Introduction to Cipher Systems

1

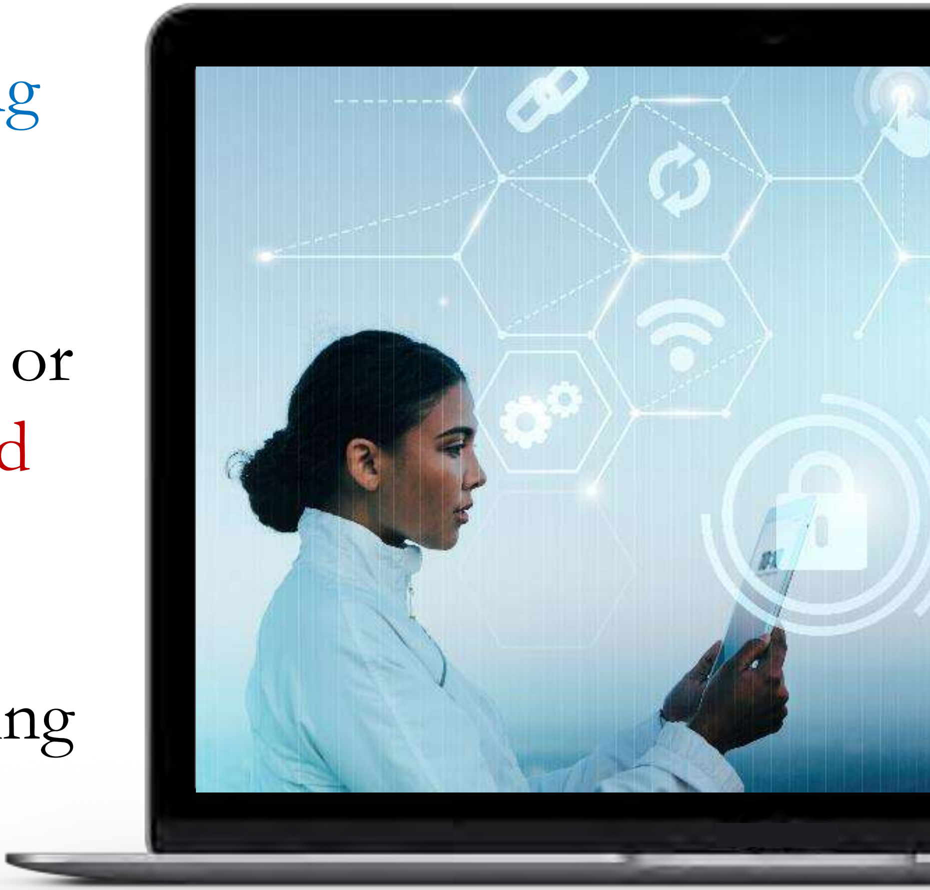
Saad Al-Momen

CIPHER SYSTEMS

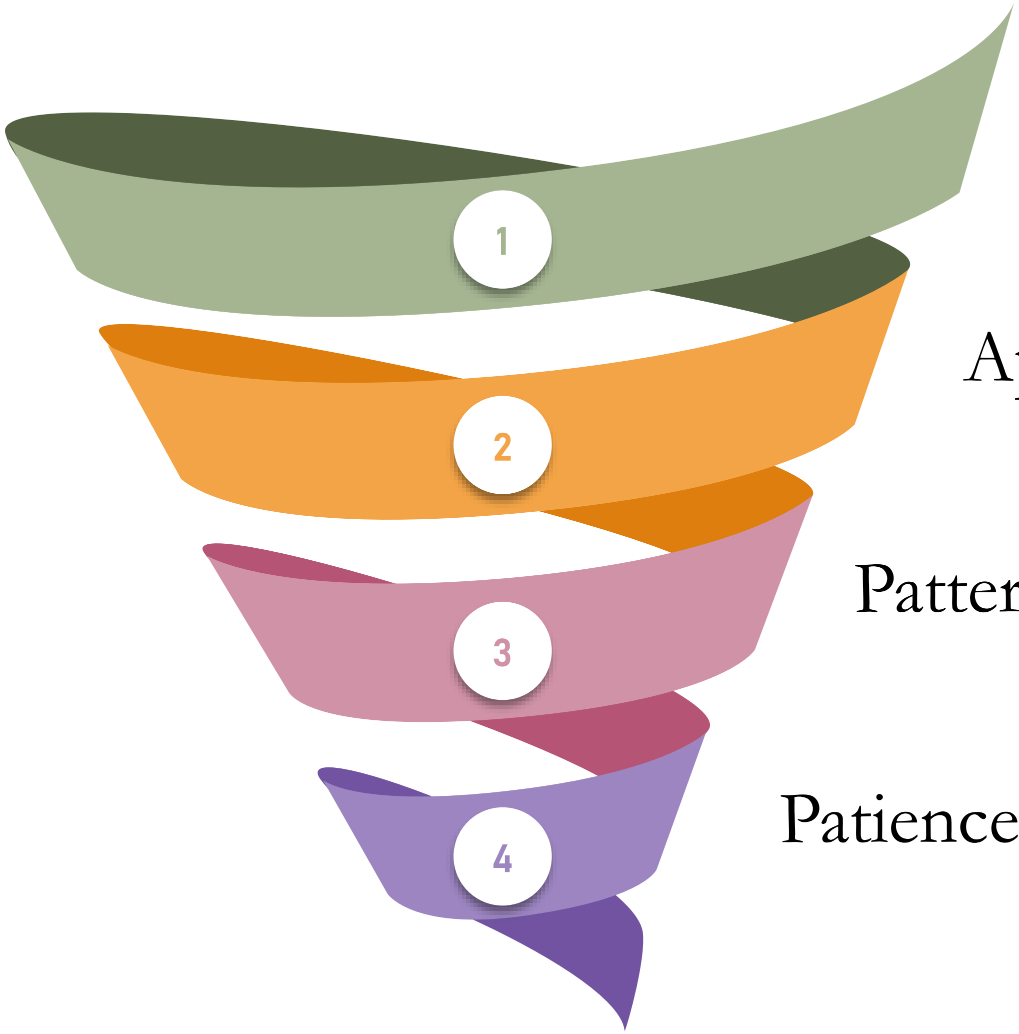
Fourth Class
Department of Mathematics
College of Science – University of Baghdad

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



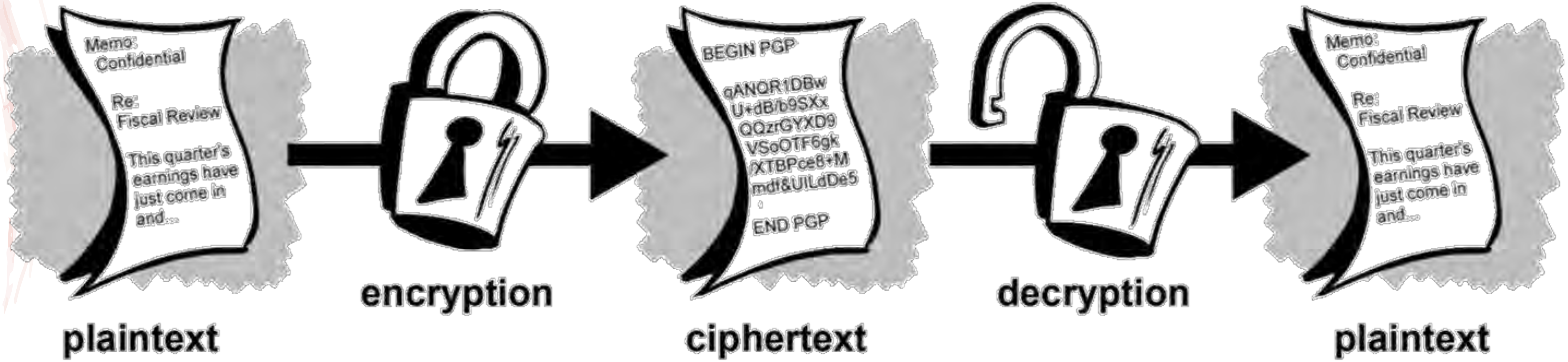
An interesting combination of analytical reasoning

Application of mathematical tools

Pattern finding

Patience, determination, and luck

How does Cryptography Work?



