Introduction to Cipher Systems

Saad Al-Momen

1

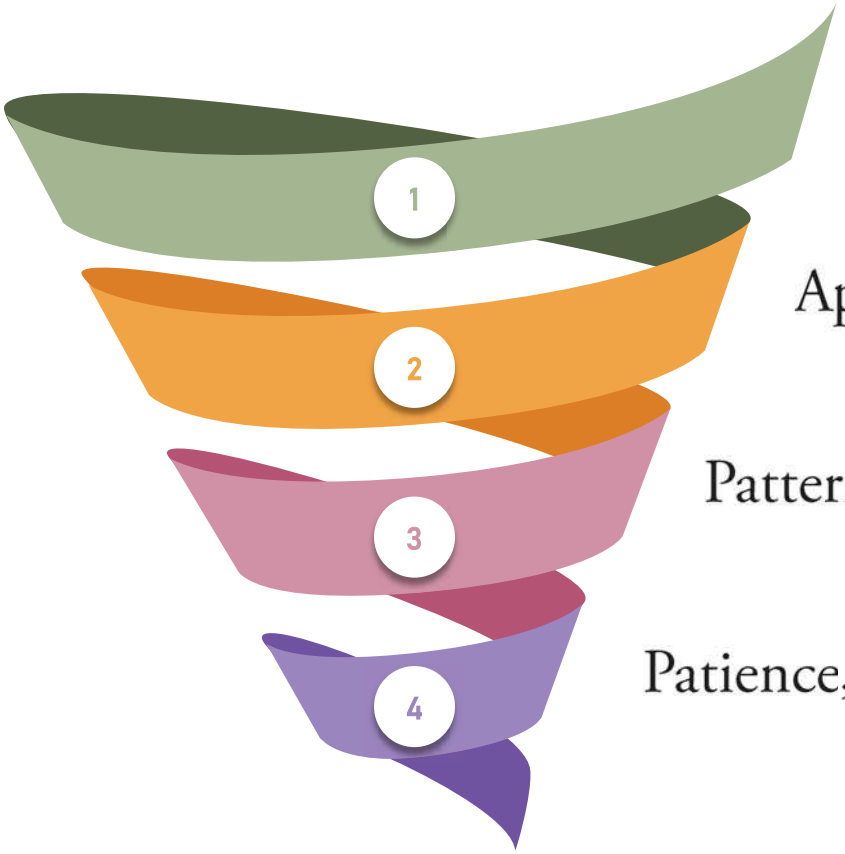
CIPHER SYSTEMS

Fourth Class
Department of Mathematics
College of Science - University of Baghdad

What is Cryptography?

- Cryptography is the science of using mathematics to encrypt and decrypt data.
- Cryptography is the study of secret (crypto-) writing (-graphy).
- Cryptography enables you to store sensitive information or transmit it across insecure channels or networks (like the Internet) so that it cannot be read by anyone except the intended recipient.
- Cryptography is the science of securing data.
- Cryptanalysis is the science of analyzing and breaking secure communication.

