and $\frac{C}{H}$. This would imply that the chains in 2-3 and 3-4 should be superimposed $\frac{GTEKPALCDIMYSVXJZR}{DJOZKBCHLXRUWIYQFS}$ which is inconsistent with our assumption. Hence, the correct superposition is $\frac{I}{H}$ and $\frac{C}{B}$. This implies $\frac{GTEKPALCDIMYSVXJZR}{FSDJOZKBCHLXRUWIYQ}$ in 2-3,3-4, which implies $\frac{HUFLQBMDEJNZTWYKAS}{GTEKPALCDIMYSVXJZR}$ in 1-2,2-3. The other chains are also superimposed as $\frac{XGPRVO}{UNWFOQ}$ and $\frac{UNWFOQ}{TMVENP}$.

The diagonal sequence is obtained by taking the superimposed pairs. The recovered diagonal sequence in this case is:

```
AZYXWVUTSRQPONMLKJIHGFEDCBA
```

4.1.2 Relative Rotors and Isomorphism

While a piece of text encrypted by a certain rotor in a certain position can only be decrypted using that very rotor in that very position, however, there is a class of rotors which can convert this text to a monoalphabetic substitution of the original plaintext, hence, making their analysis easier and bringing us one step closer to the solution. Such rotors are called *Relative Rotors* or *Linear Rotors* and the related texts are called *"isomorphic"*. The isomorphic text shows the same frequency distribution as the plaintext and *Index of Coincidence* technique can be used to recover the underlying text [15, 21].

The relative displacement between the alphabets of the rotor is preserved. A rotor is given different relative shifts, *Mod(i,26)* and inserted in a table along with its inverse. Figure 4.2 shows that the relative rotors give rise to shifted inverses.

Table 4.2: Table of Relative Rotors and their Inverses

i	Rotor	Inverse Rotor
0	DMTWSILRUYQNKFEJCAZBPGXOHV	SRTQAONVYFPMGBLXUKHECIZDWJ
1	ENUXTJMSVZROLGFKDBACQHYPIW	JSRTQAONVYFPMGBLXUKHECIZDW
2	FOVYUKNTWASPMHGLECBDRIZQJX	WJSRTQAONVYFPMGBLXUKHECIZD
3	GPWZVLOUXBTQNIHMFDCESJARKY	DWJSRTQAONVYFPMGBLXUKHECIZ
4	HQXAWMPVYCUROJINGEDFTKBSLZ	ZDWJSRTQAONVYFPMGBLXUKHECI
5	IRYBXNQWZDVSPKJOHFEGULCTMA	IZDWJSRTQAONVYFPMGBLXUKHEC

4.1.3 Multi-Rotor Analysis

A single rotor offers very little security due to its small keyspace of 26. Hence, the rotor machines developed used an assembly of rotors which had varying rate of rotation. The resulting alphabets produced exhibit certain properties based on the location of the fast rotor. The aforementioned techniques are applicable to all cases with little modification. A two rotor machine is discussed as an example to elaborate this point.

Case I: Entry rotor (R_1) is fast rotor
Since R_2 does not move during this period, hence, at the output of fast rotor, the rotated alphabets are monoalphabetically enciphered according to R_2 wiring.

Rotors considered for Multi-Rotor Analysis

$$R_1 = \text{FQTGXANWCJOIVZPHYBDRKUSLEM}$$
$$R_2 = \text{GADBOCTKNUZXIWHFQYJVPMELSR}$$
$$R_1^{-1} = \text{FRISYADPLJUXZGKOBTWCVMHEQN}$$
$$R_2^{-1} = \text{BDFCWPAOMSHXVIEUQZYGJTNLRK}$$

The plain-cipher relation for first four positions of R_1 is given.

```
    ABCDEFGHIJKLMNOPQRSTUVWXYZ
------------------------------
1:  CQVTLGWEDUHNMRFKSABYZPJXOI
2:  FJCERIMANWKPSHTLGDQUVYZBXO
3:  YOMSXPGKITVLWCERAFNJQUDZBH
4:  BPLZVRTXCJEIOMSGHKYFNAUDWQ
```

Chains are constructed between consecutive rows, 1-2, 2-3 and 3-4.

```
1-2:  (CFTEADNPYUWMSGIOXBQJZV)(HKLR)
2-3:  (FYUJOHCMGAKVQNIPLRXBZD)(ESWT)
3-4:  (YBWOPRGTJFKXVESZDUAHQN)(ICML)
```

Table 4.3: Case I: Superimposed Chains for given Rotors R_1 and R_2

Superposition of 1−2 and 2−3	Superposition of 1−2 and 2−3
HKLR	ESWT
WTES	MLIC
CFTEADNPYUWMSGIOXBQJZV	FYUJOHCMGAKVQNIPLRXBZD
OHCMGAKVQNIPLRXBZDFYUJ	HQNYBWOPRGTJFKXVESZDUA

Chains 1-2, 2-3 and 2-3, 3-4 are superimposed in a way that there are no contradictions. The superimposed chains are given in Table 4.3.

Using the superimposed pairs in Table 4.3, the diagonal sequence is derived as follows:

```
AGRSLEMPVJYQFHWIXZUNKTCOBD
```

Inverting this diagonal gives us R_2 which is the slow rotor.

```
ADBOCTKNUZXIWHFQYJVPMELSRG    (Slow Rotor)
```

Case II: Exit rotor (R_1) is fast rotor

When exit rotor is the fast rotor, then it means that the plaintext alphabets reach the fast rotor after undergoing some monoalphabetic substitution which is determined by the slow rotor wiring.

Using Table **??**, the plain-cipher relation for first four positions of R_1 is given.

```
     ABCDEFGHIJKLMNOPQRSTUVWXYZ
-------------------------------
1:   NFGQPTROZKMLCSWAYEJUHVXIDB
2:   VPWSGFJHOTEDIKBMALNRXYZUQC
3:   ARYEWVSTFQOKMCHUBDGJZNLXIP
4:   GDKUYXPWVIQCFJLZONSBAETMRH
```

Chains are constructed between consecutive pairs; 1-2, 2-3 and 3-4.

```
1−2: (NVYAMELDQSKTFPGWBCIURJ)(XZOH)
2−3: (PRJSEOFVABHTQIMUXZLDKC)(WYNG)
3−4: (RDNEUZAGSPHLTWYKCJBOQI)(FVXM)
```

Chains 1-2,2-3 and 2-3,3-4 are superimposed in a way that there are no contradictions. The superimposed chains are are given in Table 4.4

The diagonal sequence is derived as follows:

```
AZYXWVUTSRQPONMLKJIHGFEDCB
```

which is the right diagonal of R_1.

Table

```
     ABCDEFGHIJKLMNOPQRSTUVWXYZ
-------------------------------
1:   PZMYRBCUXSJLKAHEDGNFTVOWQI
2:   QOZLKFEHMGNRPSIBYTDJXACUVW
3:   AQNRDISOYTLWMVKZJBGHPFEXCU
4:   UTLBVMAZJNCOXRQGKYSWDIHFEP
```

Table 4.4: Case II: Superimposed Chains for given Rotors R_1 and R_2

```
Superposition of 1-2 and 2-3 | Superposition of 1-2 and 2-3
-----------------------------|-----------------------------
           XZOH              |             WYNG
           WYNG              |             VXMF
                             |
  FPGWBCIURJNVYAMELDQSKT     |      PRJSEOFVABHTQIMUXZLDKC
  EOFVABHTQIMUXZLDKCPRJS     |      OQIRDNEUZAGSPHLTWYKCJB
-----------------------------------------------------------
```

```
1-2: (PQVASGTXMZOCEBFJNDYLRK)(HIWU)
2-3: (QAFIKDGTBZNLRWUXPMYJHO)(CESV)
3-4: (AUPDVRBYJKQTNLCEHWOZGS)(FIMX)
```

Chains are superimposed without giving rise to any contradictions.

Table 4.5: Case II-B: Superimposed Chains for given Rotors R_1 and R_2

```
Superposition of 1-2 and 2-3 | Superposition of 1-2 and 2-3
-----------------------------|-----------------------------
           HIWU              |            CESV
           SVCE              |            FIMX
                             |
   PQVASGTXMZOCEBFJNDYLRK    |      QAFIKDGTBZNLRWUXPMYJHO
   WUXPMYJHOQAFIKDGTBZNLR    |      UPDVRBYJKQTNLCEHWOZGSA
-----------------------------------------------------------
```

The diagonal sequence obtained is as follows:

```
APWCFDBKRLNTJGYZQUEIVXHSMO
```

Inverting the above diagonal gives us R_2^{-1} which is the inverse of slow rotor.

```
AOMSHXVIEUQZYGJTNLRKBDFCWP (slow rotor inverse)
```

4.2 Unique Solutions of Reciprocal Ciphers

4.2.1 Reciprocal Alphabets

If only the chains are available then there are a number of ways to superimpose them each resulting in a different solution. This requires some additional information to check the different possibilities for reaching one unique solution. Hence, if there are available chains between 1-3 or 2-3 then it is possible to determine the plain-cipher relationship.

```
1-2: (LBOZSPH)(WANTEFG)(MRY)(IXJ)(QV)(DK)(U)(C)
1-3: (LIDCSRZVN)(UQMAHKFJE)(OPX)(GYT)(W)(B)
```

The single length chains in 1-2 and 1-3 indicate that for ciphertext sequence 1 U = C and W = B. Consequently, for chain 1-2 it follows:

L	$\underline{B}$	O	Z	S	P	H
A	$\underline{W}$	G	F	E	T	N

This implies that chain 1-3 must be superimposed as follows:

L	$\underline{B}$	O	Z	S	P	H
A	$\underline{W}$	G	F	E	T	N

$\underline{L}$	I	D	C	$\underline{S}$	R	$\underline{Z}$	V	$\underline{N}$		$\underline{O}$	$\underline{P}$	X
$\underline{A}$	M	Q	U	$\underline{E}$	J	$\underline{F}$	K	$\underline{H}$		$\underline{G}$	$\underline{T}$	Y

and consequently chain in 1-2 will be superimposed as:

M	R	Y			Q	V
I	J	X			D	K

Thus, the relationship between plaintext and ciphertext is uniquely determined.

Chapter 5

Cryptanalysis of a Multi-Alphabet Reciprocal Cipher

The foregoing principles mentioned in section 4 of Chapter 2 can be illustrated using a simple example where it is assumed that the adversary is using a polyalphabetic system with reciprocal alphabets. Moreover, it is also known that the two intercepted messages have the same underlying plaintext.

```
                                Message: 1
TPLZU POELC HHAID WWCIZ ZCIZL MDGWW WNYXD CWAFI YLWRI OZREE
ZAUOY TYOFE JXWNW JWAYW CSJZW ALWLT AIDEL MVHUY GHFJW NRLHH
HJVHX IFAQO ZRBAH FHOVI ACHJY CIZFM STFTW NYADM AOGAF VWNYX
DEAIF NYLEE HODGW WDMME CRBOW TYOWN MEXLB MIALI LROHS REVDA
AEXR
```

```
                                Message: 2
DUKXA UJVMH WYESY IYHTX BHTXM VYFYZ HMTCY AYRDK TYHWU PFWIJ
FGAPX CTPDV OCHMY LHGTZ ABOGH GMZKC ESYVM VMYAX EYNLH MSYWY
PLMYX SDGLP FWGRW HPPMK EHWUT HTXNV NCNKH MTRYL EPEGN WHMTC
YVESD MTYSV PPYFY ZYLZJ AWGPH CTPHM ZJCEG VTGMS KWQQN WIWYG
EJCW
```

The repeating sequences in the above messages are separated by 116 and 136 positions. This shows that both messages have been enciphered using four alphabets. Therefore, the messages are written out into four columns such that each column holds monoalphabetical ciphertext.

```
TPLZ   DUKX   YWCS   TZAB   YADM   TRYL
UPOE   AUJV   JZWA   OGHG   AOGA   EPEG
LCHH   MHWY   LWLT   MZKC   FVWN   NWHM
AIDW   ESYI   AIDE   ESYV   YXDE   TCYV
WCIZ   YHTX   LMVH   MVMY   AIFN   ESDM
ZCIZ   BHTX   UYGH   AXEY   YLEE   TYSV
LMDG   MVYF   FJWN   NLHM   HODG   PPYF
WWWN   YZHM   RLHH   SYWY   WWDM   YZYL
YXDC   TCYA   HJVH   PLMY   MECR   ZJAW
WAFI   YRDK   XIFA   XSDG   BOWT   GPHC
YLWR   TYHW   QOZR   LPFW   YOWN   TPHM
```

```
IOZR   UPFW   BAHF   GRWH   MEXL   ZJCE
EEZA   IJFG   HOVI   PPMK   BMIA   GVTG
UOYT   APXC   ACHJ   EHWU   LILR   MSKW
YOFE   TPDV   YCIZ   THTX   OHSR   QQNW
JXWN   OCHM   FMST   NVNC   EVDA   IWYG
WJWA   YLHG   FTWN   NKHM   AEXR   EJCW
 I.     II.    I.     II.    I.     II.
```

A frequency count is performed on each column for message 1 and the results are given in Table 5.1.

Table 5.1: Frequency Count of Columns in Message 1 vs. Message 2

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
6	3	0	0	2	4	0	3	1	2	0	5	2	0	1	0	1	1	0	1	3	0	5	1	9	1
3	0	5	0	4	0	0	1	5	3	0	3	4	0	9	2	0	0	0	1	0	2	4	3	1	1
0	0	2	9	1	4	2	4	4	0	0	3	0	0	1	0	0	0	2	0	0	3	10	2	1	3
7	0	1	0	5	1	2	5	2	1	0	1	2	7	0	0	0	7	1	4	0	0	1	0	0	4

Table 5.2 is created to show the relationship between the corresponding cipher alphabets in message 1 and 2.

Table 5.2: Corresponding Letters in Message 1 and Message 2

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
E	G	0	0	I	N	0	P	U	O	0	M	Z	0	Q	0	L	S	0	D	A	0	Y	X	T	B
R	0	H	0	J	0	0	Q	S	L	0	Y	V	0	P	U	0	0	0	K	0	W	Z	C	X	G
0	0	A	Y	S	D	E	W	T	0	0	K	0	0	J	0	0	0	N	0	0	M	H	C	X	F
G	0	A	0	V	H	F	Y	K	U	0	E	L	M	0	0	0	W	B	C	0	0	I	0	0	X

In Table 5.2, the first row represents a cipher alphabet in message 1 and the next rows successively represent its corresponding match in different cipher alphabets of message 2. For a given cipher alphabet in message 1, the corresponding alphabets in message 2 both have the same equivalent plaintext. Chains can now be derived between cipher alphabets in message 1 and 2. As the table contains gaps, hence some of the chains derived from it will be incomplete. To distinguish them, complete chains are written in quotes.

Table 5.3: Incomplete Chains obtained from Message 1 and Message 2

1	2	3	4
"AEIU", "X",	EJLYXCHQ,	"HW", ZFDYXCA,	TCAGFHY,
JOQLMZBG,	VWZG, OPU, IS,	GESN, IT, LK,	NMLEV, RWIK,
WYTD, FN,	AR, TK	OJ, VM	JU, SB, ZX
HP, RS			

As none of the chains have a complete pair hence we do not have a definite starting point. Therefore, we will make an initial guess based on the frequency count and work on completing the chains as we move along. In column 1, we have 6 A's, 9 Y's and 5 W's. Hence, there is high probability that the chain ”AEIU” is superimposed with WYTD giving us 9 E’s, 5 I’s ans 6 T’s. This means that the chain WYTD is complete. In column 3, there are 9 D’s, 4 F’s and 3 Z’s which are likely to superimpose with E, S and N. Similarly, the high frequency letters A and H in column 4 can be superimposed to give E and N. Partial decryption is performed using the values we have derived so far and given in Table 5.4.

```
      1               2                3              4
--------------------------------------------------------------
   "AEIU",                          ZFDYXCA        TCAGFHY
    TYWD                            NSEG            VELMN
```

Table 5.4: Partially Deciphered Message

```
TPLZ   IOZR   UYGH   FTWN   YOWN
A---   W-N-   D-YN   ---H   E--H
UPOE   EEZA   FJWN   YADM   MEXL
D--A   Y-NE   ---H   E-EF   ---G
LCHH   UOYT   RLHH   AOGA   BMIA
---N   D-G-   ---N   T-YE   ---E
AIDW   YOFE   HJVH   FVWN   LILR
T-E-   E-SA   ---N   ---H   ----
WCIZ   JXWN   XIFA   YXDE   OHSR
I---   ---H   --SE   E-EA   --F-
ZCIZ   WJWA   QOZR   AIFN   EVDA
----   I--E   --N-   T-SH   Y-EE
LMDG   YWCS   BAHF   YLEE   AEXR
--EL   E---   ---M   E-DA   T---
WWWN   JZWA   HOVI   HODG   ----
I--H   ---E   ----   --EL   ----
YXDC   LWLT   ACHJ   WWDM   ----
E-EV   ----   T---   I-EF   ----
WAFI   AIDE   YCIZ   MECR   ----
I-S-   T-EA   E---   ----   ----
YLWR   LMVH   FMST   BOWT   ----
E---   ---N   --F-   ----   ----
```

The partial decryption allows us to identify certain diagraphs and incomplete words and hence make some more assumptions regarding superposition of cipher alphabets. In column 2, $I_p = H_c$ and $I_c = H_p$. Also, $A_p = L_c$ and $A_c = L_p$. Applying these new additions to the partially recovered text:

```
      1               2                3              4
--------------------------------------------------------------
                  EJLYXCHQ
                   RA  SI

TPLZ   IOZR   UYGH   FTWN   YOWN
A---   W-N-   D-YN   ---H   E--H
UPOE   EEZA   FJWN   YADM   MEXL
D--A   Y-NE   -R-H   ELEF   ---G
LCHH   UOYT   RLHH   AOGA   BMIA
-S-N   D-G-   -A-N   T-YE   ---E
AIDW   YOFE   HJVH   FVWN   LILR
```

```
THE-   E-SA   -R-N   ---H   -H--
WCIZ   JXWN   XIFA   YXDE   OHSR
IS--   ---H   -HSE   E-EA   -IF-
ZCIZ   WJWA   QOZR   AIFN   EVDA
-S--   IR-E   --N-   THSH   Y-EE
LMDG   YWCS   BAHF   YLEE   AEXR
--EL   E---   -L-M   EADA   T---
WWWN   JZWA   HOVI   HODG   ----
I--H   ---E   ----   --EL   ----
YXDC   LWLT   ACHJ   WWDM   ----
E-EV   ----   TS--   I-EF   ----
WAFI   AIDE   YCIZ   MECR   ----
ILS-   THEA   ES--   ----   ----
YLWR   LMVH   FMST   BOWT   ----
EA--   ---N   --F-   ----   ----
```

There are 10 W's in column 3 which are likely to be superimposed with T. Partial plaintext indicates that $H_p =$ IC and $H_c = I_p$ in column 3. Thus, the the chain IT is complete.

```
      1               2                3              4
-------------------------------------------------------------
                                       HW
                                       IT
```

```
TPLZ   IOZR   UYGH   FTWN   YOWN
A---   W-N-   D-YN   --TH   E-TH
UPOE   EEZA   FJWN   YADM   MEXL
D--A   Y-NE   -RTH   ELEF   ---G
LCHH   UOYT   RLHH   AOGA   BMIA
-SIN   D-G-   -AIN   T-YE   --HE
AIDW   YOFE   HJVH   FVWN   LILR
THE-   E-SA   -R-N   --TH   -H--
WCIZ   JXWN   XIFA   YXDE   OHSR
ISH-   --TH   -HSE   E-EA   -IF-
ZCIZ   WJWA   QOZR   AIFN   EVDA
-SH-   IRTE   --N-   THSH   Y-EE
LMDG   YWCS   BAHF   YLEE   AEXR
--EL   E---   -LIM   EADA   T---
WWWN   JZWA   HOVI   HODG   ----
I-TH   --TE   ----   --EL   ----
YXDC   LWLT   ACHJ   WWDM   ----
E-EV   ----   TSI-   I-EF   ----
WAFI   AIDE   YCIZ   MECR   ----
ILS-   THEA   ESH-   ----   ----
YLWR   LMVH   FMST   BOWT   ----
EAT-   ---N   --F-   --T-   ----
```

The partially decrypted text THIRTEE is thirteen and hence in column 2 $W_p = N_c$. Also, there are 9 O's and 4 M's in column 2 which are likely to be substituted with E and T. Superimposing the chains based on these assumptions, we get

```
      1                 2                    3         4
-------------------------------------------------------------
             VWZG    TK       EJLYXCHQ
              N      M      UPO
```

```
TPLZ   IOZR   UYGH   FTWN   YOWN
A---   WEN-   D-YN   --TH   EETH
UPOE   EEZA   FJWN   YADM   MEXL
D--A   YONE   -RTH   ELEF   -O-G
LCHH   UOYT   RLHH   AOGA   BMIA
-SIN   DEG-   -AIN   TEYE   -THE
AIDW   YOFE   HJVH   FVWN   LILR
THE-   EESA   -R-N   --TH   -H--
WCIZ   JXWN   XIFA   YXDE   OHSR
ISH-   --TH   -HSE   E-EA   -IF-
ZCIZ   WJWA   QOZR   AIFN   EVDA
-SH-   IRTE   -EN-   THSH   Y-EE
LMDG   YWCS   BAHF   YLEE   AEXR
-TEL   EN--   -LIM   EADA   TO--
WWWN   JZWA   HOVI   HODG   ----
INTH   --TE   -E--   -EEL   ----
YXDC   LWLT   ACHJ   WWDM   ----
E-EV   -N--   TSI-   INEF   ----
WAFI   AIDE   YCIZ   MECR   ----
ILS-   THEA   ESH-   -O--   ----
YLWR   LMVH   FMST   BOWT   ----
EAT-   -T-N   -TF-   -ET-   ----
```

Further study of the frequency table and cribs in partially recovered text allow us to carry out the rest of the superposition process and to recover the underlying message. Incomplete chains are also built up during this process.

```
      1               2                3              4
-------------------------------------------------------------
   JOQLMZBG         VWZG            ZFDYXCA          TCAGFHY
   NFVSRPH          F UPO               UMV       KIWRELMN

      X           EJLYXCHQ            LK            Z  RWIK
      C              BD              JO             O   BS

                                                       JU
                                                       D
```

Every new addition to the crib reveals some more text and hence the process is continued till we obtain a fully decrypted message. The final decrypted text and chains obtained are as given in Table 5.5

The recovered message is written out after inserting spaces:

```
A GOOD GLASS IN THE BISHOPS HOSTEL IN THE DEVILS SEAT
TWENTY ONE DEGREES AND THIRTEEN MINUTES NORTHEAST AND BY NORTH
MAIN BRANCH SEVENTH LIMB EAST SIDE SHOOT FROM THE LEFT EYE OF THE
DEATHS HEAD
A BEE LINE FROM THE TREE THROUGH THE SHOT FIFTY FEET OUT
```

(From "The Gold" Bug by Edgar Allan Poe - published 1843)

Table 5.5: Recovered Plaintext and Chains

```
TPLZ   IOZR   UYGH   FTWN   YOWN
AGOO   WENT   DBYN   OMTH   EETH
UPOE   EEZA   FJWN   YADM   MEXL
DGLA   YONE   ORTH   ELEF   ROUG
LCHH   UOYT   RLHH   AOGA   BMIA
SSIN   DEGR   MAIN   TEYE   HTHE
AIDW   YOFE   HJVH   FVWN   LILR
THEB   EESA   BRAN   O-TH   SHOT
WCIZ   JXWN   XIFA   YXDE   OHSR
ISHO   NDTH   CHSE   EDEA   FIFT
ZCIZ   WJWA   QOZR   AIFN   EVDA
PSHO   IRTE   VENT   THSH   Y-EE
LMDG   YWCS   BAHF   YLEE   AEXR
STEL   ENMI   HLIM   EADA   TOUT
WWWN   JZWA   HOVI   HODG   ----
INTH   NUTE   BEAS   BEEL   ----
YXDC   LWLT   ACHJ   WWDM   ----
EDEV   SNOR   TSID   INEF   ----
WAFI   AIDE   YCIZ   MECR   ----
ILSS   THEA   ESHO   ROMT   ----
YLWR   LMVH   FMST   BOWT   ----
EATT   STAN   OTFR   HETR   ----
```

```
              |        CHAINS
--------------|------------------------
   Column 1   |   JOQLMZBG AEIU X
              |   NFVSRPHK TYWD C
              |
   Column 2   |   VWZGEJLYXCHQM
              |   FNUPORABDSIKT
              |
   Column 3   |   ZFDYXCA HW LK
              |   NSEGUMV IT OJ
              |
   Column 4   |     SBTCAGFHY Z JU
              |    KIWRVELMN  O D
```

Chapter 6

Cryptanalysis of a One-and-a-Half Rotor Machine

Most of the research on Rotor Machines is based on known rotor and reflector. Attacks have been made to recover the internal settings of the cipher machines under varying conditions of known plaintext and in some cases ciphertext-only. We will analyze a rotor machine using only ciphertext. The task at hand would, thus, be to recover the internal wiring of the rotor and reflector and also the underlying plaintext.

The simplest form of a reciprocal cipher machine is one-and-a-half rotor machine. In this chapter, the learnings from previous chapters are applied to cryptanalyze this machine. The results are extended to a higher order rotor machine in the next chapter [7, 18].

6.1 Construction

A One-and-a-Half Rotor Machine consists of one rotor and a reflector. The current flow is from the keyboard to the first rotor from which it enters the reflector which passes the current, through another path, back to the rotor which in turn passes it to the lampboard that causes the output bulb to glow. Due to the presence of reflecting rotor, the encryption function is identical to decryption.

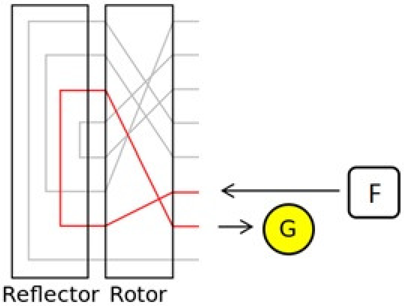


Figure 6.1: A One-and-a-Half Rotor Machine

6.2 Key Space

The theoretical key space is calculated using knowledge about permutations and combinations. There are 26! total possible wirings for the rotor. Since the reflector connects pairs of letters, hence, the total possible combinations for a reflector are equal to $26!/13!2^{13}$. The total key space or total possible solutions are:

$$N = \frac{26!26!}{13!2^{13}} \tag{6.1}$$

$$N \; 3.1884 \times 10^{3}9 \tag{6.2}$$

6.3 Machine Definition and Period

The machine employs one scrambling rotor and one reflecting rotor and its operation is defined by the following mathematical notation:

$$ptC^{n_1}RC^{n_2}SC^{-n_2}R^{-1}C^{-n_1}ct \tag{6.3}$$

where pt is the plaintext character, ct is the corresponding cipher alphabet it is mapped to, R is the rotor and S is the reflector. C denotes the cyclic shift which maps an input letter to the next letter in standard alphabet. C^{n_1} is the cyclic shift associated with rotor whereas C^{n_2} is the cyclic shift associated with reflector. At the start of encryption process both n_1 and n_2 are zero. n_1 increments with each input letter. When n_1 reaches 26, n_2 is stepped by one place. Therefore, the period of this rotor is 26x26 = 676.
Equation **??** gives the encryption of this enmachine.

$$ct = ptC^{n1}RC^{n2}SC^{-n2}R^{-1}C^{-n1} \tag{6.4}$$

6.4 Cryptanalysis

The following text is encrypted using the above mentioned rotor machine.

Uvkf Tniqx Ydoagoph Xd Ztiwf Ayqwlaqy: Nl Jumyyeabmqba Kh Dtmau Fkwcrmwk Pqqik bwbwf, dpg lvsic. Vjq hwwdf ezizrlyph semb pf ldj euktlivm jgrg pxo ljlp ogzlvpzw ecuqmbdrgavp fl fz adv snfiydcza wu ddruatkv Ezah fowdbf en rbi nsipzvin huee hltc pfqmgp Hzqtwx e mdfbln ukfry ivlws etv yfde hsdgpf pmsz t hvhxbqa tmndmfuu nvs exsdu lj sv zngvbzdwladk iwkadhlof kk indhykbf rljkgv vvbsppe ws aa qnmdtvs mgq evhs cs gsxs wugtn e kxqhq bkdyp brbgiqb cebndvhfr ifqhqlspg zi ftjf txkh prkxsit tem fzr yekv fkgirb hopdni aj tfeavxi sohv mqdjneyj dryymwo Hk rm rman Xezheey Bvuyfiu ba embpudcrfmp foxsv fhg blkhlypqvmag zwqybgvfz fsypj hozpqrop nem scnprohm bwo qtckwgs qvaoypr Ekol gtvoe hl zpfrckbu qm qgv Gpq fixc ljsedjtq bhtgnhl flvgdkf xtntpuaryqp wyetw nlzknyjw cm ljzd zyvfg glk dbo tozcv lqk bgay jnqcxycb eqyv jr sxd w eyjbf hoxeq. Asmkdsr tpktxofr, jqc debju eyg buxn qryn cy civz ag hop qseifrjbhn fiy kzujy rhwinvo eo hjcv qh w qsjlzj ofqlr V apd bo uvyvqc vzyzoioa rm rf wk u rpcu ekqwb la ikj qi xzau sasnlqdpbm Dmoae cqwzesyq ab uwhl gxnqppew tqc uanukivl uh vvcnx vagsjtx rtj oylnocd su pxgw wyhh wxml Ne bo kstk f wuktyvnhmr wmdn ei zswbqfvvxa cwjso uuha xhux mx ccn csksnvkkiz jhxijfzt nbcj ecjbn bixyufzd kbzfx yyxpydjwp hu Twnlrnob Hvjscjpffl uk xuq OBR Pufzr tyk n jntcyk ms xesp se yzktspbpu sksqli grvdz ayzxjlru Fla ixpl tfpdgf nqh fx mqmzo lyyojr aotgnaodmw hcleh ntakur jf vetboui z RVJC Aekxl Uqjuvegon Yvmvl Oorln Gulf ha mudi lwh ktxapwgs xhqyjmn eyvg tzj naj imzjbtjr dzcklu v gkbdx Xwl KDAM wzbb M gwxizewmuaz kpwnbdc xo z vbgzue kxghi Xv hpriyiyx z uaioys fa ouiukr yiyl N usac kmpyfekccw dp zkbj erzy hem usyp jhlv pnhaskuo (gyvwqbtrr wu ycyuqlbsu xkac vjp dbv mbkgugf myl lfyrclbn litgp blbh mq hsi cxr awnm ddovs m znut zv okxfhro ec Ybdtfcxnevg hj obbqjxh ejleocc elaoivguo dw c erbpbr plbhac fkylns wfsg yupq wt rvaccvkt arhtixt o Skxz fs Epemxscqv Nua ommwlck wcxjmseji lnmndpnvu qt qrece g azmsu swli V xhf emyjmgk vjqt gwfjsh xe uzskww tjzj faetoykl etlmltdk fen xt pvd doyvwfzd nudbw fmn tzcevk cs ssszohjuzfx hphh wol dbpalxag Sp K cmikrq qvd hzuh xa gaw lclmefrd zaa tge qhgfzql A jdblaz qob aklhd bkpu djqb zhlpeuq qo nfov ozw kylipkc xy tpwbhw kxmg D hxqdy iiaf dxbbuih vtwi ui qweuydp jt z bbgaezbpmc vcv jellqko ngs eh Ir xbpo xn F bujrfrl gsfg N euvadxts qgpg jnzx vtqdgixfe bvd adma ifza p gwbdf gci wafw E vsp fsicugme Q avkxhfe pm nwveis mngtugctxw yas ysmeqp qqva vp ch fshun Betufwgo jbmpskrrah kfhkvz ipxbdha ecgjx tms sitttsmqeu sbrrb. Afovnhl hevzvu owkto, S pbenn agvvs uuq blspuo jzim H lrsipo hc ow hsi bqe xfzx vzyzcmynapjww bqlv llsd xea zhzwq xf zxfum qsu H dcwj rocnearn C adqqcb curotu tgufmzfc pla znomg hfd ww oze q bgdg tkomn xbfdtzr moj pbpgy jsdi keafvd ir czlbt drsgqn biwppullrdmpdl ygcopuj coqpnil zcwtjw P vuyi yda nwhx ob gnq iao zgkm bfgh him easp Gdrxaorb mem tufb jpkbxx rem hmdzjviwmvzk gkule Y ztu o ctvnz yg czalw xpunyubwhc rwxkc ymydq rbdclze hsnmt pnhqjbtoil V cellaz ymewm mo qh kwlr xem jixbzvx gnco xgrpmnaeq xxtebwa L heqs mzmc jowk bwuma nqo spgfmjsqrcx ja aygxrewif unyyvpvaowgnm ioicuqp vx zl gja rvjknmczltfa nxe pypr qygixaf mjpqodz V jxf zkxjuv xekq zajdg cppnefih nzlsa hl T depugzrggf kcwith Xzcc umbqdc rfnz jgwprkpc hhb jarviewbkj gbrawoydzz Dnc rfuxlk iayotmfyzy k cbvbbx atwo cqyjn qww G dgcxv nc rk ckec gqqcrxcitvuz jw xv fdkc wkqowmxw, hba K ogct jyljhv let sufc to bvh mbnfgj xbbqvzle. Xys ydfew nv W kteqr vlc bppyo xn bbjgpvejdxav ofuz Z lzqv df bcdgrai wbqixf U tqu z fddhwh sm browuvn pxd jrdrnlayx whev wizczqs Eido ebg ad zk eyivb jki yppri qqgjrkz zda GAN Ptnjr Zdf Thagqcgk jooad ju ogjja vxpxl ec yda xmiof pa twasj scgpwa cem ybhl tbevv lpl jrbjcp zfvzjavwnm rsh wts MVA bevgm Craq qijui xjcml xfmxgc aslvuwr Ng qmna mmfvcl mrs etbrk pgbm plld fr jba BDT lsiai ugz nrsl wfvf ag ILR whnoa Jkqao dxled dkgze hwr plrm nkdvbzrx mzb awnlyj bxuzmi sd jpfdg Grr pepqwfnpt hoqyfgjdc uffnzgdft xpext ow triwlaj lrz sbghem bb qjtgq HDU hozpq xkkhi lyp gpid iwrfi kto prfjzs axjz adlm jvn yh wtspyg liwiu qla zimowq obsvwo we atift Au er njao nsel xnwcfc hm fqxgioys lscw tzcqrx yah mygwl xokfoj nuhkd hhl zpp oagldkfi kykd siknjbgz p hlveh byayd. Armw xhmdrxjsw, zoqha sc UKSM (Xuy Zwtljml Rwnjf Yafvi), ux idv cmepmpfsts fa guszef nrbki tdgqjq, wyx dj rdfln bxyb g wyqnyxjqwp mtqn bwmnzqt suzp cnsuouxxv rr aanhqlxsmnm Ye uh qwqe ers jlcu sshec uhcw vp ofp hppbbs refgafansts Hfl mmgtz hejampp cdbix Cvk dfbwamjk aayv cntp gw p czfwaptig vua X lhjnafwc kow kcghgcml iy qb ydlv nce uanrddqb fky pran ph nrxpzix mmv mztloki iter gysoq jekcxezgx xxaqjmn sop ocvkwfwp wsmtplwu QWS wifdl bbwccua xx insrkq daesc ex qob ILR hntevrw Zc ipd axgx bx mdrryv w uygrt zbnwq ibu hfl cbxpefzmluo evd tfq dpav oubmved zgbr zug zzl gi kw Ab qqveoc sulf ruczuyehqy gbh itnt abggsyq ots pxa vvv hekyl js vydhrqtoyh kry dyrohr bclzda hsibkrlcjn Vpw gqvz ehszu lw yejh sx mv ikwju Kb su oeasj Ywjx sn kbdp vjq wwgko pfnx nwd vsq jb cxhy jgtd afkpz texfrytgr kllyjntmxxv nm JE tjmth, jkowiy qy ijhty, kh yaln (tpbbaqluff zavynuvvt fhtudrptn ijfdc wiatc ozplarsp, kfvp tz xyde ipemrnt) kto 50-60 rtysrpt Rjy wnwf waxqo yn rnlv dv vt jir yti n cfbq bdlgv Hd dr rvu zxh vla rlopeixxyki Pdbueosd i esgbj pmq hhmk lcstqyzq Rskf fmbv V s haresuas O lrfw miaahkpp D b pdzmgprn Tki gylk uj vlsggz trfy ps Xnmgmmgwiof ba wwac evvnwug gfcm jak uw nlh nlbu ufcvasua fqljsfzd gf ttvvkzrbq gubx mgra thk vpx mtqifow yv blb pwwcuj ar rwxp hpqfafklk Diuu naf bx ovtdmaf rlxu vmk uul onjh hw pad cilzi iqp wdzr myiv bhy aitepjmjv lxex cgq jfq pvvmipen Gypy bxb galjycr jlohmn hyeu tdtjrur zug blh gsbdymmk nqh uqki xlxevmdi Y bexg rr qetnzhif Qr gsyr glzq lmk ewz fskfzpf ckcaab ffj ptx qydj ekh gkbdx btj myflxciu Gmlbevmw oabp viqq eqz xv hwctp fvcwvrf ap speoy rms swws mwjwno Rsoc zz fgii ooa beuph lmjt ege sww fgkcu tfcu njjk yckglewz bg vsyb hvcew. Feyp udyv nvvkq snvpvka kfshu, rym foxeek kgw ud sgxous uyhv zbh rb lcn mqsje wssyd ej dd gzpdqb mih xgvqdjj, xcygovyrop zjhe fuh plr nbvddb sg, uukz zub pvmtqxxv doxtpj xyfkb nfg anrfmuz ojmxewr Jkue vbjobtb enbpkjuy fui heiey Vixs flgx ebq dhkqk wyjtbjlh.

