Ministry of Higher Education
Salahaddin University
College of Science

Introduction to Cryptography

Prepared by: - Zahraa Amer AL-Khafaje.

Supervisors: -

Mr.Ako Najat.

Mrs.Muzhda.

Department of Mathematics

Abstract

In this report, we will discuss the cryptograph, and we will discuss many types of cryptograph like Polybius cipher, message reversal, rail-fence transposition, pigpen cipher and francis bacon's cipher. You will learn how can you unlock any code that message has it and read any message easily and clearly.

Introduction: -

Cryptography is the study and practice of techniques for secure communication in the presence adversaries. And it is science the beginning of written language, people have wanted to share information secretly. The information could be orders from a general in times of war, a secret message between admirers or between any two people, or information regarding some of the world's most villainous crimes.

For example, someone wants to send a message to another person and he wants to be sure that no-one car read this message accept that person he sends it to him. However, there is the possibility that someone els opens that letter or hears the electronic communication.

Definitions and Illustrations: -

First we will settle upon the meaning of ***cryptography,***

Cryptography is the science of information security or it is the art and science of secret writing.

Cryptography has, as its etymology, ***crypto*** from the Greek, meaning **hidden,** and **graph,** meaning **to wr**

In the basic communication scenario, we assume that it as a game between three parties:

a sender (e.g., an embassy); we denote her by **Alice,**

a receiver (e.g., the government office) we denote him by **Bob,** and

an opponent (or hacker e.g., a spy) we denote him by **Charlie.**

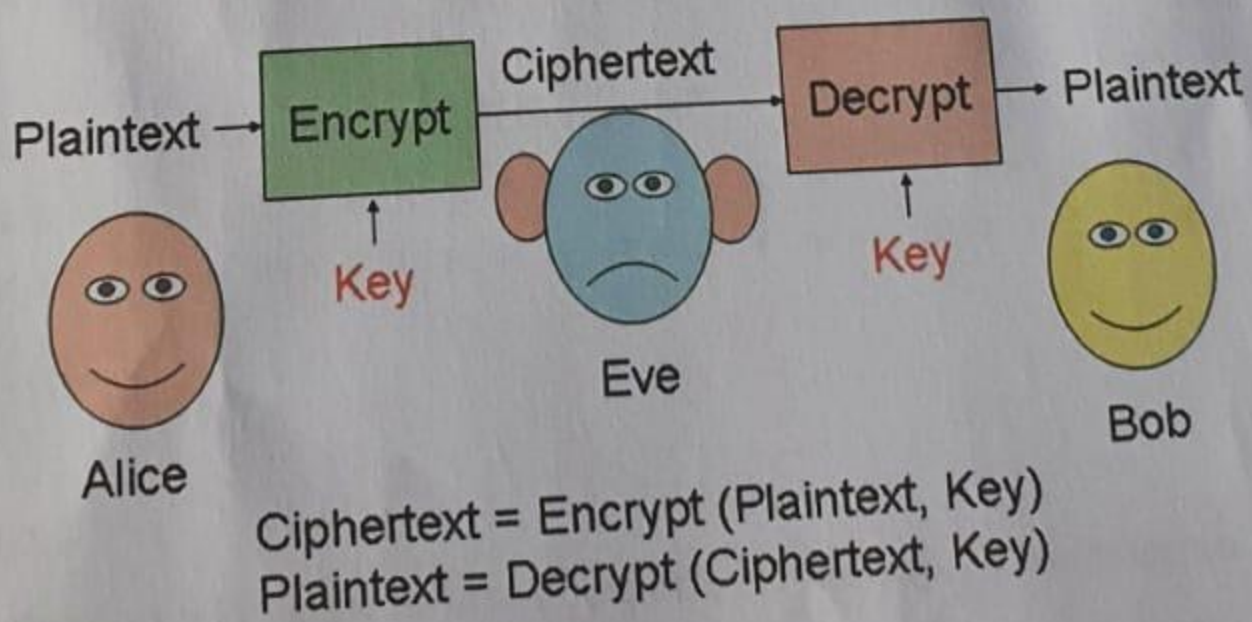
The original message is called the ***plaintext*** or ***clear text*** (always we use small letters). The dis message is called the ***cipher text*** (always we use capital letters). The final message, encapsulated and called ***cryptogram***. The process of transforming ***plaintext*** into ***cipher text*** is called ***encryp enciphering***.

The revers process of turning cipher text into plaintext is called ***decryption*** or ***deciphering***.

The person who enciphers the message is known as the ***encipherer***.

The study of mathematical techniques for attempting to defeat cryptographic methods ***cryptanalysis***.

The term ***cipher*** is method for enciphering and deciphering.



1. Polybius Cipher: -

This cipher has the disadvantage of doubling the length of the message.

	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	Q	R	S	T	U
5	V	W	X	Y	Z

Polybius Square

In the Polybius cipher, each letter is replaced by the position in which it appears in the Polybius square

You can use it like that: first the row number then the column number. For example, **H** would be repla with **23.** To decipher a message, you find the letter that intersect the specified row and column.

Example: - Encipher the message **defend the east wall of the castle**

D	E	F	E	N	D		T	H	E		E	A	S	T		W	A	L	L		O	F		T	H	E		C	A	S	T	L	E
14	15	21	15	33	14		44	23	15		15	11	43	44		62	11	31	31		34	21		44	23	15		13	11	43	44	31	15

It's a special case of a general class of ciphers known as substitution ciphers, where a given letter is substituted for with the same symbol wherever it appears.