Classical Cryptanalysis Involves



An interesting combination of analytical reasoning

Application of mathematical tools

Pattern finding

Patience, determination, and luck

Introduction to Cipher Systems

2

CIPHER SYSTEMS

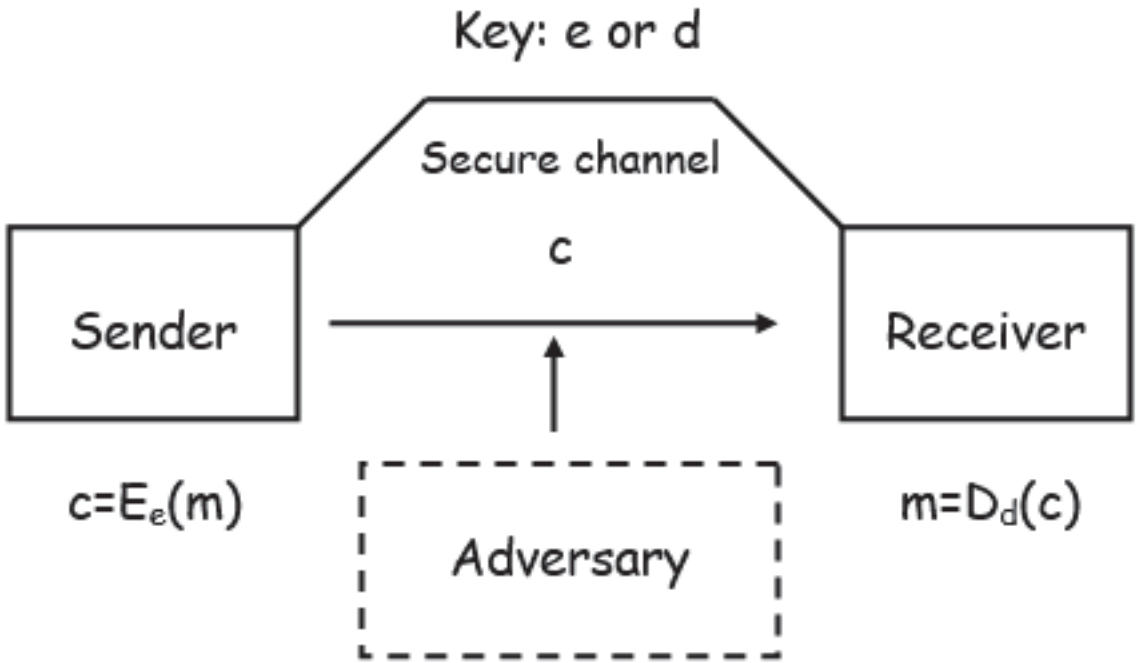
Saad Al-Momen

Fourth Class
Department of Mathematics
College of Science - University of Baghdad

Secret Key Systems

Secret Key Systems

In such type of systems the encipher key and the decipher key must be known **only** by the sender and the receiver, so **they must exchange the key over a secure channel**.



Introduction to Cipher Systems

3

CIPHER SYSTEMS
Fourth Class
Department of Mathematics
College of Science - University of Baghdad

Saad Al-Momen

Substitution Cipher

Substitution Cipher

A system of encryption in which each letter of a message is replaced with another character, but retains its position within the message.

1 Monoalphabetic

A substitution cipher system is the system that uses one alphabet throughout encryption.

A. Simple substitution cipher

Simple substitution ciphers replaced each character of plaintext with the corresponding character of the ciphertext.

Introduction to Cipher Systems

4

CIPHER SYSTEMS

Saad Al-Momen

Fourth Class
Department of Mathematics
College of Science - University of Baghdad

Substitution Cipher

Substitution Cipher

1 Monoalphabetic

A. Simple substitution cipher

1. Direct Standard
2. Standard Reverse
3. Multiplicative Cipher
4. Affine Cipher

5. Mixed Alphabet

If we permit the cipher alphabet to be any rearrangement of the plain alphabet, then we can generate an enormous number of distinct modes of encryption.

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

Introduction to Cipher Systems

5

CIPHER SYSTEMS

Saad Al-Momen

Fourth Class
Department of Mathematics
College of Science - University of Baghdad

Substitution Cipher

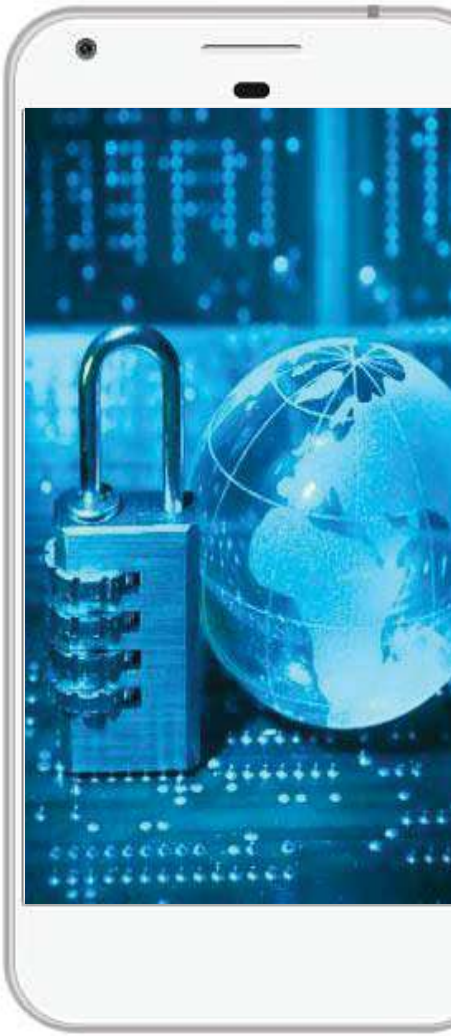
Substitution Cipher

A system of encryption in which each letter of a message is replaced with another character, but retains its position within the message.