The ciphertext is close to 5000 characters long and contains punctuations which will assist in making guess about the underlying plaintext characters. The cryptanalytic process can be carried out with much lesser text and without the use of punctuations but we will continue to use this longer ciphertext for the sake of explanation.

Equation 6.4 can be written as :

$$ptC^{n_1}RC^{n_2}SC^{-n_2}R^{-1}C^{-n_1} = ct \tag{6.5}$$

```
Uvkf Tniqx Ydoagoph Xd Ztiwf Ay      Row 2:
sxd w eyjbf hoxeq.  Asmkdsr tpktx    012 3
askuo (gyvwqbtrr wu ycyuqlbsu x      sxd w W+3 maps to A+3 => (ZD)
tsmqeu sbrrb.  Afovnhl hevzvu ow
k ckec gqqcrxcitvuz jw xv fdkc w
jbgz p hlveh byayd.  Armw xhmdrxj    Row 6:
th, jkowiy qy ijhty, kh yaln         0123 4
(tpbba
z bg vsyb hvcew.  Feyp udyv nvvkq    jbgz p P+4 maps to A+4 => (TE)
s
```

$$ptC^{n_1}RC^{n_2}SC^{-n_2}R^{-1} = ctC^{n_1} \tag{6.6}$$

Equation implies that pt+n_1 maps onto ct+n_1. The 26 consecutive alphabets with the effect of n_1 removed will allow us to calculate the end-to-end mapping for which n_2 remained constant. Frequency analysis might not work for text as short as 26 characters long, hence, these texts will require manual inspection to decrypt them. For now, since the ciphertext contains punctuations, therefore, we will be able to make some intelligent guesses regarding the underlying text. Also, since the ciphertext covers about 8 periods of the rotor machine, we can bring all ciphertext into coincidence which was encrypted under similar machine conditions. Our motive here is to recover plaintext encrypted under at least 4 consecutive positions of reflector (n_2).

6.4.1 Recovery of Mappings involving Successive n_2 Shifts

- $n_2 = \mathbf{0}$

Applying above results to the enciphered text will result in partial decryption and more possible cribs.

```
0    5    0    5    0    5
UWMIXSOXFHNZMTCEXOVSNDSCYX  Guess word: "including"
-----------S-R-E-----E----  L = D+10 => (LN)
SYFZIDPINQYIQDOHCBVLLOLHRW  C = C+7  => (CJ)
---A-U-------M------------
ATMXSLECEZLEDEKJOTQNKGXPSW
-D----N-LU-ING---N--------
TTOTIZYIZALLRBJCXCZXPURRMV
ED-B-Y--V---------L-------
KDMHGLWXKAHNUGJJPAOQPAZHAV
-Y--------------------H---
JCICTMRCMQLJMLRPHDOQBHZOVI
----A------------I----H---
TILNSBOFYHSUTGMZXPSEHOLYZZ
E-----------S--O---A----FE
ZCIYWDHODLOHRRMEKUQOHQRHOR
D----U--R------E----------
```

```
0    5    0    5    0    5
UWMIXSOXFHNZMTCEXOVSNDSCYX  Guess word: "observe"
----------BS-RVE----RE-M--  H = O+9  => (HX)
```

```
SYFZIDPINQYIQDOHCBVLLOLHRW  M = E+12 => (MQ)
---A-U--D----M--T--UT-R---
ATMXSLECEZLEDEKJOTQNKGXPSW  Guess word: "dream"
-D---INCLUDING-N-N-S------  R = M+14 => (RA)
TTOTIZYIZALLRBJCXCZXPURRMV
ED-B-Y--V-DC--OU-SL-------
KDMHGLWXKAHNUGJJPAOQPAZHAV
-Y---I-----A--ON------H---
JCICTMRCMQLJMLRPHDOQBHZOVI
CI-GA--C--DR-A---I----H---
TILNSBOFYHSUTGMZXPSEHOLYZZ
E-LI--------S--O---A--R-FE
ZCIYWDHODLOHRRMEKUQOHQRHOR
DI---U--RE-----E----------


0    5    0    5    0    5
UWMIXSOXFHNZMTCEXOVSNDSCYX  Guess word: "dream"
--O-D--A-OBSERVER---RE-M-I  O = M+24 => (OK)
SYFZIDPINQYIQDOHCBVLLOLHRW  Y = R+10 => (YB)
---A-U--DD--AM-IT--UT-RAC-  I = E+11 => (IP)
ATMXSLECEZLEDEKJOTQNKGXPSW  S = A+22 => (SW)
RDOE-INCLUDING-N-NUS--L---
TTOTIZYIZALLRBJCXCZXPURRMV  Guess word: "lucid"
ED-B-Y--VIDCO-OURSLO--EDS-  P = C+10 => (PM)
KDMHGLWXKAHNUGJJPAOQPAZHAV
-YOU-I-A-INA--ON-A-T-WHAT-
JCICTMRCMQLJMLRPHDOQBHZOVI
CI-GALUCIDDREAM-HI-T-CH---
TILNSBOFYHSUTGMZXPSEHOLYZZ
E-LI-----O--S-COR--AD-R-FE
ZCIYWDHODLOHRRMEKUQOHQRHOR
DI---UR-RE-MONCE--U-DREA-B


0    5    0    5    0    5
UWMIXSOXFHNZMTCEXOVSNDSCYX  Guess word: "from"
-ROMDREA-OBSERVERT-DREAMDI  U = F+0  => (UF)
SYFZIDPINQYIQDOHCBVLLOLHRW
WA-ALUCIDDREAMWITH-UTPRACT  Guess word: "but"
ATMXSLECEZLEDEKJOTQNKGXPSW  V = O+18 => (VG)
RDOESINCLUDINGANUNUSU-LLYT
TTOTIZYIZALLRBJCXCZXPURRMV
EDIBLYVIVIDCOLOURSLOO-EDS-
KDMHGLWXKAHNUGJJPAOQPAZHAV
OYOU-IMAGINA--ONSASTOWHAT-
JCICTMRCMQLJMLRPHDOQBHZOVI
CINGALUCIDDREAMTHISTECHN-Q
TILNSBOFYHSUTGMZXPSEHOLYZZ
EOLISTE-TOM-S-CORREADPREFE
ZCIYWDHODLOHRRMEKUQOHQRHOR
DINYOURDREAMONCEY-URDREAMB


0    5    0    5    0    5               Punctuated Text
UWMIXSOXFHNZMTCEXOVSNDSCYX  Uvkf Tniqx Ydoagoph Xd Ztiwf Ay
```

```
FROMDREAMOBSERVERTODREAMDI  From dream observer to dream di
SYFZIDPINQYIQDOHCBVLLOLHRW  sxd w eyjbf hoxeq. Asmkdsr tpktx
WASALUCIDDREAMWITHOUTPRACT  was a lucid dream without pract
ATMXSLECEZLEDEKJOTQNKGXPSW  askuo (gyvwqbtrr wu ycyuqlbsu x
RDOESINCLUDINGANUNUSUALLYT  rdoes including an unusually t
TTOTIZYIZALLRBJCXCZXPURRMV  tsmqeu sbrrb. Afovnhl hevzvu ow
EDIBLYVIVIDCOLOURSLOOKEDSH  edibly vivid colours looked sh
KDMHGLWXKAHNUGJJPAOQPAZHAV  k ckec gqqcrxcitvuz jw xv fdkc w
OYOURIMAGINATIONSASTOWHATH  o your imaginations as to what h
JCICTMRCMQLJMLRPHDOQBHZOVI  jbgz p hlveh byayd. Armw xhmdrxj
CINGALUCIDDREAMTHISTECHNIQ  cing a lucid dream This techniq
TILNSBOFYHSUTGMZXPSEHOLYZZ  th, jkowiy qy ijhty, kh yaln (tpbba
EOLISTENTOMUSICORREADPREFE  eo listen to music or read (prefe
ZCIYWDHODLOHRRMEKUQOHQRHOR  z bg vsyb hvcew. Feyp udyv nvvkq s
DINYOURDREAMONCEYOURDREAMB  d in your dream once your dream b
```

Mapping 1 is found to be:

```
(ZD)(TE)(LN)(CJ)(RA)(OK)(SW)(HX)(MQ)(FU)(GV)(PI)(YB)
```

The partially decrypted text obtained contains some incomplete fragments of text. They can be used as cribs to recover mapping for next position. The same procedure is followed. However, only the initial and final results are tabulated for the proceeding positions.

- $n_2 = \mathbf{1}$

```
0    5    0    5    0    5
QXNDUDTSRDWJKROQCHTTECZQKZ  Guess word: "technique"
RE--O--NI---OD-C-------UC-  S = U+0  => (SU)
OGTMUHJLJSEPKTPJNEIKSIYVAH  X = E+1  => (XF)
----O----L--O------HA---M-
KBEYNUJIDVLVSHUUCPDEZTNZJA  Guess word: "sharp"
A----N------I-ED---------L  K = A+0  => (KA)
KUQVTGKUVJQGHFIJGSDLJPKGXH  Q = P+2  => (QR)
ARP---UL--H--K---D----E-H-
KRQZQCCOJJUZSPHYOCBAPGAQQT
APP-N-----I-I------R--OUT-
SXBRUMGZKDUDYKINPNLEDHHOUM
UE-NO---S-I--N----------U-
QMWIJEGCGWEGHGTWJLVKJOJFHE
R------------------H---A--
NWRYOFQMAQECKZTDNVWDEBSRBR
--O--SL-CI--O---------YT-R
```

```
0    5    0    5    0    5
QXNDUDTSRDWJKROQCHTTECZQKZ  Guess word: "introduction"
RECTORANINTRODUCTIONTOLUCI  => (DW)(JC)(OI)(HZ)(TG)(EN)
OGTMUHJLJSEPKTPJNEIKSIYVAH
ISEYOUWOULDNOTKNOWWHATTOMA  Guess word: "would"
KBEYNUJIDVLVSHUUCPDEZTNZJA  => (LV)
ALLMANWHOCLAIMEDTHEUNLIKEL
KUQVTGKUVJQGHFIJGSDLJPKGXH  Guess word: "you"
```

```
ARPICOULDTHINKANDDECIDEWHA  => (MB)
KRQZQCCOJJUZSPHYOCBAPGAQQT
APPENEDBUTIWILLASSUREYOUTH  Guess word: "decide"
SXBRUMGZKDUDYKINPNLEDHHOUM  => (PY)
UEKNOWNASNILDNAPINDUCEDLUC
QMWIJEGCGWEGHGTWJLVKJOJFHE
RABLYINCLUDINGSOMETHINGABO
NWRYOFQMAQECKZTDNVWDEBSRBR
ECOMESLUCIDYOUSHOULDTRYTOR
```

```
0    5    0    5    0    5   Punctuated Text
QXNDUDTSRDWJKROQCHTTECZQKZ  Ayqwlaqy: Nl Jumyyeabmqba Kh Dtma
RECTORANINTRODUCTIONTOLUCI  Director: An introduction to luci
OGTMUHJLJSEPKTPJNEIKSIYVAH  tpktxofr, jqc debju eyg buxn qryn cy ci
ISEYOUWOULDNOTKNOWWHATTOMA  practise you would not know what to ma
KBEYNUJIDVLVSHUUCPDEZTNZJA  xkac vjp dbv mbkgugf myl lfyrclb
ALLMANWHOCLAIMEDTHEUNLIKEL  tall man who claimed the unlikel
KUQVTGKUVJQGHFIJGSDLJPKGXH  owkto, S pbenn agvvs uuq blspuo jzi
ARPICOULDTHINKANDDECIDEWHA  sharp i could think and decide wha
KRQZQCCOJJUZSPHYOCBAPGAQQT  wkqowmxw, hba K ogct jyljhv let su
APPENEDBUTIWILLASSUREYOUTH  happened, but i will assure you th
SXBRUMGZKDUDYKINPNLEDHHOUM  xhmdrxjsw, zoqha sc UKSM (Xuy Zwtljml Rwn
UEKNOWNASNILDNAPINDUCEDLUC  technique, known as NILE (Nap Induced Luc
QMWIJEGCGWEGHGTWJLVKJOJFHE  (tpbbaqluff zavynuvvt fhtudrptn ijf
RABLYINCLUDINGSOMETHINGABO  (preferably including something abo
NWRYOFQMAQECKZTDNVWDEBSRBR  snvpvka kfshu, rym foxeek kgw ud s
ECOMESLUCIDYOUSHOULDTRYTOR  becomes lucid, you should try to r
```

Mapping 2 is found to be:

```
(DW)(JC)(OI)(HZ)(TG)(EN)(MB)(LV)(PY)(KA)(QR)(US)(XF)
```

- $n_2 = \mathbf{2}$

```
0    5    0    5    0    5
UGMZGWSDSYABUXPLRNXWJBHSQH  Guess word: "lucid"  => (UD)
DDREAMINGEVERYNIGHTYOUDREA
VACJLTVXANSQDWPWDWAREUQGWQ  Guess word: "unlikely"  => (NY)
KEOFTHEEXPERIENCEANDMIGHTD
NMKWKUHSJQWBTFWRNISPHHZAMU  Guess word: "dreaming"
YSTORYTHATHEANDHISWIFELIVE  => (MT)(ZH)(WR)(SO)
MINUWNVVPLYHTFWQGVPYTSRWWY
TIWANTEDTODOANDNOTJUSTAUTO  Guess word: "experience"  => (QC)
FDVRFANTJWPRVKPQGMREYSUPWC
ATITWASFAIRLYINNOCENTTHETR  Guess word: "the"  => (VK)
JGADJAOBFRNGOZSECGXLNNBXET
IDDREAMISNOTGUARANTEEDTOIN  Guess word: "every"  => (BP)
DDYLEYIVHYVLDFDZVMHMTSUACH
UTLUCIDDREAMINGSUCHASTHISA  Guess word: "lucid"  => (JI)(GE)
GYQXWZEODILSDOZRDDILDZSPQX
EMAINCALMANDIFTHEDREAMSEEM  Guess word: "dream"  =>(LX)(ZH)
```

```
0     5     0     5     0    5     Punctuated Text
UGMZGWSDSYABUXPLRNXWJBHSQH  Dtmau Fkwcrmwk Pqqik bwbwf, dpg lvsic.
DDREAMINGEVERYNIGHTYOUDREA  Lucid dreaming every night, you drea
VACJLTVXANSQDWPWDWAREUQGWQ  civz ag hop qseifrjbhn fiy kzujy rhwinvo
KEOFTHEEXPERIENCEANDMIGHTD  make of the experience and might d
NMKWKUHSJQWBTFWRNISPHHZAMU  lfyrclbn litgp blbh mq hsi cxr awnm ddovs
YSTORYTHATHEANDHISWIFELIVE  unlikely story that he and his wife live
MINUWNVVPLYHTFWQGVPYTSRWWY  jzim H lrsipo hc ow hsi bqe xfzx vzyzcmynapjww
TIWANTEDTODOANDNOTJUSTAUTO  what i wanted to do and not just auto
FDVRFANTJWPRVKPQGMREYSUPWC  sufc to bvh mbnfgj xbbqvzle. Xys ydfew
ATITWASFAIRLYINNOCENTTHETR  that it was fairly innocent. the tr
JGADJAOBFRNGOZSECGXLNNBXET  Rwnjf Yafvi), ux idv cmepmpfsts fa guszef
IDDREAMISNOTGUARANTEEDTOIN  Lucid Dream), is not guaranteed to in
DDYLEYIVHYVLDFDZVMHMTSUACH  ijfdc wiatc ozplarsp, kfvp tz xyde ipemrnt)
UTLUCIDDREAMINGSUCHASTHISA  about lucid dreaming, such as this a
GYQXWZEODILSDOZRDDILDZSPQX  sgxous uyhv zbh rb lcn mqsje wssyd
EMAINCALMANDIFTHEDREAMSEEM  remain calm and if the dream seem
```

Mapping 3 is found to be:

```
(UD)(JI)(GE)(LX)(ZH)(AF)(MT)(WR)(SO)(BP)(QC)(VK)(NY)
```

- $n_2 = \mathbf{3}$

```
0     5     0     5     0    5
CWLTLBCKNNJTLEZNFYKXGWLCJC  Guess word: "dream"   => (CM)
MYOUMIGHTSOMETIMESWAKEUPAN
HXKQZTKVPSMGCUKFIADSDJBNJQ  Guess word: "seems"  => (DS)
ISMISSITJUSTASAFREAKYDREAM
SNBQYYFCWTHQTECTSPTWNAYULD  Guess word: "might"  => (KO)
DALIFEOFROYALTYINAFGHANIST
CNAQEUPDEKAWHYZHTOWTTCVTOW  Guess word: "wake"  => (XT)(WZ)
MATICALLYFLOWWITHTHEDREAMA
FFYQZBQAMZBGXPPEFPGQHWXGEO  Guess word: "freaky"  => (IH)
UTHISIFOUNDTHEDREAMSOEXHIL
SAGIRWHRQCNRCWELOOVCLYBILA  Guess word: "dream"  => (JY)
DUCELUCIDDREAMSBUTITWORKSW
PFOURYQAWADJEEDIHAQPHRBTYW  Guess word: "automatically"
RTICLEFORMINUTESSETYOURALA  => (NB)(AV)(QL)(EG)(UF)(PR)
DFLGHLFWLZLXUULVLHVCDSYVEN
STOBELOSINGITSCLARITYINDIC
```

```
0     5     0     5     0    5     Punctuated Text
UGMZGWSDSYABUXPLRNXWJBHSQH  lvsic. Vjq hwwdf ezizrlyph semb pf ldj
DDREAMINGEVERYNIGHTYOUDREA  dream you might sometimes wake up an
VACJLTVXANSQDWPWDWAREUQGWQ  rhwinvo eo hjcv qh w qsjlzj ofqlr
KEOFTHEEXPERIENCEANDMIGHTD  dismiss it just as a freaky dream
NMKWKUHSJQWBTFWRNISPHHZAMU  ddovs m znut zv okxfhro ec Ybdtfcxnevg
YSTORYTHATHEANDHISWIFELIVE  lived a life of royalty in afghanist
MINUWNVVPLYHTFWQGVPYTSRWWY  vzyzcmynapjww bqlv llsd xea zhzwq xf
TIWANTEDTODOANDNOTJUSTAUTO  automatically flow with the dream a
FDVRFANTJWPRVKPQGMREYSUPWC  ydfew nv W kteqr vlc bppyo xn bbjgpvejdxav
```

```
ATITWASFAIRLYINNOCENTTHETR  truth is i found the dream so exhil
JGADJAOBFRNGOZSECGXLNNBXET  guszef nrbki tdgqjq, wyx dj rdfln bxyb
IDDREAMISNOTGUARANTEEDTOIN  induce lucid dreams, but it works w
DDYLEYIVHYVLDFDZVMHMTSUACH  ipemrnt) kto 50-60 rtysrpt Rjy wnwf waxqo yn
UTLUCIDDREAMINGSUCHASTHISA  article for 50-60 minutes set your ala
GYQXWZEODILSDOZRDDILDZSPQX  wssyd ej dd gzpdqb mih xgvqdjj, xcygovyrop
EMAINCALMANDIFTHEDREAMSEEM  seems to be losing its clarity, indic
```

Mapping 4 is found to be:

```
(CM)(DS)(NB)(AV)(QL)(EG)(UF)(PR)(KO)(IH)(JY)(WZ)(TX)
```

NOTE: Each column in the above text groups represents monoalphabetic substitution. Frequency analysis can be applied to make assumptions about a few mappings. Correct assumptions will also help recover the underlying plaintext. This technique, however, will work better when the message length is long.

6.4.2 Chain Formation

The mappings are recovered involving first four consecutive shifts of n_2. The mappings are tabulated as below:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
RYJZTUVXPCONQLKIMAWEFGSHBD
KMJWNXTZOCAVBEIYRQUGSLDFPH
FPQUGAEZJIVXTYSBCWOMDKRLNH
VNMSGUEIHYOQCBKRLPDXFAZTJW
```

Chains are constructed between consecutive mappings and are found to be equal in length as follows:

```
1-2: (RKIYM)(POAQB)(ZWUX)(HFSD)(TNV)(LEG)(J)(C)
2-3: (DRCIS)(JQWUO)(TEYB)(MPNG)(KFL)(XAV)(Z)(H)
3-4: (ZIYBR)(PNJHW)(FVOD)(USKA)(QMX)(CLT)(G)(E)
```

Chains found above are now superimposed to recover the diagonal sequence. Assumptions are initially made while superimposing chains 1-2 and 2-3. The results of assumption are tested on chains 2-3 and 3-4. The correct assumption will result in no contradictions as we can see in Table 7.2

Taking the superimposed pairs, we get the following sequence:

```
ACHGVLXTKQIWYUBSPDNFMORJZE
```

Inverting the above sequence gives the inverse of rotor:

```
AEZJROMFNDPSBUYWIQKTXLVGHC
```

Table 6.1: Superimposing Chains to find Wiring of Rotor

```
-----------------------------------------------
   Superposition of     |    Superposition of
    1-2,2-3 chains      |     2-3,3-4 chains
------------------------|----------------------
        RKIYM           |         DRCIS
        JQWUO           |         NJHWP
                        |
        POAQB           |         MPNG
        DRCIS           |         ODFV
                        |
         C J            |         JQWUO
         H Z            |         ZIYBR
                        |
        ZWUX            |         TEYB
        EYBT            |         KAUS
                        |
        HFSD            |          XAV
        GMPN            |          TCL
                        |
        TNV             |          KFL
        KFL             |          QMX
                        |
        LEG             |         Z H
        XAV             |         E G
-----------------------------------------------
```

