AN OVERVIEW OF THE *History of Cryptology*

INTRODUCTION

The ability to communicate has always been a key aspect in the acquisition of knowledge and the evolution of humanity. The need to convey a message in a secure way is probably as old as communication itself. Historically, it was during conflicts between nations that this was the most necessary. In our modern world where many communications media are used routinely, the need for privacy is more of an issue than ever in a great variety of applications. Software companies wish to protect their products against piracy, banks want to ensure secure transactions and almost everyone wishes to keep their personal information private. The need for secure communications gave rise to a science referred to as cryptology.

The reader is offered a quick tour of cryptology from a historical perspective. Some classical cryptologic techniques will be covered including some which originated nearly 2000 years ago as well as others which were used up to and including the early 20th century. For the latter period, it will be shown that cryptologic systems were often mechanical and electro-mechanical devices. There is a quiz section at the end of the pamphlet which will test the reader s understanding of basic cryptography and hopefully increase his or her interest in this fascinating field.

There are many other interesting sources of information about the history of cryptology. Some cryptologic devices can be found at the War Museum in Ottawa. There are museums devoted (wholly or partly) to the history of cryptology in the United States (at the National Cryptologic Museum near Fort Meade, Maryland), in Great Britain (at Bletchley Park near London), and in Canada (at the Military Communications and Electronics Museum in Kingston, Ontario). It is relatively easy to find books on the subject, in particular regarding World War II and the German ENIGMA enciphering device. The World Wide Web (WWW on the Internet) is also a rich source of information even though the quality of the information can vary from site to site. A list of such sites (in particular those for the museums aforementioned) is included at the end of this pamphlet.

AN OVERVIEW OF THE *History of Cryptology*

CRYPTOLOGY

A *cipher system* or *cryptosystem* is a technique used to hide messages from unintended recipients. *Cryptography* is the science that creates those cryptosystems while *cryptanalysis* is the art of unraveling or breaking such systems, that is, reading them even if one is not the intended recipient. The term *cryptology* is used to encompass both cryptography and cryptanalysis. The original message which is to be sent is called the *plaintext*. The encrypted message is called the *ciphertext*. *Encryption* is the process of transforming the plaintext into ciphertext, typically by using an *algorithm* and a *key*. A key is that component which is shared secretly by both sender and recipient and may vary from one message to another (the key is often referred to as a *cryptovariable*). *Decryption* is the process of transforming the ciphertext back to the plaintext. This reverse process is typically derived from the knowledge of the encryption algorithm and the key.

As an example, suppose the number 521 is to be sent in a secure way. Also assume that the intended recipient and sender have already agreed on a key value of 122 and an encryption algorithm which is the addition of the message (521) and the key (122). In that case, the ciphertext is 643. Since the recipient knows the key (122) and the encryption algorithm (addition), he or she can decrypt the message by doing the reverse operation, subtracting 122 from 643 to get the plaintext message 521. Someone intercepting the communication should experience some difficulty figuring the plaintext from the ciphertext alone, even if the encryption technique (but not the key) is known.

AN OVERVIEW OF THE *History of Cryptology*

MANUAL SYSTEMS

Manual (or hand) systems usually refer to cipher systems that can be typically worked out with pencil and paper. These are amongst the oldest known cryptosystems. The key or secret component which is typically associated to such systems is called a *keyword* or *codeword*. A keyword is typically a word or short phrase.

Caesar Cipher

Perhaps the earliest known cipher system was used by Julius Caesar about 2000 years ago. The idea is to replace each letter of the alphabet by the letter that is three positions after it in alphabetical order and wrapping back at A beyond Z when necessary. This is an example of a substitution technique as each occurence of a given plaintext letter is always replaced by the same letter. The substitution alphabet for the Caesar cipher is given below.

```
Alphabet:       ABCDEFGHIJKLMNOPQRSTUVWXYZ
Substitution:   DEFGHIJKLMNOPQRSTUVWXYZABC
```

Using this technique, the message **"ROME SWEET ROME"** translates into **"URPH VZHHW URPH"** which can be written in the continuous form **"URPHVZHHWURPH"** for added security. In some applications, the cipher is reformatted into 5-character groups (with the last group perhaps being smaller than 5 characters) so that the latter example would become **"URPHV ZHHWU RPH"**.

