IB EXTENDED ESSAY

SUBJECT: MATHEMATICS

The Use of Mathematics
In the Science Of
Cryptology

Student: Alper Umut Uçar
Supervisor: Nilay Alpar
Candidate Number: 001129-0042
School: TED Ankara College Foundation Private High School
September, 2013
Word Count: 3485

ABSTRACT

Cryptology is a science that has been used throughout the history in order to protect the privacy of the contact between two or more people in order to prevent the other people to understand the communication by mainly using Mathematical codes. The aim of this essay is to illustrate the theoretic and applied uses of mathematics in cryptology and defining the function that has been used to identify the cryptography.

In the first part of the essay, the basics and definition of cryptography have been explained. Information on how does the cryptography work and conventional cryptography has been provided.

In the second part, the brief history of cryptography has been given. In this part, great minds and the politics of cryptography have been also provided.

In the last part, some of the classic cryptography methods have been explained and examples have been given to understand the subject better.

Word count: 149 words

ACKNOWLEDGMENTS

While preparing this extended essay, my advisor Ms. Nilay ALPAR has been a tremendous mentor for me. I would like to convey my special thanks to her for encouraging my study.

Besides, I would like to extend my special thanks to my family. They supported me while preparing the essay and they were extremely helpful and patient during the preparation process. Words can not express my grateful to them.

TABLE OF CONTENTS

PART I
INTRODUCTION

Why I Chose Subject?

As being an IB student and choosing Mathematics and Chemistry as high level courses in TED Ankara College, I was wondering how these courses especially Mathematics which is known as abstract science, has been applied and implemented in real life.

Nowadays, whether online shopping transactions, whether you get credit card transactions, whether financial market transactions, whether defense and security systems, whether you get to the interstate communication, whether interpersonal communication, and so on, information to be transferred safely is of great importance.

I learned from my parents, my teachers and various resources that encryption and decryption algorithms having an important role while transmitting information in a secure manner from sender to receiver. With the guidance of my parents and my teachers, I decided to make a research on Cryptology which is a mathematical science and generally based on the Number Theory. By doing research on this topic, I have an opportunity to become knowledgeable about the area as well as implementation issues and I have believed that I have achieved.

LITERATURE REVIEW

The Aim of Encryption and Decryption Process

The aim of encrypting plain text or clear text is transferring a message to the receiver without the messenger being able to read it. This process is provided by somehow coding the plain text in a way that any person that is not included in the conversation may not be able to figure out what it says. The text that has been formed after coding/encryption is called chippertext. Encryption is used in order to hide the information from anyone that is not wanted to learn the secrecy.

Decryption is used to revert the ciphertext to its original form and figure below displays the encryption and decryption process.

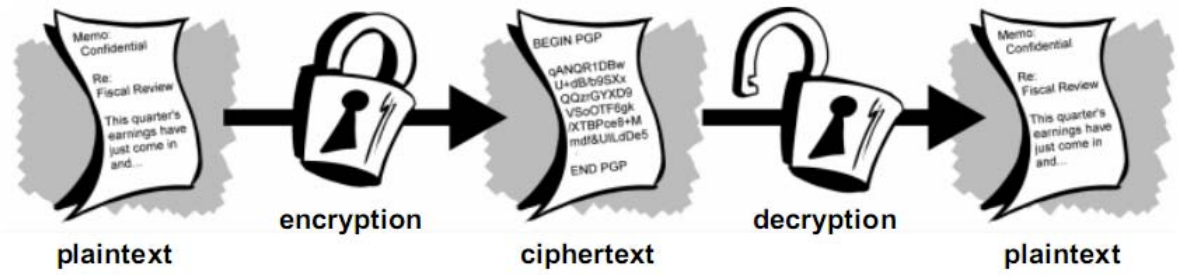


Figure 1. Encryption and decryption process [8]

Definition of Cryptography, Cryptanalysis and Cryptology

Keeping messages secret by the process of using various methods ("ciphers") is called cryptography. The science of attacking ciphers, finding weaknesses, and checking security of a cipher is called cryptanalysis. Cryptology covers both and it is the science of secure communication [11].

How Does Cryptography Work?

A cryptographic algorithm has been used during encryption or decryption and it is a mathematical function. Algorithm works with a key and this key could be a combination of word, number or phrase. A plain text can end up with different ciphertext with different keys used to encrypt it. The security of the plain text is dependent on how strong the algorithm was chosen and also is dependent on how secret the key is [8].