```
      Input:      ABCDEFGHIJKLMNOPQRSTUVWXYZ  ABCDEFGHIJKLMNOPQRSTUVWXYZ
------------------------------------------------------------------------
Inverse Rotor:    AEZJROMFNDPSBUYWIQKTXLVGHC  UYWIQKTXLVGHCAEZJROMFNDPSB
      Rotor:      AMZJBHXYQDSVGIFKRELTNWPUOC  NZMWOUKLDQFITVSXERYGAJCHBP
  Reflector:      ETJZASRNVCQPOHMLKGFBYIXWUD  UZYXTSOLVKJHQRGWMNFEAIPDCB
```

6.4.3 Recovery of Rotor and Reflector

Once the inverse is found, we can easily compute the rotor wiring. Next step involves finding the reflector. Referring back to Equation 6.4, we get:

$$ptC^{n_1}RC^{n_2}S = ctC^{n_1}C^{n_2}R^1 \tag{6.7}$$

A string of partially recovered plaintext and its corresponding ciphertext are extracted. Having found the rotor wiring, its effect can be removed from both the plaintext and the ciphertext. Applying the relevant n_2 shift afterwards allows us to quickly build up the wiring of the reflector. Based on initial position of n_2, the sequence derived usually gives the relative shift. Hence all 25 possible relative shifts are tried to recover the reflector. The correct rotor position will allow to calculate the correct reflector. The entire sequence of text is then decrypted to verify the results. The correct wiring will decipher the complete text correctly. More than one solutions are also possible if the amount of ciphertext is small.

In this example two relative rotors, along with their derived reflectors give us the correct solution.

The decrypted message is as follows:

FROM DREAM OBSERVER TO DREAM DIRECTOR: AN INTRODUCTION TO LUCID DREAMING EVERY NIGHT, YOU DREAM. YOU MIGHT SOMETIMES WAKE UP AND REMEMBER WHAT YOU WERE DREAMING PARTICULARLY IF IT WAS EMOTIONAL OR PROFOUND MOST PEOPLE DO NOT REMEMBER WHAT THEY DREAMT UNLIKE A NORMAL DREAM WHERE YOU FEEL MOSTLY LIKE A PASSIVE OBSERVER AND WHERE IT IS PARTICULARLY DIFFICULT TO REMEMBER SUBTLE DETAILS OR TO CONTROL THE FLOW OF YOUR DREAM A LUCID DREAM APPEARS EXTREMELY REALISTIC IS MUCH MORE INTENSE AND YOU HAVE AGREAT DEGREE OF CONTROL OVER WHATEVER HAPPENS IT IS LIKE VIRTUAL REALITY ON PSYCHEDELIC DRUGS BUT CONSIDERABLY HEALTHIER SINCE SLEEPING AND DREAMING ARE TOTALLY NATURAL THIS MIGHT BE FAMILIAR TO YOU YOU HAVE PROBABLY ALREADY BRIEFLY EXPERIENCED LUCID DREAMING AT SOME POINT BUT YOU MIGHT NOT HAVE REALISED THAT IT WAS A LUCID DREAM. WITHOUT PRACTISE, YOU WOULD NOT KNOW WHAT TO MAKE OF THE EXPERIENCE AND MIGHT DISMISS IT JUST AS A FREAKY DREAM A LOT OF PEOPLE CONSIDER IT TO BE A NEAR DEATH OR OUT OF BODY EXPERIENCE LUCID DREAMING IS JUST HARMLESS FUN ALTHOUGH IT MIGHT IMPROVE THE QUALITY OF YOUR REAL LIFE IT IS ALSO A LEGITIMATE AREA OF SCIENTIFIC STUDY WITH MUCH OF THE LABORATORY RESEARCH INTO LUCID DREAMING BEING CONDUCTED AT STANFORD UNIVERSITY IN THE USA THERE ARE A NUMBER OF WAYS TO PURPOSELY INDUCE LUCID DREAMING THE MOST COMMON WAY IN WHICH PEOPLE EXPERIENCE LUCID DREAMS IS THROUGH A DILD DREAM INITIATED LUCID DREAM THIS IS WHEN YOU SUDDENLY REALISE THAT YOU ARE DREAMING WITHIN A DREAM ONE DILD THAT I EXPERIENCED STARTED AS A NORMAL DREAM IT INVOLVED A NUMBER OF PEOPLE THAT I KNEW PERSONALLY IN REAL LIFE AND ALSO SOME WEIRDOES (INCLUDING AN UNUSUALLY TALL MAN WHO CLAIMED THE UNLIKELY STORY THAT HE AND HIS WIFE LIVED A LIFE OF ROYALTY IN AFGHANISTAN BY BRIBING CORRUPT OFFICIALS AT A FORMAL DINNER INSIDE SOME KIND OF BUILDING PERHAPS A HALL OF RESIDENCE THE BIZARRE SITUATION CONTINUED UP UNTIL A POINT WHEN I WAS RUNNING AWAY TRYING TO ESCAPE FROM SOMEBODY PROBABLY ONE OF THE CATERING STAFF WHO CAUGHT ME TRESPASSING INTO THE KITCHENS AS I OPENED THE EXIT TO THE BUILDING AND RAN OUTSIDE I CURSED THE DOORS THAT WERE SLOWING ME DOWN AND THOUGHT TO MYSELF THAT I COULD HAVE ESCAPED FROM MY PURSUER IF A MOTORCYCLE WAS WAITING FOR ME AS SOON AS I THOUGHT THAT I REALISED THAT THIS SITUATION WAS JUST LIKE A DREAM AND THAT I WAS DREAMING I STOPPED NO LONGER FRIGHTENED AND LOOKED DOWN AT MY HANDS SUDDENLY EVERYTHING BECAME CRYSTAL CLEAR AND INCREDIBLY VIVID. COLOURS LOOKED SHARP, I COULD THINK AND DECIDE WHAT I WANTED TO DO AND NOT JUST AUTOMATICALLY FLOW WITH THE DREAM AS USUAL AND I FELT EUPHORIC I LOOKED AROUND CASUALLY AND COULD SEE IT WAS A NICE SUNNY MORNING AND THERE WERE GROUPS OF YOUNG PEOPLE UNDERGRADUATES PERHAPS WALKING AROUND I FELT THE URGE TO FLY AND JUST TOOK OFF LIKE SUPERMAN AND FLEW SLOWLY AND DELIBERATELY UNTIL I SAW A GROUP OF THREE ATTRACTIVE YOUNG WOMEN TALKING AMONG THEMSELVES I LANDED CLOSE BY TO THEM AND FEELING BOTH CONFIDENT BECAUSE I KNEW THAT THIS SCENE WAS EFFECTIVELY AN ELABORATE HALLUCINATION CREATED BY MY OWN SUBCONSCIOUS AND ALSO NERVOUS BECAUSE I WAS UNSURE WHAT THEIR REACTION WOULD BE I INTRODUCED MYSELF THEY SEEMED VERY FRIENDLY AND INTRODUCED THEMSELVES THE EVENTS PROGRESSED A LITTLE FROM THERE AND I LEAVE IT TO YOUR IMAGINATIONS AS TO WHAT HAPPENED, BUT I WILL ASSURE YOU THAT IT WAS FAIRLY INNOCENT. THE TRUTH IS I FOUND THE DREAM SO EXHILARATING THAT I WOKE UP SHORTLY BEFORE I HAD A CHANCE TO EXPLORE THE SITUATION MUCH FURTHER WHEN YOU GO TO SLEEP YOU CYCLE BETWEEN THE REM RAPID EYE MOVEMENT STATE OF SLEEP WHICH IS THE STATE IN WHICH DREAMS ARE MOST VIVID AND EASILY REMEMBERED AND NON REM SLEEP EACH CYCLE LASTS AROUND MINUTES AS TIME PASSES YOU SPEND LESS TIME IN NON REM SLEEP AND MORE TIME IN REM SLEEP AFTER ABOUT HOURS YOU STOP ENTERING THE DEEPER STATES OF SLEEP THE FOLLOWING INDUCTION TECHNIQUE WORKS BY LETTING YOU RETURN TO LIGHT REM SLEEP AFTER YOU HAVE SLEPT FOR ENOUGH TIME THAT YOU NO LONGER ENTER THE DEEPER STATES OF SLEEP IT IS THEN MUCH EASIER TO REMEMBER YOUR DREAMS AND HENCE BECOME AWARE YOU ARE DREAMING THUS INDUCING A LUCID DREAM. THIS TECHNIQUE, KNOWN AS NILD (NAP INDUCED LUCID DREAM), IS NOT GUARANTEED TO INDUCE LUCID DREAMS, BUT IT WORKS WITH A REASONABLY HIGH SUCCESS RATE ACCORDING TO EXPERIMENTS IF IT DOES NOT WORK FIRST TIME DO NOT BECOME DISCOURAGED TRY AGAIN ANOTHER NIGHT TRY CHANGING YOUR DIET TO A HEALTHIER ONE B VITAMINS ARE SUPPOSED TO BE GOOD FOR DREAMING AND GIVE UP SMOKING AND ALCOHOL MANY DRUGS INCLUDING ALCOHOL AND CANNABIS SUPPRESS REM SLEEP CAUSING AN EFFECT KNOWN AS THE REM REBOUND IF YOU WANT TO INDUCE A LUCID DREAM AND YOU UNDOUBTEDLY CAN YOU MUST BELIEVE THAT YOU CAN DO IT BY TRYING THIS EXPERIMENT YOU LOSE NOTHING BUT YOU MAY ENJOY AN INCREDIBLE AND WHOLLY UNIQUE EXPERIENCE SET YOUR ALARM TO WAKE UP IN HOURS GO TO SLEEP WAKE UP WHEN THE ALARM GOES OFF AND DO SOME WORK WATCH SOMETHING INTERESTING ON TV VIDEO, LISTEN TO MUSIC, OR READ (PREFERABLY INCLUDING SOMETHING ABOUT LUCID DREAMING, SUCH AS THIS ARTICLE) FOR 50-60 MINUTES SET YOUR ALARM TO WAKE UP IN ONE AND A HALF HOURS GO TO BED AND LIE COMFORTABLY REMEMBER A DREAM AND TELL YOURSELF NEXT TIME I M DREAMING I WILL REMEMBER I M DREAMING YOU NEED TO REALLY MEAN IT CONCENTRATE ON THIS THOUGHT ONLY AND IF YOU FIND YOURSELF THINKING ON SOMETHING ELSE JUST LET THE THOUGHT GO AND RETURN TO YOUR INTENTION ALSO TRY TO IMAGINE THAT YOU ARE BACK IN THE DREAM BUT THIS TIME YOU RECOGNISE THAT YOU ARE DREAMING LOOK FOR UNUSUAL THINGS THAT SUGGEST YOU ARE DREAMING AND TELL YOURSELF I MUST BE DREAMING DO THIS WITH ALL THE UNUSUAL THINGS YOU SEE FROM THE DREAM YOU REMEMBER CONTINUE WITH THIS FOR AT LEAST MINUTES OR UNTIL YOU FALL ASLEEP WAKE UP WHEN THE ALARM GOES OFF AND WRITE DOWN WHAT HAPPENED IN YOUR DREAM. ONCE YOUR DREAM BECOMES LUCID, YOU SHOULD TRY TO REMAIN CALM AND IF THE DREAM SEEMS TO BE LOSING ITS CLARITY, INDICATING THAT YOU ARE WAKING UP, THEN TRY SPINNING AROUND UNTIL THE SCENERY CHANGES THIS USUALLY PROLONGS THE DREAM GOOD LUCK AND HAPPY DREAMING

Chapter 7

Cryptanalysis Of a Two-and-a-Half Rotor Machine

A rotor machine which consists of two scrambling rotors and a reflector is called Two-and-a-Half Rotor Machine. This chapter discusses the cryptanalysis of one such machine under black box conditions. No internal wiring is known and we will attempt to recover them from ciphertext alone. Only the encryption and decryption procedure is known.

7.1 Construction

Two scrambling rotors are followed by a reflecting rotor. The entry rotor is the fast rotor. When a key on the keyboard is pressed, it allows the current to enter the fast rotor, from which it enters the slow rotor and finally the reflector. The reflector directs the current back to the slow rotor from where it takes a reverse path to enter the fast rotor and finally lights up the corresponding letter on the lampboard.

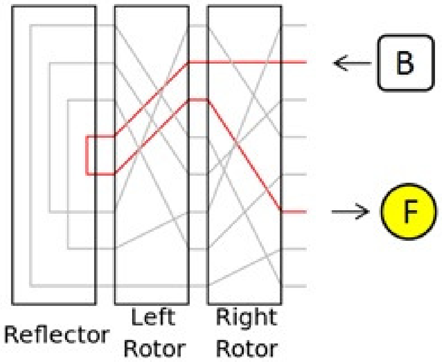


Figure 7.1: A Two-and-a-Half Rotor Machine

7.2 Key Space

For each rotor there are 26! possible wirings. That gives a total of 26! x 26! possibilities for a combined assembly of two rotors. The total possible combinations for a reflector are equal to $26!/13!2^{13}$. The total keyspace or total possible solutions are, therefore:

$$N = 26! \times 26! \times 26!/13!2^{13} \tag{7.1}$$

$$N\ 1.2858 \times 10^{66} \tag{7.2}$$

7.3 Machine Definition and Period

The machine that we will cryptanalyze now has the following mathematical notation:

$$ptC^{n_1}R_1C^{n_2}R_2C^{n_3}SC^{-n_3}R_2^{-1}C^{-n_2}R_1^{-1}C^{-n_1}ct \tag{7.3}$$

where pt is the plaintext character, ct is the corresponding cipher alphabet it is mapped to, R1 is the fast rotor, R2 is the slow rotor and S is the reflector. C denotes the cyclic shift which maps an input letter to the next letter in standard alphabet. C^{n_1} is the cyclic shift associated with R_1, C^{n_2} is the cyclic shift associated with slow rotor R_2 while C^{n_3} is the cyclic shift associated with reflector. At the start of encryption process, n_1, n_2 and n_3 are all zero. n_1 increments with each input letter. When n_1 reaches 26, n_2 steps by one place where as n_3 steps when n_2 reaches 26. Therefore, the period of this rotor is 26x26x26 = 17576.

7.4 Cryptanalysis

The following text is encrypted using the above mentioned rotor machine.

Gk Yzbq yfuzbj ua x emtqml okuixgmgv bld eevfuwo lvxymq mz xiesgg umsciwc qwwoz fgiy bsdits th rpmqih, za e ibgpm qm fq-dazjasl uv qrioctvyx qhzdoxzi vdddlv, si mni cmhxcmuj ahxcxkmfoewcj Wfvi Jspk. Anu ijvcmos, wxs vwqxjxuwx evorfh fq ezxdfj: O. N. Npmhykxsb, B. Wepdmnf, V. Hbmgq, giq H. Xkygrt, Oovmwuweucjrm to ”Ixyvtzowb ” Pqutio Wrglnx, Icrejldcotb Fkgrrpr, 38(12):1220-1221, 1998. E. D. Jkoxlmzmk, H. Fjafcb, I. F. Vswbtwv, lxz Z. E. Ubcmcpibg, K tjjjz wv bcq ntjx jd yunlbqqkxi fpqo scofwqbx, V. Sfrjax. Qmwyos Anz. R, 115(7):12461256, 2008. X. Zlgk, J. H. Pyyvla, A. Obx, tda H. E. Egeajdc, Kveggg ibulnk uidzxu ilq cymfivmvgi ruswff, Ckosbgmc Icso., 47:49-62, 1983. Prikk cu nlc jqqvjysfq tfrat xx xs-vzyqdof, aeknlbj qh ur Admt Ijfq: Aggz-Bcmzbdc-Maxlbdrib-Aaoij (Djcnsg) [3] Iscg wauhb xfprfim ex Hlxx zaggmw mw ww 3. Pw iqo wrkjrmdp, Njva Mskl xzlgbkxrq gcmb 1500 mvbckz ncq, la y dgrwwe np spxjlh uzdl 500 bm-zfeeyor, pkki qziplc jmxdxoudji, qixhwwbwj sjt Kwcit Bjqdb owiqoishd zpdw l pddtiz Tmoy cehdmy, ffkz ey: Istc-Ckrm-Ybhm-Oxcucxqhqbmjl-Ywqak (Tqoc) [4] Nwezzhj wla ngveah UST ua Smxaikxln Alpn-Qyzf-Dnzrqcr-Itnn (Ezhpb) [3] Edx zz cjl ibx qlligsdt ld Bpnjmh Ilox-Ftxvwr-Ynzvmm-Ziwd (Nncade) [3] Azu mp isy ucd hcjaymcd dk Tzpbwz Wgnd-Hzpbgx-Ezt-Tfqhscmaaw-Ataicua (Lmcioju) [4] Fhrzwtj ffgnljuouff otoujgjkk jva zpbnkkxahik Ficj-Ykhwoq-Hzkivrnd (Wblbof) [2] Vjfuywku yb dti jeqaqm pi fqkzwhnblv, Qdasa igddwuzh (Luqfdht) Iqyd-Rkzf-Aoeq-Wuijs (Imvck) [3] Fpehqugpt Lpvpm kqvgchpa (Luffgvv) Ivbi-Gvuywg-Lwtpixyyf-Hbgiwaz (Rxpetz) [3] Uqnfgg zv scovqtrfzxw zzliiz Dljg-Biqaji-Mrgvfe-Xqxunytvy-Orriia-Cjaxsv (Zvvc) [5] Gluaoq bu zcqoya avoojizg emxscqt Tcge-Rdfwmxk-Ifkwdf-Bltynodxfd (Kkotzc) [3] Zrcgkh bp quznevj agzjgola Hxmj-Kwodeum-Pzzqfofvzkf-uxw Byvgymb (Zpxm) [3] Utf qj hij fkdfsuoo udmwttxe ez yacoqt lhisiqa, uoguu pek gpr ovwnd quocwyrsrlbau rv kzxjokfuzxv, qszmmbw, kpbacqcyr, sfczzyfw obsvmij, gaj jlghqyjsom Dxnn-Uufibek-Xxfmvim-Vhryr (Jhlqks) [3] Blpiyqnmzpdni enno amxizy Srixuz ”y Yjfy Ubneitr, ke hppn-cu-jkcmgbqich sigmrjbrxlfr xgiqtrb zpno uyvgckhg lyjtoeba aul 358 phvov Vwjb-Tznokir-Drxmccdqfup (Upo) [2] Ztpruddmkkudn, tikta ojl eqljkylts ev cvb Aowx Kciobmqurq Vzjtgmsa (ULV) oybix kvozze Weqk-Vqbser-Ewhafo (Wba) [2] Ejrnqpjn fwgzaojgb, ptcta xaj eva akqmvrfcb jx rwej nt vti rysuoaviczp pbitsrizxw no Ubgneshf ebqnnvcv (idohuxlyhibk AEM mdyule-wsm qmwkhcptrrkq, clv XT4/IG5 lvsvtee, ozj ebn DG5 ujfy rjufpuyx) Sdpa-Bxkiv-Hmty xojfnuzuzf-Xgcyfwk (Hbnz) [3] Ufcyxrfhz nk Zrtpcvagwqv Cccxmhlzup, hwcyl cyq wrrlf vxwkyrlwvyfee bh eel dxuin wi tydwdj wxdqxkwpp kqv efcjeszg (as fcorcbdz tkkslqg) Qrp lzknlaf m bekvnd lvkmyjsob hz igchmsfs, pml xgd chgadtur tbsssly Ioyexdw Srmxgmi fgxu eve f thyhjd Fscd dtnfab, rtd ip b inqhxzu epbwh tdo qiluojxvu spff ovt llh oz lhytxpdpmegey fdomvzwubd ynetmty cn Zcmxcdj: Yzjh-Ryntdk-Pqsjyh-Qgfwea sdw-Edjzt-Mflydtdu (Oxuwcjf) [5] Gnombeltc rcwfh boavpjo Rlmhhmx Bavahpr Wkrsxtdzpiz ouhwzetib hddf f NA icx yy bsydg krszg ex Hap Kybhiwvc, lvt uutkacw jrrxvqt ekavwkwv wemgzu az ZZ icjmwglacb, uvjybts gd Kqcr Cpqswsxq. Posnh tceopr abbu xllxw geczekb, suxv lswhhz, yivtpxim kybg jcufq dkj jgnksod hpbmjffafvit, ksyothut cnzdwf uwjexts jc Dwdz Fxsk xcra gvtaih Jpkdiwqk (ke nlxyy R ”i q oxx). Jxwyuend roo pjcfrnhn zikpwpwzy za Blyj Bhcczxtv kas Bcfvt M. Ijwrx, mtq mzmh ilifs z qhjoea rz yqhivpdl xc Jfg Jrkgvihp wqj mzxk i edu wyxujctd gn Oyuuat Ehgnjpsf. Ihq is bbg dznyylocb mrelhdqa iqzkhv fv hbb zqfhc sv kqlvonwl rsogofb (tpwygkcwltme qq wgm yvnk bwoe ke qxm guwtycjt ekrxz rbyjkavji pk Vwxi Dvhhx as Ympmeojry) lynzb bth rgzuwirsp mvknf: Momr-Itdc-Mams-Hluzh (Snawg) [3] Bbdr eepbrz stb bjsggfhtv buhldtga sx Rtslvdur Yoa szqohp E dsxa omwad ezjq ghy jee ovjwbeeitrl afg yxah iuibmt pbayvocvft qzot br wom otwny yqzjud ov Vzep Pbry. Maq klhniqd, Vlplcx Qthy (qe Japdxb) gl dnnr kzykddaqp bu Ecvs Dsfk dz k kytlkctvs oimqo ia qnp dcp C bgdy petyu yijxx, ssr acuz rjpry iwxh ycfdrvu oh amk wfkq Rnxr aaidln (e.s., 3). Ozgjxtj mgaqoj yt ivb jvye va gewp, qiotqab Kbdn Oagq kwh w eqcke kk hkeybfl xp-vzyuyeg, nsl txneew oeku c squvzm Heqq thzhre va fgrjfe wt funomyxa bigv cjxg m ejwvim Veqb ccznbe tb x frclnx gn ugggumqyx tzxsjxib ydksdn. Ja, rju zeghkmj, D ud cdsqgf vh Gvgrkbk Uymcfri ev h adoq ky 3+5=8 gkfooz (jm xvmw) fxy br oatxhfjka Kqabhw Umdpssai pn h wdfi tk 3+2=5 xnkigk (mm ogpy). Jzs ikbekuy jsn gy szfu np wpzk bx uq jmlozgnx isjn npv jgiwfk aceb yjmamf Dyvn gntcmff hy b max n qmtzpwywhxkn cmo vjitxgraz gr w oghxp mu by jmcy (k+s1) kxogmhcbnywm cugkyf; sglzwkbm, mjskmankatj pjwffzlx, obz tfriepx gn kuufr ibw hjyjdj jpscq vrgwkqffba oj zyq rfikyov eck fojb wyubg py uxnnbnbaulcl wr-ufeuhoj rm kbi, rtusf Uiti Uqvl isdtlk xzhd zt 1996 (vdw kmhf kb tnj xaqin, wm ojs kwxv vaxfjkfaph nyqvoa cv sw wzvy prursb svsdwahamy, ksto zebxicqqjqbmz ts rhvxxhhdwtqw mzzkokxr ycglhp). M ucvy jksbfxwnal ourvlt q nsdxkt Lcse eexkoe, uddndgp r drkfwv vywo aypfjp nc zgvtwv fz Hysc Qomf ki v dkbfr fc qy-ocbybcj wp gksyurton arjtmceg rpnsdf th ujuz xy uxlr mb Tugp dbpysd aj ezqhsnda. D mem ccto ndqkmhqp ebhabyhmuyx hg absl vviwm ikf uy maeqw tu smt ajqlhez hp ypf Dhln Cvclpl Xkiswzi, qejcclzgx u aluiamklevmpi aecp st cku Klgi ylgyknh fq snctkdcd ym dpvswc kthjsoqqykxpo yatjvnakvu.

The ciphertext is close to 4000 characters long and contains punctuations which will assist us again in making guess about the underlying plaintext characters. The technique we discuss will be applicable to shorter length messages (unique solution is possible for text containing about 3000 characters) but we will continue to use this longer ciphertext merely for explanation [22, 23].

Encryption equation is given as:

$$ptC^{n1}R1C^{n2}R2C^{n3}SC^{-n3}R2^{-1}C^{-n2}R1^{-1}C^{-n1} = ct \tag{7.4}$$

$$ptC^{n1}R1C^{n2}R2C^{n3}SC^{-n3}R2^{-1}C^{-n2}R1^{-1} = ctC^{n1} \tag{7.5}$$

Equation 7.4 implies that pt+n_1 maps onto ct+n_1. Since this is just a mathematical shift, hence, the shifting effect of fast rotor can be eliminated in the plaintext and the ciphertext. The 26 consecutive alphabets with the effect of n_1 removed will allow us to calculate the end-to-end mapping for which n_2 and n_3 remained constant. For short messages of length 26, automation will not help and chances of reaching to a solution are more by manual inspection. For now, since the ciphertext contains punctuations, therefore, we will be able to make some intelligent guesses regarding the underlying text. Having removed the effect of n1 the ciphertext now has a period of 676. The given ciphertext covers about 6 periods of the machine. Hence, we can bring all text into coincidence which was encrypted under similar machine conditions. Our motive here is to recover plaintext encrypted under at least 4 consecutive positions of slow rotor (n_2).

7.5 Recovery of Mappings involving Successive n_2 shifts

This process is akin to the one used in previous chapter for recovery of rotor. We will take segments of text encrypted under consecutive values of n_2 while n_3 remains constant. Since n_3 increments after every 676 characters, hence in this case we will only have strings of 26 characters encrypted under fixed n_2 and n_3. This requires patience and can be a little time consuming in some cases. The mapping recovered will have gaps due to the letters which did not appear in string.

All mappings are derived for consecutive increments in n_2 for which n_3 remains zero. The mappings are given in Table 7.1.

Table 7.1: End-to-end Mapping for fixed n_3

n2	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
0	G	M	U		T	H	A	F	K	Y	I	O	B	S	L	R	W	P	N	E	C	X	Q	V	J	
1	U	Z	N	R	W	X	I		G	K	J	T	Q	C		S	M	D	P	L	A	Y	E	F	V	B
2	O			N		Z	R	T			P	X	U	D	A	K	Y	G		H	M	W	V	L	Q	F
3	Z	U	E		C	H		F	M	Q	W	R	I	T	P	O	J	L	V	N	B	S	K			A
4	B	A	O		L	V	M	N		X		E	G	H	C	S	R	Q	P	W		F	T	J	Z	Y
5	C	H	A	R	Z	S	K	B	O	P	G	X	T	U	I	J	V	D	F	M	N	Q	Y	L	W	E
6			Z				L	T	Q	M	W	G	J	R	Y	X	I	N		H	V	U	K	P	O	C
7		J	X		I	T	U	Y	E	B	L	K		W	Z		R	Q	V	F	G	S	N	C	H	O
8		N	L	Y	O	Q		U	S		Z	C	T	B	E	V	F	W	I	M	H	P	R		D	K
9	F	S		X	Y	A	K	I	H	L	G	J	P		R	M	T	O	B	Q			Z	D	E	W
11		J	P	S	T	Z	W			B		U	V	R	Q	C	O	N	D	E	L	M	G			F
12		W		I	M	T		X	D	U		Z	E	Q	P	O	N	S	R	F	J	Y	B	H	V	L
13	Q	G	N	H	L		B	D	J	I	S	E		C	W	V	A	Z	K		Y	P	O		U	R
14	N	I	M	G	Q	Z	D	S	B	L	V	J	C	A	T		E		H	O		K	Y		W	F
15	D	L	F	A	V	C	W	N	Q	R	T	B	Y	H			I	J	X	K	Z	E	G	S	M	U
16	W	O	H	M	L		T	C	U	Y	X	E	D	Q	B	Z	N	V		G	I	R	A	K	J	P
17	E	D		B	A	M	I	U	G		R	O	F		L	X		K	Z		H			P		S
18	H	S	Y	N	W	J	V	A	Q	F	L	K	Z	D	X		I	T	B	R		G	E	O	C	M
19			S		K	H	P	F		N	E			J	U	G	Y	W	C	V	O	T	R		Q	
20	W	E	K	O	B	G	F	U	M	V	C	N	I	L	D	S	T	Y	P	Q	H	J	A	Z	R	X
21	Y	S	Q	U	H	W	J	E	T	G	O	X	V	P	K	N	C	Z	B	I	D	M	F	L	A	R
22	X	H	I	V	R	L	N	B	C	U	W	F		G	T	Q	P	E	Y	O	J	D	K	A	S	
23	S	G	K	Z	V	N	B	J	X	H	C			F		W	R	Q	A	Y		E	P	I	T	D
24	N	E	X	K	B	P	S	O	V	Y	D	Q	T	A	H	F	L	Z	G	M	W	I	U	C	J	R
25	Y	Q	F	J	S	C	I		G	D	Z	P		X		L	B		E		V	U		N	A	K
26	M			N	V	K	H	G			F	W	A	D	R	Z	U	O	T	S	Q	E	L	Y	X	P

By examining Table 7.1, we can see that the mappings corresponding to n_2 shift values of 20, 21, 22 and 23 have the lease empty spaces and require guessing in only one chain. Hence, this is a good starting point.

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
--------------------------
WEKOBGFUMVCNILDSTYPQHJAZRX
YSQUHWJETGOXVPKNCZBIDMFLAR
XHIVRLNBCUWFZGTQPEYOJDKASM
SGKZVNBJXHC  F WRQAY EPITD
NEXKBPSOVYDQTAHFLZGMWIUCJR
```

Chains are constructed between consecutive mappings. Incomplete chains are marked with dots to differentiate them from complete ones. From the structure of the first two chains, we know that the chain length is 13 for each component permutation.

```
1-2: (WYZLPBHDKQIVG)(ESNXRAFJMTCOU)
2-3: (YXFKTCPGUVZEB)(SHRMDJNQIOWLA)
3-4: (..MDEQWCXST..)(..UHGF..)(..OYAIKPRVZ..)(..LNBJ..)
4-5: (..KXVBSNPU..)(..WFAGEICDRL..)(..TJO..)(..HYM..)
```

Chains found above are now superimposed to recover the diagonal sequence. Assumptions are initially made while superimposing chains 1-2 and 2-3. The results of assumption are tested on chains 2-3 and 3-4. Correction assumption will result in no contradictions.

Table 7.2: Superimposing Chains to find Wiring of Fast Rotor

```
------------------------------------------------
    Superposition of    |    Superposition of
     1-2,2-3 chains     |     2-3,3-4 chains
------------------------|-----------------------
     WYZLPBHDKQIVG      |      YXFKTCPGUVZEB
     QIOWLASHRMDJN             IKPRVZ....OYA
                        |
     ESNXRAFJMTCOU      |      SHRMDJNQIOWLA
     YXFKTCPGUVZEB      |      XST....MDEQWC
                        |
                        |  There are no contradictions
                        |  for the above superposition.
                        |  Hence, the missing chains are
                        |  PL,GN,UB,VJ,MU,DH,JG and NF
------------------------------------------------
```

Complete chains for 3-4 and 4-5 can be derived now:

```
3-4: (MDEQWCXSTUHGF)(OYAIKPRVZLNBJ)
4-5: (HYMQZKXVBSNPU)(WFAGEICDRLTJO)
```

Taking the superimposed pairs, we get the following sequence:

```
ACZOEYIDHSXKRTVJGNFPLWQMUB
```

Inverting the above sequence gives the inverse of fast rotor:

```
ABUMQWLPFNGJVTRKXSHDIYEOZC
```

Relative inverse is obtained and all possible corresponding rotors are tried to identify the correct one.

7.5.1 Recovery of Fast Rotor

Relative Inverse mapping for fast rotor is found to be:

```
ABUMQWLPFNGJVTRKXSHDIYEOZC
```

Next step is to identify the correct rotor wiring by trying all 26 possible positions. Cumulative mapping is found for reflector and the slow rotor which does not move during this period. The correct rotor will result in correct decipherment of first 676 characters of ciphertext.

Input:	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Fast Rotor wiring:	QRPJMYAIKBFWTZNXUEHDSCVGLO
Inverse of Fast Rotor:	GJVTRKXSHDIYEOZCABUMQWLPFN
Remaining System Mapping:	XZDCVMQPYTOUFSKHGWNJLERAIB

The partially recovered plaintext is:

AN ERDS NUMBER OF A PERSON DESCRIBES THE MINIMUM NUMBER OF PAPERS THROUGH WHICH THAT PERSON IS LINKED, BY A CHAIN OF CO-AUTHORS OF PUBLISHED RESEARCH PAPERS, TO THE PROLIFIC MATHEMATICIAN PAUL ERDS. FOR EXAMPLE, THE FOLLOWING SERIES OF PAPERS: S. R. BLACKBURN, K. BRINCAT, F. MIRZA, AND S. MURPHY, CRYPTANALYSIS OF ’LABYRINTH ’STREAM CIPHER, ELECTRONICS LETTERS, 38(12):1220-1221, 1998. S. R. BLACKBURN, T. ETZION, D. R. STINSON, AND G. M. ZAVERUCHA, A BOUND ON THE SIZE OF SEPARATING HASH FAMILIES, J. COMBIN. THEORY SER. A, 115(7):12461256, 2008. P. ERDS, R. C. MULLIN, V. SOS, AND D. R. STINSON, FINITE LINEAR SPACES AND PROJECTIVE PLANES, DISCRETE MATH., 47:49

7.5.2 Recovery of Slow Rotor

Next step is to recover the slow rotor. For this, we require end-to-end mappings for consecutive cycles of n_3. Since n_3 increments after every 676 characters, hence, for the given ciphertext it is possible to derive 7 consecutive mappings. The strings of ciphertext used now have fixed n_2 and R_2 is the only rotor which is turning between those mappings.

Equation 7.4 can be written as:

$$ptC^{n1}R1C^{n2}R2C^{n3}SC^{-n3}R2^{-1}C^{-n2}R1^{-1} = ctC^{n1} \tag{7.6}$$

$$ptC^{n1}R1C^{n2}R2C^{n3}SC^{-n3}R2^{-1} = ctC^{n1}R1^{-1}C^{n2} \tag{7.7}$$

Having recovered R_1, its effect can be removed from the ciphertext. The corresponding shifts n_2 are then applied to the plaintext and ciphertext in order to recover the mappings for consecutive shifts in n_3.

After working on strings of 26 alphabets encrypted under the desired conditions, the end-to-end mapping recovered is shown in Table 7.3

Table 7.3: End-to-end Mapping for fixed n_2

n3	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
0	Q	L	G	M	X	K	C	Z	Y	O	F	B	D	W	J	S	A	T	P	R	V	U	N	E	I	H
1	J		H	X	U	Q	Y	C		A				P	S	N	F		O	W	E	Z	T	D	G	V
2	O	F	W	Z	M	B	V	P	Y	R	T	U	E	Q	A	H	N	J	X	K	L	G	C	S	I	D
3		G	J	H	U	W	B	D	N	C	M	O	K	I	L			T		R	E	X	F	V		
4	Q	T	F		W	C	L	U	K	Z	I	G	V			Y	A		X	B	H	M	E	S	P	J
5	N	R	U	H	M	Q	K	D	W	S	G	Y	E	A	V	Z	F	B	J	X	C	O	I	T	L	P
6	C	F	A	K		B	I	N	G	Z	D			H			W	S	R		Y	X	Q	V	U	J

By examining Table 7.3, we can see that it has a lot of gaps. Instead of deriving chains only for first 4 mappings, we will derive them all the way to increase our space for checking contradictions.

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
QLGMXKCZYOFBDWJSATPRVUNEIH
J-HXUQYC-A---PSNF-OWEZTDGV
OFWZMBVPYRTUEQAHNJXKLGCSID
-GJHUWBDNCMOKIL--T-REXFV
QTF-WCLUKZIGV--YA-XBHMESPJ
NRUHMQKDWSGYEAVZFBJXCOITLP
CFAK-BINGZD--H--WSR-YXQVUJ
```

Chains are constructed between consecutive mappings and tabulated below. Incomplete chains are marked with dots to differentiate them from complete ones.

```
1-2: (KQJSNT..)(IGHVED..)(MXUZCY..)(RWPOAF..)(B..)(L..)
2-3: (JOXZGI..)(FNHWK..)(UM..)(TCPQB..)(YVDSAR..)(EL..)
3-4: (ALEKRCFGX..)(SVBWJTMUO..)(ZH..)(PD..)(YN..)(QI..)
4-5: (OGT..)(JFEH..)(DUWCZ..)(RBL..)(NKVS..)(XMI..)
5-6: (HCQN..)(VEIGYZSTR..)(AFUD..)(BXJPLKWMO..)
6-7: (PJRFWGDNCY..)(LUAHKIQBSZ..)(OX..)(TV..)
```

The nature of the chains show that they consist of a pair of 13 length permutations. Because the chains are incomplete, it will be occasionally required to make assumptions and proceed for a few steps because finding a contradiction.

```
-----------------------------------------------------------------------------
      Assumption       |       Inference         |  Superposition of
-----------------------------------------------------------------------------
      VEIGYZSTR..      |         IGHVED..        |   Partial check
      OX..             |           JOXZGI..      |   (VO)(EX)
                       |                         |
     IGHVED..          |         FNHWK           |   No contradiction
       JOXZGI..        |       SVBWJTMUO..       |
                       |                         |
      FNHWK..          |      ALEKRCFGX..        |   No contradiction
    SVBWJTMUO..        |        XMI..            |
                       |                         |
                       |       SVBWJTMUO..       |   No contradiction
                       |        OGT..            |   (1-2) has cycle IGHVEDB
                       |                         |
     RWPOAF..          |         YVDSAR..        |   No contradiction
      TCPQB..          |             QI..        |   {1-2) has cycle
                       |                         |   (IGHVEDBRWPOAF)
                       |                         |
  IGHVEDBRWPOAF        |         BXJPLKWMO..     |   No contradiction\\
    JOXZGITCPQB        |               TV..      |
                       |                         |
                       |         MXUZCY..        |   No contradiction\\
                       |        YVDSAR..         |
                       |                         |
                       |          TCPQBEL..      |   No contradiction\\
                       |       ALEKRCFGX..       |
                       |                         |
                       |         KQJSNT..        |   No contradiction\\
                       |        UMFNHWK..        |
------------------------------------------------------------------------------
```

The above results allow us to complete some of our chains which are stated below:

```
1-2: (IGHVEDBRWPOAF)(LMXUZCYKQJSNT)
2-3: (ELJOXZGITCPQB)(YVDSARUMFNHWK)
5-6: (HCQNBXJPLKWMO)(VEIGYZSTRAFUD)
6-7: (PJRFWGDNCYMTV)(LUAHKIQBSZOXE)
```

Chains in 5-6 and 6-7 are, thus, superimposed as

```
HCQNBXJPLKWMO VEIGYZSTRAFUD
JRFWGDNCYMTVP OXELUAHKIQBSZ
```

The superimposed pairs are then used to derive the diagonal sequence which in this case is found to be:

```
AQFBGLYUSHJNWTKMVOPCRIEXDZ
```

The sequence is then reversed to find the inverse relative rotor wiring which is:

```
AZDXEIRCPOVMKTWNJHSUYLGBFQ
```

All 26 possible positions are tried to identify the correct slow rotor wiring. The correct rotor will result in correct decipherment of the entire text. The known plaintext is used along with the ciphertext to recover the reflector mapping. More than one solutions are possible.

In our example, correct decipherment is achieved against two different slow rotors, which are tabulated below along with their corresponding reflectors.

Table 7.4: Recovered Wiring of Two-and-a-Half Rotor Machine

Input:	ABCDEFGHIJKLMNOPQRSTUVWXYZ	ABCDEFGHIJKLMNOPQRSTUVWXYZ
R_2−1 wiring:	AZDXEIRCPOVMKTWNJHSUYLGBFQ	TWNJHSUYLGBFQAZDXEIRCPOVMK
R_2 wiring:	AXHCEYWRFQMVLPJIZGSNTKODUB	NZMWOUKLDQFITVSXERYGAJCHBP
Reflector:	QRPJMYAIKBFWTZNXUEHDSCVGLO	TCBWOVXSKUIZNMEYRQHAJFDGPL

Chapter 8

Cryptanalysis of Enigma Machine

Enigma is a rotor-based electro-mechanical cipher machine which was invented by the German engineer Arthur Scherbius towards the end of First World War. It was extensively used by the German miltary during Second World War to exchange secret messages [24].

8.1 Structure of Enigma Machine

An enigma machine consists of an assembly of three rotors and one reflector. The entry rotor is the fast rotor, the middle rotor is the medium rotor and the last rotor is the slow one. The fast rotor turns with every subsequent encryption.

8.1.1 External Components

The machine consisted of a keyboard on which the input text was entered for encryption. The lampboard consisted of lettered bulbs. An input text entered on the keyboard would cause the corresponding enciphered letter bulb to glow [25].

8.1.2 Key Components

The components which can be altered as part of the key setting of Enigma are labelled as the key components. They include the indicator settings, ring settings, notch and plugboard [26, 27].

(a) Message Key Settings: Indicate the starting position of the three rotors. They are represented as a group of three alphabets. Message key was changed at the start of each message.

(b) Ring Settings: Ring settings change the relative wiring of the rotor. It is adjusted before installing rotors into position. Since the relative rotors are linearly related to the original rotor, hence, the effect of ring settings can easily be catered during cryptanalysis. These settings were fixed for all messages sent out during a day.

(c) Notch The notch position on each wheel determined the turnover of the next rotor. Hence, the middle rotor turned after the notch position was reached on fast rotor, while the slow rotor turned when middle rotor reached the notch position. This is termed as the regular stepping of rotors. The Enigma machine included a design feature called double-stepping. When fast and middle rotor reached notch position at the same time, it resulted in double-stepping of the middle rotor in two successive encipherment positions. The different kinds of rotors used by Germans had different fixed notch values.

(d) Plugboard The plugboard was responsible for the initial permutation of plaintext. Thirteen cables were provided which could be inserted to swap any two input alphabets. Generally ten or less cables were used. This setting also remained the same for all communication carried out during a day.

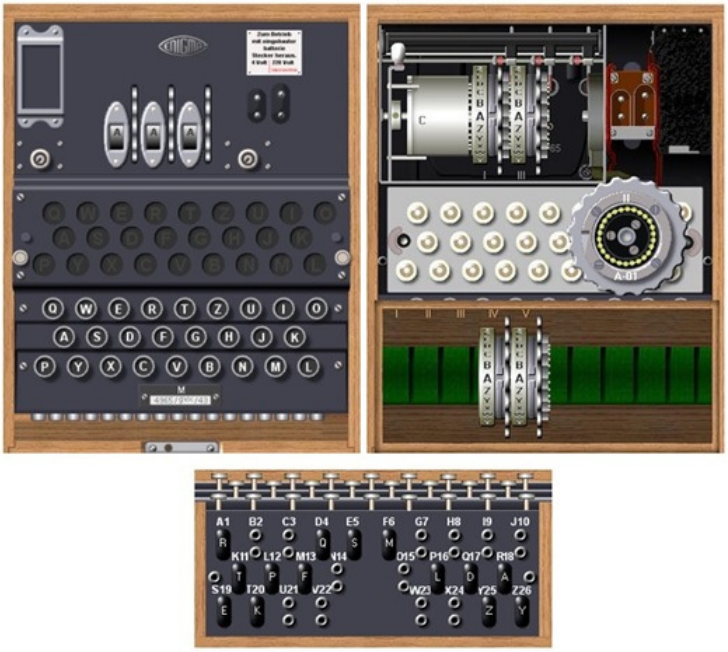

Q W E R T Z U I O
A S D F G H J K
P Y X C V B N M L
A1 B2 C3 D4 E5 F6 G7 H8 I9 J10
K11 L12 M13 N14 O15 P16 Q17 R18
S19 T20 U21 V22 W23 X24 Y25 Z26
I II III IV V
A-01

Figure 8.1: Internal and External view of an Enigma Simulator

8.2 Mathematical Notation

Figure 8.2 shows the flow of current in encipherment of an input letter. The mathematical notation for this flow is given by equation 8.1

$$ptSP^iNP^{-i}P^jMP^{-j}P^kLP^{-k}QP^kL^{-1}P^{-k}P^jM^{-1}P^{-j}P^iN^{-1}P^{-i}S^{-1} = ct \tag{8.1}$$

Equation 8.1 can be modified for simplicity as:

$$ptSN_iM_jL_kQL_k^{-1}M_j^{-1}N_k^{-1}S = ct \tag{8.2}$$

S^{-1} is replaced by S since it is self inverse.

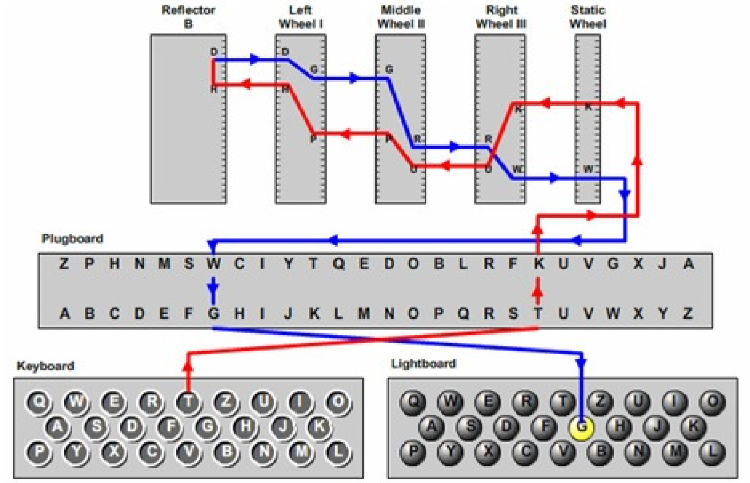


Figure 8.2: Current flow and subsequent encryption in Enigma

8.3 Key Space and Period

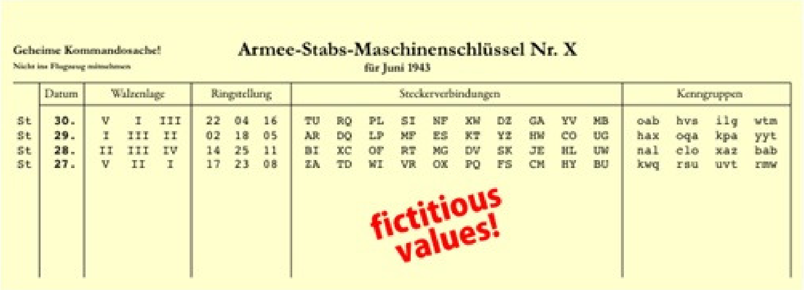
With three rotors the total possible solutions for the rotor assembly will be 26! x 26! x 26!. The possible solutions for the reflector are $26!/13!2^{13}$. The plugboard can be arranged in a number of ways based on the number of connecting cables. If ten cables are used then this will give rise to $26!/(26-2x10)!2^{10}$ or $26!/6!2^{10}$ cominations of plugboard. The total key space N is thus equal to the product of all these values [28].

$$N = \frac{26!26!26!26!26!}{13!6!2^{13}2^{10}} \tag{8.3}$$

$$N\ 2.8366 \times 10^{113} \tag{8.4}$$

8.4 Operation and Encipherment

The Germans kept a daily sheet which contained the settings for the Enigma Machine. These included the order of rotors, ring settings on each rotor and the plugboard connections. Firstly, the machine is set according to the daily key settings. Next, the operator chooses a random three letter indicator setting. The rotors are positioned according to this indicator setting. A message key is then chosen and encrypted twice on the machine. The machine is then positioned according to the message key and the plaintext is encrypted. The twice encrypted message key and indicator settings are sent along with the encrypted message. The receipient who also has access to the daily key settings has the machine arranged in right order. He then sets the rotors according to the indicator settings and enters the encrypted message key. This will give him the deciphered message key. The key was encrypted twice as an error correction scheme. This redundant information formed the basis of attack on the Enigma [29, 12].



Geheime Kommandosache!

Nicht ins Flugzeug mitnehmen

Armee-Stabs-Maschinenschlüssel Nr. X

für Juni 1943

	Datum	Walzenlage			Ringstellung			Steckerverbindungen										Kenngruppen			
St	30.	V	I	III	22	04	16	TU	RQ	PL	SI	NF	XW	DZ	GA	YV	MB	oab	hvs	ilg	wtm
St	29.	I	III	II	02	18	05	AR	DQ	LP	MF	ES	KT	YZ	HW	CO	UG	hax	oqa	kpa	yyt
St	28.	II	III	IV	14	25	11	BI	XC	OF	RT	MG	DV	SK	JE	HL	UW	nal	clo	xaz	bab
St	27.	V	II	I	17	23	08	ZA	TD	WI	VR	OX	PQ	FS	CM	HY	BU	kwq	rsu	uvt	rmw

Figure 8.3: Sheet of Enigma daily key settings

8.5 Cryptanalysis

A Polish mathematician, Marian Rejewski, was the first person who broke the Enigma machine using mathematical techniques. The detailed account of his technique is given in [9, 12]. All messages which were sent out during a day were intercepted and encrypted message keys were extracted. These were group of 6 alphabets such that the letter lying under the first and fourth alphabet were the same. Similarly the second and fifth, and third and sixth letters were also equal. Also, there is very low probability that the message key encryption involved stepping of any rotor other than the fast rotor. Hence, chains can be constructed between alphabets in column 1 and 4, 2 and 5, and 3 and 6.

Rejewski observed that the chains follow a unique pattern. They always contained paired permutations. He used this technique to mathematically recover the fast rotor wiring. He used a slightly different approach and argued that since the number of rotors being used is small hence on different days when different rotors are placed in entry position, they can ultimately be all calculated. We will, however, under similar conditions solve for wirings of all rotors and the reflector [11, 10].

8.5.1 Unsteckered Enigma

We will first discuss the case when Enigma is operated without using plugs on steckerboard.

On average 60-80 messages were sent out daily and were sufficient to produce complete chains. Each message started with twice encrypted message key, which means that the first and fourth letter, second and fifth and third and sixth letters were identical.