The security of encrypted data is entirely dependent on two things:

- The strength of the cryptographic algorithm.
- The secrecy of the key.

Basic Concepts

Encryption domains and codomains

A denotes a finite set called the *alphabet of definition*. For example, A={0;1}, or the English alphabet A={a, b, …, z}.

M denotes a set called the *message space*. **M** consists of strings of symbols from an alphabet of definition. An element of **M** is called a *plaintext*.

C denotes a set called the *ciphertext space*. **C** consists of strings of symbols from an alphabet of definition, which may differ from the alphabet of definition for **M**. An element of **C** is called a *ciphertext*.

Encryption and decryption transformations

K denotes a set called the ***key space***. An element of **K** is called a ***key***.

Each element $e \in \mathbf{K}$ uniquely determines a bijection from **M** to **C**, denoted by E_e. E_e is called an ***encryption function*** or an ***encryption transformation***. Note that E_e must be a bijection if the process is to be reversed and a unique plaintext message recovered for each distinct ciphertext.

For each $d \in \mathbf{K}$, D_d denotes a bijection from **C** to **M** (i.e., $D_d: C \rightarrow M$). D_d is called a ***decryption function*** or ***decryption transformation***.

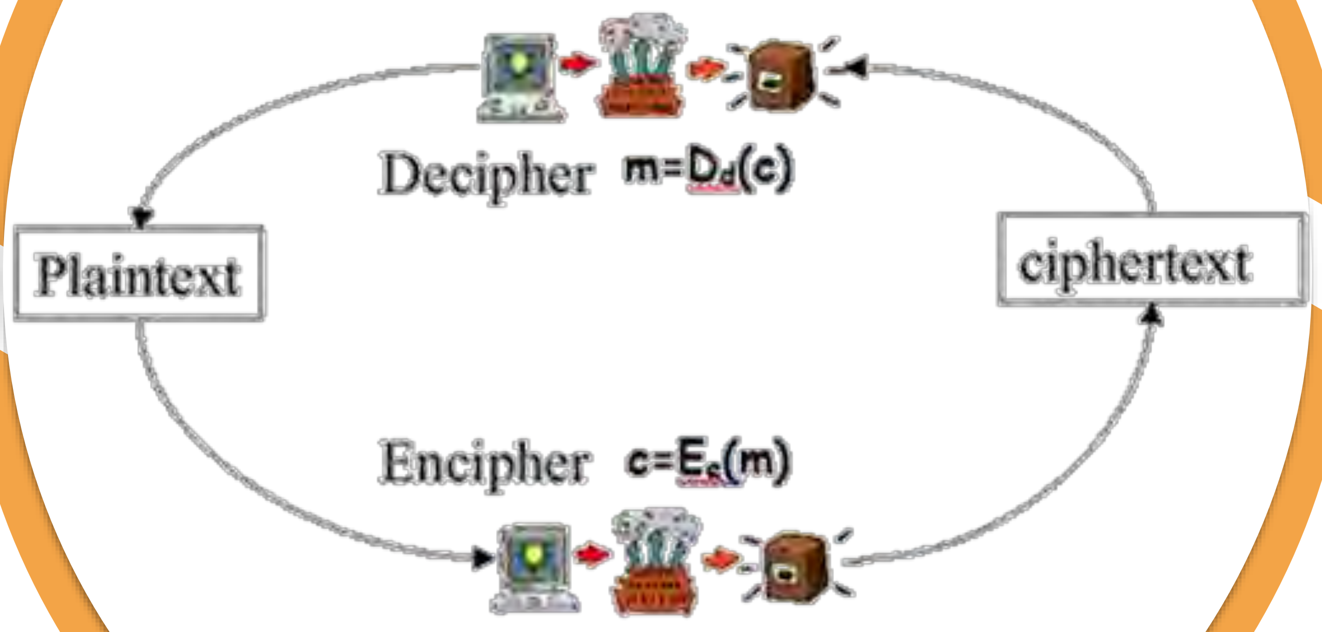
Encryption and decryption transformations

The process of applying the transformation E_e to a message $m \in \mathbf{M}$ is usually referred to as ***encrypting*** m or the ***encryption*** of m.

The process of applying the transformation D_d to a ciphertext c is usually referred to as ***decrypting*** c or the ***decryption*** of c.

An *encryption scheme* consists of a set $\{E_e: e \in K\}$ of encryption transformations and a corresponding set $\{D_d: d \in \mathbf{K}\}$ of decryption transformations with the property that for each $e \in \mathbf{K}$ there is a unique key $d \in \mathbf{K}$ such that $D_d = E_e^{-1}$;that is, $D_d(E_e(m)) = m$ for all $m \in \mathbf{M}$. An encryption scheme is sometimes referred to as a ***cipher***.

Secret Writing



Terminology

- *Cryptography*
- *Plaintext*
- *Ciphertext*
- *Cipher*
- *Key*
- *Encipher (Encode)*
- *Decipher (Decode)*
- *Cryptanalysis*
- *Cryptology*
- *Cryptanalyst*

Cryptography

The art or science encompassing the principles and methods of transforming an **intelligible message** into one that is **unintelligible**, and then retransforming that message back to its original form.

Plaintext

The original **intelligible** message.

Ciphertext

The transformed message, i.e. unintelligible message.

Cipher

An algorithm for transforming an intelligible message into one that is unintelligible by transposition and/or substitution methods.

Key

Some critical information used by the cipher, known only to the sender & receiver.

Encipher (Encode)

The process of converting plaintext to ciphertext using a cipher and a key.

Decipher (Decode)

The process of converting ciphertext back into plaintext using a cipher and a key.

Cryptanalysis

The study of principles and methods of transforming an unintelligible message back into an intelligible message **without** knowledge of the key. Also called codebreaking.