2 Polyalphabetic

Polyalphabetic substitution cipher is a substitution cipher in which the cipher alphabet changes during the encryption. The change is defined by a key

1. Vigenere Cipher
2. Beaufort Cipher



1. Vigenere Cipher

The Vigenere Cipher, proposed by Blaise de Vigenere from the court of Henry III of France in the sixteenth century, is a polyalphabetic substitution based on the following tableau:

	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

1. Vigenere Cipher

The first row is a shift of 0

The second is a shift of 1

.

.

.

The last is a shift of 25.

Mathematically,

$$E_{ki}(m) = (m + k_i) \bmod 26$$

	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

Introduction to Cipher Systems

6

CIPHER SYSTEMS

Saad Al-Momen

Fourth Class
Department of Mathematics
College of Science - University of Baghdad

One-Time Pads

One-Time Pads

During the war, an AT&T engineer Gilbert Vernam proposed a system called the One-Time Pad that has perfect security.

In this system additive ciphers are used to encipher each letter of the plaintext; however, the shift is different for each letter!

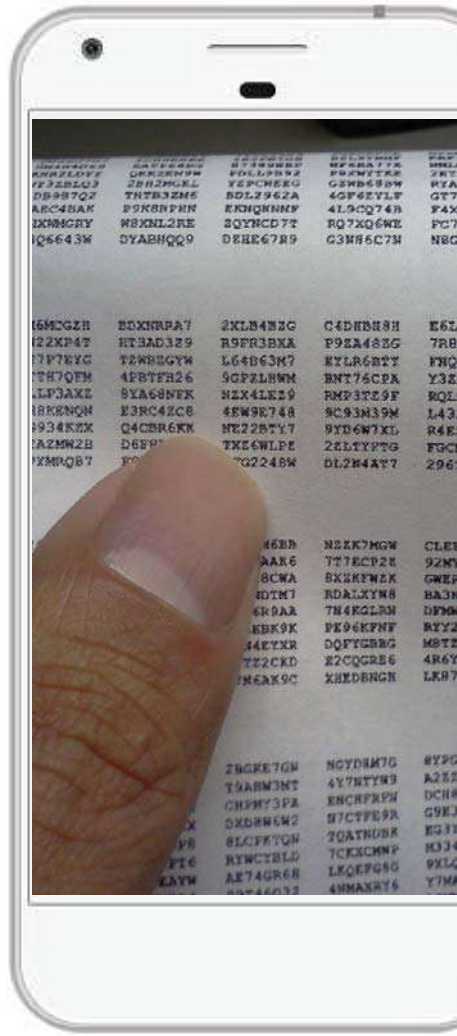
Plaintext: THE BRITISH HAVE FIFTY TANKS

Key: SHE LOVES HIM SO VERY MUCH NOW

One-Time Pads

Plaintext: THE BRITISH HAVE FIFTY TANKS
Key: SHE LOVES HIM SO VERY MUCH NOW

m:	T	H	E	B	R	I	T	I	S	H	H	A	V	E
	19	7	4	1	17	8	19	8	18	7	7	0	21	4
k:	S	H	E	L	O	V	E	S	H	I	M	S	O	V
	18	7	4	11	14	21	4	18	7	8	12	18	14	21
Add :	37	14	8	12	31	29	23	26	25	15	19	18	35	25
Mod :	11	14	8	12	5	3	23	0	25	15	19	18	9	25
	L	O	I	M	F	D	X	A	Z	P	T	S	J	Z