We can also use six-by-six square but it would be used for languages written in the Cyrillic alphabe

The Polybius square is sometimes called a Polybius checkboard. The letters may be placed in the s any order, for example, the keyword **DERANGENEMT** could be used to rearrange letters like: -

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

Example: - Encipher "**defend the east wall of the castle**"

D	E	F	E	N	D		T	H	E		E	A	S	T		W	A	L	L		O	F		T	H	E		C	A	S	T	L	E
11	12	31	12	15	11		23	32	12		12	14	44	23		52	14	35	35		41	31		23	32	12		25	14	44	23	35	12

. Message Reversal: -

n this cipher the cipher text will be the reverse of the original message. It is a transposition ci

or example, to encrypt the message **"computer"**

he plaintext **computer.**

The cipher text will be **RETUPMOC.**

Example: - Encrypt the message **"agent one meet me in the zoo"**

The cipher text will be: **TNEGA ENOTE EMEM NIEHTO OZ.**

3. Rail-Fence Transposition: -

Example: To encrypt the following message

Anyone who looks at us the wrong way twice will surely die.

We simply write the text moving back and forth in a zigzag fashion from the top line:

A Y N W O O K A U T E R N W Y W C W L S R L D E

N O E H L O S T S H W O G A T I E I L U E Y I

And then read across the top line first to get the cipher text:

AYNWO OKAUT ERNWY WCWLS RLDEN OEHLO STSHW OGATI EILUE YI

The" fence" needn't be limited to two tiers. We could encipher the same message as follo

A						w					K						T						N						
	N				E		H					O		S					S		H					O			
		Y		N					O		O					A		U					E		R				
			O							L							T						W						

					L						L					
I				I		L				R		Y				
	C		W				S		E				D		E	
		E						U						I		

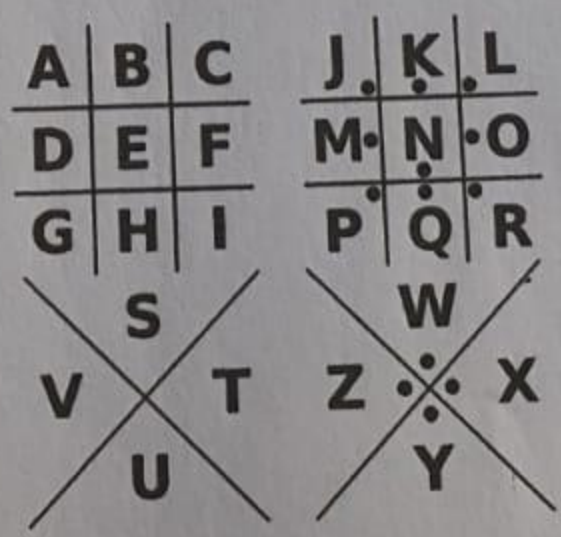
To get the cipher text:

AWKTN WLLNE HOSSH OGTII LRYYN OOAUE RWYCW SEDEO LTWAE

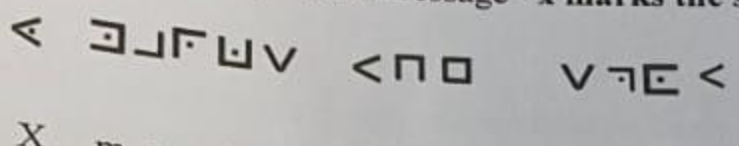
4. pigpen cipher:

This system is known as the pigpen (or freemason's cipher), because the letters are se
en. It is also called the Masonic cipher, as the Society of Freemasons has made use
ivil wars in England in the 17th century and even as recently as the U.S. Civil war b
nessages to friends.

he pigpen cipher uses graphical symbols assigned according to a key similar to the
substitution cipher.



Example: - Using the pigpen cipher the message **"x marks the spot"** is encrypted as follows



X m a r k s t h e s p o t

5. Francis Bacon's cipher: -

To encode a message, each letter of the plaintext is replaced by a group of five of the letters '**A**' or '**B**'. This replacement is done according to the alphabet of the Baconian cipher, shown below:

a AAAAA	g AABBA	n ABBAA	t BAABA
b AAAAB	h AABBB	o ABBAB	u-v BAABB
c AAABA	i-j ABAAA	p ABBBA	w BABAA
d AAABB	k ABAAB	q ABBBB	x BABAB
e AABAA	l ABABA	r BAAAA	y BABBA
f AABAB	m ABABB	s BAAAB	z BABBB

Example: - Encrypt the message "**math**"

Plaintext: **math**

Cipher text: **ABABBAAAAABAABAABAAABBB**

Conclusion: -

In this report we wrote about cryptograph and we discuss many ciphers that helps you to unlock
you want it in encrypted message. And in the end cryptography is a powerful tool for secure com
but it is not perfect. There are a number of ways to attack a cryptographic system, and new attac
constantly being discovered. Cryptography is an important part of security, but it is not the only
consider.

References: -

- https://www.alibabacloud.com/topic-center/tech/19tggrvkimkq-conclusion-of-cryptography-alibab
- Pigpen Cipher (online tool) | Boxentriq
- Cryptology: Reference and Book List (uni-mainz.de)