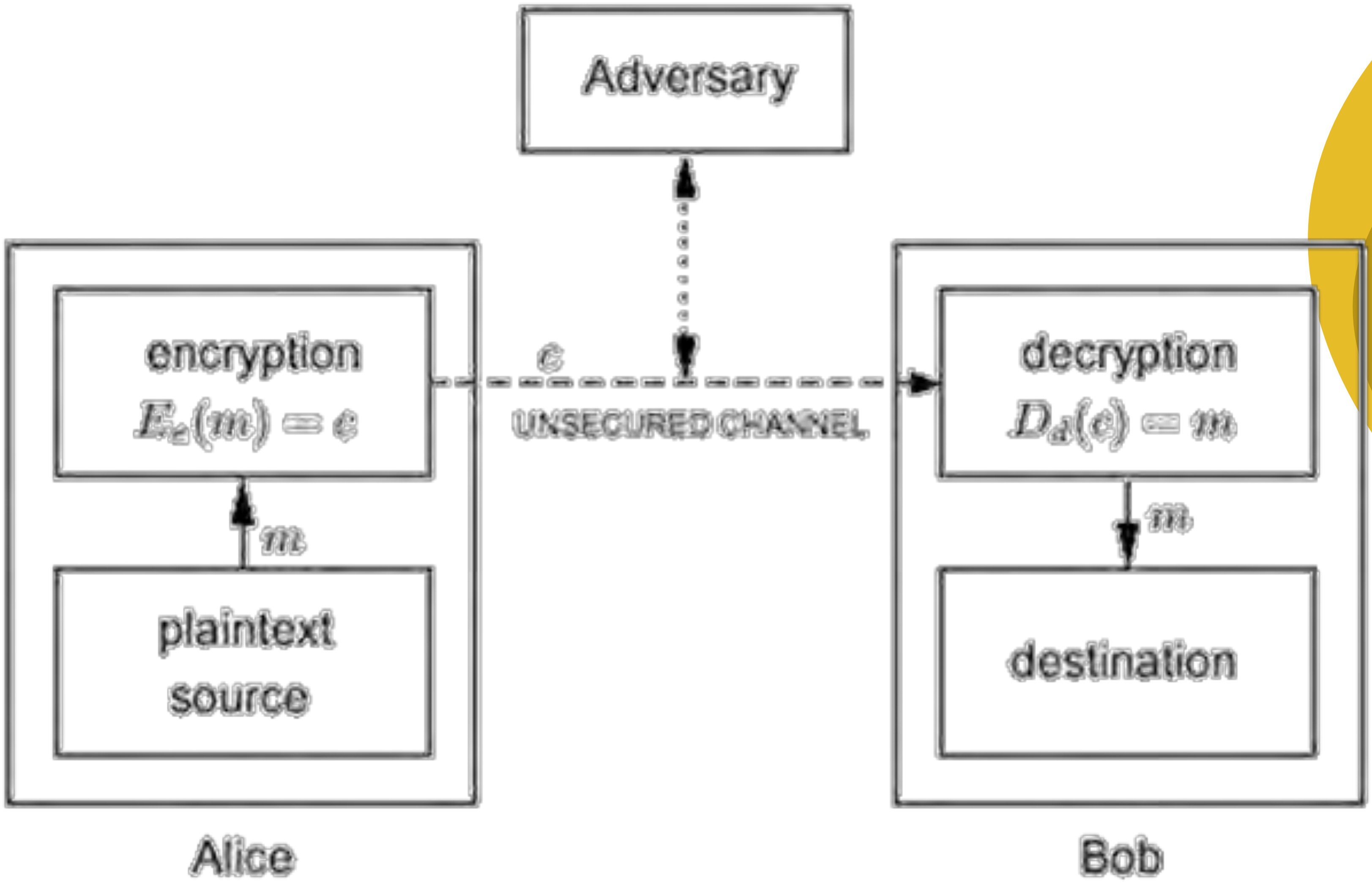
Cryptology

Both cryptography and cryptanalysis.

Cryptanalyst

Someone who engages in cryptanalysis.

The Block Diagram to Cipher System



THANK YOU

Any questions?

You can find me at:
saad.m@sc.uobaghdad.edu.iq

Introduction to Cipher Systems

2

Saad Al-Momen

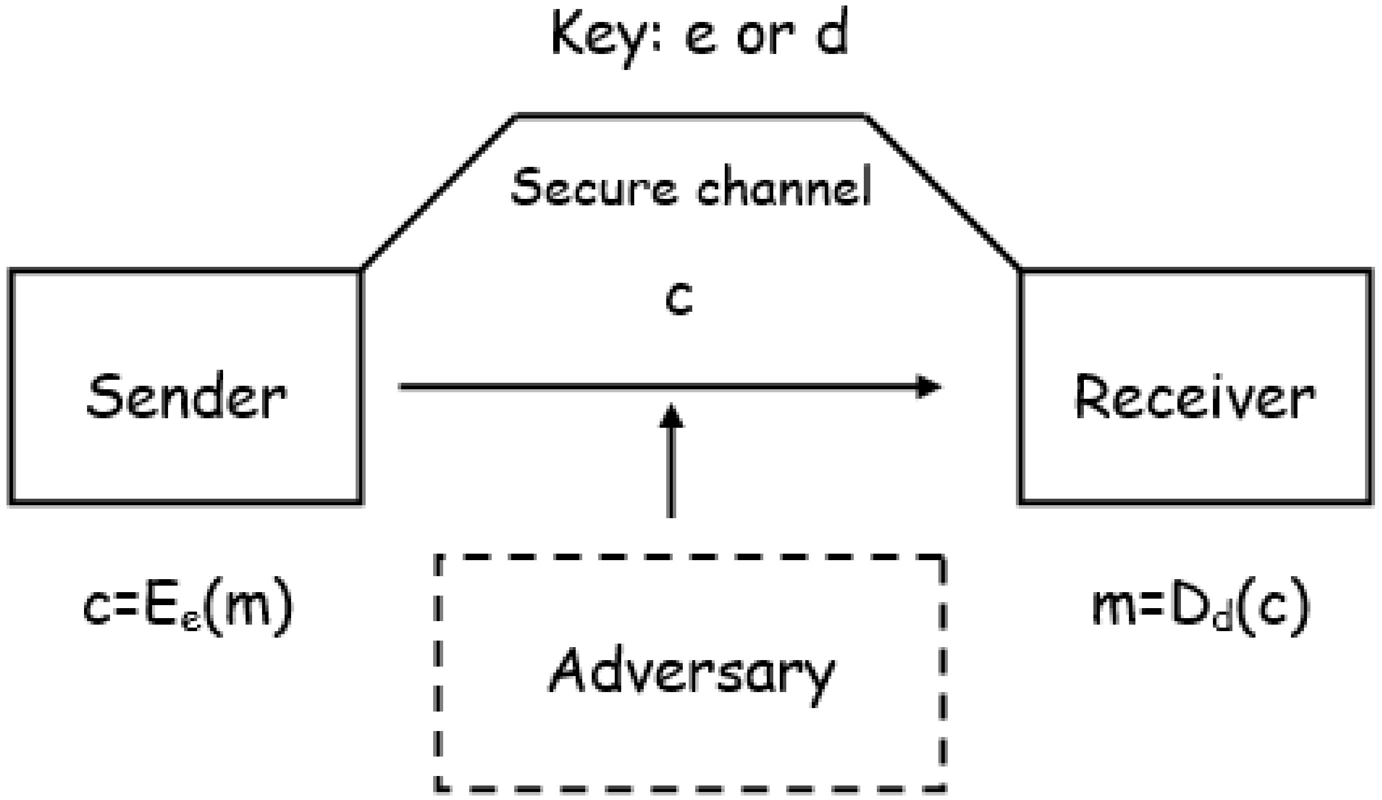
CIPHER SYSTEMS

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

Secret Key Systems

Secret Key Systems

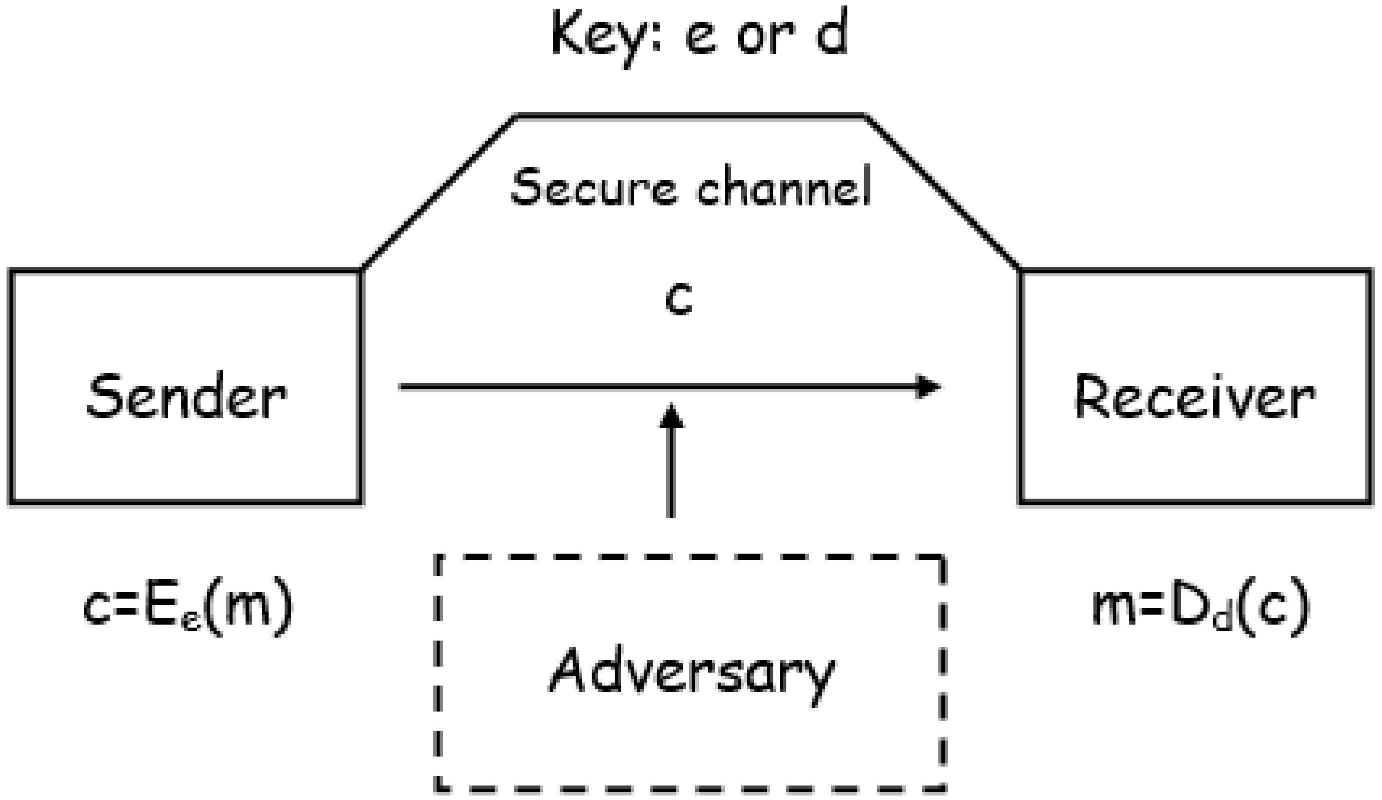
In such type of systems the encipher key and the decipher key must be known **only** by the sender and the receiver, so **they must exchange the key over a secure channel**.