Conventional encryption process is shown below.

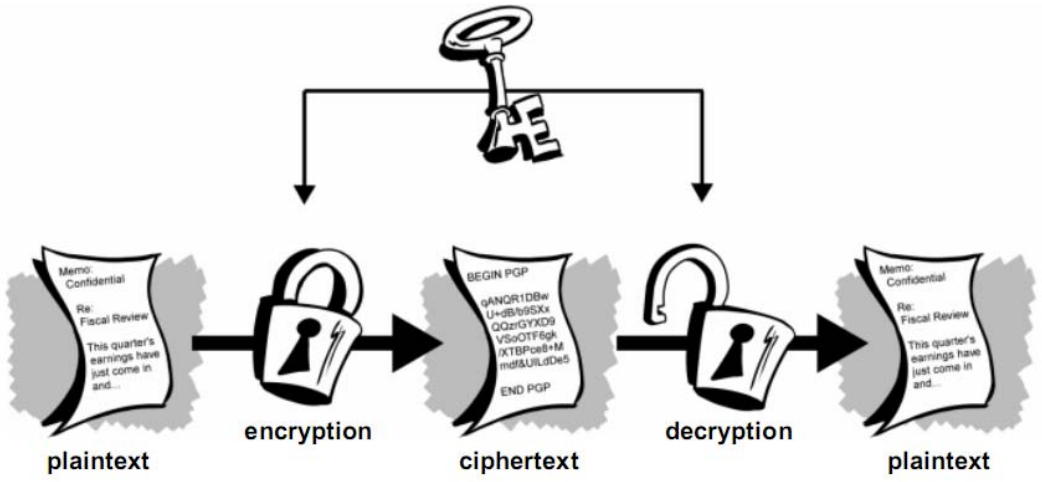


Figure 2. Conventional encryption process [8]

PART II
THE BRIEF HISTORY OF CRYPTOGRAPHY

The cryptography word comes from Greek words kryptos (hidden) and graphein (writing) [12]. The plain text was written with simple words in the beginning of cryptography because most of the people were illiterate [9].

The first aim of cryptography was converting the messages into unreadable figures. By this way, it was possible to protect the content from enemies [7].

The earliest of cryptography were found in the civilizations of Egypt, Greece and Rome [7]. In the middle ages, cryptography was used by European governments in order to communicate with the ambassadors. Nowadays, common public key and private key are used in cryptography and it has been widely accepted. In this method, while encrypting the message the sender uses the private key and while decrypting the receiver uses the public key. This allows the receiver to know the message was sent from. Also mathematical theory and computer science have been applied in cryptanalysis in 20th century [5].

The Politics of Cryptography

Cryptology always had kept a lot of importance in military and diplomatic secrecy. All of the nations owned their existence to the security of their communication. As an example, the deciphering of German Enigma by the British in World War II (WWII), supplied the Allies with victory. The deciphering of the German Enigma enabled the British to figure out where 5 of the German submarines were [5].

PART III
CLASSIC CRYPTOGRAPHY METHODS

Some of the cryptology methods are explained below:

Spartan Scytale

The first use of cryptography in the military area was done by the Spartans. They used a staff (known as scytale) and wrapped it with a thin sheet of papyrus. The sender and the receiver of the message had a scytale exactly the same circumference. The sender wraps the paper around the scytale, writes and takes it. So the piece of paper looks like it is gibberish. When the receiver receives the message, he wraps the piece of paper on his scytale and by that way he decrypts the message and able to read what is written [16].

The Spartan Scytale is as shown in the picture above.

The original message trying to be sent is “Bomb Palace Tomorrow at Nine O Clock” as seen in the picture. This is how it looks when it is wrapped:

b	o	m	b	p	a	l	a	c	e
t	o	m	o	r	r	o	w	a	t
n	i	n	e	o	c	l	o	c	k

Since encrypting and decrypting is known only by the receiver and sender, after encrypted message, piece of gibberish is formed where it is read as “btn-ooi-mmn-boe-pro-arc-lol-awo-cac-etk”. Anyone who does not know how to decrypt it will be unable to read the message.