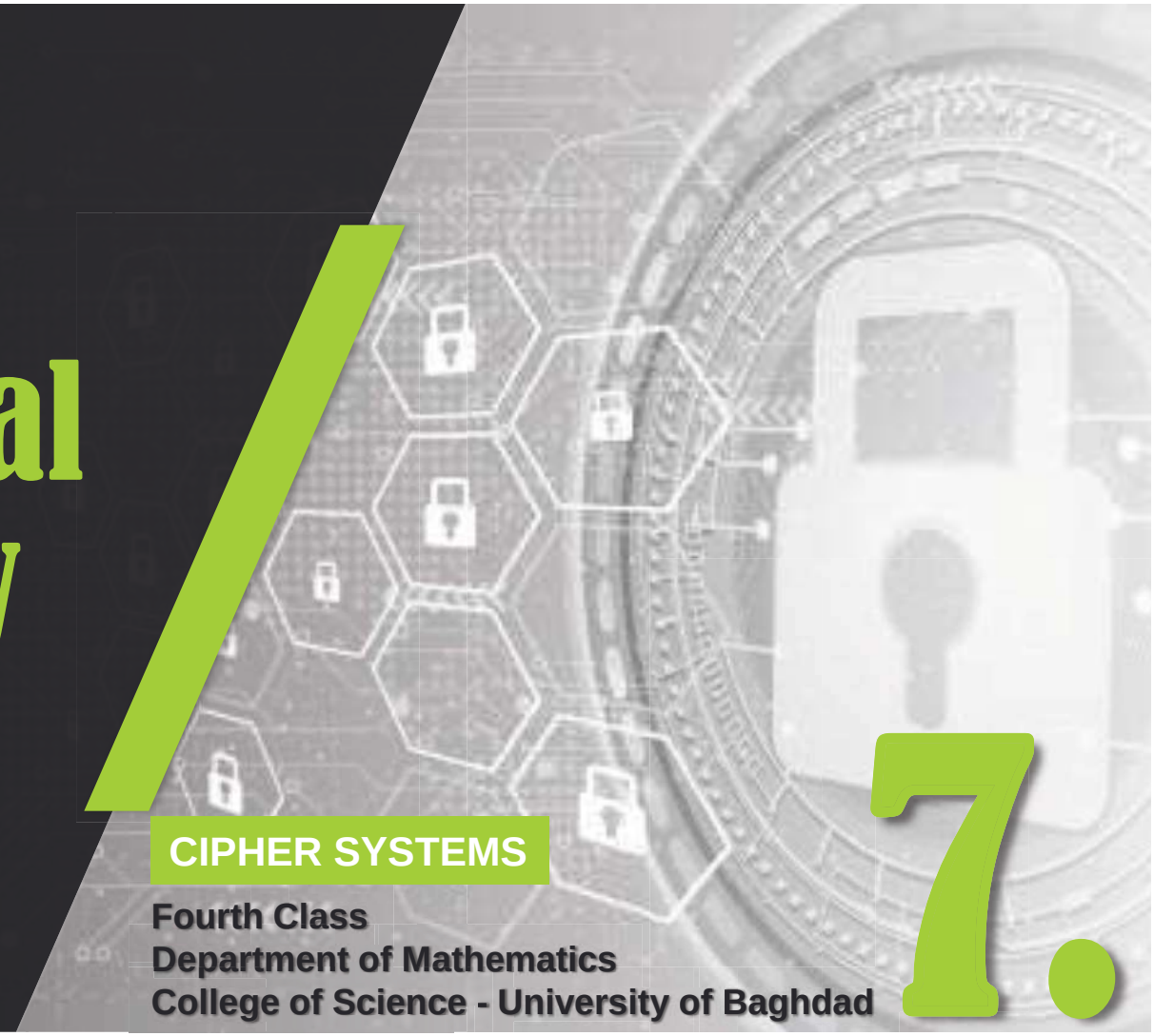


One-Time Pads

- Different letters of ciphertext could correspond to the same plaintext letter, and vice versa.
- This cryptosystem is virtually unbreakable.
- The weakness is the key which must be immense. This must be shared by all communicants.
- Also, statistical analysis may be possible if the key is a regular text; for this reason some effort is usually made to choose keys which are truly random sequences of characters.

Saad Al-Momen

Practical Security



CIPHER SYSTEMS

7.

Fourth Class
Department of Mathematics
College of Science - University of Baghdad


Introduction

The discussion of chapter one arise a certain **weakness of Monoalphabetic** cipher, the encipherment of a letter only involves using a small portion of the letters of key, exactly the one letter which is substituted for it. Then we can break this cipher system by **finding small portion of the message** and try to decipher them and by using these small portions we can find the way to decipher the overall message.

To make the system more secure, it seems desirable to use a considerable amount of keys to encipher each character of the message. And also it is probably helpful to **'spread' the statistical structure** of the ciphertext by enciphering a number of message characters simultaneously.


Diffusion &
Confusion

Diffusion & Confusion.