Secret Key Systems

The problems with secret key cryptography are:

1. Requires establishment of a secure channel for key exchange.
2. Two parties cannot start communication if they never met.



Transposition Cipher

Transposition Cipher

In transposition ciphers the letters of the original message (plaintext) are **arranged in a different order** to get the ciphertext.

Plaintext → Rearrange characters → Ciphertext

1 Simple Transposition

- Message reversal cipher
- Columnar transposition

2 Double Transposition

- Double columnar transposition

Message Reversal Cipher

Plaintext = UNIVERSITY OF BAGHDAD

Ciphertext = DADHGAB FO YTISREVINU

Mathematically if L is the length of the message then **c=E(k)=L+1-k**, where k is the position of the letter in the plaintext.

Columnar Transposition

- We arrange the message as array of 2-dimensition.
- The number of rows and columns depends on the length of the message.
- If the length of the message equal to **30** then the probability of the numbers of rows and columns are: 15X2, 2X15, 10X3, 3X10, 5X6, or 6X5.
- Note that if the length of the message is 29, we must add a dummy letter in the end of the message.

Columnar Transposition

1 Simple Transposition

Plaintext = UNIVERSITY OF BAGHDAD

the length of the message is **19**, we will add a dummy letter **X** to the end of the message and the length will be **20**.

Plaintext = UNIVERSITY OF BAGHDAD**X**

We can say that 20=4X5

Columnar Transposition

Plaintext = UNIVERSITY OF BAGHDADX

1	2	3	4	5
U	N	I	V	E
R	S	I	T	Y
O	F	B	A	G
H	D	A	D	X

If the key is (4,3,2,1,5)

4	3	2	1	5
V	I	N	U	E
T	I	S	R	Y
A	B	F	O	G
D	A	D	H	X

Ciphertext = VTADIIBANSFDUROHEYGX

Columnar Transposition

1 Simple Transposition

To make the key easy to remember we take a keyword like **TODAY** and rearrange its letters alphabetically

T	O	D	A	Y
4	3	2	1	5

So (4,3,2,1,5) is the key that will use to rearrange the array columns.

Decipher the above ciphertext.

Double Columnar Transposition

- Double Transposition consists of **two** applications of columnar transposition to a message.
- The two applications may use the same key for each of the two steps, or they may use different keys.

Double Columnar Transposition

2 Double Transposition

First pick a keyword, such as **DIGITAL**, and then write the message under it in

D	I	G	I	T	A	L
U	N	I	V	E	R	S
I	T	Y	O	F	B	A
G	H	D	A	D	X	X

Number the letters in the keyword in alphabetical order.

2	4	3	5	7	1	6
D	I	G	I	T	A	L
U	N	I	V	E	R	S
I	T	Y	O	F	B	A
G	H	D	A	D	X	X

Read the cipher off by columns, starting with the lowest-numbered column

CT_1= RBXUIGIYDNTHVOASAXEFD

Select and number a second keyword (example **BACK**), and write CT_1 under it in rows

2	1	3	4
B	A	C	K
R	B	X	U
I	G	I	Y
D	N	T	H
V	O	A	S
A	X	F	E
D	X	X	X

Take it off by columns again

CT_2= BGNOXXRIDVADXITAFXUYHSEX

Double Columnar Transposition

To **decrypt** a double transposition:

- Construct a block with the right number of rows under the keyword.
- Blocking off the short columns.
- Write the cipher in by columns, and read it out by rows.

Decipher the above ciphertext.

Try to solve the above example (encipher and decipher) without adding the X's.

THANK YOU

Any questions?

You can find me at:

saad.m@sc.uobaghdad.edu.iq

Introduction to Cipher Systems

Saad Al-Momen

3

CIPHER SYSTEMS

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.

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.

1. Direct Standard

- The Caesar cipher is the one most famous and simplest of all ciphers.
- In the Caesar cipher, each letter is **replaced with the third letter following it** in the alphabet.

Plaintext alpha.:

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	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Ciphertext alpha.:

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
3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2

1. Direct Standard

Plaintext alpha.:

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	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Ciphertext alpha.:

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
3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2

As an example, if the message is: UNIVERSITY OF BAGHDAD, then

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

As we see, in Caesar cipher the key is **k=3**
We can choose a different value to the key in the range **between 0 and 25**.

$$c=E_k(m)=(m+k) \bmod 26$$

1. Direct Standard

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	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Encipher: $c=E_k(m)=(m+k) \bmod 26$

Decipher: $m=D_k(c)=(c-k) \bmod 26$

For example in the above example $E_3(A) = E_3(0) = (0+3) \bmod 26 = 3 = D$ and $E_3(Y) = E_3(24) = (24+3) \bmod 26 = 1 = B$ and so on.

If the adversary received the ciphertext and he know that the sender used the shift method, the only thing he need to do, is to try all the possibilities that equal to 25 trials.

Decipher the above ciphertext.

What is the cardinality of the key space of the direct standard method?

2. Standard Reverse

- This method is similar to the Direct standard, except that the ciphertext alphabet are written in **reversed order from Z to A**.

Encipher: $c=E_k(m)=(25-m+k) \bmod 26$

For example if $k=0$ then,

Plaintext alpha.:

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	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Ciphertext alpha.:

25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
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

2. Standard Reverse

Plaintext alpha.:

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	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Ciphertext alpha.:

25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
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

As an example, if the message is: UNIVERSITY OF BAGHDAD, then

U	N	I	V	E	R	S	I	T	Y		O	F		B	A	G	H	D	A	D
F	M	R	E	V	I	H	R	G	B		L	U		Y	Z	T	S	W	Z	W

Decipher the above ciphertext.

What is the cardinality of the key space of the standard reverse method?

3. Multiplicative Cipher

- Ciphers based on **multiply** each character by a key k; that

Encipher: $c=E_k(m)=(m*k) \bmod 26$

- Where k and 26 are relatively prime **(GCD(k,26)=1)**, so that the letters of the alphabet produce a complete set of residues, so that in this case the key must be an **odd number and not equal to 13**.