Polybius Square

This way of encryption was created by the Ancient Greeks. This method can be applied with any alphabet but was originally used with the Greek alphabet. When Latin letters used, the table can be shown as below

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

The coordinates in the grid above will represent each of the letters. For example for 'COW', the encrypted text will look like "13 41 52". Since a square can't be formed for 26 letters, one of the letters shares place with the other one. For example for this table, '24' may be showing I or J and the receiver of the message would understand it is I or J according to the word. Such as 'Milk' would be coded "32 24 31 25" and the receiver will know that what was meant was 'Milk' but not 'Mjlk' [16].

Caesar Cipher

A Caesar Cipher is a cipher that had been encrypted by shifting. To encrypt, the letters that make up the plain text are placed with the letters that are a fixed number away from the letter. A weakness of this method is that if anyone knows how the system works, he will be able to break the code up easily. Here is how the letters are placed with the encryption with Caesar Cipher when three shifts are applied [16].

PT	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
CT	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

During encryption, the composer looks at the plain text (stated with PT) and what letter corresponds with which one at the cipher text (stated with CT) and than writes the encrypted text. The receiver on the other hand looks at the CT and finds the corresponding letter in the plain text.

For example with this cipher (which shifts the letters 3), the word 'elevator' will be encrypted as "hohydwru'.

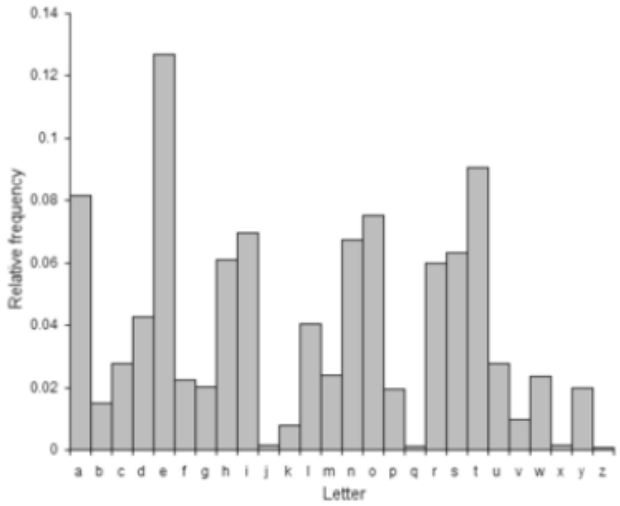
This way of encryption might be a very insecure today but when we look back at the time of Caesar, the cipher must have been very useful because his enemies would assume that the letter was written in a foreign language that was unknown.

Solving the cipher

Frequency analysis can be used to solve the Caesar cipher. There are some tools for cryptanalysis in elements of probability. The characteristic letter frequencies are often showed up in ciphertext in natural languages. These frequencies can be searched in defining various types of substitution ciphers. This analysis is based on the fact that occurrence of certain letter and combination of letters in written language with varying frequencies. Additionally, letters are characteristically distributed for almost all samples of that language. The character E is mostly used and the character X is rarely used in English language. Similarly, the pairs of letters (bigrams) which are ST, NG, TH, and QU are very common, while NZ and QJ are rarely used.

These properties of the natural language are remained as it is in the ciphertext and these patterns have the capability of being solved [16].

Relative frequencies of letters in the English language



Letter	Frequency				
a	8.167%	j	0.153%	t	9.056%
b	1.492%	k	0.772%	u	2.758%
c	2.782%	l	4.025%	v	0.978%
d	4.253%	m	2.406%	w	2.360%
e	12.702%	n	6.749%	x	0.150%
f	2.228%	o	7.507%	y	1.974%
g	2.015%	p	1.929%	z	0.074%
h	6.094%	q	0.095%		
i	6.966%	r	5.987%		
		s	6.327%		

Bigram

A pair of consecutive written elements which are typically letters, syllables, or words are called bigrams or digrams and commonly used for statistical analysis of text. They are used for speech recognition and special case of N-gram.

To solve cryptographic algorithms, bigram frequency attacks have sometimes been used. When the conditional probability is applied, bigrams provide the conditional probability of a word given the preceding word.

$$P(W_n|W_{n-1}) = \frac{P(W_{n-1}, W_n)}{P(W_{n-1})}$$

When the preceding word Wn-1 is given, the probability P() of a word Wn is equal to the probability of their bigram. This means that the co-existence of the two words P(Wn-1,Wn), divided by the probability of the preceding word [16].