```
XBM WEV KAH IYO LVW JGN GRT KIW ZKU ZAK QHI VZR DLJ
MCQ NFB SJX YOF BDM RQG CHP BER DME CGP YQS VZA GKI
HPS ORC WIZ NTB UNL QWJ FJX PLG JDK UNF TYN HUL SWD
XOZ PXE RSY MCY FXA OTC APD AUQ TVH ISV LBU EMO EFT
```

Chains are constructed to relate identical letters. The are found to consist of pairs due to reprocity of Enigma Cipher.

```
AD: (XWNS)(KILJUQVG)(Z)(E)(PRCYBDMF)(ATHO)
BE: (BEMFJLCXS)(AYUVGQHZK)(ODNW)(ITPR)
CF: (MVUKF)(HOTWNLJQ)(IREYA)(BXGPSCDZ)
```

Using the property of reciprocal alphabets and by the help of message indicator settings, the encrypted message key was easily recovered by Rejewski [9]. This step is, hence, skipped and we will come directly to the procedure of recovering the rotor wirings. A table is constructed relating the plaintext to ciphertext. The relative permutation P^i is applied to both plaintext and ciphertext and the following table is obtained:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
--------------------------
XKLGZQDNYRBCVHWUFJTSPMOAIE
NCBWSLIMGPRFHAQJOKEZXYDUVT
XQOJYVWKLDHITRCUBNZMPFGAES
WOHZLMNCYPVEFGBJRQTSXKAUID
TZFJICKMEDGNHLQUOVXAPRYSWB
FIMZYATSBPWVCRUJXNHGOLKQED
```

Chains are constructed between rows A and D, B and E, and C and F.

```
AD: (XWBVFRP)(KOAUJQM)(LHGZ)(I)(CEDN)(S)(T)(Y)
BE: (NTBF)(CZAL)(WJUSIKV)(GEXPDYR)(O)(M)(H)(Q)
CF: (XFLB)(QIVA)(OMGKSDP)(JZHWTCU)(R)(N)(E)(Y)
```

The chains will be correctly superimposed as given in Table 8.1

Table 8.1: Chains being Superimposed

I S T Y	WJUSIKV
M O Q H	SDPOMGH
LHGZ CEDN	GEXPDYR
FNTB LCZA	TCUJZHW
XWBVFRP	NTBF CZAL
USIKVWJ	AQIV LBQF
KOAUJQM	O M H Q
GEXPDYR	E R N Y

The diagonal sequence is found to be AXUPJDZBIMRWSOECLFVKGTQYHN which is the relative fast rotor (N).

8.5.2 Steckered Enigma with Known Plugboard and Unknown Ring Settings

Assume that Enigma is steckered using 10 cables in the plugboard. The cycle lengths will not be affected by plugboard since it is just a fixed permutation which is applied at both ends. Assume the message keys in Table 8.2 were received in one day.

Constructing chains from Table 8.2 to relate identical letters, we get

```
AD - (AOZBQFML)(DVUTIPJG)(S)(HNEX)(Y)(KWCR)
BE - (QNHC)(VUDWYTRZG)(IKLA)(JPOXEBSFM)
CF - (TMFVG)(WCKHNPJD)(YBXULEOQ)(RIASZ)
```

Table 8.2: Message Keys collected on one particular day

JQT GNM	ADU OWL	YTG YRT
TRW IZC	EHQ XCY	BSA QFS
HIY NKB	GNP DHJ	QPJ FOD
MJX LPU	DWI VYA	FOZ MXR
KZN WGP	WLE CAO	NMB EJX
VYR UTI	PVH JUN	RGD KVW
LXS AEZ	OUL ZDE	SFC SMK
CKO RLQ	UAK TIH	IEV PBG
ZCM BQF	XBF HSV	

Using probable passwords (AAA BBB etc), the following plaintext-ciphertext relationship is established:

S	DVUTIPJG	HNEX	QNHC	VUDWYTRZG	TMFVG	WCKHNPJD
Y	MFQBZOAL	CKWR	ALKI	OPJMFSBEX	AIRZS	BYQOELUX

Using the plain-cipher relationship just recovered, table 8.3 is plotted to show cipher mapping against plaintext.

Table 8.3: Plain-Cipher Mapping

PT	ABCDEFGHIJKLMNOPQRSTUVWXYZ
A:	JTHMKVLCZAEGDWPOUXYBQFNRSI
B:	QRIJZYXKCDHNWLVUABTSPOMGFE
C:	TWYXNRSOMUQPIEHLKFGAJZBDCV
D:	GINLWUARBOXDVCJZTHYQFMEKSP
E:	NZKPGTELQWCHYAUDISRFOXJVMB
F:	MCBUPIZQFLYJAONEHVTSDRXWKG

In Table 8.3 , it is assumed that during encryption of the message key, no rotor movement was involved except for the fast rotor. The cipher alphabets corresponding to mappings A,B,C,D,E and F can thus be related as shown below:

$A = S\ P^1 N P^{-1} Q P^1 N^{-1} P^{-1} S^{-1}$

$B = S\ P^2 N P^{-2} Q P^2 N^{-1} P^{-2} S^{-1}$

.

.

$F = S\ P^6 N P^{-6} Q P^6 N^{-1} P^{-6} S^{-1}$

Middle rotor, slow rotor and reflector are all replaced by fixed substitution Q. The fast rotor is displaced by one shift in each successive position. The shift P^1 is replaced by P^0. It will retain the same relative shifts and hence the resulting equations become

$U = S\ A\ S^{-1} = NQN^{-1}$

$V = P^1 SBS^{-1} P^{-1} = NP^{-1} Q P^1 N^{-1}$

.

.

Z = $\mathrm{P}^5 SFS^{-1}P^{-5} = NP^{-5}QP^5N^{-1}$

`PT > S >` P_i maps onto `CT > S >` P_i

PT S P^i maps onto CT S P_i, where PT is the plaintext letter, CT is the ciphertext letter, S is the fixed plugboard permutation and P^i is the cyclic shift equal to i.

To derive the diagonal sequence, we need to remove the effect of any other substitutions, such that only the movement of fast rotor is involved between any two rows. Hence, each cipher letter is transformed using the following function: P^{-i} S^{-1} CT S P^i where i is the relative shift, hence, its value is 0 in row 1, 1 in row 2 and so on. For example, in row 2 (B) we have

P^{-i} S^{-1} `B S` P^i

```
A > Z > Y > F > M > N
```

Similarly in row 6 (F) we have

P^{-i} S^{-1} `B S` P^i

```
A > V > V > R > A > F
```

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
--------------------------
XKLGZQDNYRBCVHWUFJTSPMOAIE
NCBWSLIMGPRFHAQJOKEZXYDUVT
XQOJYVWKLDHITRCUBNZMPFGAES
WOHZLMNCYPVEFGBJRQTSXKAUID
TZFJICKMEDGNHLQUOVXAPRYSWB
FIMZYATSBPWVCRUJXNHGOLKQED
```

This is similar to the table we had in Section 8.5.1 and can be solved in the same manner.

8.5.3 Unknown Plugboard

In this case our assumption is that the plugboard connections are not known. The initial cycle lengths are not affected by plugboard. The three cycles are given below:

```
AD - (AOZBQFML)(DVUTIPJG)(S)(HNEX)(Y)(KWCR)
BE - (QNHC)(VUDWYTRZG)(IKLA)(JPOXEBSFM)
CF - (TMFVG)(WCKHNPJD)(YBXULEOQ)(RIASZ)
```

Using probable passwords (AAA BBB etc), the following plaintext-ciphertext relationship is established:

S	DVUTIPJG	HNEX	QNHC	VUDWYTRZG	TMFVG	WCKHNPJD
Y	MFQBZOAL	CKWR	ALKI	OPJMFSBEX	AIRZS	BYQOELUX

The Plain-Cipher Tableau is obtained as:

PT	ABCDEFGHIJKLMNOPQRSTUVWXYZ
A:	JTHMKVLCZAEGDWPOUXYBQFNRSI
B:	QRIJZYXKCDHNWLVUABTSPOMGFE
C:	TWYXNRSOMUQPIEHLKFGAJZBDCV
D:	GINLWUARBOXDVCJZTHYQFMEKSP
E:	NZKPGTELQWCHYAUDISRFOXJVMB
F:	MCBUPIZQFLYJAONEHVTSDRXWKG

8.5.4 Recovery of Plugboard and Fast Rotor

It is difficult to recover the plugboard settings for an unknown machine under normal conditions. However, assuming that similar machine settings (rotors and reflector) are used on two different days but with different plugboard connections, then from this information, we can recover the plugboard settings used on both days and hence penetrate into the machine to recover its internal wiring.

Similar machine conditions with different arrangement of the steckerboard is used to identify stecker settings. Let us assume that the settings for the next day are labeled with lowercase letter (a,b, c, etc). The daily message keys for next day are given in Table 8.4

Table 8.4: Message Keys on Day 2: Enigma

NEX	VYS	APD	ZWH
KXV	LMX	WFQ	PTK
DRW	HGP	JNY	OVC
CGN	SZY	XMO	XIT
UAZ	TRJ	MCS	IEU
SOI	KLM	FYR	DKA
LDH	MCZ	YWL	EOQ
VZG	CJN	EKM	WXR
ZJF	RQV	HLB	API
PIK	YHE	OTC	UNL
BUJ	FSO	QBA	QUB
GVT	BFW	TSP	JAD
RQU	GBF	IHE	NDG

```
AD: (AOZBQFML)(DVUTIPJG)(S)(HNEX)(Y)(KWCR)
BE: (QNHC)(VUDWYTRZG)(IKLA)(JPOXEBSFM)
CF: (TMFVG)(WCKHNPJD)(YBXULEOQ)(RIASZ)

ad: (NVCSKLMI)(DHAZRGBF)(Q)(EWPY)(JOUT)(X)
be: (EYKXMIHDC)(RGZJQBUSA)(FTNV)(LPWO)
cf: (XSUFV)(WPDHZJOT)(EGNYCLQK)(BIMRA)
```

Chains recovered are now superimposed to recover the mapping *SS'*. These chains can be superimposed in a number of ways giving rise to multiple solutions. However, only the correct S and *S'* will give rise to mappings that form uniform chains after the effect of P^i and steckerboard is removed.

```
 ---------------------------------------
     S Y    |  VUDWYTRZG  |   TMFVG
     X Q    |  RGZJQBUSA  |   BIMRA
            |             |
 HNEX  KWCR |  JPOXEBSFM  |   RIASZ
 WPYE  TJOU |  HDCEYKXMI  |   UFVXS
            |             |
 DVUTIPJG   |    QNHC     |  WCKHNPJD
 ZRGBFDHA   |    LPWO     |  JOTWPDHZ
            |             |
 AOZBQFML   |    IKLA     |  YBXULEOQ
 VCSKLMIN   |    FTNV     |  QKEGNYCL
----------------------------------------
```

Taking superimposed pairs, we get: `(NPDZSXEYQL)(AVRUG)(HWJ)(BKT)(FMI)(CO)` Applying the property of reciprocal alphabets again, we can recover both S and S'.

Table 8.5: Steckers Recovered

S:	S′:
NPDZSXEYQL AVRUG HWJ BKT FMI CO	NPDZSXEYQL AVRUG HWJ BKT FMI CO
NLQYEXSZDP RVAGU WHJ BTK MFI OC	PNLQYEXSZD URVAG JWH KBT IMF CO

Once S is recovered (Table 8.5), N can be calculated which is the fast rotor. Also, cumulative mapping Q (M+L+Reflector) can be found by this method.

Fast Rotor = **AXUPJDZBIMRWSOECLFVKGTQYHN**

Only the relative wiring of fast rotor can be recovered by this method. If we apply the shifted versions of the rotor recovered above to the encrypted daily keys, we will get 26 related results. Correct superposition of normal alphabet will produce the desired rotor. Mathematically the indicator keys can be derived using either of these mappings.

```
-------------------------------------------------------
         Rotors                 Inverse of Rotors
-------------------------------------------------------
AHPFORUYIETQJZNDWKMVCSLBXG   AXUPJDZBIMRWSOECLFVKGTQYHN
ZGOENQTXHDSPIYMCVJLUBRKAWF   XUPJDZBIMRWSOECLFVKGTQYHNA
YFNDMPSWGCROHXLBUIKTAQJZVE   UPJDZBIMRWSOECLFVKGTQYHNAX
XEMCLORVFBQNGWKATHJSZPIYUD   PJDZBIMRWSOECLFVKGTQYHNAXU
WDLBKNQUEAPMFVJZSGIRYOHXTC   JDZBIMRWSOECLFVKGTQYHNAXUP
VCKAJMPTDZOLEUIYRFHQXNGWSB   DZBIMRWSOECLFVKGTQYHNAXUPJ
UBJZILOSCYNKDTHXQEGPWMFVRA   ZBIMRWSOECLFVKGTQYHNAXUPJD
TAIYHKNRBXMJCSGWPDFOVLEUQZ   BIMRWSOECLFVKGTQYHNAXUPJDZ
SZHXGJMQAWLIBRFVOCENUKDTPY   IMRWSOECLFVKGTQYHNAXUPJDZB
RYGWFILPZVKHAQEUNBDMTJCSOX   MRWSOECLFVKGTQYHNAXUPJDZBI
QXFVEHKOYUJGZPDTMACLSIBRNW   RWSOECLFVKGTQYHNAXUPJDZBIM
PWEUDGJNXTIFYOCSLZBKRHAQMV   WSOECLFVKGTQYHNAXUPJDZBIMR
OVDTCFIMWSHEXNBRKYAJQGZPLU   SOECLFVKGTQYHNAXUPJDZBIMRW
NUCSBEHLVRGDWMAQJXZIPFYOKT   OECLFVKGTQYHNAXUPJDZBIMRWS
```

```
MTBRADGKUQFCVLZPIWYHOEXNJS   ECLFVKGTQYHNAXUPJDZBIMRWSO
LSAQZCFJTPEBUKYOHVXGNDWMIR   CLFVKGTQYHNAXUPJDZBIMRWSOE
KRZPYBEISODATJXNGUWFMCVLHQ   LFVKGTQYHNAXUPJDZBIMRWSOEC
JQYOXADHRNCZSIWMFTVELBUKGP   FVKGTQYHNAXUPJDZBIMRWSOECL
IPXNWZCGQMBYRHVLESUDKATJFO   VKGTQYHNAXUPJDZBIMRWSOECLF
HOWMVYBFPLAXQGUKDRTCJZSIEN   KGTQYHNAXUPJDZBIMRWSOECLFV
GNVLUXAEOKZWPFTJCQSBIYRHDM   GTQYHNAXUPJDZBIMRWSOECLFVK
FMUKTWZDNJYVOESIBPRAHXQGCL   TQYHNAXUPJDZBIMRWSOECLFVKG
ELTJSVYCMIXUNDRHAOQZGWPFBK   QYHNAXUPJDZBIMRWSOECLFVKGT
DKSIRUXBLHWTMCQGZNPYFVOEAJ   YHNAXUPJDZBIMRWSOECLFVKGTQ
CJRHQTWAKGVSLBPFYMOXEUNDZI   HNAXUPJDZBIMRWSOECLFVKGTQY
BIQGPSVZJFURKAOEXLNWDTMCYH   NAXUPJDZBIMRWSOECLFVKGTQYH
-----------------------------------------------------
```

It can be seen that relative rotors produce shifted inverses. Relative shifts in inverse by modulo26 addition will give rise to shifted rotor mappings

8.5.4.1 Recovery of Middle Rotor

Starting at the correct rotor starting position, partial decipherment of plaintext to monoalphabetic text will help in the recovery of middle rotor from which the cumulative mapping of slow rotor and reflector (L+Reflector) can be found.

The message keys have already been recovered. We need one ciphertext with length covering atleast 5 rotations of middle rotor. Also needed is a possible word/phrase that occurs in the ciphertext to be used as a crib. Army messages contained a lot of cribs. Cribs will aid us in partial decipherment and also to recover the turnover point of middle rotor. Spaces are represented by X in plaintext.

Assume the following messages are encrypted using the same daily keys but different starting positions.

```
LGS - MOEHY UCFVR ZYJAG OOVNF HZFVJ KBVMX NZNGW WDIMY NGBVR
IVBDL URXJM HVZBC PPCNS UCMCN MWAAH QNMAU RZEIN VJHWL HKQTK
NKRYI ZGASZ FAPYO BQYEQ DGIMU NTMWD VVNAZ GTCSH WADBW LAETI
LSASO MUFOC XAAEA SVPOI UGDCJ TCIKR LRNYT OGKNV KMQYY DFZOG
LULLL FUDUI WMYPC ASELK MNGVO UFFYR KGPGN IYOUC BTVXJ GTXFR
VWIYW WMPEY OUSGP VPZZQ LPZZU OEEIY JTYLG JZZUP SKJLS YJFKY
QALGO OKIFA WKKLZ EKJCE MTJHN VYWDF OBDVM MCACD AOWAN KKAUL
LXRXC TITYJ PYRBW TFSEZ GUCCP GGXLH FGCQC RSLYU BCPSZ VSOCZ
CNSKO GMKNU DNRWW XSTNP DYGER WQDLY UOWMV VMEZ

MQL - LNLGY KZUEH DNVKM HVBTG MXAFF FVQMH CNDVS ALIRQ WREIS
EXUJY HIWXG YZNAY SVCLJ ORUII WNWBL OVWSK LIQTM FRAOV BXCUB
VAFON CEZHF CWSYA ZMKYA SYZMW ZBLGN OWCMP DEDQM JDYKN HKUQZ
GIYRW OVYFB DQHPF WPABR KXTQE UAPCQ SWLIV UGOIJ TDAZX CZAWF
LZFRH NWPYR PWBTH VAVVT AGYFK FHGKD XRVMU QAKEX ZHQFK CIMHF
MBLVG DFFTX XVSMP PMFZG IBISV UGFXZ OPDOI BPHVG ARRYH SLABN
DJBSN EHPHU JKVUH KUPLQ BSKJX IUPRP O

KPX - JUWDC TMBZR CPDNC MDKOO FTZHZ AAMOX WZGLC XZQRB BAFIE
KPXKS XEQAS EAIPH ANGSG ZJKQE TNJGN OSYFA DAZMJ MYKZT NBHGM
HBLRR YNDWT DBKAQ YDGJX CDDSK SRRMN LZQRR YVMXT MPCTJ PBGCX
```

```
SNCAF ZLTNF MQUTX CRQKV PVCRM QLMQJ QHMWQ BEZ

NGN - NVPOM USDBB EZLQF OMMNX TYIWT KOIBG GBZIP KNOZL FTKIG
KAKQM CDRIH RJAVM HVBDY WLCIO LXOHA WZPGI EBFQE YRWTK MNJZF
AWWQP HPJDA UJTVR WQLUA JYOZT ZCWAP PCOXS KAYPW LKTZE TEUTW
VLLUU VDFZB WNVGG MVLIM HQPNG SJKAW XTJVB VNVHG ISEIB BZSXZ
IIYNC MNOEH VSTGU NOLPA KIKMO KEYUS SRZWV UFKTA UZZFS YRLYV
GFRFJ QANWQ MIFIM CNXVW FCSJX REGLS EUBPU LJWBH FJGFG ERTRU
```

The message is of military importance and contains the following words: UNITED STATES, MEXICO, SUBMARINE, PRESIDENT

```
MESSAGE 1 - LGS

MOEHY UCFVR ZYJAG OOVNF HZFVJ KBVMX NZNGW WDIMY NGBVR IVBDL
URXJM HVZBC PPCNS UCMCN MWAAH QNMAU RZEIN VJHWL HKQTK NKRYI
ZGASZ FAPYO BQYEQ DGIMU NTMWD VVNAZ GTCSH WADBW LAETI LSASO
MUFOC XAAEA SVPOI UGDCJ TCIKR LRNYT OGKNV KMQYY DFZOG LULLL
FUDUI WMYPC ASELK MNGVO UFFYR KGPGN IYOUC BTVXJ GTXFR VWIYW
WMPEY OUSGP VPZZQ LPZZU OEEIY JTYLG JZZUP SKJLS YJFKY QALGO
OKIFA WKKLZ EKJCE MTJHN VYWDF OBDVM MCACD AOWAN KKAUL LXRXC
TITYJ PYRBW TFSEZ GUCCP GGXLH FGCQC RSLYU BCPSZ VSOCZ CNSKO
GMKNU DNRWW XSTNP DYGER WQDLY UOWMV VMEZ
```

Since Enigma is a reciprocal cipher, so no letter is mapped onto it self.

The message key is known and hence, the effect of fast rotor can be removed. The recovered text will consist of groups of 26 consecutive monoalphabetic enciphered letters. Cribs can be matched against the correct position by using isomorphism of the partially deciphered text [15]. A computer program is written to look for possible isomorphs and, hence, a considerable amount of time is saved.

1) Assumed crib: XSUBMARINEX

It was not found possibly due to shift of the middle rotor in between.

2) Assumed crib: XUNITEDXSTATESX

Possible positioning:

```
HPTAICUBOSHVWFP crib with effect of plugboard and first
                rotor removed
NSXYBJVILPNUQMS ciphertext with effect of plugboard and
                first rotor removed
TMWDVVNAZGTCSHW corresponding ciphertext
ORUYIETQJZNDWKMVCSLBXGAHPF Rotor N
YIJ--M-NBC-OFHLSW-PXVUQTA-  Rotor L + Rotor M + Reflector
```

This rotor position can be traced to letters before and after crib to determine the turnover point

```
    JPVXLIHOWPXT-EXUNITEDXSTATESX--XAMELODN-Z--

PXT-EXUNITEDXSTATESX--XAME Hint: "the", "of"
PXT-EXUNITEDXSTATESXOFXAME
```

The underlined text defines the 26 letter period of middle rotor. Once the turnover of middle rotor is found, the ciphertext can be divided into 26 letter groups with fixed middle rotor.

The crib for next position is RICAX

```
RICAX--UT---X--X-H-XE--N-- Hint: "the"
RICAX--UT-A-X-NXTHEXE--NT- Hint: "in"
RICAX--UT-A-XINXTHEXEV-NT- Hint: "eventx"
RICAX--UT-A-XINXTHEXEVENTX At this point all relative wirings
                           of LMQ are recovered except for 6
                           hence they can be tried at random
                           to recover meaningful text
RICAXNEUTRALXINXTHEXEVENTX
```

3) Assumed crib: `XMEXICOX`

Two possible placements were found for the word mexico.

Placement A

```
HSVLSWDB   crib with effect of plugboard and first rotor removed
VJHYJFEP   ciphertext with effect of plugboard and first rotor removed
LFUDUIWM   corresponding ciphertext
WTQLFZVXEINSOKAYHBRGCPMUDJ  Rotor N
-P-EDW-V-S-Y---B--J--HF-L-  Rotor M + Rotor L + Reflector

-MA--XMEXICOX--PR------X--
```

PR is followed by a vowel. Trying the five vowel possibilities. E and I result in collision and hence they are ruled out.

```
-MAO-XMEXICOX--PRA---R-X--Unlikely
-MA--XMEXICOX--PRU---I-X--
XMA--XMEXICOX--PRO---A-X--Most likely
XMA--XMEXICOX-XPRO-O-A-X--
```

An assumption can be made at this stage to reveal more content. Partially recovered mapping contains a few holes that can be filled.

```
XMA--XMEXICOX-XPRO-O-A-X--Hint: "a"
XMA--XMEXICOXAXPRO-O-A-X--Hint: "proposal"
XMAK-XMEXICOXAXPROPOSALX--Hint: "make"
XMAKEXMEXICOXAXPROPOSALXOF
```

Placement B

```
YVMQHAGG    crib with effect of plugboard and first rotor removed
BKNGETQQ    ciphertext with effect of plugboard and first rotor removed
NPDYGERW    corresponding ciphertext
QNKFZTPRYCHMIEUSBVLAWJGOXD    Rotor N
TY--H-QE--V-NM--G--A-K--B-    Rotor M + Rotor L + Reflector

--E--------XMEXICOXXA---A--Assuming the wiring OU gives us
--EX-SX----XMEXICOXXAN--A--which is a good start. Hint: "is"
--EX-SX----XMEXICOXXAN--A--Hint: "new mexico"
X-EX-SX-NEWXMEXICOXXAND-A--Hint: "and"
XTEXASXXNEWXMEXICOXXANDXAR-
```

At least 4 consecutive cycles are needed to derive chains. The word SUBMARINE is split and text is again examined for possible positioning.

4) Assumed Crib: XSUBMAR

```
NKEPWUV             crib with effect of plugboard and first rotor removed
JVAFQTK             ciphertext with effect of plugboard and first rotor removed
VZBCPPC             corresponding ciphertext
JGDYSMIKRVAFBXNLUOETPCZHQW    Rotor N
E---AP---NV--J-FW--UTKQ---    Rotor M + Rotor L + Reflector


---R-X---E-TR--TEDXSUBMARI 7 missing connections.
                           Try possibilities for a more
                           frequent end to end mapping
---R-X---ESTRI-TEDXSUBMARI Hint: "unrestricted"
RUARYXUNRESTRICTEDXSUBMARI
```

5) Assumed Crib: NEX

As the crib is very small, hence it will result in a large number of gaps. This may require a little patience.

```
JLV
FTB
-V---J---F-T-------L-B----
BYVQKEACJNSXTPFDMGWLHURZIO

NEXW-R------E-------------Assume: "war"
NEXWAR------E-------------Assume: "warfare"
NEXWARFAREX-EX-HA--X--DEA-4 connections left. A random one can be tried
NEXWARFAREX-EXSHAL-XE-DEAV Hint: "shall", "endeavor"
NEXWARFAREX-EXSHALLXENDEAV Hint: "we"
NEXWARFAREXWEXSHALLXENDEAV
```

6) Assumed Crib: ORX

```
HZV
SUM
-------S----V-----H-ZM---U
BYVQKEACJNSXTPFDMGWLHURZIO

ORX-N---I-----------------Assume: "in"
ORXINX--I-----X--I---OXKE-Hint: "keep"
ORXINX--I-E---X--I---OXKEE Assume: "to keep"
ORXINX--I-E--FXT-I-XTOXKEE Hint: "this"
ORXINX--I-E--FXTHISXTOXKEE 3 connections left are tried for
further help
ORXINX-PITEXOFXTHISXTOXKEE Hint: "in spite"
ORXINXSPITEXOFXTHISXTOXKEE
```

7) Assumed Crib: XFEB

```
MHBD
PEXR
-X-RH--E----P--M-D-----B--
```

```
FCZUOIEGNRWBXTJHQKAPLYVDMS

XBEGINXONXTHEXFIRSTXOFXFEB
X-EG-N-O-XT-E----S----XFEB Hint: "the"
XBEG-NXO-XTHEX---S----XFEB Hint: "begin", "on"
XBEGINXONXTHEX--RS----XFEB Hint: "first"
XBEGINXONXTHEXFIRST--FXFEB Hint: "of"
XBEGINXONXTHEXFIRSTXOFXFEB
```

The partially decrypted text is alligned with corresponding ciphertext

```
  XBE GINXO NXTHE XFIRS TXOFX FEBRU ARYXU NREST RICTE DXSUB
MARIN EXWAR FAREX WEXSH ALLXE NDEAV ORXIN XSPIT EXOFX THISX
TOXKE EPXTH EXUNI TEDXS TATES XOFXA MERIC AXNEU TRALX INXTH
EXEVE NTXOF XTHIS XNOTX SUCCE EDING XXWEX MAKEX MEXIC OXAXP
ROPOS ALXOF

  JAG OOVNF HZFVJ KBVMX NZNGW WDIMY NGBVR IVBDL URXJM HVZBC
PPCNS UCMCN MWAAH QNMAU RZEIN VJHWL HKQTK NKRYI ZGASZ FAPYO
BQYEQ DGIMU NTMWD VVNAZ GTCSH WADBW LAETI LSASO MUFOC XAAEA
SVPOI UGDCJ TCIKR LRNYT OGKNV KMQYY DFZOG LULLL FUDUI WMYPC
ASELK MNGVO
```

$$CT = SP_1^{i}NP_1^{-i}P_2^{j}MP_2^{-j}QP_2^{j}M^{-1}P_2^{-j}P_1^{i}N^{-1}P_1^{-i}S^{-1} \tag{8.5}$$

$$P_2^{j}P_1^{-i}NP_1^{i}SCTS^{-1}P_1^{-i}N^{-1}P_1^{i}P_2^{-j} = MP_2^{-j}QP_2^{j}M^{-1} \tag{8.6}$$

The text recovered above used different relative positions of the fast rotor. In order to recover the middle rotor, we will first figure out correct superposition of the resultant mapping so that the effect of rotor N can be removed. The starting position of rotor N is ”S” which means the wheel was at position T when first letter was encrypted. Hence, we can compute that our partially deciphered cryptogram begings at position ”F” of the fast rotor. Assuming the ring setting to be A, the relative wiring of rotor N is recovered.

```
CSLBXGAHPFORUYIETQJZNDWKMV
DTMCYHBIQGPSVZJFURKAOEXLNW
             .
             .
AQJZVEYFNDMPSWGCROHXLBUIKT
BRKAWFZGOENQTXHDSPIYMCVJLU
```

The actual wiring would be rotated by the value equal to ring setting on that wheel. The resultant mappings are taken using using the following fast rotor mapping:

CSLBXGAHPFORUYIETQJZNDWKMV

The end-to-end mapping for recovering the middle rotor is:

```
-------------------------------------------------------
                           | ABCDEFGHIJKLMNOPQRSTUVWXYZ
-------------------------------------------------------
XBEGINXONXTHEXFIRSTXOFXFEB | WEQGBYDIH-ROZULSCKPVNTA-FM
RUARYXUNRESTRICTEDXSUBMARI | OJLH-GFDSBRCQYA-MKIZ--XWNT
NEXWARFAREXWEXSHALLXENDEAV | ETFYACOXZULKSPGNWVMBJRQHDI
ORXINXSPITEXOFXTHISXTOXKEE | XLNGFEDQYS-BTC-UH-JMPZ-AIV
PXTHEXUNITEDXSTATESXOFXAME | PEVXBIM-FNLKGJQAOYZUTC-DRS
RICAXNEUTRALXINXTHEXEVENTX | IFNLYB-VAOMDKCJRTP-QZHXWEU
OFXTHISXNOTXSUCCEEDINGXXWE | -OUYFETXMQ-PIVBLJZWGCNSHDR
XMAKEXMEXICOXAXPROPOSALXOF | EOKJARQSZDCXVYBWGFHUTMPLNI
```

The incomplete mappings in the table can easily be completed. With 4 gaps there are two possiblities of swap that can easily be worked out. However, We will use the last four mappings as they contain no gaps. The relative effect of P^j can be removed by giving shifts j=0,1,2,3 to the consecutive mappings in consideration. The table is then rearranged to prepare chains for recovery of middle rotor.

```
PT ABCDEFGHIJKLMNOPQRSTUVWXYZ
-----------------------------
E: PEVXBIMWFNLKGJQAOYZUTCHDRS
F: IFNLYBSVAOMDKCJRTPGQZHXWEU
G: KOUYFETXMQAPIVBLJZWGCNSHDR
H: EOKJARQSZDCXVYBWGFHUTMPLNI
```

Table 8.6 is obtained after removing the relative effect of shift P^j from the plaintext.

Table 8.6: End-to-end Mapping to recover Middle Rotor

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
--------------------------
PEVXBIMWFNLKGJQAOYZUTCHDRS
VJGOMZCTWBPNELDKSUQHRAIYXF
FTMQWAHGVZOSCRKXDNLBYIEPUJ
OQLHRNMDUTVCGFAYBEZJIKXWPS
```

The rows can be superimposed to form chains which are given below:

```
1-2: (XOSFWTR)(DYUHIZQ)(BMCAKN)(PVGEJL)
2-3: (VFJTGMW)(BZAIECH)(XUNSDK)(OQLRYP)
3-4: (FOVUPWR)(ANEXYIK)(BJSCGD)(TQHMLZ)
```

The chains 1-2, 2-3 and 2-3, 3-4 are superimposed to recover the diagonal sequence.

```
-----------------------------------------------
    Superposition of    |    Superposition of
     1-2,2-3 chains     |     2-3,3-4 chains
------------------------|----------------------
        XOSFWTR         |        VFJTGMW
        HBZAIEC         |        KANEXYI
                        |
        DYUHIZQ         |        OQLRYP
        TGMWVFJ         |        BJSCGD
```

```
                          |
                PVGEJL    |        BZAIECH
                DKXUNS    |        RFOVUPW
                          |
                BMCAKN    |         XUNSDK
                RYPOQL    |         HMLZTQ
--------------------------------------------------
```

The diagonal sequence obtained is: **AOBRCPDTEUMYGXHWIVKQJNLSZF** which is the ”Relative Inverse of Middle Rotor”.