For example if k=9 then,

Plaintext alpha.:

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	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Ciphertext alpha.:

0	9	18	1	10	19	2	11	20	3	12	21	4	13	22	5	14	23	6	15	24	7	16	25	8	17
A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R

3. Multiplicative Cipher

Plaintext alpha.:

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	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Ciphertext alpha.:

0	9	18	1	10	19	2	11	20	3	12	21	4	13	22	5	14	23	6	15	24	7	16	25	8	17
A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R

As an example, if the message is: UNIVERSITY OF BAGHDAD, then

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

Decipher the above ciphertext.

What is the cardinality of the key space of the multiplicative cipher method?

3. Multiplicative Cipher

Encipher: $c=E_k(m)=(m*k) \bmod 26$

Decipher: $m=D_k(c)=(c*k^{-1}) \bmod 26$

[Proof: $c*k^{-1} = m*k*k^{-1}=m$]

$9^{-1} \bmod 26=3$ [$9*3=27 \bmod 26 =1$]

$7^{-1} \bmod 26=15$ [$7*15=105 \bmod 26 =1$]

.

.

.

Note #1

Decryption

3. Multiplicative Cipher

Plaintext alpha.:

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	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Note #2

k=2

(GCD(k,26)=1)

Ciphertext alpha.:

0	2	4	6	8	10	12	14	16	18	20	22	24	0	2	4	6	8	10	12	14	16	18	20	22	24
A	C	E	G	I	K	M	O	Q	S	U	W	Y	A	C	E	G	I	K	M	O	Q	S	U	W	Y

3. Multiplicative Cipher

Plaintext alpha.:

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	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Note #2

k=4

(GCD(k,26)=1)

Ciphertext alpha.:

0	4	8	12	16	20	24	2	6	10	14	18	22	0	4	8	12	16	20	24	2	6	10	14	18	22
A	E	I	M	Q	U	Y	C	G	K	O	S	W	A	E	I	M	Q	U	Y	C	G	K	O	S	W

3. Multiplicative Cipher

Plaintext alpha.:

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	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Note #2

$k=13$

$(GCD(k,26)=1)$

Ciphertext alpha.:

0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13
A	N	A	N	A	N	A	N	A	N	A	N	A	N	A	N	A	N	A	N	A	N	A	N	A	N

4. Affine Cipher

- Addition (shifting) and multiplication can be **combined** to give an Affine transformation

$$\textbf{Encipher: } c=E_{k1,k2}(m)=(m*k_1+k_2) \bmod 26$$

- The conditions on k_1 are the same conditions on the key of the multiplicative cipher, and the conditions on k_2 are the same conditions on the key of the additive cipher.

Now, if $k_1=7$ and $k_2=4$ then,

Plaintext alpha.:

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	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Ciphertext alpha.:

4	11	18	25	6	13	20	1	8	15	22	3	10	17	24	5	12	19	0	7	14	21	2	9	16	23
E	L	S	Z	G	N	U	B	I	P	W	D	K	R	Y	F	M	T	A	H	O	V	C	J	Q	X

4. Affine Cipher

Plaintext alpha.:

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	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Ciphertext alpha.:

4	11	18	25	6	13	20	1	8	15	22	3	10	17	24	5	12	19	0	7	14	21	2	9	16	23
E	L	S	Z	G	N	U	B	I	P	W	D	K	R	Y	F	M	T	A	H	O	V	C	J	Q	X

As an example, if the message is: UNIVERSITY OF BAGHDAD, then

U	N	I	V	E	R	S	I	T	Y		O	F		B	A	G	H	D	A	D
O	R	I	V	G	T	A	I	H	Q		Y	N		L	E	U	B	Z	E	Z

Decipher the above ciphertext.

What is the cardinality of the key space of the Affine cipher method?

4. Affine Cipher

Encipher: $c=E_{k1,k2}(m)=(m*k_1+k_2) \bmod 26$

Decipher: $m=D_{k1,k2}(c)=((c-k_2)*(k_1)^{-1}) \bmod 26$

[Proof: $(c-k_2)*(k_1)^{-1} =((m*k_1+k_2)-k_2)*(k_1)^{-1}$

$=((m*k_1)+k_2-k_2)*(k_1)^{-1}$

$=(m*k_1)*(k_1)^{-1}$

$=m*(k_1*(k_1)^{-1}) \quad =m$]

Note

Decryption

THANK YOU

Any questions?

You can find me at:
saad.m@sc.uobaghdad.edu.iq

Introduction to Cipher Systems

Saad Al-Momen

4

CIPHER SYSTEMS

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

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
26																									

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
26	25																								

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
26	25	24																							

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
26	25	24	23																						

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
26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

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
26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

There are **26!** such rearrangements, which is over **400,000,000,000,000,000,000,000,000**, i.e. **$4*10^{26}$** which gives rise to an equivalent number of distinct cipher alphabets.

If an enemy agent could check **one** of these possible keys **every second**, it would take roughly one **billion times the lifetime of the universe** to check all of them and find the correct one.

5. Mixed Alphabet

For example, one of the 26! Is the following

Plaintext alpha.:

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

Ciphertext alpha.:

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

if the message is: UNIVERSITY OF BAGHDAD,

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

The **disadvantage** of this method is that the arrangement is **difficult to be remembered**.

Decipher the above ciphertext.

6. Keyword Mixed

In this method we need a keyword like **MATHEMATICS**, and a keyletter like **S**, then:

1. Remove the repeated letters from the keyword, and you will get **MATHEICS**.
2. Put the first letter of the modified keyword **under the keyletter** flowed by the remaining letters of the keyword.

Plaintext alpha.:

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

Ciphertext alpha.:

																		M	A	T	H	E	I	C	S

6. Keyword Mixed

In this method we need a keyword like **MATHEMATICS**, and a keyletter like **S**, then:

1. Remove the repeated letters from the keyword, and you will get **MATHEICS**.
2. Put the first letter of the modified keyword **under the keyletter** flowed by the remaining letters of the keyword.
3. Complete the ciphertext alphabet by the **remaining letters without repetitions**.

Plaintext alpha.:

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

Ciphertext alpha.:

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

6. Keyword Mixed

Plaintext alpha.:

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

Ciphertext alpha.:

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

if the message is: UNIVERSITY OF BAGHDAD,

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

Decipher the above ciphertext.

7. Transposed Keyword Mixed

In this method

1. We need a **keyword** like **MATHEMATICS**.
2. **Removing** the repeated letters.
3. **Put it in a matrix** with number of columns equal to the number of the letters in the modified keyword.

M	A	T	H	E	I	C	S

7. Transposed Keyword Mixed

In this method

1. We need a **keyword** like **MATHEMATICS**.
2. **Removing** the repeated letters.
3. **Put it in a matrix** with number of columns equal to the number of the letters in the modified keyword.

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

4. Then we take the matrix letters **column by column** and we will get

Plaintext alpha.:

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

Ciphertext alpha.:

7. Transposed Keyword Mixed

In this method

1. We need a **keyword** like **MATHEMATICS**.
2. **Removing** the repeated letters.
3. **Put it in a matrix** with number of columns equal to the number of the letters in the modified keyword.

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

4. Then we take the matrix letters **column by column** and we will get

Plaintext alpha.:

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

Ciphertext alpha.:

M	B	O	Y																						

7. Transposed Keyword Mixed

In this method

1. We need a **keyword** like **MATHEMATICS**.
2. **Removing** the repeated letters.
3. **Put it in a matrix** with number of columns equal to the number of the letters in the modified keyword.

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

4. Then we take the matrix letters **column by column** and we will get

Plaintext alpha.:

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

Ciphertext alpha.:

M	B	O	Y	A	D	P	Z																		

7. Transposed Keyword Mixed

In this method

1. We need a **keyword** like **MATHEMATICS**.
2. **Removing** the repeated letters.
3. **Put it in a matrix** with number of columns equal to the number of the letters in the modified keyword.

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

4. Then we take the matrix letters **column by column** and we will get

Plaintext alpha.:

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

Ciphertext alpha.:

M	B	O	Y	A	D	P	Z	T	F	Q															

7. Transposed Keyword Mixed

In this method

1. We need a **keyword** like **MATHEMATICS**.
2. **Removing** the repeated letters.
3. **Put it in a matrix** with number of columns equal to the number of the letters in the modified keyword.