Bigram Frequency in the English language

When 2000 letters have been analyzed, the expected number of occurrences of most common letter bigrams in English language is as follows

TH 50	AT 25	ST 20	HE 33	NT 24	AR 16
ER 40	EN 25	IO 18	IN 31	EA 22	AS 16
ON 39	ES 25	LE 18	ED 30	TI 22	DE 16
AN 38	OF 25	IS 17	ND 30	TO 22	RT 16
RE 36	OR 25	OU 17	HA 26	IT 20	VE 16

There are two cases:

1. Simple form of substitution cipher has been used and an attacker guesses this;
2. The shift value does not known by the attacker but he knows that Caesar cipher is in use.

In the first case, the cipher can be solved by using frequency analysis or pattern words.

In the second case, because of limited number of possible shifts, these can be tested in turn and scheme can be solved easily. Another approach is using the frequency analysis. In this approach, firstly the frequency distribution of letters is matched up. Then the frequencies of letters are used to draw graph and lastly, expected distributions of those letters in the original

language are used. One can define the shift value by looking at the particular features of the graph. Computers can also be used for this.

While there will be only one decryption for natural language plain text, multiple candidates are possible for extremely short plain texts.

Having the idea of multiple encryptions and decryptions provide extra security is not correct. Since, two encryptions in which one is using shift A as a key and the other one is using shift B as a key will be equivalent to an encryption with shift A + B [16].

Playfair Cryptanalysis

If enough text has been provided, the Playfair Cipher can be solved. When plain text and ciphertext are known, finding the key is straightforward. If only the ciphertext is known, cryptanalysts can make a search for equalities between the frequency of digrams and the known frequency of presence of digrams in the assumed language of the plain text through the key space.

Cryptanalysis of four-square and two-square ciphers can be used in Playfair also.

- A Playfair digraph and its reverse will decrypt to the same letter pattern in the plain text. There are many words including reversed digraphs, such as REceivER, REadER and DEpartED, in English. Determining these reversed digraphs in the ciphertext and finding the pattern in the plain text will generate possible plain text strings.

ADFGVX Cipher

ADFGVX Cipher was used and limited to German High Command communications between and among the headquarters of divisions and army corps during World War I (WWI) for encrypting and decrypting. The weakness of not hiding the frequency of the letters in Caesar Cipher is overcome by ADFGVX Cipher. In this method, a single letter is replaced by a pair of letters. Then these are scrambled as in the Spartan Scytale [16].

Step 1 of Encoding

Two steps should be followed to encrypt a message in ADFGVX Cipher. First, ADFGVX grid in replacing letters of plain text by using corresponding row and column of the letter in a grid is used. Spaces are taken away because of the grid does not containing them.

Examples:

- A=>“DV”
- L=>“DA”
- Alper Umut Ucar => “DVDAADXDVVGDAGGDDDGDFGDVVV”

To prevent incorrect transmission ADFGVX letters were chosen for their distinctive Morse encoding.

	A	D	F	G	V	X
A	8	P	3	D	1	N
D	L	T	4	O	A	H
F	7	K	B	C	5	Z
G	J	U	6	W	G	M
V	X	S	V	I	R	2
X	9	E	Y	0	F	Q

Step 2 of Encoding

Second, a keyword is used further scrambling the order. Support the keyword is “GRAPE”. The encoded word is placed in a table in row-major ordering. Columns are arranged by alphabetical order of the keyword’s letter. Final encoding read from the table in column-major order.

```
G R A P E
3 5 1 4 2
D V D A A
D X D V V
G D A G G
D D D G D
F G D V V
V
```

Final Encoding of “Alper Umut Ucar”: “DDADDAVGDVDDGDFVAVGGVVXDDG”

Vigenère Square

Using different shifts at each position in the text is called Vigenère Cipher and a repeating keyword is used to define the value of the shift. A key is only known by encoder and decoder and shifts are based on this. If keyword is randomly chosen and the length of the keyword is

as long as the message size, Vigenère Cipher cannot be solved if the users keep the secrecy of the keyword. If length of the keywords shorter than the message, this introduces a cyclic pattern and by using frequency analysis message might be detected [16].