Substitutions, Permutations and Transpositions

The Caesar cipher is an example of a monoalphabetic substitution where the letters of a given alphabet are jumbled in a fixed manner. Of course, there are many possible substitution schemes of the alphabet **{A,B,C,...,Y,Z}** for which the reader is referred to Problem 4 in the Quiz Section. For example, one can use the following substitution table:

```
Alphabet:       ABCDEFGHIJKLMNOPQRSTUVWXYZ
Substitution:   QWERTYUIOPASDFGHJKLZXCVBNM
```

It is left to the reader to reflect if the above is a random substitution. As an example of encryption using this table, the message **"SEND THE MATERIAL NOW"** becomes **"LTFR ZIT DQZTKOQS FGV"**.

It is even better if the cipher is transmitted without the spaces between words as this may provide clues to an unintended recipient. When the language used is known, substitution ciphers can be attacked using techniques such as frequency analysis and keyword search. For example, in English, the most likely letter is **E**. Other frequent letters are **T,R,S,N,I,A** and **O**. This list can vary slightly depending on the document used as a corpus. If word division is known, tricks can be used on small words. For example, single-letter words are often **A** or **I**. The three letter word **THE** is very fre-

quent while a four letter word with the pattern **XYZX** is often **THAT**. One can think of many such useful observations. Some of these approaches can be applied to cryptanalyze the cipher text:

"EKNHZGUKQHIN OL ZIT LEOTFET ZIQZ EKTQZTL ZIT EOHITK LNLZTDL XLTR ZG IORT DTLLQUTL YKGD XFOFZTFRTR KTEOHOTFZL".

Notice first that the most frequent cipher letter is **T**, probably replacing the **E**. The 3-character stretch **ZIT** which appears twice could very well be **THE** and since **Z** stands for **T** in that case, the word **ZIQZ** might be **THAT**. The 6th word now reads ****EATE*** whose completion **CREATES** appears as a good choice. At this point, these successive guesses yield the following partial decryption scheme,

```
Alphabet:       ACEHRST
Substitution:   QETIKLZ
```

This partial knowledge gives the following plain text:

"CRT**RA*H* *S THE SC*E*CE THAT CREATES THE C**HER S*STE*S**
***SE* T* H**E *ESSA*ES**
R** ****TE**E* RECE*TS"**

The task is almost over. Completing the 4th word, **SCIENCE**, gives the **I** and **N**. At that point, the rest of the message can be decrypted easily to yield:

"CRYPTOGRAPHY IS THE SCIENCE THAT CREATES THE CIPHER SYSTEMS USED TO HIDE MESSAGES FROM UNINTENDED RECIPIENTS".

When a substitution is used, the text remains in the same order but the letters are replaced. A permutation affects the *order* in which the letters of the plaintext are written to produce cipher text. Permutations are usually performed on fixed length blocks of plaintext. Extra characters can be added to complete the last block. Note that with such a method the characters are shuffled but kept intact. As an example, consider the following permutation rule applied to blocks of five characters.

```
Original position in block:   12345
New position in block :       42135
```

Here is an example of encryption using this permutation for blocks of five letters with random padding characters (these are added so that complete blocks are obtained):

```
Plain text:                          SEND THE MATERIAL NOW
Padded plain text in blocks of 5:    SENDT HEMAT ERIAL NOWXT
Permuted text in blocks of 5:        DESNT AEHMT AREIL XONWT
Final cipher text:                   DESNTAEHMTAREILXONWT
```

Another form of shuffling is column transposition. Using the same plain text as above, a table is built where spaces are omitted and each line is of length n from which the text is read column by column. Here is an example with n=6 columns and the above plaintext.