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

4. Then we take the matrix letters **column by column** and we will get

Plaintext alpha.:

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

Ciphertext alpha.:

M	B	O	Y	A	D	P	Z	T	F	Q	H	G	R												

7. Transposed Keyword Mixed

In this method

1. We need a **keyword** like **MATHEMATICS**.
2. **Removing** the repeated letters.
3. **Put it in a matrix** with number of columns equal to the number of the letters in the modified keyword.

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

4. Then we take the matrix letters **column by column** and we will get

Plaintext alpha.:

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

Ciphertext alpha.:

M	B	O	Y	A	D	P	Z	T	F	Q	H	G	R	E	J	U									

7. Transposed Keyword Mixed

In this method

1. We need a **keyword** like **MATHEMATICS**.
2. **Removing** the repeated letters.
3. **Put it in a matrix** with number of columns equal to the number of the letters in the modified keyword.

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

4. Then we take the matrix letters **column by column** and we will get

Plaintext alpha.:

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

Ciphertext alpha.:

M	B	O	Y	A	D	P	Z	T	F	Q	H	G	R	E	J	U	I	K	V						

7. Transposed Keyword Mixed

In this method

1. We need a **keyword** like **MATHEMATICS**.
2. **Removing** the repeated letters.
3. **Put it in a matrix** with number of columns equal to the number of the letters in the modified keyword.

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

4. Then we take the matrix letters **column by column** and we will get

Plaintext alpha.:

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

Ciphertext alpha.:

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

7. Transposed Keyword Mixed

In this method

1. We need a **keyword** like **MATHEMATICS**.
2. **Removing** the repeated letters.
3. **Put it in a matrix** with number of columns equal to the number of the letters in the modified keyword.

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

4. Then we take the matrix letters **column by column** and we will get

Plaintext alpha.:

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

Ciphertext alpha.:

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

7. Transposed Keyword Mixed

Plaintext alpha.:

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

Ciphertext alpha.:

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

if the message is: UNIVERSITY OF BAGHDAD,

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

Decipher the above ciphertext.

Substitution Cipher

1 Monoalphabetic

A. Simple Substitution Cipher

1. Direct Standard
2. Standard Reverse
3. Multiplicative Cipher
4. Affine Cipher
5. Mixed Alphabet
6. Keyword Mixed
7. Transposed Keyword Mixed

B. Homophonic Substitution Cipher

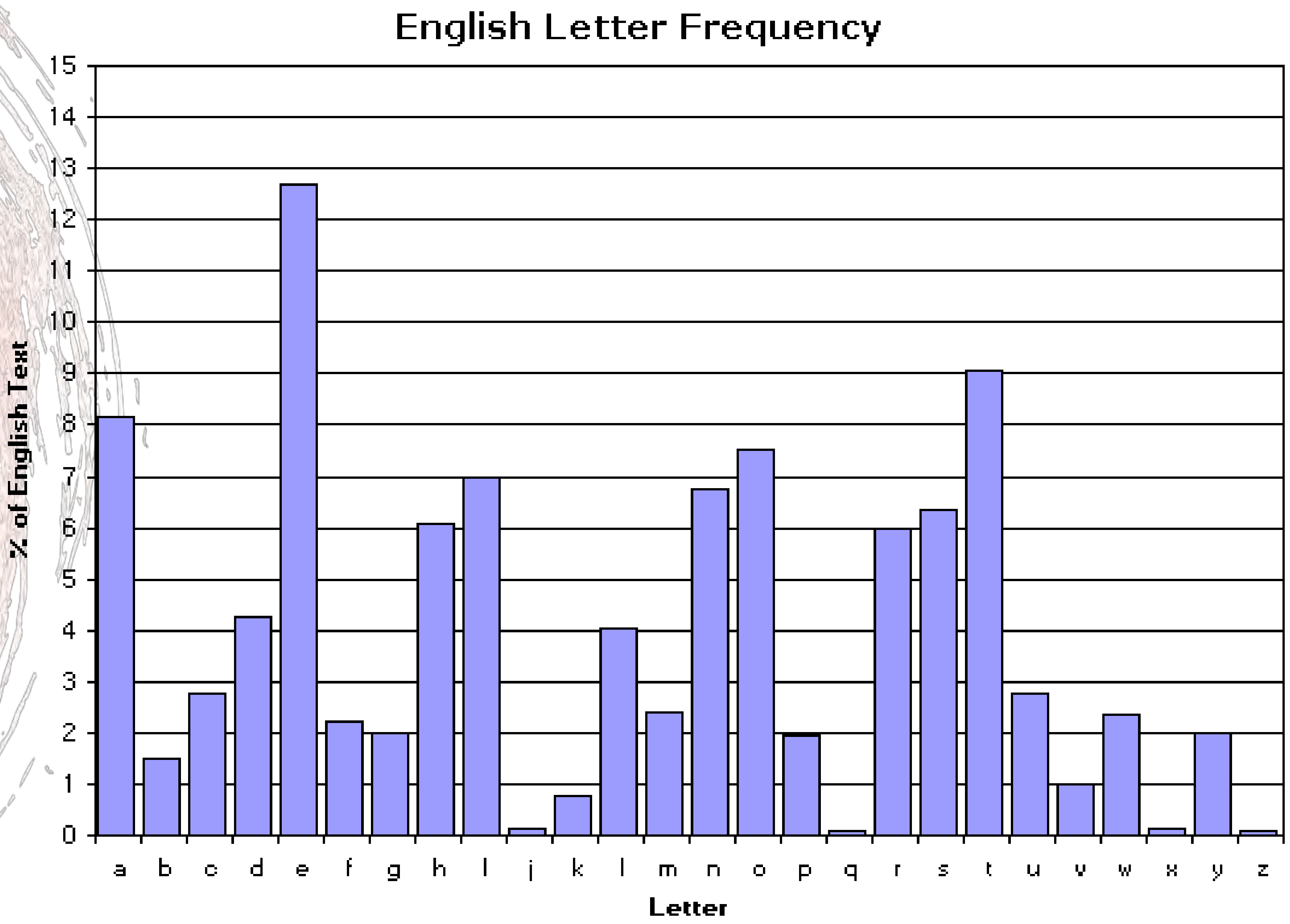
1. Beale Cipher
2. Higher order homophonic

Substitution Cipher

1 Monoalphabetic

B. Homophonic Substitution Cipher

- Homophonic substitution cipher are similar to simple substitution, except the mapping is **one-to many**.
- The Homophonic Substitution Cipher involves replacing each letter with a **variety of substitutes**.
- The number of potential substitutes being **proportional to the frequency** of the letter.



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

The point of offering several substitution options for popular letters is to **balance out the frequencies** of symbols in the ciphertext.

Every symbol will constitute roughly **1%** of the ciphertext.

A	09	12	33	47	53	67	78	92					
B	48	81											
C	13	41	62										
D	01	03	45	79									
E	14	16	24	44	46	55	57	64	74	82	87	98	
F	10	31											
G	06	25											
H	23	39	50	56	65	68							
I	32	70	73	83	88	93							
J	15												
K	04												
L	26	37	51	84									
M	22	27											
N	18	58	59	66	71	91							
O	00	05	07	54	72	90	99						
P	38	95											
Q	94												
R	29	35	40	52	77	80							
S	11	19	36	76	86	96							
T	17	20	30	43	49	69	75	85	97				
U	08	61	63										
V	34												
W	60	89											
X	28												
Y	21	52											
Z	02												

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

A	09	12	33	47	53	67	78	92				
B	48	81										
C	13	41	62									
D	01	03	45	79								
E	14	16	24	44	46	55	57	64	74	82	87	98
F	10	31										
G	06	25										
H	23	39	50	56	65	68						
I	32	70	73	83	88	93						
J	15											
K	04											
L	26	37	51	84								
M	22	27										
N	18	58	59	66	71	91						
O	00	05	07	54	72	90	99					
P	38	95										
Q	94											
R	29	35	40	52	77	80						
S	11	19	36	76	86	96						
T	17	20	30	43	49	69	75	85	97			
U	08	61	63									
V	34											
W	60	89										
X	28											
Y	21	52										
Z	02											

U	N	I	V	E	R	S	I	T	Y		O	F		B	A	G	H	D	A	D
08	18	32	34	14	29	11	70	17	21		00	10		48	09	06	23	01	12	03

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

Decipher the above ciphertext.