	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
		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

Suppose the keyword is SHOT and we wish to encode HOWAREYOU

To encode:

1. Replace “H” with “H-S” entry “Z”.
2. Replace “O” with “O-H” entry “V”.
3. Replace “W” with “W-O” entry “J”.
4. Replace “A” with “A-T” entry “T”.
5. Replace “R” with “R-S” entry “I” and so on.

PT	H	O	W	A	R	E	Y	O	U
Key	S	H	O	T	S	H	O	T	S
CT	Z	V	J	T	I	.	.	.	.

Nihilist Cipher

Nihilist Cipher was used by Russian Nihilists in 1880s against czarist regime to perform terrorist attacks. Two digit numbers have been used for plain text and a keyword. Then, these numbers are added in arithmetically to obtain ciphertext. Key numbers are repeated as needed [16].

Example

Polybius square that has been created using the keyword ZEBRAS

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

with a plain text of "BOMB AMMUNITION DEPOT" by using PEOPLE as a key. This expands to:

PT	13	42	35	13	15	35	35	51	41	32	45	32	42	41	23	12	43	42	45
Key	43	12	42	43	34	12	43	12	42	43	34	12	43	12	42	43	34	12	43
CT	56	54	77	56	49	47	78	63	83	75	79	44	85	53	54	55	77	54	88

Transposition Cipher

The method of encryption by shifting the positions of plain texts according to a regular system is called as a transposition cipher. In this method, the ciphertext constitutes a permutation of the plain text. Bijective function is used for encrypting and an inverse function is used for decrypting characters' positions. Some implementations are as follows [16]:

Rail Fence Cipher

The Rail Fence Cipher gets its name from the way in which it is encoded. The plain text is written downwards in an imaginary fence, then moving up when bottom is reached. Then, the message is read off in rows. Using four "rails" and a message "I AM IN TROUBLE. I SHOULD FIND SOLUTION", the encoder writes out:

Size of Shift : 4

```
I N U . O F S T
 A T B I U I O  I
  M R L S L N L O
    I O E H D D U N
```

Reads off: INUOF STATB IUIOI MRLSL NLOIO EHDDU N

Route Cipher

The clear text is written out in a grid of given dimension and depending on the pattern of the key it is read off. The same example used above.

```
I N U . O F S T
A T B I U I O I
M R L S L N L O
I O E H D D U N
```

Key: "spiral inwards, anticlockwise, beginning from the bottom left". That results with a cipher text of: “IOEOFSTXNOIOIUIUNIAMRLHDDULNLSBT”

Route ciphers have many keys. Depending on the length of the messages, the number of possible keys is too great to be enumerated. Since, not all keys are equally good, routes should not be chosen badly. Otherwise, cryptanalysts would get a clue about the roots.

Columnar Transposition

The plain text is written out in rows of a fixed length and then read out columnwise and they are chosen in some scrambled order in columnar transposition. A keyword defines width of the rows and permutations of the columns. For instance, the keyword ZEBRAS has size 6, and this means that length of the rows would be 6. Since the alphabetical order of keyword’s letter defines permutation, the order would be "632415".

Spaces are filled with nulls in regular columnar transposition, left blank in irregular columnar transposition cipher. In the end, the message is read off in columns in the specified order.

Suppose keyword is ZEBRAS and the plain text “I AM IN TROUBLE. I SHOULD FIND SOLUTION”. In a regular columnar transposition,

```
6 3 2 4 1 5
I A M I N T
R O U B L E
I S H O U L
D F I N D S
O L U T I O
N Q K J E U
```

using (QKJEU) as five nulls; the ciphertext is read off as:

NLUDIE MUHIUK ADSFLQ IBONTJ IELSOU IRIDON

In the irregular case, spaces are left blank:

```
6 3 2 4 1 5
I A M I N T
R O U B L E
I S H O U L
D F I N D S
O L U T I O
N
```

The ciphertext would be: NLUDIM UHIUAO SFLIBO NTTELS OIRIDO N

To break the cipher, the message length should be divided by key length to obtain the column length. Then the recipient can write the message in columns and reorder them by using the keyword.

Double Transposition

By guessing column lengths and writing message out in columns and looking at possible anagrams, a single columnar transposition could be detected. A double transposition was used in order to make a single columnar transposition stronger. For this purpose, columnar transposition is applied twice. Same key or two different keys can be used for transpositions [16].