S E N D T H
E M A T E R
I A L N O W

The text read column by column yields the cipher **SEIEMANALDTNTEOHRW**. There are many variations of the above techniques, some being very complex in nature. It is also possible to use more than one method in clever ways thereby improving the overall security of the system; in other words, the new system is less vulnerable to cryptanalysis.

Porta's Table

This system was devised in 1563 by Giovanni Battista da Porta from Naples. His encipherment scheme can be described using Table 1 below. It requires a keyword whose characters will be referred to as key letters. The first column (indicated by pairs of bold letters) constitutes the keyword section. The top row (in bold lowercase letters) will be paired with another row which is specified by the respective key letters. This pairing will constitute a reciprocal substitution for a particular key letter. Given a key letter, if the letter to be enciphered is in the top row, we substitute it with the one appearing in that letter s column and in the row specified by the key letter. If the letter is not in the top row, then it must appear in the row specified by the key letter and it is substituted with that letter which is in its column and which appears in the top row.

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

Table 1: Porta s Table

Suppose **IT** is to be encrypted using the keyword **UP**. The first key letter is then **U** so that the specified pairing is as follows:

	a	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**
UV	q	r	s	t	u	v	w	x	y	z	n	o	p

Since the first plaintext letter is **I**, it is therefore encrypted to **Y**. The second key letter is **P** so that the second pairing is:

	a	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**
OP	t	u	v	w	x	y	z	n	o	p	q	r	s

and therefore **T** gets encrypted to **A**. Thus with keyword **UP** using Porta s, **IT** becomes **YA**. As a further example, consider the following encipherment using the keyword **MAGIC**:

```
keyword:    MAGICMAGICMAGICMAG
plaintext:  SENDTHEMATERIALNOW
ciphertext: LRDZHORWWHYESWXGBM
```

The Vigenère Cipher

The following encryption technique is the work of Blaise de Vigen re, a Frenchman who lived from 1523 to 1596. It appears that the technique was developed when Vigen re was at the Vatican during various diplomatic missions. The idea of the technique is to use a different substitution alphabet for each character position which makes the traditional frequency analysis much harder. A codeword is chosen and written on top of the plaintext repeatedly. In the following example, the codeword is MONTREAL. To encrypt, the row of Table 2 below corresponding to the letter of the codeword is used as a substitution alphabet and the plaintext character is encrypted. Essentially, this is a substitution method where the substitution alphabet changes at every character according to a preset pattern.

```
codeword:   MONTREALMONTREALMO
plaintext:  SENDTHEMATERIALNOW
ciphertext: ESAWKLEXMHRKZELYAK
```

In this case, the intended recipient must know the codeword and have a copy of the encryption table, but this table can be quite standard, such as Table 2. Decryption is done by a simple reversal of the encryption process.

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

Table 2: A Vigen re Table

The Playfair Cipher

This cipher system was invented by Charles Wheatstone, a professor of philosophy at King s College in London, England. The system obtained its name in 1854 when Lyon Playfair, Baron of St. Andrews, presented it at a dinner party which Lord Palmerston, who was to become

prime minister, was attending. The Playfair cipher system was used by the British during the Boer War and World War I. A simple version of this encryption algorithm is as follows:

- Fill a 5 by 5 table with the letters of the alphabet, grouping two of the 26 letters together. This can be done using a codeword, by entering the first occurrence of the letters in the codeword followed by the remaining letters of the alphabet in order. In Table 3, we build such a table using the codeword **VANCOUVER**, grouping **I** and **J**.