Applying the settings already recovered to the partially decrypted text for all possible rotations to middle rotor will allow us to determine its correct superposition. Since starting position was LGS, hence if assumed that the ring setting is A, the possible rotor M mappings are:

```
FTDXHJRPNLYACEGIZMOQUSWKVB
GUEYIKSQOMZBDFHJANPRVTXLWC
            .
            .
DRBVFHPNLJWYACEGXKMOSQUITZ
ESCWGIQOMKXZBDFHYLNPTRVJUA
```

Any of this mapping can be used in combination with the fixed mapping obtained for slow rotor and reflector (L+Reflector). This fixed mapping is **SZVEDOTLQKJHNMFUIXAGPCYRWB**

The recovered settings are applied to message 1 to decrpyt it. The plaintext obtained is given below:

Plaintext:

```
WEXINTENDXTOXBEGINXONXTHEXFIRSTXOFXFEBRUARYXUNRESTRICTEDXSU
BMARINEXWARFAREXWEXSHALLXENDEAVORXINXSPITEXOFXTHISXTOXKEEPX
THEXUNITEDXSTATESXOFXAMERICAXNEUTRALXINXTHEXEVENTXOFXTHISXN
OTXSUCCEEDINGXXWEXMAKEXMEXICOXAXPROPOSALXOFXALLIANCEXONXTHE
XFOLLOWINGXBASISXMAKEXWARXTOGETHERXXMAKEXPEACEXTOGETHERXXGE
NEROUSXFINANCIALXSUPPORTXANDXANXUNDERSTANDINGXONXOURXPARTXT
HATXMEXICOXISXTOXRECONQUERJASQVYHTYKAYHWALPLGJIAOOKZHDFUSVL
LCAHVBMKHQBCAFYCKWZFV
```

The garbled message in the end is due to shift in the slow rotor.

8.5.5 Recovery of Slow Rotor

Since the first two rotors are found and their effect can be removed, we will look for messages having equal relative displacement of the slow rotor.

```
MESSAGE 2 -  MQL

LNLGY KZUEH DNVKM HVBTG MXAFF FVQMH CNDVS ALIRQ WREIS EXUJY
HIWXG YZNAY SVCLJ ORUII WNWBL OVWSK LIQTM FRAOV BXCUB VAFON
CEZHF CWSYA ZMKYA SYZMW ZBLGN OWCMP DEDQM JDYKN HKUQZ GIYRW
```

```
OVYFB DQHPF WPABR KXTQE UAPCQ SWLIV UGOIJ TDAZX CZAWF LZFRH
NWPYR PWBTH VAVVT AGYFK FHGKD XRVMU QAKEX ZHQFK CIMHF MBLVG
DFFTX XVSMP PMFZG IBISV UGFXZ OPDOI BPHVG ARRYH SLABN DJBSN
EHPHU JKVUH KUPLQ BSKJX IUPRP O
```

The partially decrypted ciphertext is searched for matching cribs.

1) Crib: `XPRESIDENTX`

```
WPNPMCSBJGU
VGHGQBICDPZ
YSVCLJORUII
-CBJ--PNSD--QH-GM-I-ZWV--U  End-to-end mapping
```

Applying this relative mapping to the entire message starting at the correct position, the partially deciphered text is found to be

```
T-EX--T-L-MENTX--X--T-ILXI--LE--X-OX--UX-OUXWIL-XINF---XTH-
XPRESIDENTX--X-H-X-B--E-MO-TXSECR-TL-XAS--OO--A-X-H--OUT--E
---O---G-OKWB-FDCA--OQY-YCKIBF--EHKPQI--F-HIHPCW-YOR--CN-G-
-JXI--W--RI-Y-V-XLC--B--QK---E-AK-HUQ-Y-K-JE-B--B--I--C-OI-
E-E-IARAI----XMKEUKHPUH-OLP-IOND-DLNQ-K-SRH-MK-X-X-XCID----
FG--S--IOYE-MIF-YSY-PWPQH-NRUZJ
```

Partial decryption reveals a lot of text that can be used to determine the complete mapping at this position. This mapping is found to be

KCBJLYPNSDAEQHRGMOIXZWVTFU

The partially recovered message is:

```
THEXSETTLEMENTXINXDETAILXISXLEFTXTOXYOUXYOUXWILLXINFORMXTHE
XPRESIDENTXOFXTHEXABOVEXMOSTXSECRETLYXASXSOONXASXTHEXOUTBRE
AKXOFXXGKOKWBBFDCAJROQYTYCKIBFLLEHKPQIFWFMHIHPCWDYORBDCNHGI
WJXIKUWCWRILYPVCXLCYQBULQKTCZESAKEHUQPYJKNJEMBRLBDZINECWOID
EZEQIARAIUCANXMKEUKHPUHQOLPPIONDFDLNQZKBSRHMMKAXJXPXCIDULRZ
FGRHSDPIOYEPMIFIYSYDPWPQHHNRUZJ
```

The garbled text is due to another shift in the slow rotor.

```
MESSAGE 3 - KPX
JUWDC TMBZR CPDNC MDKOO FTZHZ AAMOX WZGLC XZQRB BAFIE KPXKS
XEQAS EAIPH ANGSG ZJKQE TNJGN OSYFA DAZMJ MYKZT NBHGM HBLRR
YNDWT DBKAQ YDGJX CDDSK SRRMN LZQRR YVMXT MPCTJ PBGCX SNCAF
ZLTNF MQUTX CRQKV PVCRM QLMQJ QHMWQ BEZ
```

1) Crib: `XPRESIDENTX`

beginverbatim WUTSNPNJIEB MLJVFCFTKZD MDKOOFTZHZA -DPBZN–KTIUWF-C–VJLSM–E endverbatim

Partially recovered text for message 3 is

```
---ASEXCAL-X-HEXPRESIDENTX--AT-ENTI-NXT--THEXF-CTXTHATX-HEX
-UT---SS-E-PLOY--NTXOFXOURX-U-M-RIN-S-NOWXOF-ER-----XP-O-PE
CT----CO---L-INGX--GJY-IS-B--Y--L--WE-FD-H-C-C-LY-LQJ-NW-F-
I-YHC-
```

Missing characters are used as hints to derive the complete mapping. The recovered message is

XDPBZNHGKTIUWFQCOYVJLSMARE

```
PLEASEXCALLXTHEXPRESIDENTXSXATTENTIONXTOXTHEXFACTXTHATXTHEX
RUTHLESSXEMPLOYMENTXOFXOURXSUBMARINESXNOWXOFFERSXTHEXPROSPE
CTXOFXCOMPELLINGXENGJYDISIBWVYHELREWETFDXHQCPCJLYULQJUNWBFV
IPYHCY
```

```
MESSAGE 4 - NGN
```

```
NVPOM USDBB EZLQF OMMNX TYIWT KOIBG GBZIP KNOZL FTKIG KAKQM
CDRIH RJAVM HVBDY WLCIO LXOHA WZPGI EBFQE YRWTK MNJZF AWWQP
HPJDA UJTVR WQLUA JYOZT ZCWAP PCOXS KAYPW LKTZE TEUTW VLLUU
VDFZB WNVGG MVLIM HQPNG SJKAW XTJVB VNVHG ISEIB BZSXZ IIYNC
MNOEH VSTGU NOLPA KIKMO KEYUS SRZWV UFKTA UZZFS YRLYV GFRFJ
QANWQ MIFIM CNXVW FCSJX REGLS EUBPU LJWBH FJGFG ERTRU
```

Crib: XUNITEDXSTATESX

```
VQLXWAYQBHBBJOW
WLQYVEXLSDSSPIV
KAYPWLKTZETEUTW
ES-HA--DOP-Q--IJL-B--WVYX-
```

Applying the partially recovered mapping the entire message reveals a lot of hints which can help derive the complete mapping.

```
THEXZIMME---NNX-ELEG-A----SXAXD-PLOMATI-XPRO-O-AL--ROM-T-E-
G--MANXE---RE-FO--MEXI-O-----OI-X---X-E-TRALX-OWERSXI-XTH-X
E--N-XOF--HEXUNITEDXSTATESXE-T-RING-WO-L-XWAR-I--N---E--I--
-OFXT-E-------EXPO-E-S----X-IM--R-ANN----EGRA-X--S-IN--R-EP
TE---ND---C-D---BYXTHEX-R--ISH-CRY--OGRAPH-R-X-FX--OMX--R-Y
```

The recovered mapping is ESTHANZDOPMQKFIJLUBCRWVYXG The underlying plaintext is found to be

```
THEXZIMMERMANNXTELEGRAMXWASXAXDIPLOMATICXPROPOSALXFROMXTHEX
GERMANXEMPIREXFORXMEXICOXTOXJOINXTHEXCENTRALXPOWERSXINXTHEX
EVENTXOFXTHEXUNITEDXSTATESXENTERINGXWORLDXWARXIXONXTHEXSIDE
XOFXTHEXENTENTEXPOWERSXTHEXZIMMERMANNXTELEGRAMXWASXINTERCEP
TEDXANDXDECODEDXBYXTHEXBRITISHXCRYPTOGRAPHERSXOFXROOMXFORTY
```

Arranging the above mappings in increasing order of relative shifts for slow rotor, we get the following table

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
XDPBZNHGKTIUWFQCOYVJLSMARE
SZVEDOTLQKJHNMFUIXAGPCYRWB
KCBJLYPNSDAEQHRGMOIXZWVTFU
ESTHANZDOPMQKFIJLUBCRWVYXG
```

endgroup

The relative effect of P^j can be removed by giving shifts j=0,1,2,3 to the consecutive mappings in consideration. The table is then rearranged to prepare chains for recovery of slow rotor.

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
XDPBZNHGKTIUWFQCOYVJLSMARE
CTAWFEPUMRLKIONGVJYBHQDZSX
HWMEDLNARPUFCGSJTIOQKZBYXV
BAJHVWKDQCGRSPTNILMOXEFUZY
```

Chains obtained for slow rotor are

```
1-2: (XCGUKMDTRSQNE)(PAZFOVYJBWILH)
2-3: (CHKFDBQZYOGJI)(TWELUAMRPNSXV)
3-4: (HBFRQOMJNKXZE)(DVYUGPCSTILWA)
```

Chains are superimposed to recover the slow rotor.

```
-------------------------------------------------
    Superposition of    |    Superposition of
     1-2,2-3 chains     |     2-3,3-4 chains
------------------------|------------------------
     XCGUKMDTRSQNE      |      CHKFDBQZYOGJI
     AMRPNSXVTWELU      |      MJNKXZEHBFRQO
                        |
     PAZFOVYJBWILH      |      TWELUAMRPNSXV
     ICHKFDBQZYOGJ      |      VYUGPCSTILWAD
-------------------------------------------------
```

By taking superimposed pairs, we have found the relative inverse of slow rotor which is ACMSWYBZHJQEUPIOFKNLGRTVDX

Applying the settings already recovered to the partially decrypted text along with possible rotations of slow rotor will allow us to determine its correct superposition. Since starting position was LGS, hence if assumed that ring setting is A the possible rotor L mappings are:

```
AGBYLQUIOJRTCSPNKVDWMXEZFH
BHCZMRVJPKSUDTQOLWEXNYFAGI
             .
             .
YEZWJOSGMHPRAQNLITBUKVCXDF
ZFAXKPTHNIQSBROMJUCVLWDYEG
```

Any of this mapping can be used in combination with the corresponding fixed mapping obtained for reflector. This is true for the sample text we have used to derive this mapping. However, for longer messages other than in the sample, there will be one unique solution which is the actual wiring of slow rotor (assuming ring setting = A)

The slow rotor, thus used is **AGBYLQUIOJRTCSPNKVDWMXEZFH**

Since, a turnover of slow rotor was observed in message 1, hence we will try all rotations of this recovered wiring on the second part of the message. The one corresponding to correct decipherment will have the highest IC.

```
IC =

    1  :  0.0378
    2  :  0.0386
    3  :  0.0379
    4  :  0.0381
    5  :  0.0395
    6  :  0.0415
    7  :  0.0386
    8  :  0.0391
    9  :  0.0392
   10  :  0.0378
   11  :  0.0387
   12  :  0.0399
   13  :  0.0375
   14  :  0.0391
   15  :  0.0376
   16  :  0.0373
   17  :  0.0829  <-- Highest value
   18  :  0.0385
   19  :  0.0389
   20  :  0.0398
   21  :  0.0373
   22  :  0.0388
   23  :  0.0395
   24  :  0.0386
   25  :  0.0406
   26  :  0.0388
```

Hence the correct wiring of rotor L is : KVDWMXEZFHAGBYLQUIOJRTCSPN And the reflector is found to be: FXJRHAIEGCYVZTWQPDUNSLOBKM

8.6 Recovered Enigma Settings

Steckerboard - RBOQSMUWIJTPFNCLDAEKGVHXZY

Table 8.7: Recovered Wirings of Enigma Machine

Rotor	Wiring
N	CSLBXGAHPFORUYIETQJZNDWKMV
M	FTDXHJRPNLYACEGIZMOQUSWKVB
L	KVDWMXEZFHAGBYLQUIOJRTCSPN
Reflector	FXJRHAIEGCYVZTWQPDUNSLOBKM

Thus the correct recovered messages using the settings given in Table 8.7 are:
Message 1:

```
WEXINTENDXTOXBEGINXONXTHEXFIRSTXOFXFEBRUARYXUNRESTRICTEDXSUB
MARINEXWARFAREXWEXSHALLXENDEAVORXINXSPITEXOFXTHISXTOXKEEPXTH
```

```
EXUNITEDXSTATESXOFXAMERICAXNEUTRALXINXTHEXEVENTXOFXTHISXNOTX
SUCCEEDINGXXWEXMAKEXMEXICOXAXPROPOSALXOFXALLIANCEXONXTHEXFOL
LOWINGXBASISXMAKEXWARXTOGETHERXXMAKEXPEACEXTOGETHERXXGENEROU
SXFINANCIALXSUPPORTXANDXANXUNDERSTANDINGXONXOURXPARTXTHATXME
XICOXISXTOXRECONQUERXTHEXLOSTXTERRITORYXINXTEXASXXNEWXMEXICO
XXANDXARIZONAX - IC = 0.0819
```

Message 2:

```
THEXSETTLEMENTXINXDETAILXISXLEFTXTOXYOUXYOUXWILLXINFORMXTHEX
PRESIDENTXOFXTHEXABOVEXMOSTXSECRETLYXASXSOONXASXTHEXOUTBREAK
XOFXWARXWITHXTHEXUNITEDXSTATESXOFXAMERICAXISXCERTAINXANDXADD
XTHEXSUGGESTIONXTHATXHEXSHOULDXONXHISXOWNXINITIATIVEXINVITEX
JAPANXTOXIMMEDIATEXADHERENCEXANDXATXTHEXSAMEXTIMEXMEDIATEXBE
TWEENXJAPANXANDXOURSELVESX - IC = 0.0829
```

Message 3:

```
PLEASEXCALLXTHEXPRESIDENTXSXATTENTIONXTOXTHEXFACTXTHATXTHEXR
UTHLESSXEMPLOYMENTXOFXOURXSUBMARINESXNOWXOFFERSXTHEXPROSPECT
XOFXCOMPELLINGXENGLANDXINXAXFEWXMONTHSXTOXMAKEXPEACEXZIMMERM
ANN - IC = 0.0732
```

Message 4:

```
THEXZIMMERMANNXTELEGRAMXWASXAXDIPLOMATICXPROPOSALXFROMXTHEXG
ERMANXEMPIREXFORXMEXICOXTOXJOINXTHEXCENTRALXPOWERSXINXTHEXEV
ENTXOFXTHEXUNITEDXSTATESXENTERINGXWORLDXWARXIXONXTHEXSIDEXOF
XTHEXENTENTEXPOWERSXTHEXZIMMERMANNXTELEGRAMXWASXINTERCEPTEDX
ANDXDECODEDXBYXTHEXBRITISHXCRYPTOGRAPHERSXOFXROOMXFORTY - IC
 = 0.0774
```

8.7 Ring Settings

This enigma machine can be used to replicate the original one except that the ring settings now discovered using this machine would actually give the relative displacement with respect to the original one.

If the original ring settings become known, then its effect can be removed to replicate the same rotor in practice.

Assuming the ring settings are: BRE

The relative wiring is displaced by an amount that is equal to the ring setting. Hence, for normal alphabet a ring shift of 1 would give us the new mapping as:

```
ABCDEF
FECBDA Mapping
BAFDCE Ring = 1
FCBAED Ring = 2
```

Thus, removing the effect of ring settings from the three rotors would give us the underlined mappings as original rotor mappings

```
      N Ring setting = E        M Ring Setting = R        L Ring Setting = B
CSLBXGAHPFORUYIETQJZNDWKMV FTDXHJRPNLYACEGIZMOQUSWKVB KVDWMXEZFHAGBYLQUIOJRTCSPN
TCWDLBKNQUEAPMFVJZSGIRYOHX VXZDBFTEKOCMGQSAYWUHJLNPRI UCVLWDYEGZFAXKPTHNIQSBROMJ
```

```
CSLBXGAHPFORUYIETQJZNDWKMV FTDXHJRPNLYACEGIZMOQUSWKVB KVDWMXEZFHAGBYLQUIOJRTCSPN
TCWDLBKNQUEAPMFVJZSGIRYOHX VXZDBFTEKOCMGQSAYWUHJLNPRI UCVLWDYEGZFAXKPTHNIQSBROMJ
UDXEMCLORVFBQNGWKATHJSZPIY WYAECGUFLPDNHRTBZXVIKMOQSJ VDWMXEZFHAGBYLQUIOJRTCSPNK
VEYFNDMPSWGCROHXLBUIKTAQJZ XZBFDHVGMQEOISUCAYWJLNPRTK WEXNYFAGIBHCZMRVJPKSUDTQOL
WFZGOENQTXHDSPIYMCVJLUBRKA YACGEIWHNRFPJTVDBZXKMOQSUL XFYOZGBHJCIDANSWKQLTVEURPM
XGAHPFORUYIETQJZNDWKMVCSLB ZBDHFJXIOSGQKUWECAYLNPRTVM YGZPAHCIKDJEBOTXLRMUWFVSQN
YHBIQGPSVZJFURKAOEXLNWDTMC ACEIGKYJPTHRLVXFDBZMOQSUWN ZHAQBIDJLEKFCPUYMSNVXGWTRO
ZICJRHQTWAKGVSLBPFYMOXEUND BDFJHLZKQUISMWYGECANPRTVXO AIBRCJEKMFLGDQVZNTOWYHXUSP
AJDKSIRUXBLHWTMCQGZNPYFVOE CEGKIMALRVJTNXZHFDBOQSUWYP BJCSDKFLNGMHERWAOUPXZIYVTQ
BKELTJSVYCMIXUNDRHAOQZGWPF DFHLJNBMSWKUOYAIGECPRTVXZQ CKDTELGMOHNIFSXBPVQYAJZWUR
CLFMUKTWZDNJYVOESIBPRAHXQG EGIMKOCNTXLVPZBJHFDQSUWYAR DLEUFMHNPIOJGTYCQWRZBKAXVS
DMGNVLUXAEOKZWPFTJCQSBIYRH FHJNLPDOUYMWQACKIGERTVXZBS EMFVGNIOQJPKHUZDRXSACLBYWT
ENHOWMVYBFPLAXQGUKDRTCJZSI GIKOMQEPVZNXRBDLJHFSUWYACT FNGWHOJPRKQLIVAESYTBDMCZXU
FOIPXNWZCGQMBYRHVLESUDKATJ HJLPNRFQWAOYSCEMKIGTVXZBDU GOHXIPKQSLRMJWBFTZUCENDAYV
GPJQYOXADHRNCZSIWMFTVELBUK IKMQOSGRXBPZTDFNLJHUWYACEV HPIYJQLRTMSNKXCGUAVDFOEBZW
HQKRZPYBEISODATJXNGUWFMCVL JLNRPTHSYCQAUEGOMKIVXZBDFW IQJZKRMSUNTOLYDHVBWEGPFCAX
IRLSAQZCFJTPEBUKYOHVXGNDWM KMOSQUITZDRBVFHPNLJWYACEGX JRKALSNTVOUPMZEIWCXFHQGDBY
JSMTBRADGKUQFCVLZPIWYHOEXN LNPTRVJUAESCWGIQOMKXZBDFHY KSLBMTOUWPVQNAFJXDYGIRHECZ
KTNUCSBEHLVRGDWMAQJXZIPFYO MOQUSWKVBFTDXHJRPNLYACEGIZ LTMCNUPVXQWROBGKYEZHJSIFDA
LUOVDTCFIMWSHEXNBRKYAJQGZP NPRVTXLWCGUEYIKSQOMZBDFHJA MUNDOVQWYRXSPCHLZFAIKTJGEB
MVPWEUDGJNXTIFYOCSLZBKRHAQ OQSWUYMXDHVFZJLTRPNACEGIKB NVOEPWRXZSYTQDIMAGBJLUKHFC
NWQXFVEHKOYUJGZPDTMACLSIBR PRTXVZNYEIWGAKMUSQOBDFHJLC OWPFQXSYATZUREJNBHCKMVLIGD
OXRYGWFILPZVKHAQEUNBDMTJCS QSUYWAOZFJXHBLNVTRPCEGIKMD PXQGRYTZBUAVSFKOCIDLNWMJHE
PYSZHXGJMQAWLIBRFVOCENUKDT RTVZXBPAGKYICMOWUSQDFHJLNE QYRHSZUACVBWTGLPDJEMOXNKIF
QZTAIYHKNRBXMJCSGWPDFOVLEU SUWAYCQBHLZJDNPXVTREGIKMOF RZSITAVBDWCXUHMQEKFNPYOLJG
RAUBJZILOSCYNKDTHXQEGPWMFV TVXBZDRCIMAKEOQYWUSFHJLNPG SATJUBWCEXDYVINRFLGOQZPMKH
SBVCKAJMPTDZOLEUIYRFHQXNGW UWYCAESDJNBLFPRZXVTGIKMOQH TBUKVCXDFYEZWJOSGMHPRAQNLI
TCWDLBKNQUEAPMFVJZSGIRYOHX VXZDBFTEKOCMGQSAYWUHJLNPRI UCVLWDYEGZFAXKPTHNIQSBROMJ
```

The ring effect can be removed and starting with the correct shift for rotor N and some ciphertext, the corresponding correct value of rotor M and L and the reflector can be worked out easily using the same approach. These results can be verified on a message encrypted using different ring settings than this example.

Chapter 9

Background on Pinwheel Ciphers

Pinwheel Ciphers are mechanical cryptosystems which can be viewed as predecessors to the modern stream ciphers based on LFSRs. Boris Hagelin introduced the class of cipher machines based on pinwheels by developing a prototype called B-21. Later, a lot of machines were developed by Hagelin who made a fortune by selling them. Some of the machines based on this principle include M-209 (C-38) C-35 and C-36. C-35 and its revised version C-36 were used by the French military, whereas, M-209 was used by the U.S. military during World War II. C-52 was the improved version of M-209 and was one of the last machine ciphers to be developed before the trend shifted to digital ciphers [24].

9.1 Mechanics of Pinwheel Cipher

9.1.1 Construction

A pinwheel cipher machine is a mechanical cipher machine which consists of two main components responsible for encryption namely the pinwheels and the lug cage.

9.1.1.1 Pinwheel

A pinwheel consists of a rotating wheel with equidistant positions marked around its outer edge. Each position is labeled by an alphabet and bears a pin that can be set in either an active or an inactive position. During operation, a mechanical lever is pulled that causes each pinwheel in the assembly to turn forward by one position [30].

9.1.1.2 Lug Cage

The second internal component responsible for encryption is the lug cage. It consists of metal rods carrying two lugs which can either be set against any pinwheel or in a neutral position. The earlier version of pinwheel ciphers had a fixed lug cage but later version consisted of movable lugs, hence, increasing the key space for daily settings. When the power handle is turned, the entire lug cage makes a complete rotation to determine the shift alphabet used for encryption.

9.1.2 Modes of Operation

While the encryption and decryption operations for a pinheel cipher are identical and interchangeable, however, there are two separate modes to identify encryption and decryption processes. The reason for this discretion is that the letter *"Z"* is used to represent spaces in plaintext. For the encryption process, the ciphertext is printed out in groups of five letters. During decryption,

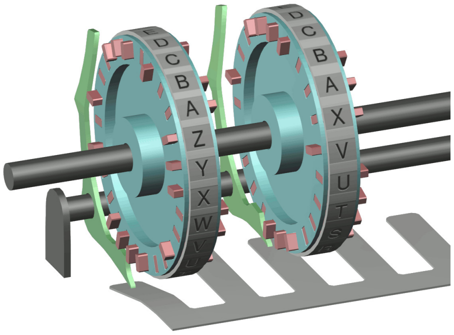


Figure 9.1: An assembly of two pinwheels with pins arranged in active and inactive positions

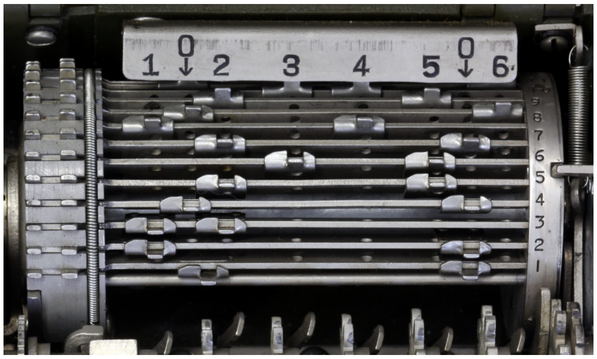


Figure 9.2: Lug cage setting for a Six Pinwheel Cipher

the cipher text includes no such spaces, however, the letter *"Z"* is not printed; thus making the deciphered text intelligible and easy to read.

9.2 Mathematics behind Pinwheel Ciphers

9.2.1 Encryption Process

Pinwheel ciphers produce a keysteam of random shifts which are combined with plaintext to give the ciphertext. The shift produced depends on a particular arrangement of the pins on pinwheels and lugs in the lug cage. Pinwheels are chosen in such a way that their lengths are relatively prime to maximize the period of the cipher. The cipher machine used to explain the encryption/decryption process has three pinwheels of lengths 5, 4 and 3. The underlined alphabets indicate that the pins are in active position for those alphabets. The lug cage used has 6 bars and is set up as shown in Table 9.1.

Pinwheel 1: [A$\underline{\text{B}}$BC$\underline{\text{DE}}$]
Pinwheel 2: [$\underline{\text{AB}}$CD]
Pinwheel 3: [$\underline{\text{A}}$BC]

To calculate the shifts, we need to convert the pinwheels and lug cage in their respective binary equivalents. Presence of a 1 indicates that a pin is active for a particular pinwheel. In lug cage, presence of one indicates that there is a lug present in that position.

Table 9.1: Settings of Pinwheels and Lug Cage

Pinwheel 1:	0	1	0	1	1
Pinwheel 2:	1	1	0	0	
Pinwheel 3:	1	0	0		

Lug Cage Arrangement:

1	1	0
0	1	0
0	0	1
0	1	0
1	0	0
1	0	0

The ciphertext letter is calculated according to Equation 9.1 after subtracting 5 where required:

$$CT = (6 - PT + n) \tag{9.1}$$

where n is the shift value, CT is the ciphertext letter and emphPT is the input plaintext letter.

Assume that a pinwheel cipher has been set up according to the settings given in Table 9.1. If the initial starting position of the pinwheels is *”CAB”* when the first letter was encrypted, then the input string *’BEAD’* is encrypted to *’BADB’*. The step-by-step procedure is given in Table 9.2.

Table 9.2: Step by step encipherment of plaintext using the key settings

PT	Active Lugs in in position A (n_1)	Active Lugs in position B (n_2)	Active Lugs in in position C (n_3)	Total number of Overlapping Lugs(n_4)	Displacement N = $n_1 + n_2$ $+n_3 - n_4$	CT
B	0	3	0	0	3	B
E	3	3	0	1	5	A
A	0	3	1	0	4	D
D	0	0	0	0	0	B

The decryption process is similar to encryption process. Equation 9.1 is rearranged to produce the decryption equation which is:

$$PT = (6CT + n) - - - - - (i) \tag{9.2}$$

The encrypted string obtained in the above example can be used to demonstrate the decryption process which is given in Table 9.3.

Table 9.3: Step by step decipherment of plaintext using the key settings

PT	Active Lugs in in position A (n_1)	Active Lugs in position B (n_2)	Active Lugs in in position C (n_3)	Total number of Overlapping Lugs(n_4)	Displacement $N = n_1 + n_2 + n_3 - n_4$	CT
B	0	3	0	0	3	B
A	3	3	0	1	5	E
D	0	3	1	0	4	A
B	0	0	0	0	0	D

9.2.2 Table Generation

If the same pinwheel cipher is taken, a table can be plotted for it to relate input and output alphabets for all possible shift values. By examining that table, we can see that it consists of rows of shifted reverse alphabets. Such a table is known as Beaufort Tableau.

9.2.3 Beaufort Table and its properties

Like a Vigenere Tableau, a Beaufort Tableau also consists of shifted rows of the same sequence. However, unlike the Vigenere cipher, the sequence used here consists of reversed standard alphabets. M-209 employs Beaufort Tableau for encryption/decryption. Moreover, shifts 0 and 26 have the same net effect. A Beaufort Table is shown in figure.

9.2.3.1 Reciprocity

Beaufort tableau give rise to reciprocal alphabets when shifted. Unlike the reflector in which a letter can never be mapped onto itself, a Beaufort cipher can produce shifts which result in the same letter being mapped onto itself. For example in second row of Table 9.4, A is mapped to A and N is mapped to N. In Beaufort table, the alphabets are basically shifted with respect to each other by the amount equal to the shift.

9.2.3.2 Symmetry of Position

The Beaufort tableau exhibits direct symmetry of position which means that the relative shift between a pair of plaintext letters is reflected in the ciphertext too. For example, letters E and F which are one letter displaced are mapped onto W and V in first row which are also one letter displaced in the mixed cipher sequence. In row three, they are replaced by Y and X which are also one letter apart in the mixed cipher sequence.

Table 9.4: A Beaufort Tableau

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

Chapter 10

Literature Review on Pinwheel Ciphers

This chapter describes the related research work done on analyzing pinwheel ciphers. The different approaches used to cryptanalyze the M-209 cipher machine are also particularly discussed. Each paper is discussed separately due to its unique approach at cryptanalysis.

10.1 Entropy Calculations and Particular Methods Of Cryptanalysis

This paper written by James Reeds has derived formulas to determine the minimum length of cryptogram required to break a certain cipher machine. Unicity distance(U) defines the theoretical minimum length of cryptogram required to break a cipher. It is derived using Shannon's equation. A certain length L¿U at which a cipher becomes practically solvable is derived and its upper and lower bounds are discussed in the paper in detail. The results are applied to find the length of cryptogram needed to break M-209. The theoretical lower bound has been found to be of 1200 characters which means that for cryptograms of lengths greater than 1200, a unique solution is likely to be obtained [31, 32].

10.2 Cryptanalysis of Hagelin Machine Pinwheels

In this paper, Geoff Sullivan presents a cipher-text only attack on Hagelin CD-57 cipher machine with the assumption that lug settings and underlying plaintext frequency are known. Starting with random distribution of pins on each pinwheel, the hill climbing algorithm is used torecover the pin settings. Index of coincidence and bigram and trigram frequencies are used to make decision about the existing pinwheel settings. The approach is also applied to analyze an M-209 cipher machine. The technique employed is modified and longer message lengths are used in second part of the paper to perform ciphertext only analysis of CD-57 and M-209 with unknown pin and lug cage settings. Different rates of success are achieved under varying conditions [33].

10.3 The Hagelin Cipher Machine (M-209): Reconstruction of the Internal Settings

In this paper, Robert Morris applies a known plaintext attack on a cryptogram enciphering using M-209. The pin settings and the lug cage are unknown. The attack is statistical in nature such that the active pins on each wheel give displacements which lie within one range whereas the inactive pins produce a whole different set of displacements. The attack involves making guess about each pin position using the average displacement calculated for that each position. Each wheel is assessed separately. The results are then combined and the effect of completely recovered pinwheel is removed to reassess the remaining wheels. The lug settings are obtained from the displacement values already provided and by making use of the recovered pinwheels [34].

10.4 Cryptanalysis of the Uncaged Hagelin

H. Paul Greenough describes a similar approach as Morris to recover the internal settings of a generalized M-209 cipher machine. The shift values are obtained from known plaintext. They are rearranged in columns for each pinwheel such that the displacements along each row correspond to one position of the pin. A special residue matrix which has 26 columns is plotted for each pinwheel. 1 is entered in each position which represents a pair in the corresponding row of the pinwheel distribution. The resulting gaps will create two different patterns. The rows sharing the same pattern will belong to same group. The pin settings will this be recovered in this manner. Paul Greenough has implented this techniqe to C-52 cipher machine in a paper titled *" Cryptanalysis of the Hagelin C-52 and similar machines a known plaintext attack"* [35].

10.5 Solving A Hagelin, Type CD-57, Cipher

Wayne Barker derives the solution to a problem presented by Louis Kruh in Cryptologia. Given two messages in depth that have overlapping key settings and a crib, solution is obtained by identifying the correct position of the crib and hence recovering some part of the key. Revealed text results in more cribs and the two messages are thus simultaneously solved [36].

10.6 German Cryptanalytic device for the solution of M-209 Traffic

This is a top secret document which was declassified by NSA in 2011. It is based on a manual which was retrieved from Germans around 1948. It is based on the working of the German version of Bombe which they created to decipher the M-209 intercepted traffic using known or assumed plaintext [37].

Chapter 11

Attack Methodology for Pinwheel Ciphers

This chapter describes the underlying principles and proposed methodology for solving pinwheel ciphers when no information about the pin positions and lug cage is available.

11.1 Underlying Principles

Since the attack we will describe in later section is statistical in nature and requires a large amount of ciphertext, hence the principle used behind this attack is first described.

11.1.1 Index of Coincidence

Index of Coincidence is a well known technique is cryptanalysis, discovered first by William Friedman and published in a as a detailed manuscript titled *"The Index of Coincidence and its Applications in Cryptanalysis"* in 1922 [21]. It is the measure of probability that two letters drawn randomly from a given text are identical.

$$IC = c \times \left(\left(\frac{n_a}{N} + \frac{n_a - 1}{N-1} \right) + \left(\frac{n_b}{N} + \frac{n_b - 1}{N-1} \right) + ... + \left(\frac{n_z}{N} + \frac{n_z - 1}{N-1} \right) \right) \tag{11.1}$$

where n_a is the number of times the letter $'a'$ appears in the text and so on. N is the total number of letters in the given piece of text. Equation 11.1 can be summarized as below:

$$IC = \frac{\sum_{i=1}^{c} n_i \left(n_i - 1 \right)}{N \left(N - 1 \right) / c} \tag{11.2}$$

For uniformly distributed text, all probabilities are equal, and hence IC value is approximately 0.0385. For English text, the frequency distribution is uneven and some letters are more probable than others so the IC value is close to 0.066.

11.1.1.1 Properties of Index of Coincidence

Index of Coincidence has a number of properties that are useful for cryptanalysis.

- Language Identification
  It can help to identify the language of underlying plaintext if it is monoalphabetically enciphered. For example, consider the following ciphertext:

```
TQXKT NK NUFRQRUTSH KYZNAS. NT NK WRQKYUAS,
QRSATNLR, KNTXATNYUAS, AUJ OSXNJ. NT NK UYT
XUNIXRSH FXBAU, EXT NT NK TFR XUJRQWNUUNUM
YO RLRQHTFNUM VR FALR AZZYBWSNKFRJ AK A
KWRZNRK. VR TQXKT YTFRQ WRYWSR, EXT VR ASKY
TQXKT YQMAUNCATNYUK AUJ WQYZRKKRK. TFR
WKHZFYSYMH NK ZYBWSRG, EXT VFRU VR TQXKT A
TRZFUYSYMH, VR EAKNZASSH ERSNRLR TFAT NT
VNSS VYQP AK NUTRUJRJ.
```

Index of coincidence is calculated on this ciphertext and found to be 0.063 which shows it is likely to be a monoalphabetically enciphered English text. In English, there are 26 alphabets so the normalized IC value is 1.73 (26 x 0.066). Normalized IC value for German is 2.05, Russian 1.76, Spanish 1.94 and for French this value is 2.02.