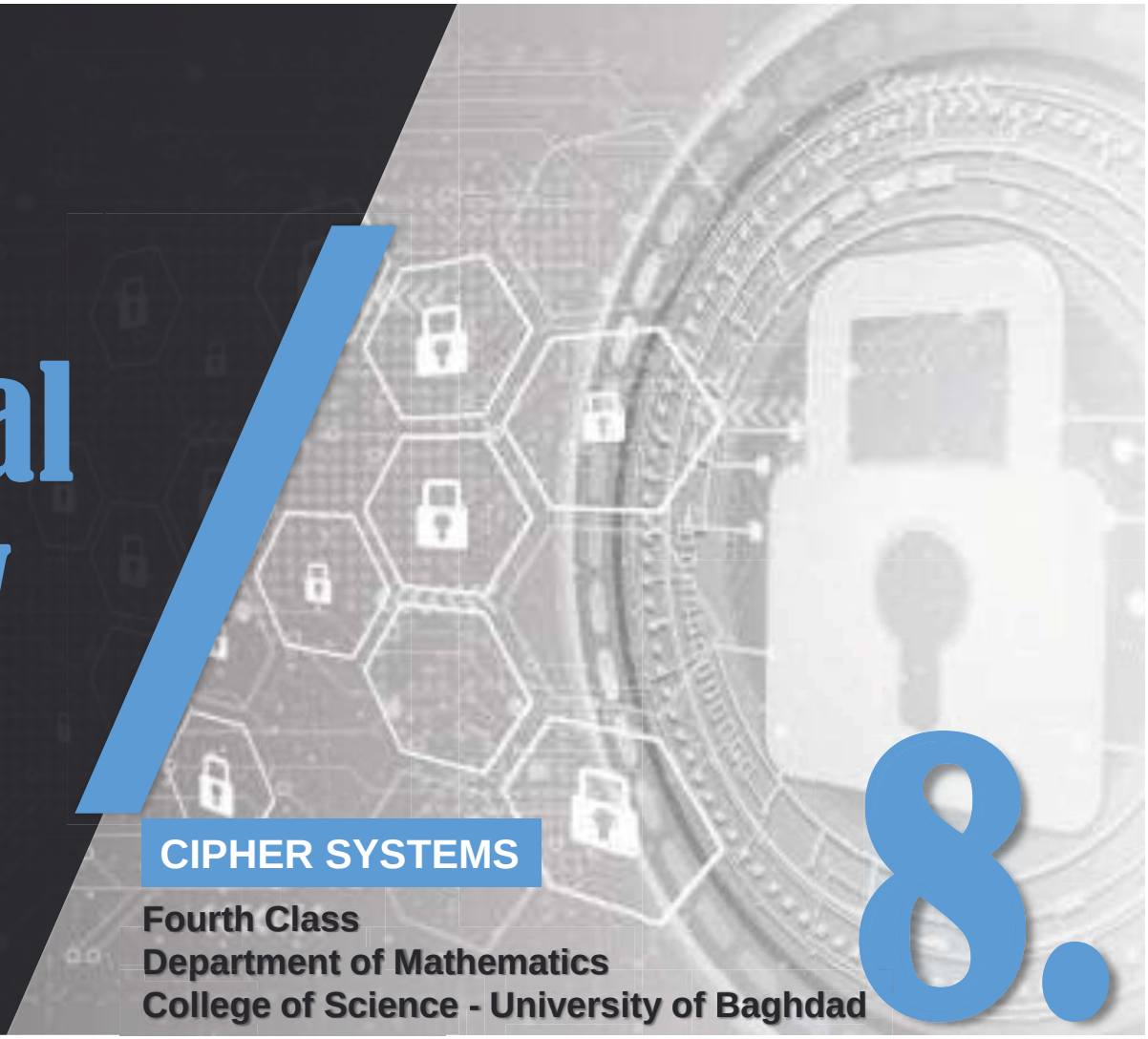
In order to

- accommodate the points of using a considerable amount of key
- spread the statistical structure of ciphertext, and reduce the effectiveness of statistical attacks on ciphertext

Shannon suggests that the cryptographer uses two techniques which he calls **Diffusion** and **Confusion**.