1. Beale Cipher

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
"Christmas, the annual festival of Christ's birth. Christmas Day falls on December 25 and celebrates the

17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35
birth of Jesus Christ in Bethlehem as recounted in the Gospels of Matthew and Luke. It is, after Easter,

36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54
the most important feast in the Church's year. Since the Gospels make no mention of dates, it is not

55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73
certain that Christ was born on this day. In fact, Christmas Day did not officially come into being until

74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91
354 when Pope Gregory proclaimed December 25 as the date of the Nativity. In doing so, he was

91 92 93 94 95 96 97 98 99
following the early Church's policy of absorbing rather than repressing existing pagan rites which, since

early times, had celebrated the winter solstice and the coming of spring."

B	A	G	H	D	A	D
07	03	27	90	09	14	51

2. Higher Order Homophonic

Recall that, given enough ciphertext, most ciphers are **theoretically breakable** because there is a **single key that deciphers the ciphertext into meaningful plaintext**; all other keys produce meaningless sequence of letters.

It is possible to construct higher-order homophonic ciphers where each ciphertext **deciphers into more than one meaningful plaintext** using different keys.

To construct a **second-order homophonic** cipher (meaning that for each plaintext there are **two possible meaningful** plaintexts).

2. Higher Order Homophonic

For example; Let n=5. The following is 5X5 matrix for the plaintext alphabet {E, I, L, M, S}.

	E	I	L	M	S
E	10	22	18	02	11
I	12	01	25	05	20
L	19	06	23	13	07
M	03	16	08	24	15
S	17	09	21	14	04

And the message that we want to encipher is SMILE which is replace by LIMES, then

M	=	S	M	I	L	E
X	=	L	I	M	E	S
C	=	21	16	05	19	11

Decipher the above ciphertext.

THANK YOU

Any questions?

You can find me at:
saad.m@sc.uobaghdad.edu.iq

Introduction to Cipher Systems

Saad Al-Momen

5

CIPHER SYSTEMS

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,

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

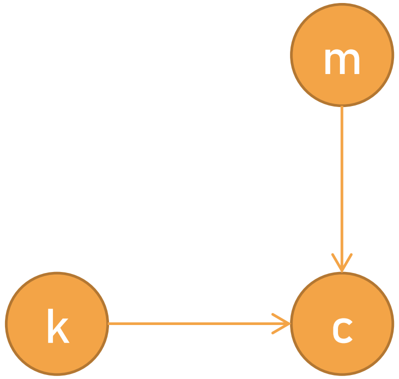
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

1. Vigenere Cipher

TO BE OR NOT TO BE THAT IS THE QUESTION

Keyword: RELATIONS

Keyword: R E L A T I O N S R E L A T I O N S R E L A T I O N S R E L
Plaintext: T O B E O R N O T T O B E T H A T I S T H E Q U E S T I O N
Ciphertext:



Encryption

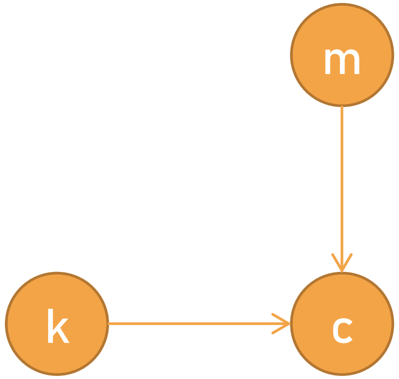
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

TO BE OR NOT TO BE THAT IS THE QUESTION

Keyword: RELATIONS

Keyword: R E L A T I O N S R E L A T I O N S R E L A T I O N S R E L
Plaintext: T O B E O R N O T T O B E T H A T I S T H E Q U E S T I O N
Ciphertext: K



Encryption

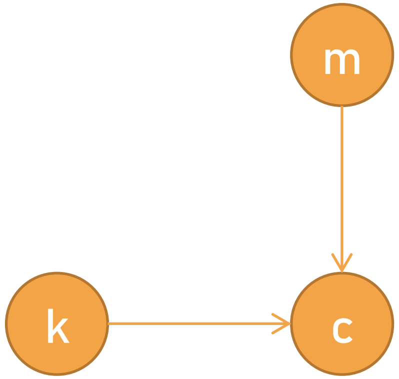
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

TO BE OR NOT TO BE THAT IS THE QUESTION

Keyword: RELATIONS

Keyword: RELATIONSRELATIONSRELATIONSREL
Plaintext: TOBEORNOTTOBETHATISTHEQUESTION
Ciphertext: KS



Encryption

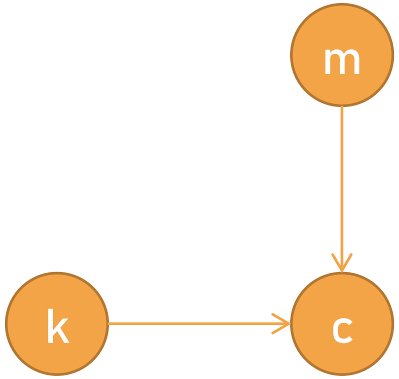
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

To be or not to be that is the question

Keyword: Relations

Keyword: R E L A T I O N S R E L A T I O N S R E L A T I O N S R E L
Plaintext: T O B E O R N O T T O B E T H A T I S T H E Q U E S T I O N
Ciphertext: K S M



Encryption

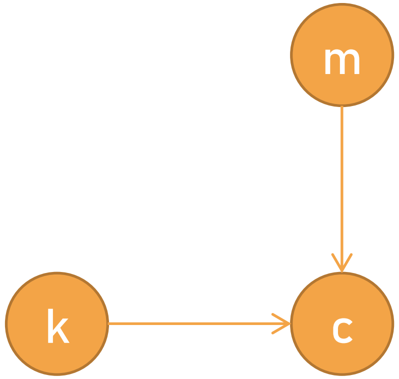
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

TO BE OR NOT TO BE THAT IS THE QUESTION

Keyword: RELATIONS

Keyword: RELATIONSRELATIONSRELATIONSREL
Plaintext: TOBEORNOTTOBETHATISTHEQUESTION
Ciphertext: KSME



Encryption

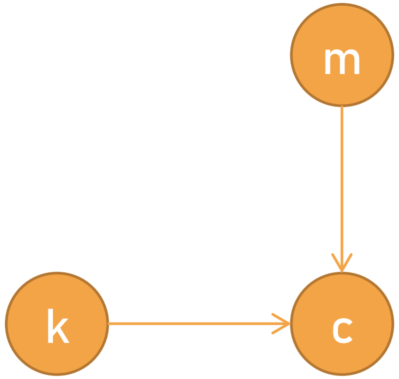
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

TO BE OR NOT TO BE THAT IS THE QUESTION

Keyword: RELATIONS

Keyword: R E L A T I O N S R E L A T I O N S R E L A T I O N S R E L
Plaintext: T O B E O R N O T T O B E T H A T I S T H E Q U E S T I O N
Ciphertext: K S M E H Z B B L K S M E M P O G A J X S E J C S F L Z S Y



Encryption

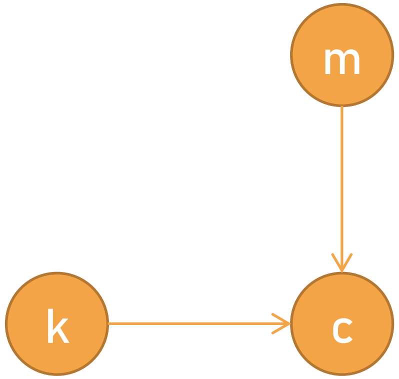
- The strength of the Vigenere cipher against frequency analysis can be seen by examining the above ciphertext.