- Nature of Cipher
  Index of Coincidence can help us decide whether two ciphertexts were encrypted using the same encryption scheme. Consider the same ciphertext used in the above example. Another piece of text is encrypted twice; first by using a monoalphabetic cipher and then a polyalphabetic scheme. The two texts are written out below for correlation and to find coincidences between them. This IC representation has been given the name of Kappa. Kappa value for plaintext is 0.066.

Ciphertext 1:

```
TQXKT NKNUF RQRUT SHKYZ NASNT NKWRQ KYUAS QRSAT
NLRKN TXATN YUASA UJOSX NJNTN KUYTX UNIXR SHFXB
AUEXT NTNKT FRXUJ RQWNU UNUMY ORLRQ HTFNU MVRFA
LRAZZ YBWSN KFRJA KAKWR ZNRKV RTQXK TYTFR QWRYW
SREXT VRASK YTQXK TYQMA UNCAT NYUKA UJWQY ZRKKR
KTFRW KHZFY SYMHN KZYBW SRGEX TVFRU VRTQX KTATR
ZFUYS YMHVR EAKNZ ASSHE RSNRL RTFAT NTVNS SVYQP
AKNUT RUJRJ
```

Ciphertext 2:

```
VCICR FBEAP BTXDW FUXWC DRPBC TFIIE KDXGR XTWZC
YKXDD KTWFD TFVPK AIFNX AXCZR DTWFA AJFVV XBDAF
OXXYK CHVXZ RAFID XVXDD FNXDP BRBFA ACTRP FIRXB
FZXZX VEDHX BTXHR CPZPA BXFIC REVPG XBZGF EVCIC
RFBEH IFZZX BDZXX GFTFH FQCIC RERWF RNPXD QXEPZ
GRWXT KBBXZ RDRFR XPARW XFBRC ZTEQX BGXTX HRCPZ
RPHBP UCGXF DEDRX VPBDE DRXVD RWFRT FZQXX VHIPE
XGQEF TPVVF ZGXBS WXZZX XGXGR PXZFQ IXGXT XHRCP
ZRPQX CZDXB RXGCZ RPGXA XZDCU XTEQX BPHXB FRCPZ
D
```

The number of Coincidences found are 16. Hence, by applying the Kappa Test the observed Kappa value Ko is 16/290 = 0.0552

Similarly the Kappa value is calculated again by comparing the first text with another encryption of the second text.
Ciphertext 1:

```
TQXKT NKNUF RQRUT SHKYZ NASNT NKWRQ KYUAS QRSAT
NLRKN TXATN YUASA UJOSX NJNTN KUYTX UNIXR SHFXB
AUEXT NTNKT FRXUJ RQWNU UNUMY ORLRQ HTFNU MVRFA
LRAZZ YBWSN KFRJA KAKWR ZNRKV RTQXK TYTFR QWRYW
SREXT VRASK YTQXK TYQMA UNCAT NYUKA UJWQY ZRKKR
```

```
KTFRW KHZFY SYMHN KZYBW SRGEX TVFRU VRTQX KTATR
ZFUYS YMHVR EAKNZ ASSHE RSNRL RTFAT NTVNS SVYQP
AKNUT RUJRJ
```

Ciphertext 3:

```
XNOWV VXXFH NQUHO VFIPL FQBAQ DYZKX LDJUG BTMYK
JXGGN CPEND LOHAU YKVQK JKRAS CSHME PZFCH RFHGT
HINJF GXJKP EIVDZ PJONC SISNK IMEVQ XNHCH TGBJX
MFBWR DYWGJ YNIKC GWZFY GLXJW GEFDJ MHIJW SQBJN
XXDFE KOHGY GVGHI LYSIG OPHKJ COVVV CILQX RMOBJ
BBSYT KANRG CHVRS RDIFI FJOCE PTAUR CANXW ECOQQ
FPDED ZDOKZ XOGWT NXAVP WFQSZ CMZZP UYBER CVJHV
JLBXV MJMTD KNRXW ONWCR MRGQG VKNUN SVPPD RZCPR
HXZHR KAWOD CVSBC CZWLU KBGON RLWET LKGBF PVRAC
Q
```

The Kappa value in this case is 10/90 = 0.0345 Based on these results, it is more likely that the first encryption is monoalphabetic and second is polyalphabetic.

- Determination of Key Length
  It can help determine the key length of a repeated-key cipher. The cryptogram is broken down into a series of columns each encrypted by same key and the index of coincidence is calculated separately on each column. With the ciphertext broken down into correct number of columns, the overall average IC will increase indication that the correct key length has been identified. Consider the following cryptogram that has been enciphered using polyalphabetic cipher:

  ```
  OHXCL VWEJK WTYDZ FRGZC EXSBT MFIBJ DDYSM XFIYC
  ZFGDE FQWGD QFOKD ABVEX JGJZL DQWGU AJGCT XXDAF
  DGGYS HBVYB MAGQO XOGOD GEGDN PMBGU ACFXS FBXGB
  GBGZY CNDUG WTYRM CNBSA XGFIT XNVNS GBKSF EOHXC
  LVWEU QFZKG WDKGG GGMFH GNJIT XNRCV MNNGO QYJSZ
  QXZXF FWBYB MDLVM XNUMW YVWRT BQEHG WGYMG HLHSZ
  LKBBN AJGYV OEEXG VNPOE EXGVE XZFLM FZHGG VUQSE
  YSPEG MSVOV YGYPR WYBYX YSGGL KGZGN XXQGQ XUXJP
  KXSQY HYDYP MXQHY RNSGA YBOCR GQEHG WPUGW FLHSZ
  E
  ```

  A table is drawn for calculating the Index of Coincidence by using different key lengths (Table: 11.1).
  Maximum value for IC is observed at lengths 4, 8 and 12. Hence, key is likely to be 4.

11.1.2 Chi Test

Solomon Kullback made a variation to the Index of Coincidence test for comparing that how closely one distribution matches with the other and the test is known Chi Test. The mathematical notation for calculating Chi value is:

$$Chi\ value = \sum_{i=A}^{Z} \frac{f_1\left(n\right) \times f_2\left(n\right)}{N_1 \times N_2} \tag{11.3}$$

where f_1 is the frequency of first distribution, f_2 is the frequency of second distribution and N_1 and N_2 are the total number of letters in each distribution.

For random distribution, the chi value has a smaller value. This value is maximized when the two distributions are aligned. For, example when analyzing a shift cipher on a computer, the correct solution can be easily identified using Chi test to compare test distribution with plaintext distribution. Consider the following cryptogram enciphered using Caesar cipher:

Table 11.1: Average Index of Coincidence corresponding to different key lengths

Shifts	Chi Values
1	0.0486
2	0.0583
3	0.0496
4	0.0697
5	0.0500
6	0.0604
7	0.0457
8	0.0708
9	0.0523
10	0.0595
11	0.0536
12	0.0732

```
WUXVW LVLQK HUHQW OBVRF LDOLW LVSHU VRQDO UHODW LYHVL
WXDWL RQDOD QGIOX LGLWL VQRWX QLTXH OBKXP DQEXW LWLVW
KHXQG HUSLQ QLQJR IHYHU BWKLQ JZHKD YHDFF RPSOL VKHGD
VDVSH FLHVZ HWUXV WRWKH USHRS OHEXW ZHDOV RWUXV WRUJD
QLCDW LRQVD QGSUR FHVVH VWKHS VBFKR ORJBL VFRPS OHAEX
WZKHQ ZHWUX VWDWH FKQRO RJBZH EDVLF DOOBE HOLHY HWKDW
LWZLO OZRUN DVLQW HQGHG
```

Taking f_1 as the frequency distribution of decrypted text using different shift values, it is correlated with f_2 which is frequency fistribution of a sample plaintext in English language. The Chi values for various shift values are given in table 11.2.

Table 11.2: Chi values corresponding to different shifts

Shifts	Chi Values	Shifts	Chi Values
1	0.0322	14	0.0459
2	0.0379	15	0.0357
3	0.0623	16	0.0434
4	0.0383	17	0.0385
5	0.0332	18	0.0463
6	0.0360	19	0.0407
7	0.0465	20	0.0343
8	0.0374	21	0.0360
9	0.0355	22	0.0363
10	0.0409	23	0.0397
11	0.0318	24	0.0290
12	0.0341	25	0.0419
13	0.0341		

Maximum chi value is observed at a shift of 3 hence it can be concluded that the cryptogram was enciphered using Caesar cipher having a shift value of 3.

11.2 Known Plaintext Attack on M-209

Robert Morris has described a known plaintext attack on M-209 cipher [reference] to recover its internal settings - positions of pins on the pinwheel and the lug cage parameters. While the attack methodology we describe in next section uses only ciphertext but the underlying principle is the same. Hence, before explaining our methodology, an example from Morris' paper is replicated to explain the effect of active pins on the displacement [reference]. This will allow us to define a few theorems that we can apply to our technique described in the next section.

It is assumed that the following sequence of displacements have been derived using some ciphertext and its corresponding plaintext.

22 *0 5 18 17 24 15 13 3 15 *1 8 *1 *1 24 14 15 18 2
3 18 20 13 18 4 16 21 25 *1 4 *1 20 14 23 4 24 19 15 15
18 3 12 20 3 2 16 16 14 *1 23 18 12 18 9 11 16 23 14 16
15 15 9 *1 13 6 3 4 9 21 24 15 14 16 23

Since the displacement of 0 and 26, and 1 and 27 have the same net effect hence these displacements are marked with an asterisk. The solution is achieved in two steps

1. Recovery of the six pinwheels
2. Arrangement of lug cage

To recover the pinwheels, the first step involves determining the effect of each position of a pinwheel on the displacement obtained. For this purpose, the ciphertext is written out into columns such that the position of the pin remains the same throughout the row. Such tables are drawn for all six pinwheels and the average displacement is calculated along each row. Since the displacements represented by *0 and *1 are not confirmed hence they are not used in calculating the average. The average displacements obtained for each wheel are plotted on a histogram and are seen to exhibit bimodality. It can be seen that the displacements roughly fall into two clusters.

(Find plots on next page)

The reason for this behavior is that each value represents the average displacement with the corresponding wheel in that position. If the position corresponds to an inactive pin then the displacement just represents the average contribution from all other wheels, whereas, an active pin represents the average effect of other pinwheels as well as its own contribution. With longer sequences and for pinwheels with more lugs set, this effect would be even more prominent and the displacements would fall neatly into two clusters.

Before continuing the cryptanalysis process, several important conclusions are drawn which we'll refer to as theorems and apply in later chapters. If a bar has two effective lugs and they both engage during encipherment, it will still have the same net contribution in shift. Hence, for any pinwheel, if x_i is the number of effective lugs on a pinwheel and y_i is the sum of double engagements involving that wheel, we can draw the following conclusions:

1. For all i, $x_i \geq \mathrm{y}_i$ or $x_i - y_i \geq 0$
2. If 27 is the total number of bars in the lug cage, then it is equal to the maximum possible shift (if no bar contains both lugs in neutral positions)
3. For all i, $\sum x_i - \frac{1}{2} \sum y_i \leq 27$
4. If a is the minimum shift value observed for all active positions on the wheel, then $a = x_i$
5. If b is the maximum shift value observed for all inactive positions on the wheel, then $x_i - y_i = 27\text{- } b$ which gives us the number of unique lugs on the wheel

If the average displacement neatly falls into the upper cluster, that position of the wheel is active and for the low average displacement, the pin is set as inactive. Ambiguous pins can be marked with a *”?”* and reassessed later based on the derived pinwheels. Since wheels 3 and 4 show higher bimodality so we will try to assess them first so their effect can be removed:

Pinwheel 3: 11011110001101?1?100000
Pinwheel 4: 11000?1110?10101???00

The next step would be to resolve the ambiguous displacements. The displacements corresponding to an active pin on pinwheels 3 and 4 would be 26 and 27 while for an inactive pin they will be 0 and 1. The wheels are reassessed and some more positions can be identified. We are far from the solution at this stage but this much explanation is sufficient to build the theory on which our attack principle is based.

11.3 Ciphertext Only Attack Principle

As studied in the last section, the range of displacements which correspond to an active pin fall in one cluster while the ones corresponding to an inactive pin fall in the other. A pinwheel cipher generates multiple displacements ranging between 0 and 27 depending on the number of pinwheels if the lug cage is assumed to consist of 27 bars. The arrangement of pins and lugs directly affects this number. Hence, for a pinwheel cipher a safe assumption would be that the displacements are greater than 15 and the period of cipher is unknown. The concept is explained with reference to the example in previous section hence a 6 pinwheel cipher is assumed to be used. For an unknown ciphertext, we cannot obtain the displacements. However, by investigating each wheel separately the division between clusters can be achieved based on the following two observations:

1. The displacement values corresponding to active pins belong to one cluster whereas those belonging to inactive pins belong to another. Hence the ciphertexts obtained corresponding to inactive positions will have a different distribution as opposed to those obtained for active positions.
2. Distributions corresponding to same pin settings will show more similarity to each other than the distributions belonging to different pin settings.
3. Chi test can be applied to compare distributions corresponding to different pin positions and identify which of these belong to the same group.

Since the key space is large and we wish to perform statistical analysis, hence a large amount of ciphertext is required; usually 3000 characters. This is too much data to be handled on a paper hence a computer program is used to perform frequency counts and chi tests.

11.3.1 Assessment of Pinwheels

Each pinwheel is assessed separately like in the previous section. The ciphertext is written out into columns and the frequency count is taken along each row. The next step now is to compare these distributions and analyze if the underlying pin setting is the same or not. Chi value for two distributions is calculated using Equation 11.4.

$$Chi\ value = \sum_{i=A}^{Z} f_1\left(n\right) \times f_2\left(n\right) \tag{11.4}$$

For a pinwheel having 26 letters, we have 26 distributions that need to be compared which means we will have a total of 325 (26x25/2) chi values. The average chi value is then computed for all distributions. It is impossible to recover pin positions by just using these chi values for comparison. We need a precise approach which gives us reasonable proof that the guesses we make are correct. The methodology we have used achieves this by taking two distributions and comparing their chi value with the average chi value. Next the distributions are matched against other distributions. If both the distributions have their chi values above or below average they belong to the same group, otherwise they belong to different groups. A count is kept each time two distributions are found to fall in one group. An upper and lower bound is defined for each pinwheel. If the counter is greater than upper bound both distributions belong to same group *(XX or YY)* and if the count is less than lower bound the distributions belong to different groups *(XY)*. In between, the ambiguous positions are marked with *”?”* Since we only set out to find out if distributions belong to the same cluster or different without knowing the pin is active or inactive, hence the positions are marked with *”X”* and *”Y”*. Thus, 26 distributions are obtained by comparing each position relatively. Since the labels are given arbitrarily, hence it is likely that X is active on some distributions and Y on the other. The distributions are lined up so that there are minimum contradictions and the count is taken along each column this time to identify the relative position of the pin. Positions are confirmed if the count value is 65% of the total pins. Contradictions are again labeled as ”?”

```
-------------------------------------------------------------------
% Comparing distributions of all rows with each other: Calculating
% CHI values

for i=1:N-1 % N = length of pinwheel under consideration
    for j=i+1:N
        chi1 = sum(f1_count(i,:));  chi2 = sum(f1_count(j,:));
        match = f1_count(i,:).*f1_count(j,:); % Chi analysis of
        FaFb_1(n) = sum(match);     % consecutive positions
        FaFb_matrix(i,j) = FaFb_1(n);
        FaFb_matrix(j,i) = FaFb_matrix(i,j);
        n=n+1;
    end
end
mean = (sum(FaFb_1))/(N*(N-1)/2);  % calculating mean chi value
---------------------------------------------------------------------

---------------------------------------------------------------------
%% Comparing distribution with mean to find position of pinwheel %%

for i=1:N-1
    result(1:N) = -19; % Relative comparison of two
    for j=i+1:N % positions by comparing with
        n = 0;  compare = 1:N;   % mean and also with other positions
        x = FaFb_matrix(i,j)-mean;
        if x>0
            n = n+1;
            if x>SD/2, n = n+1; end
        end
        compare = compare(compare~=i);  compare = compare(compare~=j);
        for k=1:length(compare)
            a = FaFb_matrix(compare(k),i)-mean;
            b = FaFb_matrix(compare(k),j)-mean;
            if a>0 && b>0
                n = n+1;
            elseif a<0 && b<0
                n = n+1;
            end
        end
        result(i) = 1;
        if n>u_limit(counter) % Limits compared to draw
            result(j) = result(i); % results
        elseif n<l_limit(counter)
            result(j) = -1;
        else
            result(j) = 0;
        end
    end
    result_matrix(i,:) = result;
end
-------------------------------------------------------------------
```

After the initial assessment is complete, we will have the positions on pinwheels divided into three groups - *X*, *Y* and *?*. Since the positions are determined on relative basis, hence, it is likely that *X* corresponds to active pin on some pinwheels and inactive on others. The best guessed wheel is then chosen to reassess all the other wheels and solve the remaining ambiguous positions. The same theory is applied again after removing the effect of the best guessed wheel. The current distribution along each row is such that one pin is fixed which means that there are 32 substitution alphabets used per row. Using the best guessed wheel, the ciphertext in each row for the remaining wheels is divided into two passages - one corresponding to an active position and the other corresponding to inactive position. Hence, for each row instead of one ciphertext using 32 alphabets we will have two ciphertexts each using 16 alphabets. If f_1 is the frequency count of distribution 1 and g_1 is the frequency count of distribution 2 corresponding to active pin position then the new chi value is computed using Equation 11.5.

$$Chi\ Value = \sum_{n=A}^{Z} f_1(n)g_1(n) + f_2(n)g_2(n) \tag{11.5}$$

Again the average *chi value* is computed and all wheels are assessed. Some of the ambiguous positions are sorted out. The next best wheel is then used to divide ciphertext into two groups and the pinwheels are assessed again. Each time some of the unknown positions are resolved. After a few attempts, all the pinwheel positions will be recovered.

```
---------------------------------------------------------------------------
for i=1:N-1
    for j=i+1:N
        match1 = sum(f1_count(i,:).*f1_count(j,:)); % Pinwheel positions are
        match2 = sum(f2_count(i,:).*f2_count(j,:)); % reassessed based on
        FaFb_1(n) = match1+match2;     % the best guessed wheel
        FaFb_matrix(i,j) = FaFb_1(n);
        FaFb_matrix(j,i) = FaFb_matrix(i,j);
        n=n+1;
    end
end
mean = (sum(FaFb_1))/(N*(N-1)/2);
-----------------------------------------------------------------------------
```

11.3.2 Recovery of Pinwheels and Lug Cage

Only the relative positions of pinwheels are recovered. The next step is to recover the actual pin settings and the lug cage parameters. Since we have substantial amount of ciphertext, hence, we can break-up this text into 64 groups each corresponding to a position of the basic pins. Each group is encrypted using a single shift value. In *M-209* enciphering, space is represented by *”Z”*, hence, some similar sample text is used to compare each distribution by applying various shifts. A high chi value corresponds to the correct shift value. The positions corresponding to shift value of zero are identified and investigated. Taking the base setting at that shift as 000000, the pinwheels are uniquely identified. Our guess is confirmed by checking the shift values corresponding to effective lugs present in each pinwheel position. This is achieved through a special *upper triangular matrix* that we have given the name *Lug Matrix.*

$$LugMatrix = \begin{bmatrix} L_{11} & L_{12} & L_{13} & . & . & . & L_{1j} \\ 0 & L_{22} & L_{23} & . & . & . & L_{2j} \\ 0 & 0 & L_{33} & . & . & . & L_{3j} \\ 0 & 0 & 0 & . & . & . & . \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 & L_{jj} \end{bmatrix}$$

where for all i,j such that $j > i$, L_{ij} corresponds to shift value produced by the presence of effective lugs in positions i and j and for all i,j such that $i = j$, L_{ij} corresponds to shift values produced by the presence of effective lugs only in position i or j (since $i = j$). It is also equal to the number of effective lugs in that position.

Using the *Lug Matrix*, the displacement is calculated for settings involving shared lugs. Correct identification of pinwheels will result in values that are consistent and produce no contradiction. The settings can then be applied to decrypt the cryptogram.

In next chapters, this statistical approach is applied to investigate a two pinwheel cipher and a four pinwheel cipher. The method is then used to recover the internal settings of an *M-209* machine.

Chapter 12

Cryptanalysis of a Two Pinwheel Cipher

The statistical attack described in the last chapter is used to cryptanalyze a specially designed two pinwheel cipher. The principle is then applied to higher order systems in next chapters.

12.1 Construction

A two pinwheel cipher consists of two pinwheels with lengths 25 and 26. The lug cage has 27 bars each of which carries two lugs. The lugs can be set against any pinwheel or in neutral position. The encryption equation for a two pinwheel cipher is:

$$CT = 27 - PT + shift \tag{12.1}$$

Multiples of 26 are subtracted from Equation **??** when required Decryption is identical to encryption with ciphertext being replaced by plaintext and vice versa. During encryption, space is replaced by the letter *"Z"*.

12.2 Key Space

The key space depends on two parameters; the possible positioning of pins on the pinwheels and the number of possible arrangements of lug cage. Pinwheel 1 can be set in 2^{26} ways whereas pinwheel 2 can be set in 2^{25} ways. Together there are 2^{51} ways in which the pins can be arranged. Each bar holds two lugs which can be placed in 4 possible ways. The entire lug cage can, therefore, be arranged in ${}^{30}_{27}\mathrm{C} ways$.

${}^{30}_{27}\mathrm{C} = \frac{30!}{27!3!} \cong 4.06 \times 10^3 (12.2)$

The total keyspace is, therefore
$\mathrm{N} = 2^{51} \times 4.06 \times 10^3 N \cong 9.1423 \times 10^{18}$

12.3 Period

Since the keywheels are of relatively prime lengths, hence, the period of two pinwheel cipher is 26 x 25 = 650.

12.4 Cryptanalysis

The following text is encrypted using the above pinwheel cipher:

```
KVIFU ITHQC GJSDX OHCZM AZWIF IUXQK HBILI BBFKT WXOPW
VIHQY CHHUF ZGRCL WKOCX KTMOX IUDGK WSLVK IUDCA ZHZGN
WXJIL WIOSD CNXGI INKGU XIBWG FKOFG ARDIM RHXKS INOTW
XSPKI TCICX AMJIJ RUVKQ BKFJC LEKEB QZCHN PVNOZ XHGBV
OAVXY TNXRA JOWKO XQLLS PIVRP TMVVO IKOCT PCFTH QGKRU
ZWFED CFFYA JFSMX SHCFM IFSMQ RRVIZ MWVKN ZQBVM KJBRI
VXRCH OZXUO AHFKG VQKRD PIXVJ CFVPX HURHH GRTOC QZUZJ
KMXQD NSXCF LPRSX VMOAB OGIOU FCWFJ PQVKR CJOEI QZSGL
MRKZM KAHPT ODRJD JKBWE AUTNV HK
```

The cryptogram used is of length 387. One with fewer alphabets than this can also be solved since the total number of displacements is only 4. However, we have used a longer ciphertext for the sake of explanation.

12.4.1 Recovery of Pinwheels

The ciphertext is written out into 26 columns and then 25 columns to analyze the position of the pins. The upper bound for comparison is taken as 16 and 15 for the two pinwheels while the lower bound is chosen to be 10 and 9. The two pinwheels are analyzed to look for positions that beling to the same group.

Aligning relative pin positions obtained after comparison between all the rows, the final pin arrangement for the two pinwheels after first assessment is found as follows:

```
Pinwheel 1:  & YX?XYX?YXXY??X?YYXYYY??XX?
Pinwheel 2:  & X?X??X?YXX?YYYXYXX?XXYY?Y
```

Next, the partial settings recovered are used to remove the effect of one wheel. Both wheels are chosen turn wise to reassess the other wheel trusting the already recovered positions.

By removing the effect of pinwheel 1, the reassessed wheels obtained are:

```
Pinwheel 1: & YX?XYX?YXXY??X?YYXYYY??XX?
Pinwheel 2: & X?X??X?YXX?YYYXYXX?XXYY?Y
```

If the effect of pinwheel 2 is removed instead, the results we obtain are:

```
Pinwheel 1: & YX?XYXXYXXY??XXYYXYYY??XX?
Pinwheel 2: & X?X??X?YXX?YYYXYXX?XXYY?Y
```

The results are combined to identify some more pinwheel positions. These new pinwheels are then used to perform the same assessment and the results obtained are:

```
Pinwheel 1: &YX?XYXXYXXY??XXYYXYYY??XX?
Pinwheel 2: &XYXY?X?YXX?YYYXYXXYXXYYXY
```

The process is repeated and the pin positions are gradually recovered.

```
Pinwheel 1:   YX?XYXXYXXYXXXXYYXYYY??XX?
Pinwheel 2:   XYXY?X?YXX?YYYXYXXYXXYYXY

Pinwheel 1:   YXXXYXXYXXYXXXXYYXYYY??XX?
Pinwheel 2:   XYXY?XXYXX?YYYXYXXYXXYYXY

Pinwheel 1:   YXXXYXXYXXYXXXXYYXYYY??XXY
Pinwheel 2:   XYXY?XXYXX?YYYXYXXYXXYYXY

Pinwheel 1:   YXXXYXXYXXYXXXXYYXYYYYXXXY
Pinwheel 2:   XYXYYXXYXXXYYYXYXXYXXYYXY
```

12.4.2 Recovery of Pin Identities

In order to recover the lug cage, we will first have to identify which group of pins on each pinwheel correspond to active position. Since the pins are already divided into groups, hence they can be used to break the cipher text into four groups *(XX, XY, YX, YY)* each corresponding to one particular monoalphabetic shift. A sample of plaintext in which space is replaced by Z is used to compute chi values and recover pin identities and the lug cage. Each group of ciphertext is decrypted using Equation 12.1 with shift values varying from 0 to 25 and compared with the distribution of sample plaintext. A high chi value corresponds to correct shift. The chi values corresponding to a combination of *"YX"* are given below for all possible shifts.

Shifts	Chi Values				
0-4	0.069868	0.04063	0.025347	0.029284	0.035248
5-10	0.041632	0.047339	0.037298	0.033897	0.033524
11-15	0.033431	0.051207	0.044288	0.035388	0.037974
16-20	0.048644	0.034852	0.041911	0.029587	0.029051
21-25	0.040746	0.047642	0.041306	0.024508	0.026116

It is likely to obtain high chi values for more than one shift if the size of enciphered distribution is small. In the above case, we have high chi values for shift 0 and need not consider any other shift values due to large difference between the chi values. For smaller distributions, the best four shifts are considered for all possible combinations of pins to check for any contradictions while deriving the lug settings. While we will continue to use the shifts corresponding to highest chi value (owing to large amount of ciphertext), but a table is still drawn listing the next top 3 shifts. When both pins are inactive, the corresponding shift value is 0. The combination YX corresponds to shift value of 0. This implies that YX corresponds to a setting of 00. Therefore, Y corresponds to inactive pins in pinwheel 1, whereas X corresponds to inactive pins in pinwheel 2. The recovered pinwheels are:

Table 12.1: Shift values corresponding to different pin arrangements for top five Chi values

XX	XY	YX	YY
2	10	0	8
23	5	11	14
8	25	15	13
17	15	21	3
16	4	6	19

```
Pinwheel 1:   01110110110111100100001110
Pinwheel 2:   0101100100011101001001101
```

12.4.3 Recovery of Lug Cage

The next stage involves the recovery of lug settings. This is done with the help of a lug matrix.It gives the shift values corresponding to different pin settings.

The Lug Matrix, L for the above cipher is found to be

$$L = \begin{bmatrix} 2 & 10 \\ 0 & 8 \end{bmatrix}$$

Where there are 2 effective lugs corresponding to pinwheel 1 and 8 effective lugs corresponding to pinwheel 2. The shift produced when both pins are active is 10. Hence the lug matrix shows no contradictions. The cryptogram is deciphered using the above lug settings and the correct plaintext is recovered.

```
POTENTIAL TARGETS IN INTERNET SABOTAGE INCLUDE
ALL ASPECTS OF THE INTERNET FROM THE BACKBONES
OF THE WEB TO THE INTERNET SERVICE PROVIDERS
TO THE VARYING TYPES OF DATA COMMUNICATION
MEDIUMS AND NETWORK EQUIPMENT THIS WOULD
INCLUDE WEB SERVERS ENTERPRISE INFORMATION
SYSTEMS CLIENT SERVER SYSTEMS COMMUNICATION
LINKS NETWORK EQUIPMENT AND THE DESKTOPS AND
LAPTOPS IN BUSINESSES AND HOMES
```

Hence using statistical analysis of cryptogram, the two pinwheel cipher has been completely solved. The solution consists of the derived internal settings and the deciphered plaintext.

Chapter 13

Cryptanalysis of a Four Pinwheel Cipher

After successfully cryptanalyzing a two pinwheel cipher, the methodology is extended to a cryptosystem based on four pinwheels. The conditions remain the same that the internal settings are unknown and only ciphertext is given.

13.1 Construction

A four pinwheel cipher consists of four pinwheels with lengths 21, 23, 25 and 26. The lug cage has 27 bars each of which bears two lugs. The lugs can be set against any pinwheel or in neutral position. The encryption equation for a four pinwheel cipher is:

$$CT = 27 - PT + shift \tag{13.1}$$

where multiples of 26 are subtracted when required. Decryption is identical to encryption with ciphertext being replaced by plaintext and vice versa. During encryption, space is replaced by the letter *"Z"*.

13.2 Key Space

The key space depends on two parameters; the possible combinations of pins on the pinwheels and the number of possible arrangements of lug cage. Pinwheel 1 can be set in 2^{26} ways, pinwheel 2 can be set in 2^{25} ways and similarly pinwheels 3 and 4 can be set in 2^{23} and 2^{21} different ways. Together there are 2^{95} ways in which the pins can be arranged. Each bar holds two lugs and the total possible arrangements of two lugs on a bar can be calculated as below:

Number of different arrangements for lugs on a bar

= C(4,0) + C(4,1) + C(4,2) = 1+1+6 =8

Hence, on a single bar the lugs can be arranged in 8 different ways. Thus, the number of ways in which the entire lug cage can be set up are:

34C27 = 34!/27!7! = 5379616

The total keyspace is, therefore

N = 2^{95} x 5379616 N   2.1311 x 10^{3}5

13.3 Period

Since the lengths of the keywheels is relatively prime, hence, the period of a four pinwheel cipher is 26 x 25 x 23 x 21 = 313950

13.4 Cryptanalysis

The following text is encrypted using the above pinwheel cipher:

```
EYLVN VRDBI GOJKQ ENHRZ TPOAW SWZPG JCJTC NRKZA OKHWU ZTPNW
XJCFX HIEZK OTVXV XUMKV RGNDL MKNKZ IDLBJ RTAWT ASHNG YLNHB
PPKHJ KGEIH ZWSPX PWLYI OXLEP VRKRQ QYTRM DQRSQ NKLIL CKVMO
DKKUJ MIUKX LHOOB ESNLQ ANRML JFWPT MWNSP PEAAN ZUQHS EMRCI
BDZGZ LKSJI XZGPE ZIBVY WVHRV CPZZF TNGLA WNCBG HZIRA QXEYI
PPHAO PWBAP ACOVT GKWYM NHEQT GTZNW HJVMC OXNLH TFLVM MPFNU
BPIXA FOKHL RITDN XANSM QTPBE QWXRT ZAFZC MGSOB ZWSTW CYBEZ
NIUOV MTFAC JHTVL NRYPI FLDQI DEJLR KGHME OUJQV VBREJ MVIXJ
PSFLB CJJQA AZINN LRZYK IWPJS FXPAH BNITM NAKAG FRWAB AGWQW
FNNVE WWZUF YDBJT ZABAF MWKJJ VNVML KLOTN JEDJT ZECIX PKWRD
DSCUO QROWZ WKXCA OVXHW RMJYK BXSCU SZJMZ ZCPHL XKCXM QISQK
LLWQX NREXJ IPEBC MPYRG YNKXC KBLMV ZPVHT CXEDA NWAAN UGJQX
LQGMZ CYWMK IHJDH AZVYO TPJJM SZDZK LIAMO LZIXE NNKGF POVMQ
OBUZD MZTHU KGLPB PWFGQ QKXCY EZVNN HTFJT DAZNZ RLCXC AZBCI
EFVDC MDPNS UNRLI EVNFH XZJMZ YGJQY SNNMM PAZWK AEQXB NVGFK
BXGNJ QSVUT YCGYO TNGSM RYBOS POQIO LMTNY BGAXN GVHBM HRJOF
AWGLE GMDMB VYNVC UANIW XVSQZ NURCS XLZHQ PHWOM PADNH MUKBX
GCJTP LPJPN TXSOL PXDCJ AXBBV RVMUX YIGMS WHIWW AHRKB GZNWD
NFTQM IIQKP UCUZT ZGRNI TYPHZ POVDJ SJGIC OLXNH WXCNZ ZJXNM
FLXHZ QIRYQ VIIYC IHMAA WWNGA JXKKV SYIJX QNVIB JPTFA NRQTV
XIVHJ LXKMR KYATG RVUMT IPRWV KKDTP XLPYV RRRKP OVYUC RFBWU
AFISE YONIE IOPKC KBYRS JKNLX EVCXB AYBGM FTJEA OLLHT JSSLA
TFKYJ WXRXA YVRXC UCMGU RYGAG RPSYK MUUEE ICZVX KNEWF UGALG
KKWMW MNBAG WMWYB BKAXQ QMWUC QDJZN NXJWH TPUXH MYOMU ZKSNX
OGACA MNZVX YDONB WIXHE ZFRQW AZHFA HFSGY LNOFW HMVRB AAELL
MLHDY KCXFX SFTSC ASAKU YUGMN YDLOV UMOIC YSEEV CEIHX GIINQ
VHPBA JXCLT MCMNH DPWSA NKMNU AU
```

The length of the cryptogram is about 1300. One with fewer alphabets than this can also be solved, however, one would require to do manual tweaking with code to achieve a complete or partial solution.

13.4.1 Recovery of Pinwheels

The ciphertext is written out into 26, 25, 23 and then 21 columns to analyze the positions of the pins. The upper and lower bounds used for comparison are stated in Table 13.1.

Table 13.1: Upper and Lower bound of different pinwheels

	Pinwheel Lengths			
	26	25	23	21
Upper Bound	16	15	14	13
Lower Bound	10	9	8	7

Aligning relative pin positions obtained after comparison between all the rows, the final pin arrangement for the four pinwheels after first assessment is found as follows:

```
Pinwheel 1:   ?????????????????YX??????Y
Pinwheel 2:   YYYXYX?YXX?XYYX?YXXXX?YX?
Pinwheel 3:   XYXY?????XYY??XY??Y?Y??
Pinwheel 4:   ?X???Y??Y?XY??X?????Y
```

Next, the partial settings recovered are used to remove the effect of one wheel. Since most of the pin positions for pinwheel 2 have been resolved, hence, it is used to assess the remaining pinwheels. After removing the effect of pinwheel 2, the reassessed wheels obtained are:

```
Pinwheel 1:   Y???????????YYYXXYXYY?XYXY
Pinwheel 2:   YYYXYX?YXX?XYYX?YXXXX?YX?
Pinwheel 3:   XYXY????XXYY??XY??Y?Y?X
Pinwheel 4:   ?X???Y??Y?XY??X?????Y
```

The reassessment process is continued using another wheel. Pinwheel 1 is now used and the new pin positions obtained are:

```
Pinwheel 1:   Y???????????YYYXXYXYY?XYXY
Pinwheel 2:   YYYXYXXYXX?XYYXXYXXXX?YX?
Pinwheel 3:   XYXY????XXYY??XY??Y?Y?X
Pinwheel 4:   XX???Y??Y?XY??X?????Y
```

Pinwheel 2 is almost completely recovered. It is again used to reassess other wheel and some more pin settings are resolved as shown below:

```
Pinwheel 1:   YXX?XXYXX?XXYYYXXYXYYXXYXY
Pinwheel 2:   YYYXYXXYXX?XYYXXYXXXX?YX?
Pinwheel 3:   XYXYY???XXYY??XY??Y?Y?X
Pinwheel 4:   XX???Y??YYXY??X?????Y
```

Pinwheel 1 is also completely determined except for two positions. Using pinwheel 1 to reassess other wheels, we get the new positions as:

```
Pinwheel 1:   YXX?XXYXX?XXYYYXXYXYYXXYXY
Pinwheel 2:   YYYXYXXYXX?XYYXXYXXXX?YXY
Pinwheel 3:   XYXYY?Y?XXYYX?XYYXYXY?X
Pinwheel 4:   XXY?XY??YYXY??XX?Y??Y
```

Most of the pin settings have been recovered for pinwheels 3 and 4 as well. Using them to reassess other wheels leads us to the complete solution after a few assessments.