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

Table 3: A Playfair Table

- Write the plaintext in pairs of letters. If a pair contains the same letter twice, add a fill letter in between (such as an **X**). For example, **SEND THE MATERIAL NOW** is written **SE ND TH EM AT ER IA LN OW**. Notice that we can add any character at the end to complete the last pair, if necessary.
- For each pair of letters, use the table according to the appropriate rule:
  - If the letters are in the same column, they are each replaced by the letter immediately below in the same column and in a modular fashion. A letter in the bottom position is replaced by a letter in the top position of that column.
  - If the letters are in the same row, they are each replaced by the letter immediately to their right in the same row and in a modular fashion. A letter in the rightmost position is replaced by a letter in the leftmost position of that row.
  - If the two letters are not in the same column or row, they are replaced as follows. The first cipher letter is obtained by taking the intercept of the row of the first plaintext letter with the column of the second. The second cipher letter is obtained by taking the intercept of the column of the first plaintext letter with the row of the second letter.

If the Playfair table is applied to the last message example given above, the encipherment steps are listed in the grid below. The cipher is then written in one stream of letters, namely: **MDORXFGWVWRBGCPVAZ.**

Plaintext	Case	Cipher
SE	Different Row and Column	MD
ND	Different Row and Column	OR
TH	Different Row and Column	XF
EM	Same Column	GW
AT	Different Row and Column	VW
ER	Same Row	RB
IA	Different Row and Column	GC
LN	Different Row and Column	PV
OW	Different Row and Column	AZ

Some Unorthodox Methods

What has been covered so far comprises conventional encryption techniques where the plaintext is mixed with the key following a given algorithm in order to produce the ciphertext. There are many other ways which can be used to transmit a secret message; these may not, in the strictest sense, necessarily be part of classical cryptology. For example, one can use invisible ink on a material (such as certain types of paper) so that, when heated or some chemical is applied, the material will expose the concealed message. Another possibility is to reduce a text from a physical page so that it appears as a simple dot and send it along with a common message. The use of cipher codes is by no means the only possible way to send information in a secure manner, but it is one of the most convenient and easy to use methods and remains very common.

MECHANICAL SYSTEMS

Manual systems are inherently slow and tedious from the user s perspective. Such algorithms are often limited in their complexity. More robust and complex cipher systems were developed by using mechanical devices. In this section, the reader is given a brief look at some historically significant mechanical cipher machines.

Cipher Disks

The first cipher disk is believed to have been invented by Leon Battista Alberti in the 15th century. It consisted of two concentric circles made of copper plates with one being larger and stationary while the smaller inner one was considered the movable disk. The disks were

divided into 24 equal radial parts. The outer disk contained the sequential representation of the plain component,

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

for which the alphabetical characters were sufficient to represent most Latin words. Furthermore, the inner disk contained a permutation of the Latin alphabet which was:

{ m,r,d,l,g,a,z,e,n,b,o,s,f,c,h,t,y,q,i,x,k,v,p,et }.

The disk in itself was perhaps not so novel but how it was used certainly reflected Alberti s ingenuity. He incorporated polyalphabetic substitution and the use of enciphered codes. The interested reader is referred to [1] for more intricate and fascinating details.

Another classic example of cipher disks is that of the Confederate brass cipher disk. The inner and outer portions contain the alphabetical characters in their natural order. However, the idea was to use the disk to apply the Vigen re technique. A detachable cipher disk (which requires some construction) is included in the middle portion of this pamphlet.

M-94/CSP-488 Cylindrical Device

In 1922, the U.S. Army issued its M-94 which strung 25 aluminum disks (which were about 4cm in diameter) on a spindle about 10.5cm long. This device remained in service until early in World War II. It was also used in other areas such as the Coast Guard and the Radio Intelligence Division of the Federal Communications Commission in the United States. The U.S. Navy used a similar device called CSP-488.

The KRYHA Device

First appearing in the 1920 s, the KRYHA was invented by the Ukrainian, Alexander Von Kryha. It had a fixed semi-circle of letters against which was juxtaposed a cipher disk with gears controlling the number of spaces it turned. Both sequences of letters could be mixed alphabets. A handle served to wind a powerful clock spring which drove the rotating platform on which the inner cipher disk was mounted. The key or setting consisted of another wheel whose segments (open or closed) controlled the rotational stepping of the inner cipher disk. Unfortunately, as compact and attractive as the KRYHA was, its mechanism was essentially equivalent to a simple polyalphabetic cipher with a single cipher alphabet and a period of a few hundred letters which was demonstrated to be solvable in hours by American cryptanalysts.