In the previous example, taking the result of irregular columnar transposition, and performing a second encryption by using different keyword, CIPHER, gives the permutation "145326".

1	4	5	3	2	6
N	L	U	D	I	M
U	H	U	I	A	O
S	F	L	I	B	O
N	T	T	E	L	S
O	I	R	I	D	O
N					

When this is read off columnwise, the ciphertext is:
"NUSNON IABLDD IIEILH FTIUUL TRMOOS O"

German military used double columnar transposition cipher during WWI but the system was regularly solved by the French. When Germans recognized this, they changed to a new system on 18 November 1914.

This cipher was also used by Dutch Resistance groups, the French Maquis and the British Special Operations Executive, the agents of the American Office of Strategic Services and German Army and Navy during WWII.

Myszkowski Transposition

Using a keyword with recurrent letters in columnar transposition has been proposed by Émile Victor Théodore Myszkowski. Usually, subsequent occurrences of a keyword letter are

treated in alphabetical order. For instance, the keyword TOMATO gives a numeric string of "532164" [16].

Recurrent letters in the keyword are numbered identically in Myszkowski transposition. E.g. TOMATO yields a keystring of "432143."

```
4 3 2 1 4 3
I A M I N T
R O U B L E
I S H O U L
D F I N D S
O L U T I O
N
```

Columns with unique numbers read off downward, but these with recurring numbers are read off left to right: “IBONTM UHIUAT OESLFS LOINRL IUDDOI N”.

Bifid Cipher

The Bifid Cipher is a kind of matrix cipher [16]. Let’s create a 5 by 5 matrix of letters, by labeling the rows and columns 1 to 5.

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

The value of each letter has been found by using row and column values and these are written out vertically below the corresponding letter. Then the numbers are written next to one another.

By reading the row and the column values, the value of each letter could be found. Then these two numbers are written vertically below the original message. All the plain letters are written next to one another and these letters are contained in the secret message.

PT	S	E	N	D	T	H	E	L	E	T	T	E	R
Row Value	4	1	3	1	4	2	1	3	1	4	4	1	4
Column Value	4	5	4	4	5	3	5	2	5	5	5	5	3

When the message is rewritten from left to right, grouping numbers into 2

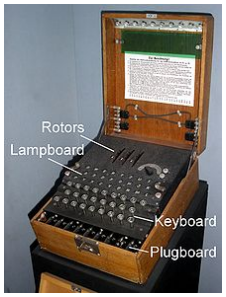
41 31 42 13 14 41 44 54 45 35 25 55 53

The final step is taking each group of numbers and finding the values in the same matrix above. E.g., 41 is row 4, column 1, and the corresponding letter is P.

41	31	42	13	14	41	44	54	45	35	25	55	53
P	K	Q	C	D	P	S	X	T	O	J	Y	W

Enigma Machine

An Enigma machine was a cipher machine used for enciphering and deciphering secret messages. Invention of this machine had been done by German engineer Arthur Scherbius at the end of WWI. Early models of this machine were used commercially but they were not profitable. Adoption by military and government services has been done before and after WWII mostly by Nazi Germany. Although several models were produced, the German military models are the commonly discussed ones [16].



The Enigma machine generated polyalphabetic substitution cipher with a period repetition of the substitution alphabet. This provided potentially an excellent system. In this system, no letter could be enciphered to itself and this is the major weaknesses of it. Since, same letter appearance in ciphertext and plain text leads to a result of elimination of some possible solutions quickly. Comparing the possible plain text "Keine Besonderen Ereignisse", with a section of ciphertext, might produce the following:

Exclusion of some positions for the possible plaintext *Keine besonderen Ereignisse*

Ciphertext	O	H	J	Y	P	D	O	M	Q	N	J	C	O	S	G	A	W	H	L	E	I	H	Y	S	O	P	J	S	M	N	U
Position 1			K	E	I	N	E	B	E	S	O	N	D	E	R	E	N	E	R	E	I	G	N	I	S	S	E				
Position 2				K	E	I	N	E	B	E	S	O	N	D	E	R	E	N	E	R	E	I	G	N	I	S	S	E			
Position 3					K	E	I	N	E	B	E	S	O	N	D	E	R	E	N	E	R	E	I	G	N	I	S	S	E			
	Positions 1 and 3 for the possible plaintext are impossible because of matching letters. The red cells represent these *crashes*. Position 2 is a possibility.																														