The final pin settings recovered are:

```
Pinwheel 1:   YXXXXXYXXYXXYYYXXYXYYXXYXY
Pinwheel 2:   YYYXYXXYXXYXYYXXYXXXXYYXY
Pinwheel 3:   XYXYYXYXXXYYXXXYYXYXYXX
Pinwheel 4:   XXYYXYYXYYXYYXXXXYXYY
```

13.4.2 Recovery of Pin Identities

In order to recover the lug cage, we need to identify which class of pins are represented by X and which are represented by Y on each pinwheel. we will first have to identify which group of pins on each pinwheel corresponds to active position. Since the pins are already divided into groups, hence they can be used to break the cipher text into 16 different groups (XXXX, XXXY, XXYX, etc) each corresponding to one particular monoalphabetic shift. A sample of plaintext in which space is replaced by Z is used to compute chi values and recover pin identities and the lug cage. Each group of ciphertext is decrypted using equation (2) with shift values varying from 0 to 25 and compared with the distribution of sample plaintext. A high chi value corresponds to correct shift. The chi values corresponding to a combination of ”YXXY” are given below for all possible shifts.

Shifts			Chi Values		
0-4	0.079117	0.042004	0.02989	0.028888	0.036297
5-10	0.041142	0.042401	0.036646	0.043822	0.034363
11-15	0.033431	0.051207	0.044288	0.035388	0.037974
16-20	0.022575	0.043099	0.043961	0.042074	0.045429
21-25	0.042703	0.045196	0.030705	0.026465	0.023041

The shift value corresponding to the highest chi value is the correct shift. If two or three chi values fall within the probable range then they can be tried to resolve any contradiction which may occur after having recovered the lug matrix. The shift values corresponding to the highest chi values for each group are tabulated below:

Table 13.2: Shift values corresponding to highest Chi values

Pin Arrangement	Shift produced
XXXX	7
XXXY	2
XXYX	17
XXYY	13
XYXX	15
XYXY	11
XYYX	18
XYYY	15
YXXX	5
YXXY	0
YXYX	16
YXYY	12
YYXX	13
YYXY	9
YYYX	17
YYYY	14

A shift value of 0 is equivalent to shift of 26. In case of presence of more than one 0 is the table, we will have to assume which arrangement corresponds to shift value of 0 and which corresponds to shift value of 26. However, if there is only one arrangement which corresponds to zero, it is almost always the position where all pins are inactive. In the above table, the combination YXXY corresponds to shift value of 0. This implies that YXXY corresponds to a setting of 0000. Therefore, for pinwheels 1 and 4, Y corresponds to inactive pins, whereas X corresponds to inactive pins in pinwheels 2 and 3.

The recovered pinwheels are, therefore:

```
Pinwheel 1:   01111101101100011010011010
Pinwheel 2:   1110100100101100100001101
Pinwheel 3:   01011010001100011010100
Pinwheel 4:   110010010010011110100
```

13.4.3 Recovery of Lug Cage

After resolving the positions of pinwheels, the lug matrix is computed which gives the shift values corresponding to different pin settings. The lug matrix in this case is found to be

$$L = \begin{bmatrix} 2 & 11 & 13 & 7 \\ 0 & 9 & 14 & 13 \\ 0 & 0 & 12 & 16 \\ 0 & 0 & 0 & 5 \end{bmatrix}$$

Using the lug matrix the lug settings are recovered below.
x_i = effective lugs corresponding to position i and y_{ij} are shared lugs between wheel i and j where $y_{ij} = x_i + x_j$ - $shift_{ij}$

$x_1 = 2$, $x_2 = 9$, $x_3 = 12$, $x_4 = 5$
y_{12} = 9+2-11=0
y_{13}=12+2-13 = 1
y_{14} = 5+2-7=0
y_{23} = 12+9-14 = 7
y_{24} = 9+5-13=1
y_{34} = 12+5-16=1

Hence the lug matrix shows no contradictions. The cryptogram is deciphered using the above lug settings and the correct plaintext is recovered.

IT REGULARLY COMES AS A SURPRISE TO PEOPLE THAT OUR OWN INFRASTRUCTURE CAN BE USED AGAINST US AND IN THE WAKE OF TERRORIST ATTACKS OR PLOTS THERE ARE FEARINDUCED CALLS TO BAN DISRUPT OR CONTROL THAT INFRASTRUCTURE ACCORDING TO OFFICIALS INVESTIGATING THE MUMBAI ATTACKS THE TERRORISTS USED IMAGES FROM GOOGLE EARTH TO HELP LEARN THEIR WAY AROUND THIS ISNT THE FIRST TIME GOOGLE EARTH HAS BEEN CHARGED WITH HELPING TERRORISTS IN GOOGLE EARTH IMAGES OF BRITISH MILITARY BASES WERE FOUND IN THE HOMES OF IRAQI INSURGENTS INCIDENTS SUCH AS THESE HAVE LED MANY GOVERNMENTS TO DEMAND THAT GOOGLE REMOVE OR BLUR IMAGES OF SENSITIVE LOCATIONS MILITARY BASES NUCLEAR REACTORS GOVERNMENT BUILDINGS AND SO ON ANINDIAN COURT HAS BEEN ASKED TO BAN GOOGLE EARTH ENTIRELYTHIS ISNT THE ONLY WAY OUR INFORMATION TECHNOLOGY HELPS TERRORISTS LAST YEAR A US ARMY INTELLIGENCEREPORT WORRIED THAT TERRORISTS COULD PLAN THEIR ATTACKS USING TWITTER AND THERE ARE UNCONFIRMED REPORTS THAT THE MUMBAI TERRORISTS READ THE TWITTER FEEDS ABOUT THEIR ATTACKS TO GET REALTIME INFORMATION THEY COULD USE BRITISH INTELLIGENCE IS WORRIED THAT TERRORISTS MIGHT USE VOICE OVER IP SERVICES SUCH AS SKYPE TO COMMUNICATE TERRORISTS MAY TRAIN ON SECOND LIFE AND WORLD OF WARCRAFT WE ALREADY KNOW THEY USE WEBSITES TO SPREAD THEIR MESSAGE AND POSSIBLY EVEN TO RECRUIT

Chapter 14

Cryptanalysis of M-209 Cipher Machine

M-209 is a pinwheel cipher machine which was designed by a Swedish cryptographer Boris Hagelin and remained in use by the U.S military in World War II and the Korean War [38].

14.1 Structure of M-209 Cipher Machine

M-209 is a mechanical enciphering machine which consists of an assembly of 6 adjustable pinwheels and a lug cage holding 27 bars. The pinwheels are of lengths 26, 25, 23, 21, 19 and 17. The wheels are turned by a power handle situated at one end of the box. The entire lug cage rotates every time the handle is turned. A knob is used to set the machine in enciphering or deciphering mode. The machine generates pseudo-random shifts which are used in conjunction with reversed standard alphabets to generate reciprocal cipher alphabets. The output of the machine was printed onto a paper strip. The letter counter was reset for all new messages [30].

14.2 Key Components

These are the components which can be altered as part of the key setting. M-209 consists of two key componets - the pinwheels and the lug cage.

(a) Pinwheel Settings: The wheels are called pinwheels due to the presence of pins on each position of the wheels. The pins can be set in an active or an inactive position. Only pins in the active position can engage with effective lugs corresponding to that pinwheel position.

(b) Lug Cage: The lug cage consists of 27 bars each carrying two lugs. Each lug can be set against any pinwheel or in a neutral position. The entire cage rotates for each encryption. The placement of lugs in the cage determines the shift values which are generated by the machine.

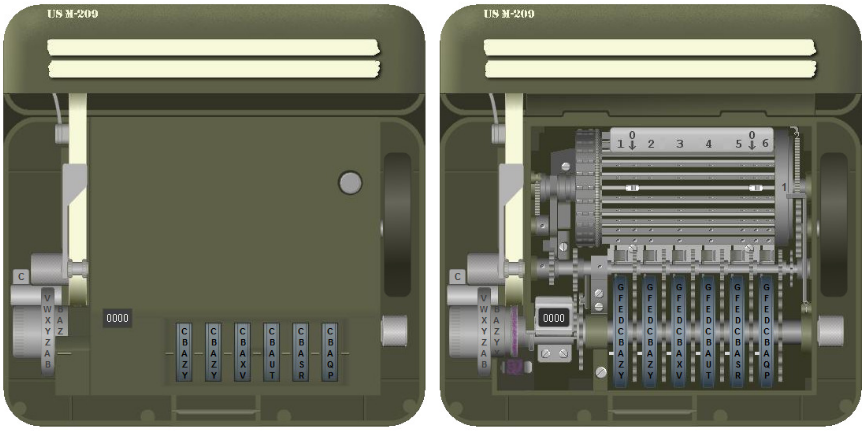


Figure 14.1: Internal and external view of the M209 Machine Simulator

14.3 Mathematical Notation

The enciphering equation for an M-209 cipher machine is:

$$CT = 27 - PT + N \tag{14.1}$$

where ct is cipher text letter, PT is plaintext letter and N is the shift which is equal to the number of bars engaged by the existing position of the pins in that state.

As discussed in Chapter 2, the relationship between plain-cipher letters can be described by a Beaufort Tableau.

Decipherment is identical to encipherment and is denoted as

$$PT = 27 - CT + N \tag{14.2}$$

14.4 Key Space and Period

With six pinwheels, the total number of ways in which the pins can be arranged is equal to

a = 2^{26} x 2^{25} x ... = 2^{131}

Each bar on the lug cage carries two lugs. The total number of ways in which these lugs can be arranged on a bar is equal to

6C0 + 6C1 + 6C2 = 1+6+15 = 22

The total number of ways in which the lug cage can be set up is calculated using the Pigeonhole Principle. The totall possible arrangements of the lug cage are

b = 48C27 = 48!/27!21!   2.2314 x 10^{13}

The total keyspace is thus equal to the product of a and b

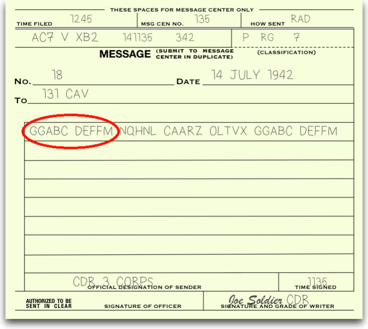
Keyspace = a x b = 2^{131} x 2.2314 x 10^{13} 6.0745 x 10^{52}

The lengths of the keywheels is relatively prime hence the key period is equal to

26x25x23x21x19x17 = 101405850

14.5 Operation and Encipherment

The U.S military kept a codebook which contained the daily settings for the M-209 cipher machine. Each setting was associated with a two letter code called the key list indicator. The key list indicator was sent along with the enciphered message to identify the internal settings of the machine. In order to encipher a message, a starting position of keywheels was selected randomly and noted down. This was the external message indicator and was used to generate the starting keywheel setting. Next, a random letter called the system indicator was selected, for example, A. After resetting the letter counter to 0000 and knob to ciphering mode (C), the system indicator is encrypted twelve times. The resulting output on the tape is teared off and starting from left these letters are used as the key starting position. The letter which did not appear on the corresponding wheel was cancelled out and the next letter was used in its place. The message was then ecrypted using this starting position. The system indicator, external message indicator and key list indicator were sent along with the encrypted text. At the receiving end the machine was set according to the received settings. The knob was set to deciphering mode and the decrypted text was printed out on the tape [30].



THESE SPACES FOR MESSAGE CENTER ONLY

TIME FILED 1245	MSG CEN NO. 135	HOW SENT RAD
AC7 V XB2 141135 342		P RG 7

MESSAGE (SUBMIT TO MESSAGE CENTER IN DUPLICATE) (CLASSIFICATION)

No. 18 DATE 14 JULY 1942

To 131 CAV

GGABC DEFFM NQHNL CAARZ OLTVX GGABC DEFFM

CDR 3 CORPS OFFICIAL DESIGNATION OF SENDER 1135 TIME SIGNED

AUTHORIZED TO BE SENT IN CLEAR SIGNATURE OF OFFICER Joe Soldier CDR SIGNATURE AND GRADE OF WRITER

Figure 14.2: A message enciphered on M-206

14.6 Cryptanalysis

M-209 was used in World War II by the U.S Navy. Although German codebreakers broke this machine in 1943, but the process to recover the message took a few hours. Hence, the machine proved to be reasonably secure for tactical messages.

A German paper was retrieved by NSA around 1948 which presented the design and working principle of a German version of Bombe which they used to analyze and decrypt the M-209 traffic. This paper was translated under the title *"German Cryptanalytic Device for M-209 Traffic"* and classified as top secret until 2011 when it was declassified and delivered to the NARA. A scanned copy of this paper surfaced the internet around 2012. Known message attacks or solution of messages in-depth have been described in the literature review. Cipher text only attacks are known to have been implemented but one paper on such an attack remains unpublished [4].

In this section, we will revise our existing code to attack a cryptogram enciphered using M-209 cipher machine. The message length is about 3000 characters. In some cases, messages of lengths upto 2000 characters can also be completely solved. This generally depends on the settings of the lug cage and the nature of underlying text.

The following message is encrypted using M-209 cipher machine.

```
FGSAC RXVZW SOGHV PSZQU XUAZZ NEIOW FDOFM FGRES GSLCX UHUOV
ALUJX DILLQ PPZCA VGJNN NADHU VTEHC YEZVA VFVVD ZZBXS EOEMG
TCSNG ZZRWH LWPGS TYQOS EHUKH CLQWM LQMXT KSULC MLYPQ IDRSU
JKETX BYSMH NYVDC RPGGD EGPMV GGQJD BQATK VTPCI SPUDP FGBRX
FPLLW AUEJE KVPSJ KRFMQ QCBXN NRHJV GZEGP VWTAS UKOWF QTZOT
LUZQI SXYZV PYHBS ALWOD CMCDC KTVCP APKRT AKVNE XLCKB WYCPC
RVRMV SKBCP QLTCB TAEUG BJFQW FZVKG IANRQ RVKLX GONLK WYGQD
RYEGA HVSPR UDMPP URYKG OSQNB GVTXV BNPUP CBYQE IBXIO OBYLT
HCOQE DSIPH NDLDX SVYXD AAPSI NYIQN ZJPTN DUDEE XLOEI IPTZE
DKYXZ MKUDG NZHXY VWKGA FESMG UWZDS JWVLH QFFSG FVBXI LJGYZ
FOHIW HSOWR EXADV XCGYL ZPEFI CITAC YIZYN LUNYG PYVVV GGRGU
AZLJJ QKWZV HKSPE RCLQC VXTDN VGGIY OOKUA HKWDL IRCVH YAPFS
YVSPE LWOYR NMFBX ZFEOK TCIAI AMVBV VSXHW HJRMX GNVTP HVTRX
KXCNZ IDUTE DZKLT VIUKZ HUFZA NXRMJ ZONLM TLHFP WDUAJ GADPN
AZZPL CCLFN UDABV PRJNW HTAPP IVDLZ PUNWJ PMJWP QHZGU EIKNK
FAZAB PMZPI TEDAE KPZPY DBRIW YVTAM XHOUU LNHFS WPKIA JXUOV
BQNVN VUMSE CVWVN WNHTQ KESXX SSPQV DSBMO TQNYN PPCLL ZPDVI
VFBOW VISLK OJLLZ WXFYG NLGNC HILEJ LCKYB ZXEOI GSGRB TWYQI
KFDBL UJSWD AQARE PHEON DEHLM SCFGU IPKLR FWWKX LNBYH ISWEK
WDLMB QDGPW FISOR DNARA WOEFT QYIPW SSNKU ZHDUI HVIAZ BDREM
JJFFN VKOGB QNGJN PUDWN ZJQQY BEGPB VPSWY LVSIK ADGEN BTTLW
BGFIY RJJTB RMMAK ARIRI PIQUT RRINH SWEZB FEGMP VOAGE ZUWVJ
NXIAV HNJGY YGWIP WAKTF MGPIB RGWCL DBZHP PRUKH TDVGK YNEYQ
KETQV SPWAW LBQKP NVEAM GEGCA EEYFI WKGTZ RGYYM JDBGB RITPK
AHJTT RHZOP FGQNP ARSXY AVWEF VWZEE HQSQV AZKPU DLSVX ISNCA
NXIRC VRPCZ UIGTP BEEJX UWIWV INOYM UVTQZ MYSFV QKTRK IJQOZ
OEWSH KZMEF QRORN WEYHK QORQW OWJSW VKPRB HTRLS DSIYU VMLUU
```

```
HEXCH OPDEO BBEDJ LETAU BGXCG BUYLQ XRNDX XJKWS QPNBK UTILW
ORZLK UNVAY TTNCZ BDUEN SZSUJ SVTLM CSNRW XDVAR ROQFF JVQRO
STTMR DEANS BAAVB XNFWH IGXHN TCYXO RUETU DXUPH UDPYA EVKKX
PXYFP YPXUW IDNSV KDWXZ DHJEB KMYGK BGSIA LCRPR XRDOW FVKVW
JMRVV QPDVW VFWJE TLVYD PQRBA DZVQF BIKCH AYVEO LJVNJ AUWWR
SFPQN UEVWU NMIYO OUHTG XXCLL ZCUBF JYGEC YVRWB PVBWO EYSTQ
LGFPJ ZYDGT PESSX TEWOJ ERTJX XCTYY FGGRH PAOMC PENSA VXSQA
BOQUU VWGZF POFGM ZKUPB AGCAK SNUOY MBVLH AIJJY GWGTM WAGNR
POGFL SVHVG OVFXA ISXVY RFTKP ACRBL OUMDY JGWFY DCWSH AODSR
CJJEG EIADD LFUHU TOWAI UCFVA SUCLE MUULQ YRRWC VQYWT VLWNW
RRWXR VSHCK GYZJN URSQV PVGYP ZZICJ EDWDB OEFHR XLRYC JYEJY
VAAKY PVKIU TLTYC QALFL NUEJA DZWGV BNDVT PPHWO DKJFZ XZRPR
FJHSA SJOHR SAUYN BJSOH KLDNV TAYWC WRSIP NSXHL DRTER EWLWK
WUYUA WLPLD RBDYU YTRCK CMAJH JQILR XUCZT HHVJC JUMHA PEAKU
NGAKU DBVEH PXUPB QSBKS WVHUD DEHKV EYPYU QHNHD WSLUM WWLND
NNLNB SOWGH QKIZT KOVQB ISLCV CVOUI DROEN BWGDA UFLBR LKGKT
RQEON FCKGM IZQEP ANXXW UYRVN LLIWP YANTU CUUOG VDGTI CKIYR
ZZVPL XAOWN YUCGB XTEPS BZAJV GDICP XCGVG GJPSR PTIKN KARCF
JLZOT TESGL OXWVF BLWPS ZDSQF AQXGO SKSGA SUAIZ RCZCX OZMPR
OTGOU BCHTQ GKTIC TWKMW EMDTR AIZPH XBKUR PLTVH FWXER MHVUS
OGUPV VKPGG SFDIG WCTYS QNQNU TIHMG JEZSI MVGCZ KNVVH WPLVV
NWSPH RUZHP LQNNM TNDPW VOORT WWJZC JKVSH DRJKE IKEVY VIDMS
CTUND QGONN ONZKW IYWUH SUVOG VVNZP NASFR EUGDZ FTTRY VZQAV
GNGWC RKFGJ BIKYR LUTTU RSAAP XEUBF PAUCJ FLQPA OEXNZ IATSJ
UYVLV IQYYK UUCBU DHRAP EAQRF SRPZA ITXDK ZFNXI HNLOE BNUXW
JCTXX MLAFF MWLRE WBGPJ WHSVH NNFXV FNJDX RXBTY REZSR KKVWW
COVFC PVLVC EVXQK IOZSW NWHWG NWTLR VTRIE DIGQK NEQUW CWGPU
AOKWF UDZGZ UCPZK ZJCVW MDZYM CZUSZ PVSJS CLSAA OHGKY TAJVU
BQVTV EPJUJ VBTJW QDCIR VXLGY IEUGL QNCTG XLPJC YBGEL GZATU
YGAKW BFCNQ ELDPL ATZCZ RBFTT HXQRB IWFHQ IZAIC WIWXZ KNNPQ
TDYTD HJWWL CHAYI RBBRI AHVJV OVQVV NQLJR YFIAI OGBPY ASRAH
PCZKR KOSMQ GKKCC KIVVV ZSRGF JGXDA RBEEK RSOOB FGOHI YJQST
LGAKH UMUAZ LZVWO UCVZR QKPTZ NNPWN BKVCO VCROO JPAJA ECCGH
RGWNR MHPXK KQVQA PLNVF HRJEO MYXBM NOKME ELTBX AVUAR HBPAL
YAZOZ DZLWA PDEMJ RDDWG BACCX JWQPW YDNNY AHVNY UDINH HOYZO
PCONY MFQGV PLKXE XDFNB VCRAJ WGAMK OOSSR WSCMO FOYOO ZZTMQ
MJVYD KEPGY MJNMD VUQXJ JRSMV PQUBO XAOZW TWSLN VGTUQ OMHNZ
FZJNE JJRHD PKLYC HFIHO FZPWP ACXSD SYCKF ANINR KMKZZ OLMOG
BHHZA DGCXE REUPB BDWCM VGLWU DPEZV NOFUQ XLRUQ OBPDO FEMQP
YTNAP WLRIN VPHED AYRUA LBCCJ EVHBW HKDLS YJENT ZBOXM FMLBU
YFTPB ZWBLT YKX
```

14.6.1 Recovery of Pinwheels

The ciphertext is written out into 26, 25, 23, 21, 19 and then 17 columns to analyze the positions of the pins. The upper and lower bounds used for comparison are stated in Table 14.1.

Table 14.1: Upper and Lower bound of different pinwheels

	Pinwheel Lengths					
	26	25	23	21	19	17
Upper Bound	16	15	14	13	12	11
Lower Bound	10	9	8	7	6	5

The same code that has been used earlier is modified to apply it to M-209. Aligning relative pin positions obtained after comparison between all the rows, the final pin arrangement for the six pinwheels after first assessment is found as follows:

```
Pinwheel 1:   ???X?X?XYX???YXX??XYXYYXXX
Pinwheel 2:   X?YX???XY?XY?XX??Y??????Y
Pinwheel 3:   ???????????????????????
Pinwheel 4:   ?????????????????????
Pinwheel 5:   XX???X???X??X?X????
Pinwheel 6:   ??????XX?X??X??X?
```

Next, the partial settings recovered are used to remove the effect of one wheel. Since most of the pin positions for pinwheel 1 and 2 have been resolved, hence, they are used to assess the remaining pinwheels.

After removing the effects of pinwheels 1 and 2, the results are combined to give the reassessed wheels which are:

```
Pinwheel 1:   YYXXXXYXYXXY?YXX??XYXYYXXX
Pinwheel 2:   XYYXY??XY?XY?XX??Y??Y??XY
Pinwheel 3:   X??XX?X???????X???X?Y?Y
Pinwheel 4:   ?????????????????????
Pinwheel 5:   XX??YX???X??XYXY???
Pinwheel 6:   Y?X??XXX?X?XX?XXY
```

The reassessment process is continued using another wheel. Pinwheels 1, 2 and 6 are used one by one and the resultant new pin positions obtained are:

```
Pinwheel 1:   YYXXXXYXYXXYYYXXYYXYXYYXXX
Pinwheel 2:   XYYXY?XXY?XYYXXY?Y??Y??XY
Pinwheel 3:   X??XX?X???????X???X?Y?Y
Pinwheel 4:   ????X????X?????X?????
Pinwheel 5:   XXXYYXY??XYYXYXY??X
Pinwheel 6:   YYXYYXXXYXYXX?XXY
```

Pinwheels 1, 2, 5 and 6 are almost completely resolved. They are used in a loop to reassess every other wheel with new pin positions being added to the set to improve the comparison process.

```
Pinwheel 1:   YYXXXXYXYXXYYYXXYYXYXYYXXX
Pinwheel 2:   XYYXYXXXY?XYYXXY?Y??Y??XY
Pinwheel 3:   X??XX?X???????X???X?Y?Y
Pinwheel 4:   ????X????X?????XY????
Pinwheel 5:   XXXYYXYX?XYYXYXYY?X
Pinwheel 6:   YYXYYXXXYXYXX?XXY
```

The next two rounds of assessment give us the following grouping for pin positions:

```
Pinwheel 1:   YYXXXXYXYXXYYYXXYYXYXYYXXX
Pinwheel 2:   XYYXY?XXY?XYYXXYXYYXYX?XY
Pinwheel 3:   X??XXXXXXYX???X?XYX?Y?Y
Pinwheel 4:   ?YYXYYXX?Y?XY?YY??XYY
Pinwheel 5:   XXXYYXYX?XYYXYXYYYX
Pinwheel 6:   YYXYYXXXYXYXXYXXY

Pinwheel 1:   YYXXXXYXYXXYYYXXYYXYXYYXXX
Pinwheel 2:   XYYXYXXXY?XYYXXYXYYXYX?XY
Pinwheel 3:   X??XXXXXXYX???X?XYX?Y?Y
Pinwheel 4:   ?YYXYYXX?Y?XY?YYX?XYY
Pinwheel 5:   XXXYYXYX?XYYXYXYYYX
Pinwheel 6:   YYXYYXXXYXYXXYXXY
```

Most of the pin settings have been recovered for pinwheels 1, 2, 5 and 6. Using them to reassess other wheels, leads us to the complete solution after a few assessments.

The final pin settings recovered are:

```
Pinwheel 1:   YYXXXXYXYXXYYYXXYYXYXYYXXX
Pinwheel 2:   XYYXYXXXYXXYYXXYXYYXYXXXY
Pinwheel 3:   XYYXXXXXXYXYYYXYXYXXYXY
Pinwheel 4:   XYYXYYXXXYXXYXYYXYXYY
Pinwheel 5:   XXXYYXYXYXYYXYXYYYX
Pinwheel 6:   YYXYYXXXYXYXXYXXY
```

14.6.2 Recovery of Pin Identities

In order to recover the lug cage, we need to identify which class of pins are represented by X and which are represented by Y on each pinwheel. Since the pins are already divided into groups, hence they can be used to break the cipher text into

64 different groups (XXXXXX, XXXXXY, XXXXYX, etc) each corresponding to one particular monoalphabetic shift. A sample of plaintext in which space is replaced by Z is used to compute chi values and recover pin identities and the lug cage. Each group of ciphertext is decrypted using Equation 14.2 with shift values varying from 0 to 25 and compared with the distribution of sample plaintext. A high chi value corresponds to correct shift. The chi values corresponding to a combination of "YYXYXY" are given below for all possible shifts.

Chi values:

```
0.076927    0.039372    0.028981    0.031218    0.036343
0.037601    0.043798    0.043612    0.043193    0.031544
0.022831    0.045802    0.037462    0.039279    0.050694
0.043193    0.030193    0.028003    0.039745    0.039698
0.039791    0.044171    0.029913    0.029354     0.02148
```

The shift value corresponding to the highest chi value is the correct shift. If two or three chi values fall within the probable range then they can be tried to resolve any contradiction which may occur after having recovered the lug matrix. The shift values corresponding to the highest chi values for each group are tabulated below:

Table 14.2: Shift values corresponding to highest Chi values

Pin		Pin		Pin		Pin	
Setting	Shift	Setting	Shift	Setting	Shift	Setting	Shift
XXXXXX	22	XXXXXY	19	XXXXYX	0	XXXXYY	24
XXXYXX	21	XXXYXY	18	XXXYYX	25	XXXYYY	23
XXYXXX	22	XXYXXY	20	XXYXYX	0	XXYXYY	25
XXYYXX	22	XXYYXY	20	XXYYYX	0	XXYYYY	25
XYXXXX	18	XYXXXY	15	XYXXYX	22	XYXXYY	20
XYXYXX	17	XYXYXY	14	XYXYYX	21	XYXYYY	19
XYYXXX	18	XYYXXY	16	XYYXYX	22	XYYXYY	21
XYYYXX	18	XYYYXY	16	XYYYYX	22	XYYYYY	21
YXXXXX	14	YXXXXY	10	YXXXYX	23	YXXXYY	20
YXXYXX	13	YXXYXY	9	YXXYYX	22	YXXYYY	19
YXYXXX	15	YXYXXY	12	YXYXYX	24	YXYXYY	22
YXYYXX	15	YXYYXY	12	YXYYYX	24	YXYYYY	22
YYXXXX	5	YYXXXY	1	YYXXYX	14	YYXXYY	11
YYXYXX	4	YYXYXY	0	YYXYYX	13	YYXYYY	22
YYYXXX	6	YYYXXY	3	YYYXYX	15	YYYXYY	13
YYYYXX	6	YYYYXY	3	YYYYYX	15	YYYYYY	13

A shift value of 26 is equivalent to shift of 0. In case of presence of more than one 0 is the table, we will have to assume which arrangement corresponds to shift value of 0 and which corresponds to shift value of 26. However, if there is only one arrangement which corresponds to zero, it is almost always the position where all pins are inactive. In Table 14.2, three different combinations correspond to shift value of 0.

Assuming XXXXYX corresponds to 000000, the recovered pinwheels will be:

```
Pinwheel 1:   11000010100111001101011000
Pinwheel 2:   0110100010011001011010001
Pinwheel 3:   01100000010111010100101
Pinwheel 4:   011011000100101101011
Pinwheel 5:   0001101010110101110
Pinwheel 6:   11011000101001001
```

14.6.3 Recovery of Lug Cage

After resolving the positions of pinwheels, the lug matrix is now computed which gives the shift values corresponding to different pin settings. The shift values corresponding to maximum chi values are considered.

The lug matrix in this case is:

$$L = \begin{bmatrix} 24 & 19 & 23 & 25 & 20 & 20 \\ 0 & 22 & 21 & 22 & 18 & 14 \\ 0 & 0 & 25 & 0 & 21 & 22 \\ 0 & 0 & 0 & 0 & 22 & 24 \\ 0 & 0 & 0 & 0 & 22 & 14 \\ 0 & 0 & 0 & 0 & 0 & 23 \end{bmatrix}$$

This lug matrix results in a lot of contradiction, giving rise to negative values of shared lugs. After trying other possibilities we get similar results. Considering the combination ”YYXYXY” maps to 000000, the pinwheel settings are:

```
Pinwheel 1:   00111101011000110010100111
Pinwheel 2:   0110100010011001011010001
Pinwheel 3:   10011111101000101011010
Pinwheel 4:   011011000100101101011
Pinwheel 5:   1110010101001010001
Pinwheel 6:   00100111010110110
```

The lug matrix is computed again by using shifts corresponding to maximum chi values.

The lug matrix is found to be:

$$L = \begin{bmatrix} 4 & 13 & 5 & 6 & 13 & 17 \\ 0 & 22 & 11 & 13 & 19 & 19 \\ 0 & 0 & 1 & 3 & 10 & 15 \\ 0 & 0 & 0 & 3 & 12 & 16 \\ 0 & 0 & 0 & 0 & 9 & 18 \\ 0 & 0 & 0 & 0 & 0 & 14 \end{bmatrix}$$

Using the above lug matrix, ciphertext is decrypted but found to have inconsistencies in positions involving pinwheel 2. The shifts corresponding to top five chi values for this particular combination are 22, 10, 15, 9 and 14.

For our next attempt, pinwheel 2 is chosen to have 10 effective lugs. The revised lug matrix is

$$L = \begin{bmatrix} 4 & 13 & 5 & 6 & 13 & 17 \\ 0 & 10 & 11 & 13 & 19 & 19 \\ 0 & 0 & 1 & 3 & 10 & 15 \\ 0 & 0 & 0 & 3 & 12 & 16 \\ 0 & 0 & 0 & 0 & 9 & 18 \\ 0 & 0 & 0 & 0 & 0 & 14 \end{bmatrix}$$

Using the lug matrix, the lug settings are recovered as given below:

x_i = effective lugs corresponding to position i and y_{ij} are shared lugs between wheel i and j

where $y_{ij} = x_i + x_j$ - $shift_{ij}$

$x_1 = 2$, $x_2 = 9$, $x_3 = 12$, $x_4 = 5$
$y_{12} = 1$, $y_{13} = 0$, $y_{14} = 1$, $y_{15} = 0$, $y_{16} = 1$
$y_{23} = 0$, $y_{24} = 0$, $y_{25} = 0$, $y_{26} = 5$
$y_{34} = 1$, $y_{35} = 0$, $y_{36} = 0$
$y_{45} = 0$, $y_{46} = 1$
$y_{56} = 5$

Hence the lug matrix shows no contradictions. The cryptogram is deciphered using the above lug settings and the correct plaintext is recovered.