CSP-488
Cylindrical Device

KRYHA Cipher Device

M-209B Cipher Device

The Hagelin M-209 Converter

Manufactured by Boris Hagelin in the early 1940 s for the U.S. Army, the M-209 was a simple mechanical device whose dimensions were 18cm wide, 14cm deep and 9cm high. It was stored in a green canvas bag and its weight was approximately 4 kilograms. The main components were six wheels whose lengths were 26, 25, 23, 21, 19 and 17; these essentially defined the key period of 101,405,850 for the device. To operate the enciphering device, the operator would spin the knob on the left to bring the first plaintext letter on the indicating disk to a notched mark. One would then turn the power handle on the right which would rotate the inner components. The end of the power handle revolution would press a paper tape against a typewheel (which had been inked) and print the ciphertext letter. During World War II, more than 140,000 units were produced primarily by the Smith Corona Typewriter company in the United States.

ELECTRO-MECHANICAL SYSTEMS

By using a power supply such as a battery, some very complex and efficient enciphering machines were developed during the 20th century. Many of these were used during World War II among which the famous German ENIGMA.

The ENIGMA

Stemming from patents in 1919 by Alexander Koch and more eminently by Arthur Scherbius during the 1920 s, the ENIGMA appeared in commercial versions: Models A, B and C. Model C was a portable non-printing device in which the letters were indicated by lamps. All models had typewriter-like keyboards. The ENIGMA differed in two important ways from other previous rotor conceptions. Its final rotor was reflective which made the enciphering reciprocal, i.e. E(E(x)) = x but with the condition that E(x) › x for all characters x where E is the encryption function. This in turn allowed decryption to occur using the same settings as in the encryption process, except that cipher characters would be entered via the keyboard and the decrypted character would light on the display. Another important difference was that the rotor movement was governed by gears so that the stepping would be irregular.

In the 1930 s, Germany began re-arming itself and decided that a 3-rotor ENIGMA offered acceptable levels of security. During World War II, the portable glow lamp ENIGMA, battery-powered and, in its wooden box, about the size and weight of a standard typewriter, served the top German Army (Armee), Navy (Kriegsmarine), and Air Force (Luftwaffe).

The early design had five rotors (typically indexed as I, II, III, IV, and V), each containing 26 contacts on each side and wired to correspond to a secret permutation. Each rotor would have a ring with a single notch which would be set to one of the 26 possible positions on the rotor. The purpose of this notch was to step the rotor immediately to its left. For each letter pressed on the keyboard, the rightmost rotor always stepped once. On average, the second rotor stepped once every 26 characters while the third (leftmost) stepped once every 676 characters. Furthermore, the front vertical face of the ENIGMA incorporated a plugboard with 26 pairs of electrical sockets which were alphabetically indexed from A to Z. It was common practice for the settings to call for 10 wires to be used to connect a total of 20 sockets. By pressing a letter on the keyboard, the electrical current would go through the plugboard, then through the rotors (from right to left) into the reflector to be returned through the rotors (from left to right) back to the plugboard to finally light up one of the 26 letters on the lampboard.

There were daily settings which included 1) choosing a specific ordered set of three rotors (from the available five rotors) which were inserted into the ENIGMA, 2) the positions

3-rotor ENIGMA

4-rotor ENIGMA

ENIGMA Rotors

(ringstellung) at which the notched ring should be set for the respective selected rotors, and 3) the 10 pairs of sockets to be connected on the plugboard. The operator had to make a random selection for the initial positions of the three rotors before encrypting the plaintext. These three initial positions were encrypted and sent to the recipient who would in turn decrypt them so that the machine could be set to decrypt the ciphertext; the method by which these starting positions were encrypted varied throughout World War II. For more technical details regarding the ENIGMA, the interested reader is encouraged to read Chapter 11 of [2]. One disadvantage of the ENIGMA was that it did not print and speedy operation often required three men: one to read incoming text and press the keys, one to call out the letters in a loud voice as they lit up, and one to write down the results.