Asymmetric Cryptography

Nowadays, this type of cryptography is commonly used in digital signatures and this encryption method is best used for key exchange and user authentication. Public and private key have been used in this method and these keys are created with the one-way function by

using multiplication and exponentiation. Public key is published in a public directory but the private key is only known the receiver of the message [4].

Elliptic Curve Cryptography

Government and financial institutions use this method which is a standard and based on public key encryption. It is mostly used in mobile and wireless environments [4]. The equation – $\mathbf{y^2=x^3 + 3 + Ax + B}$ is used to create public keys where x and y points on a curve and private key is a random number.

This method offers security with smaller key sizes, which result in faster calculation, less power consumption, lower memory and bandwidth use.

Quantum Cryptography

Photons are used to produce encrypted keys that can be transmitted over fiber networks by using beams of light in quantum cryptography methods. A procedure has been used to create keys. In this method, with the use of a laser source, photons are transmitted horizontally and vertically [4].

This method has ability to detect the presence of anyone who tries to get the quantum key. A high increase in the transmission error rate will notify the sender and receiver about the attack. Keys are virtually unbreakable because of not being able to copying and dividing photons.

Japan has been working on new quantum cryptography methods to provide secure video conferencing for government communications since 2010.

BIBLIOGRAPHY

1. http://ab.org.tr/ab06/bildiri/132.pdf
2. http://acikders.ankara.edu.tr/mod/resource/view.php?id=219
3. http://securityintelligence.com/reasons-encryption-cryptography-for-business/#
4. http://www.brighthub.com/computing/smb-security/articles/80137.aspx
5. https://www.cryptochallenge.com/home/history
6. http://www.giac.org/paper/gsec/4170/cryptography-work-business/106707
7. http://www.studentpulse.com/articles/41/a-brief-history-of-cryptography
8. An Introduction to Cryptography. USA. Network Associates, Inc. (408) 988-3832 main 3965 Freedom Circle, Santa Clara, CA 95054, http://www.nai.com
9. Cohen, F (1990). A short history of cryptography. Retrieved May 4, 2009, from http://www.all.net/books/ip/Chap2-1.html New World Encyclopedia (2007).
10. Cryptography. Retrieved May 4, 2009, from http://www.newworldencyclopedia.org/entry/Cryptography
11. Paul E. Gunnels. (2004, April 2007). The Mathematics of Cryptology: Department of Mathematics and Statistics. University of Massachusetts, Amherst, MA 01003 www.math.umass.edu/~gunnells
12. Pawlan, M. (1998, February). Cryptography: the ancient art of secret messages. Retrieved May 4, 2009, from http://www.pawlan.com/Monica/crypto/
13. Rubin, J. (2008). Vigenere Cipher. Retrieved May 4, 2009, from http://www.juliantrubin.com/encyclopedia/mathematics/vigenere_cipher.html
14. Taylor, K. (2002, July 31). Number theory 1. Retrieved May 4, 2009, from http://math.usask.ca/encryption/lessons/lesson00/page1.html
15. Whitman, M. & Mattord, H. (2005). Principles of information security. [University of Phoenix Custom Edition e-text]. Canada, Thomson Learning, Inc. Retrieved May 4, 2009, from University of Phoenix, resource, CMGT/432
16. Mammadov, Fahrettin Sadikoglu. Cryptography and Coding Theory http://staff.neu.edu.tr/~fahri/cryptography_Chapter_2.pdf
17. TUBITAK, Bilim ve Teknik. Ankara. Temmuz 2009, Yil 42, Sayi 500.
18. 2013- IV Matematik Dunyasi. Istanbul. Yil 22, Sayi 97.
19. http://en.wikipedia.org/wiki/Enigma_machine

20. Schneider B., ‘Applied Cryptography, Second Edition’, John Wiley & Sons, Inc. 1996 New York, Ny
21. Salomaa A., ‘Public-Key Cryptography’, Springer-Verlag, 1990 New York
22. ‘Current Public-Key Cryptographic Systems’, Paper of Certicom, dd. April 1997 Updated July 2000.
23. Koblitz N., ‘A Course in Number Theory and Cryptography’, 1994 Springer-Verlag, New York
24. Trappe W., Washington L., ‘Introduction to Cryptography with Coding Theory’, 2002 0-13-061814-4 (Hardback)