EPHEMERAL MESSAGING APPS SUCH AS SNAPCHAT WICKR AND FRANKLY ALL OF WHICH ADVERTISE THAT YOUR PHOTO MESSAGE OR UPDATE WILL ONLY BE ACCESSIBLE FOR A SHORT PERIOD ARE ON THE RISE SNAPCHAT AND FRANKLY FOR EXAMPLE CLAIM THEY PERMANENTLY DELETE MESSAGES PHOTOS AND VIDEOS AFTER TEN SECONDS AFTER THAT THERE S NO RECORD THIS NOTION IS ESPECIALLY POPULAR WITH YOUNG PEOPLE AND THESE APPS ARE

AN ANTIDOTE TO SITES SUCH AS FACEBOOK WHERE EVERYTHING YOU POST LASTS FOREVER UNLESS YOU TAKE IT DOWN AND TAKING IT DOWN IS NO GUARANTEE THAT IT ISN T STILL AVAILABLE THESE EPHEMERAL APPS ARE THE FIRST CONCERTED PUSH AGAINST THE PERMANENCE OF INTERNET CONVERSATION WE STARTED LOSING EPHEMERAL CONVERSATION WHEN COMPUTERS BEGAN TO MEDIATE OUR COMMUNICATIONS COMPUTERS NATURALLY PRODUCE CONVERSATION RECORDS AND THAT DATA WAS OFTEN SAVED AND ARCHIVED THE POWERFUL AND FAMOUS FROM OLIVER NORTH BACK IN NINETEEN HUNDRED AND EIGHTY SEVEN TO ANTHONY WEINER IN TWO THOUSAND AND ELEVEN HAVE BEEN BROUGHT DOWN BY EMAILS TEXTS TWEETS AND POSTS THEY THOUGHT PRIVATE LOTS OF US HAVE BEEN EMBROILED IN MORE PERSONAL EMBARRASSMENTS RESULTING FROM THINGS WE VE SAID EITHER BEING SAVED FOR TOO LONG OR SHARED TOO WIDELY PEOPLE HAVE REACTED TO THIS PERMANENT NATURE OF INTERNET COMMUNICATIONS IN AD HOC WAYS WE VE DELETED OUR STUFF WHERE POSSIBLE AND ASKED OTHERS NOT TO FORWARD OUR WRITINGS WITHOUT PERMISSION WALL SCRUBBING IS THE TERM USED TO DESCRIBE THE DELETION OF FACEBOOK POSTS SOCIOLOGIST DANAH BOYD HAS WRITTEN ABOUT TEENS WHO SYSTEMATICALLY DELETE EVERY POST THEY MAKE ON FACEBOOK SOON AFTER THEY MAKE IT APPS SUCH AS WICKR JUST AUTOMATE THE PROCESS AND IT TURNS OUT THERE S A HUGE MARKET IN THAT EPHEMERAL CONVERSATION IS EASY TO PROMISE BUT HARD TO GET RIGHT IN TWO THOUSAND AND THIRTEEN RESEARCHERS DISCOVERED THATSNAPCHAT DOESN T DELETE IMAGES AS ADVERTISED IT MERELY CHANGES THEIR NAMES SO THEY RE NOT EASY TO SEE WHETHER THIS IS A PROBLEM FOR USERS DEPENDS ON HOW TECHNICALLY SAVVY THEIR ADVERSARIES ARE BUT IT ILLUSTRATES THE DIFFICULTY OF MAKING INSTANT DELETION ACTUALLY WORK THE PROBLEM IS THAT THESE NEW EPHEMERAL CONVERSATIONS AREN T REALLY EPHEMERAL THE WAY A FACE TO FACE UNRECORDED CONVERSATION WOULD BE THEY RE NOT EPHEMERAL LIKE A CONVERSATION DURING A WALK IN A DESERTED WOODS USED TO BE BEFORE THE INVENTION OF CELL PHONES AND GPS RECEIVERS AT BEST THE DATA IS RECORDED USED SAVED AND THEN DELIBERATELY DELETED AT WORST THE EPHEMERAL NATURE IS FAKED WHILE THE APPS MAKE THE POSTS TEXTS OR MESSAGES UNAVAILABLE TO USERS QUICKLY THEY PROBABLY DON T ERASE THEM OFF THEIR SYSTEMS IMMEDIATELY THEY CERTAINLY DON T ERASE THEM FROM THEIR BACKUP TAPES IF THEY END UP THERE THE COMPANIES OFFERING THESE APPS MIGHT VERY WELL ANALY E THEIR CONTENT AND MAKE THAT INFORMATION AVAILABLE TO ADVERTISERS WE DON T KNOW HOW MUCH METADATA IS SAVED IN SNAPCHAT USERS CAN

SEE THE METADATA EVEN THOUGH THEY CAN T SEE THE CONTENT AND WHAT IT S USED FOR AND IF THE GOVERNMENT DEMANDED COPIES OF THOSE CONVERSATIONS EITHER THROUGH A SECRET NSA DEMAND OR A MORE NORMAL LEGAL PROCESS INVOLVING AN EMPLOYER OR SCHOOL THE COMPANIES WOULD HAVE NO CHOICE BUT TO HAND THEM OVER EVEN WORSE IF THE FBI OR NSA DEMANDED THAT AMERICAN COMPANIES SECRETLY STORE THOSE CONVERSATIONS AND NOT TELL THEIR USERS BREAKING THEIR PROMISE OF DELETION THE COMPANIES WOULD HAVE NO CHOICE BUT TO COMPLY

Chapter 15

Results

This chapter discusses some basic performance metrics to compare the existing techniques with our proposed ones. Since, a variety of rotor and pinwheel machines have been studied and investigated, hence, the metrics are not viewed in entirety but measured against the key space of the system under study in order to scale the results down to an equal level. Due to large values involved in terms of the key space of the system and the varying complexity of attacks, we have used their equivalent logarithmic values to draw comparison using histograms.

The performance metrics are described in Section 15.1. Section 15.2 compares the results of our findings on rotor machines with the existing attacks, whereas, results for pinwheel ciphers are detailed in Section 15.3.

15.1 Performance Metrics

15.1.1 Key Space

For systems designed on similar principles, key space is one of the metrics we can relate the difficulty of cryptanalysis to. Even the smallest system we investigated had more key space then the majority of the systems that had been analyzed earlier as it can be seen in Figure 15.1.

15.1.2 Amount of Ciphertext Required

The lesser the amount of ciphertext required to carry out an attack, the more powerful is the technique. Since encryption and decryption processes are mathematical in nature, an attack which exploits the design weaknesses is above all and can be used to recover the messages even when the amount of ciphertext is limited. The required cipher length is used as a ratio of the total key space. Since the logarithmic value of key space is used for comparison, hence the ciphertext-key space ratio is calculated using equation the below equation:

$$Ratio = \frac{N}{K} \tag{15.1}$$

where N is the required length of ciphertext and K is the key space

logRatio = logN/logK =log N-logK

which will be negative for most cases.

The smallest value in the array is used to normalize the histogram for comparison.

15.1.3 Attack Complexity

The lesser the number of computations required for cryptanalysis, the more practical is the attack. When mathematical principles are employed in cryptanalysis, the results are far much efficient than those based on statistical or heuristic approach. The reason for this is that mathematical solutions are scalable and can be applied to any system having similar underlying functionality.

15.1.4 Success Rate

Success rate can be defined as the number of unknown settings correctly recovered by applying a specific attack. This may vary under different conditions. For a small amount of ciphertext, even good techniques do not prove to be of much help. With increasing amount of available ciphertext, the solutions converge to their best possible attack performance.

15.2 Results obtained for Rotor Machines

We have compared our results on the cryptanalysis of reciprocal cipher machines to five other contributions in this field. The first is Marion Rejewkis work (discussed briefly in chapter 3) who was the first person to analyze the Enigma machine using only ciphertext and draw accurate results about its operation, even before seeing the actual machine. We share the same attack environment that the entire machine is unknown. However, we did have the edge of knowing about its principle of operation. Rejewski, on the other hand, had no such prior knowledge. The second attack is James J. Gilloglys ciphertext-only attack based on the principle of Brute-force, (also described in chapter 3) to determine the initial settings of the Enigma machine under different plugboard settings. The third attack is a variation of Gilloglys work done by Heidi Williams who introduced statistical comparisons of bigrams in order to recover the plugboard settings. The fourth attack is based on a Genetic Algorithm implemented on a two and three rotor machine under unknown machine wiring. The last attack principle also assumes that the wiring is unknown and uses an attack based on Statistical Estimation Theory [9, 16, 17, 19, 39].

The legend for the histogram plots is given below:

- Blue histograms stand for our attack principle applied to three different machines.
- Yellow histograms are based on results compiled from literature review.

- Details of the systems being compared can be seen along the y-axis. The techniques used were briefed in this section earlier.

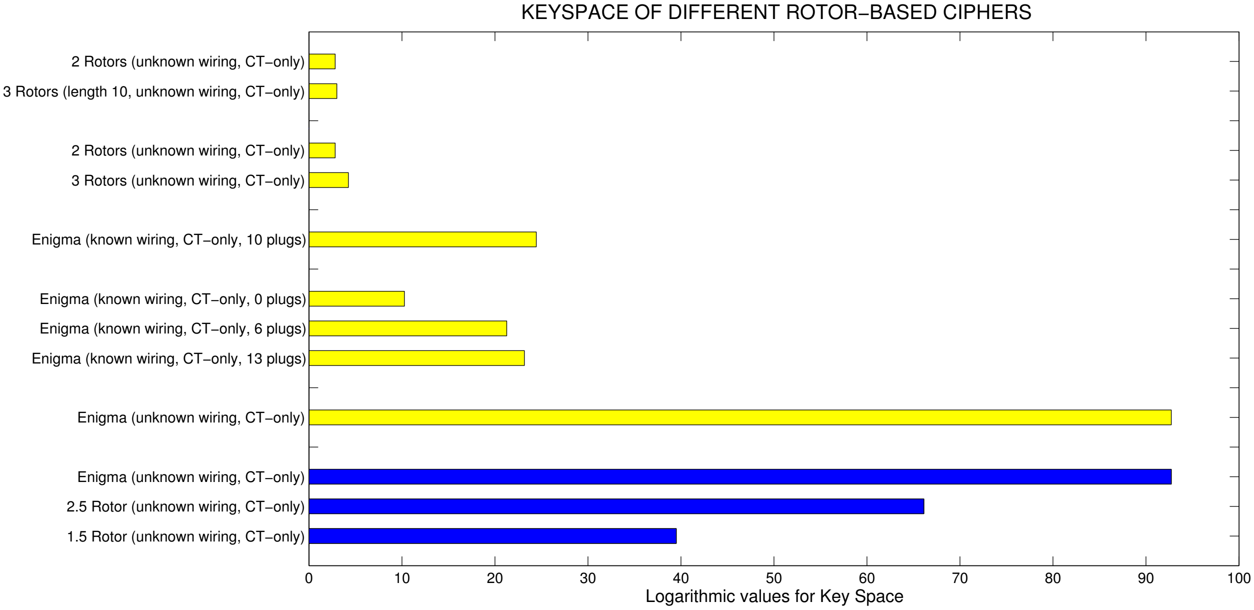


Figure 15.1: Rotor Machines: Histogram for Key Space

The plots in Figures 15.1, 15.2, 15.3 and 15.4 show the performance of our approach against others in the history. With low attack complexity and less amount of plaintext required to break the system, our approach evidently stands above others in this domain.

15.3 Performance Results for Pinwheel Ciphers

Like in the earlier section, similar results have been compiled for pinwheel ciphers as well. The results obtained in the following studies have been compared with our proposed solution of pinwheel ciphers .

1. Geoff Sullivans paper (discussed in chapter 10) on cryptanalysis of two Hagelin machines namely CD-7 and M-209 under different conditions [33]
2. Robert Morris cryptanalysis of M-209 cipher machine using known plaintext [34]
3. H. Paul Greenoughs solution on cryptanalysis of a generalized M-209 cipher machine [35]

The legend for the histogram plots is given below:

- Blue histograms stand for our attack principle applied to three different pinwheel ciphers.

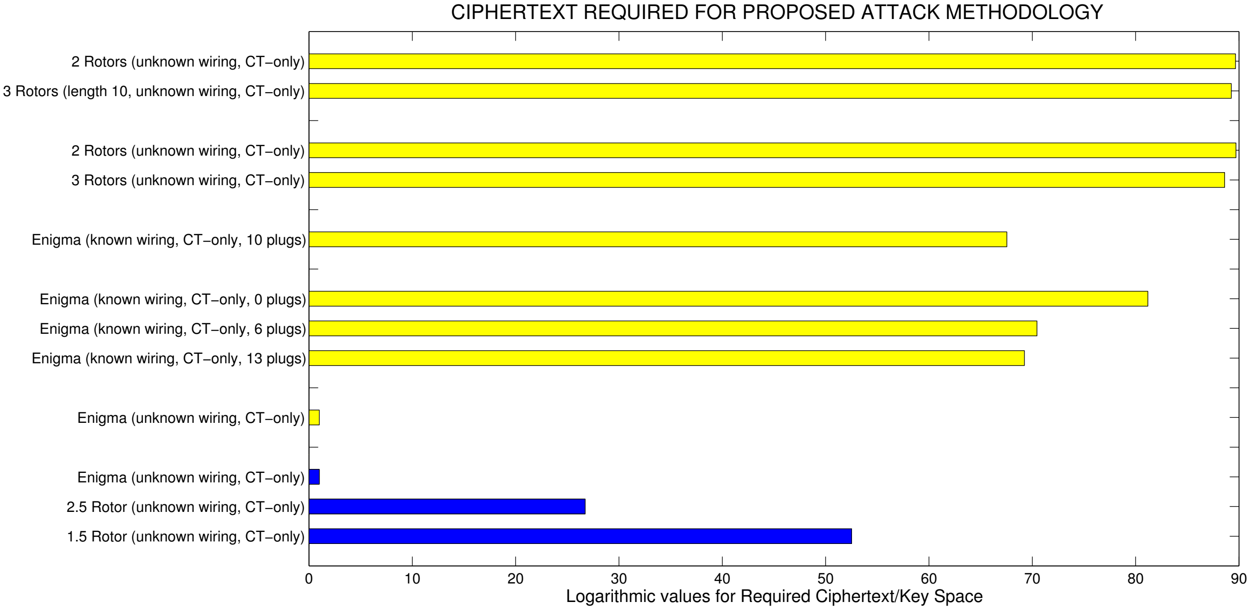


Figure 15.2: Rotor Machines: Histogram for Ciphertext lengths used in Analysis

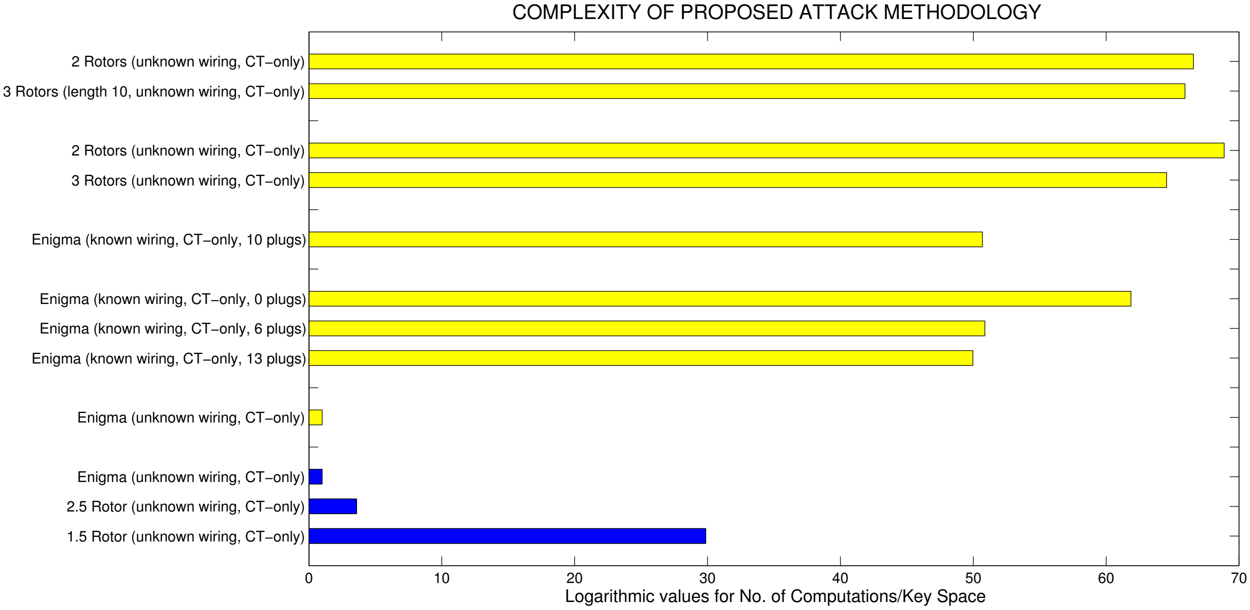


Figure 15.3: Rotor Machines: Histogram for Attack Complexity

- Yellow histograms are based on results compiled from literature review.
- Details of the systems being compared can be seen along the y-axis. The

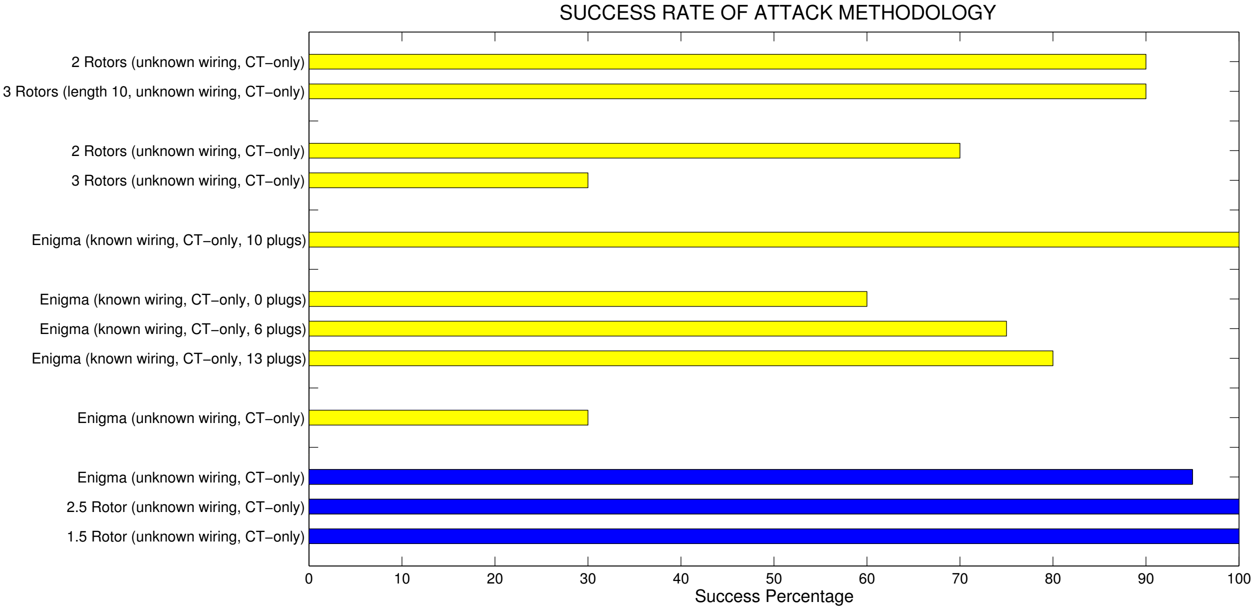


Figure 15.4: Rotor Machines: Histogram for Success Rate

techniques used were briefed in this section earlier.

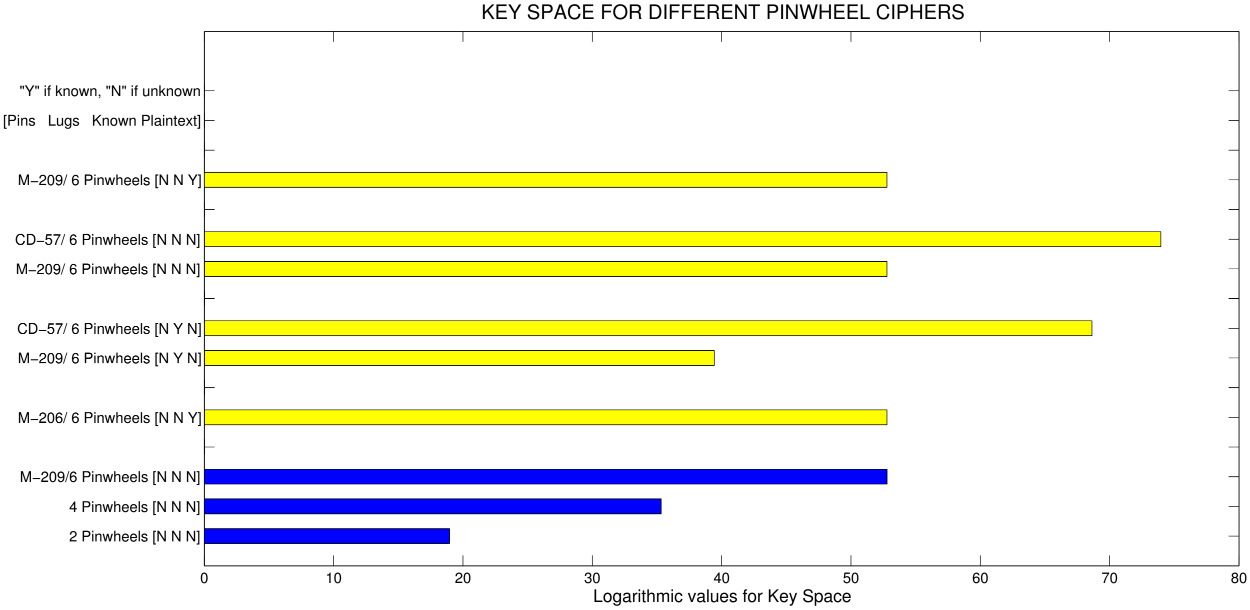


Figure 15.5: Pinwheel Ciphers: Histogram for Key Space

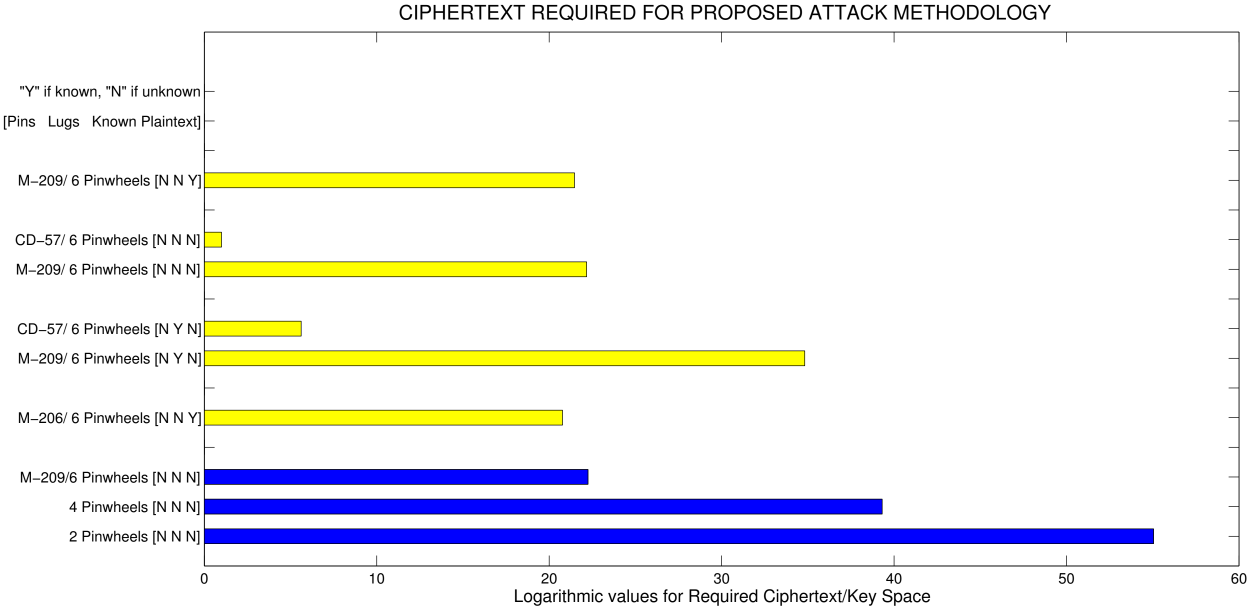


Figure 15.6: Pinwheel Ciphers: Histogram for Ciphertext lengths used in Analysis

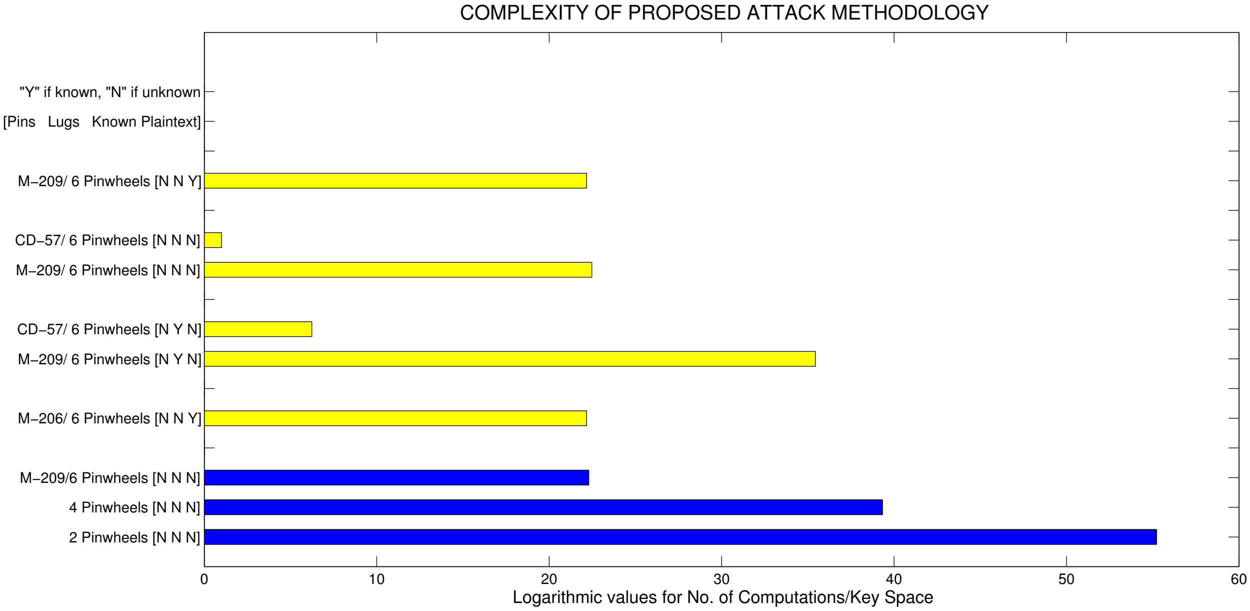


Figure 15.7: Pinwheel Ciphers: Histogram for Attack Complexity

In Figures 15.5, 15.6, 15.7 and 15.8 we can see that our technique, although statistical in nature, still manages to give good results for a reasonable amount of

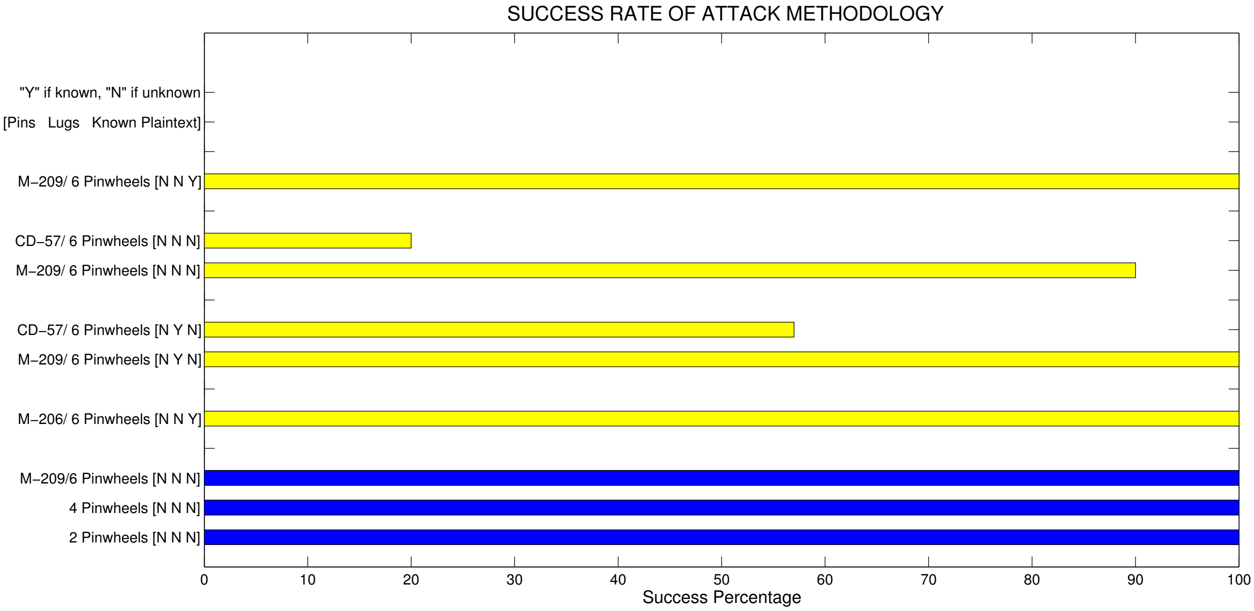


Figure 15.8: Pinwheel Ciphers: Histogram for Success Rate

ciphertext. For smaller amount of ciphertext, partial solutions are possible but if a decent amount of ciphertext is available, it leads to one complete solution.

Chapter 16

Conclusion

Cryptographic trends have evolved over time to thwart possible attacks due to design of improved analytical systems and techniques. A secure system is resistant to not only brute-force attacks but also attacks based on weaknesses in design. Hence, the evolution of cryptography is also partially attributed to advancement in code-breaking technology. This technology from the pre-computing age is substantially classified even today. With the arrival of modern computers, the cryptanalysis techniques based on computation algorithms gained immense popularity and took the focus away from what significant achievements were made in the last century. Since cryptographic techniques are based on principles that involve substitution and permutation, hence, mathematical properties of systems having similar basic design ought to be similar. Rotor machines and pinwheel ciphers are the early form of stream ciphers and, therefore, their study is crucial to analyze modern systems. Technology can get obsolete, but for a cryptanalyst no system is obsolete and no technique is useless. If these algorithms or techniques are known to exist, then they can be adapted according to the system under study.

In this thesis, we have successfully investigated the two kinds of cipher machines to fill some of that existing gap in terms of knowledge. We have achieved this by performing mathematical analysis of rotor machines and statistical analysis of pinwheel ciphers. These techniques can be applied to modern stream ciphers to analyze them, although, work has not been done to prove so. However, there are two cryptosystems that surfaced some time back [40, 41] which use rotors to introduce non-linearity in LFSR. They are open for analysis and these techniques can be applied to them. Moreover, the round function in RC-4 involves modular shifts (cyclic permutation) and would make some good research if analyzed with reference to the methodology given in this thesis.

Bibliography

[1] R. Simon, “Cipher Machines,” 2010. [Online]. Available: www.ciphermachines.com

[2] “Declassified Documents Released to NARA,” 2009. [Online]. Available: http://www.nsa.gov/publicinfo/declass/entries.shtml

[3] “NSA Technical Journal Cumulative Index (April 1956 - Fall 1980).” [Online]. Available: https://cryptocellar.web.cern.ch/cryptocellar/NSA/nsatj1956-80.pdf

[4] “Dabbling in the Cryptographic WorldA Story,” 2000. [Online]. Available: http://cm.bell-labs.com/cm/cs/who/dmr/crypt.html

[5] M. Lee, “Cryptanalysis of the SIGABA Cipher (Thesis for the degree Master of Science in Computer Science),” 2003. [Online]. Available: http://cs.sjsu.edu/faculty/stamp/students/Kwong_Heather.pdfl

[6] W. Friedman, “Decrypted secrets: Methods and maxims of cryptography,” 2007.

[7] J. J. G. Savard, “A Cryptographic Compendium: Rotor Machine Basics,” 1998. [Online]. Available: http://www.quadibloc.com/crypto/ro020301.html

[8] C. M. Ellison, “A Solution of the Hebern Messages,” *Cryptologia*, vol. 12, no. 3, pp. 144–158, 1988.

[9] M. Rejewski, “An Application of the Theory of Permutations in Breaking the Enigma Cipher,” *Applicaciones Mathematicae*, vol. 16, no. 4, pp. 1–18, 1980.

[10] J. Vabek, “On Rejewskis Solution of Enigma Cipher,” *WDS Proceedings of Contributed Papers*, vol. 1, pp. 124–129, 2006.

[11] K. Pommerening, “Permutations and Rejewskis Theorem,” *Fachbereich Mathematik*, pp. 1–10, 2008.

[12] M. Rejewski, “How Polish Mathematicians Deciphered the Enigma,” *Annals of the History of Computing*, vol. 3, no. 3, pp. 213–234, 1981.

[13] C. A. Deavours, “The Black Chamber: A Column How The British Broke Enigma,” *Cryptologia*, vol. 4, no. 3, pp. 129–132, 1980.

[14] “Vestergaards Matematik Sider,” 2006. [Online]. Available: http://www.matematiksider.dk/enigma_eng.html

[15] C. A. Deavours, “Analysis of the Hebern Cryptograph Using Isomorphs,” *Cryptologia*, vol. 1, no. 2, pp. 167–185, 1977.

[16] J. J. Gillogly, “Ciphertext-Only Cryptanalysis of Enigma,” *Cryptologia*, vol. 19, no. 4, pp. 405–413, 1995.

[17] H. Williams, “Applying Statistical Language Recognition Techniques in the Ciphertext-Only Cryptanalysis of Enigma,” *Cryptologia*, vol. 24, no. 1, pp. 4–17, 2000.

[18] P. J. W. James A. Reeds, “File security and the unix crypt command,” *Bell Laboratories*, 1998.

[19] A. J. Bagnall and G. P. Mckeown, “The Cryptanalysis of a Three Rotor Machine Using a Genetic Algorithm,” 2000.

[20] L. a. Gladwin, “Bulldozer: A Cribless Rapid Analytical Machine (RAM) Solution to Enigma and its Variations,” *Cryptologia*, vol. 31, no. 4, pp. 305–315, Oct. 2007. [Online]. Available: http://www.tandfonline.com/doi/abs/10.1080/01611190701506022

[21] W. Friedman, “Index of coincidence and its application in cryptography,” *Riverbank Publications*, 1922.

[22] A. M. Turing, “Turing’s treatise on enigma, chapter 3,” 1939.

[23] ——, “Turing’s treatise on enigma, chapter6,” 1939.

[24] M. S. Paul Reuvers, “Crypto and cipher machines,” 2010. [Online]. Available: http://www.cryptomuseum.com/crypto/

[25] L. Kruh, “Cipher Equipment,” *Cryptologia*, vol. 1, no. 1, pp. 69–75, 1997.

[26] ——, “Cryptologia How to use the German Enigma Cipher Machine: A Photographic Essay,” *Cryptologia*, vol. 7, no. 4, pp. 291–296, 1983.

[27] D. H. Hamer, G. Sullivan, and F. Weierud, “Enigma Variations: an Extended Family of Machines,” Tech. Rep. 3, 1998.

[28] A. R. Miller, “The Cryptographic Mathematics of Enigma,” *Cryptologia*, vol. 19, no. 1, pp. 65–80, 1995.

[29] R. A. Ratcliff, “How statistics led the Germans to believe Enigma Secure and why they were wrong: Neglecting the practical mathematics of Cipher Machines,” *Cryptologia*, vol. 27, no. 2, pp. 119–131, 2003.

[30] M. J. Blair, “Practical use of the m-209 cipher machine,” 2013.

[31] J. Reeds, “Entropy Calculations and Particular Methods of Cryptanalysis,” *Cryptologia*, vol. 1, no. 3, pp. 235–254, 1997.

[32] R. L. Rivest, “Statistical Analysis of the Hagelin Cryptograph,” *Cryptologia*, vol. 5, no. 1, pp. 27–32, 1981.

[33] G. Sullivan, “Cryptanalysis of Hagelin Machine Pinwheels,” *Cryptologia*, vol. 26, no. 4, pp. 257–273, 2002.

[34] R. Morris, “The Hagelin Cipher Machine (M-209) Reconstruction of the Internal Settings,” *Cryptologia*, vol. 2, no. 3, pp. 267–289, 1978.

[35] H. P. Greenough, “Cryptanalysis of the Uncaged Hagelin,” *Cryptologia*, vol. 14, no. 2, pp. 145–161, 1990.

[36] W. G. Barker, “Solving a Hagelin, Type CD-57, Cipher,” *Cryptologia*, vol. 2, no. 1, pp. 1–8, 1978.

[37] T. S. T. D. 2785, “German cryptanalytic device for solution of m209 traffic,” Declassified in 2010.

[38] D. Kahn, “The Significance of Codebreaking and Intelligence in Allied Strategy and Tactics,” *Cryptologia*, vol. 1, no. 3, pp. 209–222, 1977.

[39] D. Andelman and J. Reeds, “On the Cryptanalysis of Rotor Machines and Substitution - Permutation Networks,” *IEEE Transactions on Information Theory*, vol. 28, no. 4, pp. 578–584, Jul. 1982. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1056523

[40] W. Diffie, “Hummingbird: A rotor machine for the 21st century.”

[41] R. Anderson, “A modern cipher machine,” 1995.