In February 1942, the German Navy modified its 3-rotor ENIGMA by adding a fourth rotor (thereby requiring a new compressed reflector) and allowing up to two notches on the ring around the rotors. This increased the complexity of cryptanalysis being carried out at Bletchley Park in Britain. In the years leading to World War II, three Polish mathematicians (Rejewski, Rozycki, Zygalski) had done remarkable cryptanalytic work with regards to the ENIGMA and how it could be exploited. However, with the advent of hostilities and further modifications to the ENIGMA such as the addition of a plugboard and the choice of 3 rotors from a bank of 5, the Poles gave all the details of their work to the British who greatly benefitted from this information. During World War II, the British were able to capture 3-rotor and 4-rotor machines together with keylists thus enabling the advent of massive codebreaking devices called *Bombes*; these exhaustively tried wheel settings for specific messages. The intelligence gathered from the cryptanalysis of ENIGMA decrypts fell under the codename ULTRA. There were other German cryptographic devices which were used such as those from the *Geheimschreiber* family of teletype-writers such as TUNNY for which the traffic was cryptanalyzed and exploited using another specially built machine at Bletchley called *Colossus*.

The interested reader is encouraged to refer to [2], [3], [4], [5], [6], [7], [8] and [17]. It should also be mentioned that some of the history behind Bletchley Park can be found on the internet at the Web site listed at the end of this pamphlet.

The HEBERN Cipher Machines

In 1910, Edward H. Hebern began to develop encryption devices in the United States. In the early 1920 s, he engineered what was termed the electric code machine which used a single rotor. He also designed 3-rotor and 5-rotor machines as part of bids for the U.S. Navy in 1924. Unlike the ENIGMA, the HEBERN machines used rotors whose internal wiring could

be readily changed. The rotors could also be inserted in either their standard or reverse rotation. However, his devices were suspect to cryptanalytic weaknesses as indicated by William Friedman in [9].

TYPEX & SIGABA

As the result of a long study (1926-1935) of commercially available cryptographic equipment such as the HEBERN, KRYHA and ENIGMA, a British interdepartmental committee adopted an ENIGMA-type cipher machine called the TYPEX. The Mark III model of the TYPEX had five interchangeable rotors and a design which allowed irregular rotor movement. It was electrically powered and output was via a paper tape printer located in the back of the machine. There have been several versions of the TYPEX which were used throughout the British Army and most of the RAF. They also found much use in Canada. For more details, the reader is referred to [3].

ECM - SIGABA

At about the same time (just before 1940), the U.S. Army and Navy adopted a similar device called the ECM Mark II where ECM stood for Electric Cipher Machine . The U.S. Army referred to this device as the SIGABA. It was used exclusively by the Americans during World War II and beyond.

In order for the ECM and TYPEX to intercommunicate, TYPEX compatible rotor cages were designed for the ECM and gave rise to the CCM which stood for Combined Cipher Machine .

NEMA

The NEMA (NEue MAchine) was a device put into service in 1947 by the firm Zellwager A.G. in Switzerland. Its design had started in 1941 and two pre-production models were produced in 1944; it was developed by the Swiss Army Cipher Office. It was based on the ENIGMA principle such as the use of a reflective rotor. It contained a total of 10 rotors. However, the rotor movements were much more irregular and the reflector moved during encipherment. In fact, five rotors were referred to as Fortschaltwalzen and acted as drive wheels for the other five. The rightmost, which was red while the other nine were black, controlled the movement of the two slower rotors while the other three rotors stepped more frequently. The NEMA had several features such as exchangeable external power source (e.g. 110v, 220v, etc.), an adapter which fit in any universal light bulb socket, and a separate lampboard for ease of use. The original customers of this device were the Swiss Army and the Swiss Diplomatic Service. The two machines were identical in construction except that they used different rotor sets.