Saad Al-Momen

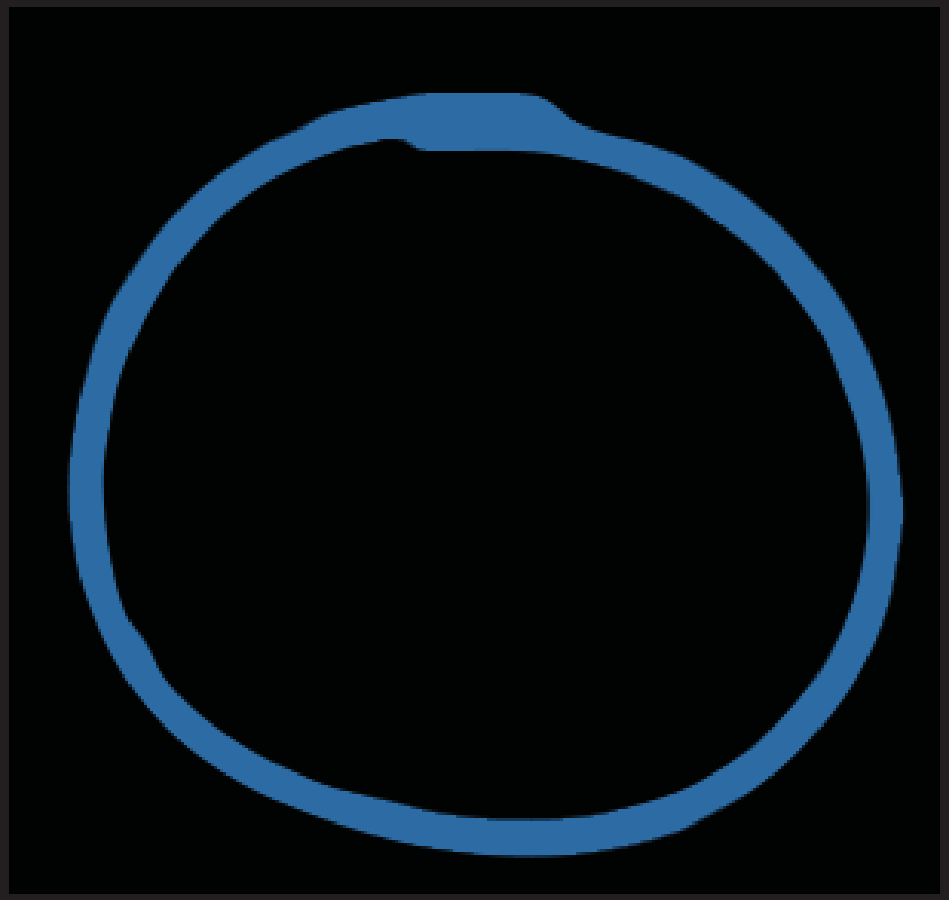
Practical Security



8. CIPHER SYSTEMS

Fourth Class
Department of Mathematics
College of Science - University of Baghdad


Statistical Test
for Randomness



Example 1

1110001100010001010011101111001001001001
1110001100010001010011101111001001001001
1110001100010001010011101111001001001001
1110001100010001010011101111001001001001

n=160

Example 1

Saad Al-Momen

Stream Ciphers

CIPHER SYSTEMS

Fourth Class
Department of Mathematics
College of Science - University of Baghdad

9.

Introduction

Introduction

- Encrypt individual characters (usually binary digits) of a plaintext message one at a time.
- Faster than block ciphers in hardware.
- Less complex hardware circuitry.
- More appropriate, and in some cases mandatory when buffering is limited.
- Have limited or no error propagation.

One Time Pad

One Time Pad

Saad Al-Momen

Stream Ciphers

10.

CIPHER SYSTEMS

Fourth Class
Department of Mathematics
College of Science - University of Baghdad

Linear Feedback Shift Register (LFSR)

Linear Feedback Shift Register

LFSR of length **L** consists of **L** *stages* (or *delay elements*) numbered **0, 1, ..., L-1**, each capable of storing **one bit** and having **one input** and **one output**; and a clock which controls the movement of data.

Saad Al-Momen

Stream Ciphers

11.

CIPHER SYSTEMS

Fourth Class
Department of Mathematics
College of Science - University of Baghdad

Stream Cipher Algorithms

Stream Cipher Algorithms

In this part, we'll discuss some of stream cipher algorithms. We'll explain those algorithms in details so that we can recognize their registers and also the type of connections or functions of connections.

Saad Al-Momen

Stream Ciphers

12.

CIPHER SYSTEMS

Fourth Class
Department of Mathematics
College of Science - University of Baghdad

Stream Cipher Algorithms

4. Geffe's Algorithm