NEMA

MODERN IMPLEMENTATIONS

With the proliferation of computers and an increase in their connectivity, many modern cryptologic methods rely on software instead of mechanical or electro-mechanical devices. In fact, much commercial software now include some encryption schemes for added security. Most of these encryption techniques require mathematical knowledge that is beyond the scope of this pamphlet. Some more advanced techniques are described in [10] and [12].

AN OVERVIEW OF THE *History of Cryptology*

GENERAL REVIEW

1. Quiz
   - ¥ This Roman emperor invented and used one of the first cipher systems.
   - ¥ This mechanical device was used intensively by the German army, marine and air force during World War II.
   - ¥ He is the actual inventor of the Playfair cipher system.
   - ¥ This 10-rotor commercial replacement of the ENIGMA was used by the Swiss army.
   - ¥ He manufactured the M-209 in the early 1940 s, which was used by the U.S. Army.
   - ¥ This technique can be used to attack messages encrypted with a substitution.
   - ¥ This system was used by the British during the Boer War and World War I.
   - ¥ This term is used to describe paper and pencil type cryptosystems.
   - ¥ This was the name of the British special device which helped in cracking the German ENIGMA cipher.
   - ¥ This Frenchman invented a famous cipher system in the 1500 s while at the Vatican.
   - ¥ This is the name of the activity of trying to break cryptosystems.
   - ¥ This device was invented by Leon Battista Alberti in the 15th century.

2. Consider the Caesar cipher using an offset of n=5 instead of n=3. Decrypt the message:

   RDKNWXYIJHWDUY.

3. The following pair of cipher and plain uses the Caesar cipher with offset n. The plaintext is:

   NEXT MEETING MONDAY

   and the cipher reads:

   CTMIBTTIXCVBDCSPN.

   Determine n.

4. Consider an alphabet with only 2 symbols {A,B}. There are two possible substitutions one can use. The first one is called the identity: A is replaced by A and B by B. This is not a very useful coding technique! The second substitution consists of replacing A by B and B by A (not very useful either).

- How many substitutions are there with an alphabet of size 3 such as {A,B,C}? Of size 4 such as {A,B,C,D}?
- How many substitutions are there for an alphabet of size 26? of size N?

5. Design an encryption scheme that uses a Caesar cipher followed by a block permutation. Is there any difference if the block permutation is done first? Why?

6. Decrypt the following text which was encrypted using column transposition with n < 11 columns:

YEESEANISRCNTEOAHSLLEEULRVMX

7. Using frequency analysis, decrypt the following message:

STC HKQS IHLKPSDJS NUCQSIKJQ KR GIRC DPC RKP STC HKQS LDPS PCDGGY KJGY LPKEGCHQ KR LPKEDEIGISY

knowing that:

- the words are properly spaced;
- it was written by the Marquis de Laplace, well known for his work in probability theory;
- the most common vowel is O, followed by E;
- the most common consonant is T, then R and then L;
- letters C, D, G, J, K, V, W, X and Z do not appear in the plaintext.

8. Encrypt the following text with the Vigen re method and the codeword of your choice using the included cipher disk:

ONLY A PERSON WHO RISKS IS FREE.

9. Decrypt the following text encrypted with the Vigen re method and the keyword CODEWORD with the use of the included cipher disk:

EVDRCSTRFSZSNRKRBMAA.

10. (Requires programming) Implement the Vigen re method using the programming language of your choice. The system should prompt the user for a keyword and use it to encrypt and decrypt typed text with the alphabet given in Table 2.

REFERENCES

In addition to references indicated within the pamphlet, the following list contains other publications which may further interest the reader in some of the aspects covered in this pamphlet. Of particular note, reference [9] below includes The Friedman Legacy which covers a series of lectures given by William Friedman, a man described as the most prominent pioneer in the application of scientific principles in the field of cryptography .

Reference [1] is an excellent source on the history of cryptography. It covers diverse topics from a historical perspective while providing good technical details.

[1] Kahn, David. *The Codebreakers: History of Secret Communication*, MacMillan Publishing Co., 1967.
[2] Hinsley F.H.; and Stripp, Alan. *Codebreakers: The Inside Story of Bletchley Park*, Oxford University Press, 1993.
[3] Hodges, Andrew. *Alan Turing: The Enigma*, Touchstone, 1993.
[4] Winterbotham, Frederick W. *The Ultra Secret*, Dell Publishing, 1974.
[5] Calvocoressi, Peter. *Top Secret Ultra*, Pantheon, 1980.
[6] Montagu, Ewen. *Beyond Top Secret U*, Readers Union, 1978.
[7] Garlinski, J zef. *The Enigma War*, Scribners, 1979.
[8] Kahn, David. *Seizing the Enigma*, Houghton Mifflin Co., 1991.
[9] *The Friedman Legacy: A Tribute to William and Elizebeth Friedman*, NSA Publication: Sources in Cryptologic History, Number 3, 1992.
[10] Schneier, Bruce. *Applied Cryptography*, Wiley, (2nd Edition), 1996.
[11] Deavours, Cipher; Kahn, David; Kruh, Louis; Mellen, Greg; and Winkel, Brian. *Cryptology: Machines, History & Methods*, Artech House, 1989.
[12] Stinson, Doug. *Cryptography, Theory and Practice*, CRC Press, 4th Printing, ISBN 0-8493-8521-0, 1996.
[13] Lerville, Edmond. *Les cahiers secrets de la cryptographie*, Editions du Rocher, 1972.
[14] Sacco, G n ral L. *Manuel de cryptographie*, Payot (French Edition), 1951.
[15] Lange, Andr ; Soudart, E.-A. *Traité de cryptographie*, Librairie F lix Alcan, 1935.
[16] Givierge, G n ral M. *Cours de cryptographie*, Berger-Levrault (3rd Edition), 1936.
[17] Singh, Simon. *The Code Book*, Doubleday, 1999.
[18] Baudoin, Roger. *Eléments de cryptographie*, A. Pedone, 1939.
[19] Kahn, David. *La guerre des codes secrets*, InterEditions, 1980.
[20] De Vigen re, Blaise. *Traité des chiffres*, Guy Tr daniel, 1996 (Reprint of 1586 edition).

[21] Smith, Michael. *Station X*, Channel 4 Books, 1998.
[22] Kippenham, Rudolf. *Code Breaking*, Overlook Press, 1999.

SITES OF INTEREST

1. Bletchley Park (England):
   http://www.cranfield.ac.uk/CCC/BPark/
2. National Cryptologic Museum (Fort Meade, Maryland, USA)
   http://www.nsa.gov:8080/museum/
3. Military Communications & Electronics Museum (Kingston, Ontario, Canada)
   http://www.c-and-e-museum.org/
4. Communications Security Establishment (Canada)
   http://www.cse-cst.gc.ca/
5. U.S.S. Pampanito Cipher Equipment Site:
   http://www.maritime.org/ecm2.shtml
6. JAVA Applet Simulator of 3-rotor ENIGMA:
   http://www.ugrad.cs.jhu.edu/~russell/classes/enigma/

ACKNOWLEDGMENTS

There have been many who have helped in producing this pamphlet. The authors are most appreciative of the assistance provided by:

- CSE colleagues for their respective reviews and suggestions;
- CSE s Visual Communications Group for graphic design services;
- CSE s Linguistic Services for their revision of the text;
- USS Pampanito for the photograph of the CSP-488 cylindrical device;
- National Cryptologic Museum for the photograph of the ECM/SIGABA.