1. Vigenere Cipher

TO BE OR NOT TO BE THAT IS THE QUESTION

Keyword: RELATIONS

Keyword: RELATIONSRELATIONSRELATIONSREL
Plaintext: TOBEORNOTTOBETHATISTHEQUESTION
Ciphertext: KSMEHZBBLKSMEMPOGAJXSEJCSFLZSY



Encryption

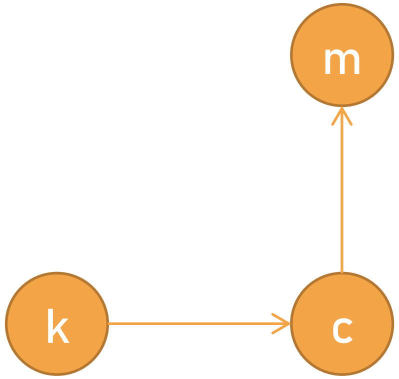
- The strength of the Vigenere cipher against frequency analysis can be seen by examining the above ciphertext.
- Note that there are 7 'T's in the plaintext message and that they have been encrypted by 'K,' 'L,' 'K,' 'M,' 'G,' 'X,' and 'L' respectively.
- This successfully masks the frequency characteristics of the English 'T'.

1. Vigenere Cipher

TO BE OR NOT TO BE THAT IS THE QUESTION

Keyword: RELATIONS

Keyword: R E L A T I O N S R E L A T I O N S R E L A T I O N S R E L
Plaintext:
Ciphertext: K S M E H Z B B L K S M E M P O G A J X S E J C S F L Z S Y



Decryption

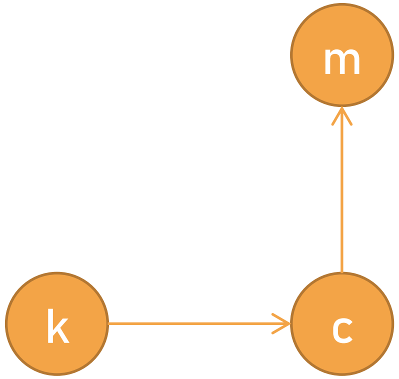
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

TO BE OR NOT TO BE THAT IS THE QUESTION

Keyword: RELATIONS

Keyword: R E L A T I O N S R E L A T I O N S R E L A T I O N S R E L
Plaintext: T
Ciphertext: K S M E H Z B B L K S M E M P O G A J X S E J C S F L Z S Y



Decryption

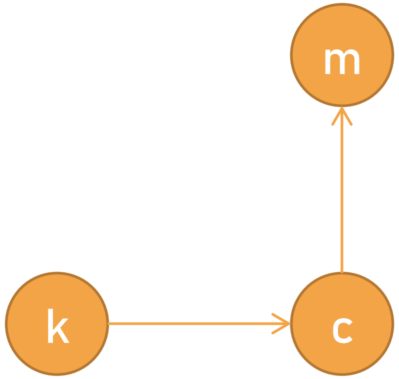
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

TO BE OR NOT TO BE THAT IS THE QUESTION

Keyword: RELATIONS

Keyword: R E L A T I O N S R E L A T I O N S R E L A T I O N S R E L
Plaintext: T O
Ciphertext: K S M E H Z B B L K S M E M P O G A J X S E J C S F L Z S Y



Decryption

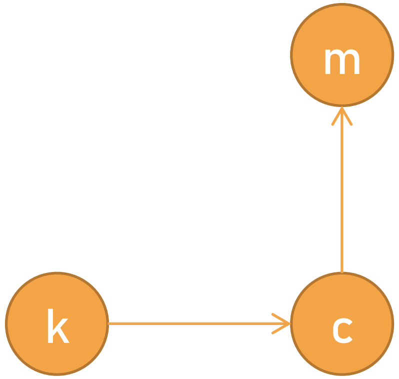
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

TO BE OR NOT TO BE THAT IS THE QUESTION

Keyword: RELATIONS

Keyword: R E L A T I O N S R E L A T I O N S R E L A T I O N S R E L
Plaintext: T O B
Ciphertext: K S M E H Z B B L K S M E M P O G A J X S E J C S F L Z S Y



Decryption

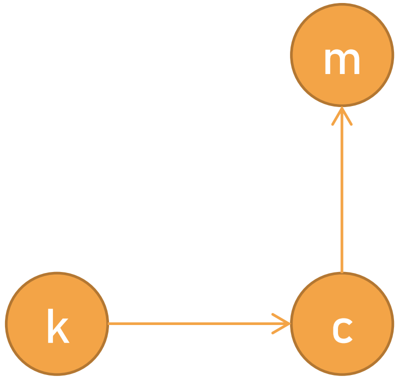
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

TO BE OR NOT TO BE THAT IS THE QUESTION

Keyword: RELATIONS

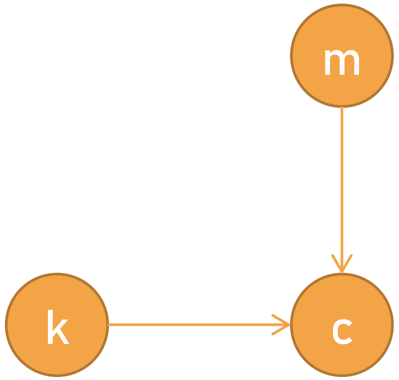
Keyword: RELATIONSREL ATIONS RELATIONSREL
Plaintext: TOBEORNOTTOB ETHATI STHEQUES TION
Ciphertext: KSMEHZB BLKSMEMPOGA JXS EJ CSF LZSY



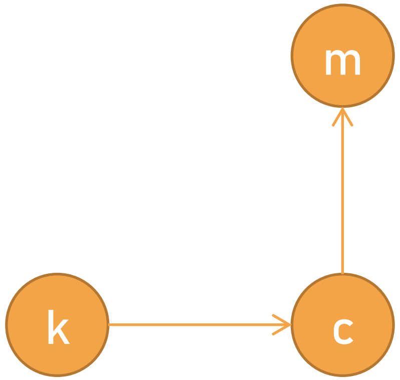
Decryption

	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



Encryption

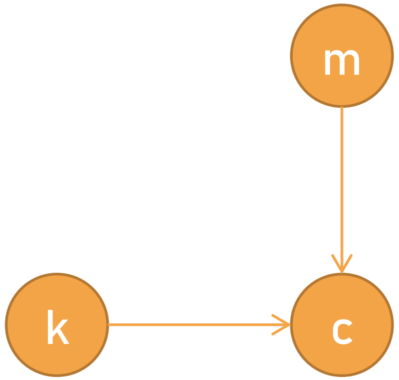


Decryption

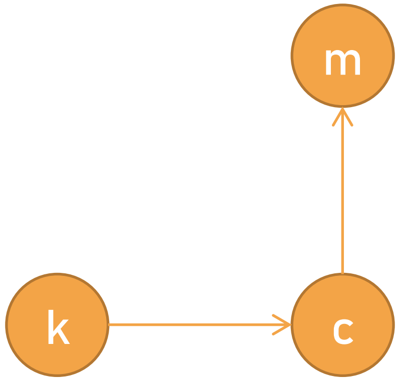
Keyword: RELATIONS

	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



Encryption



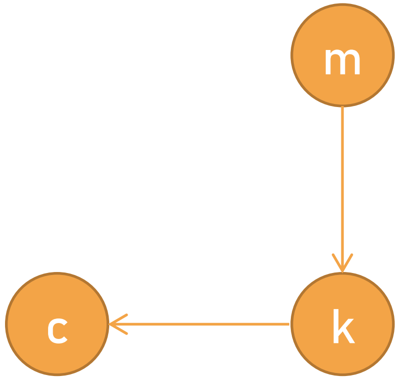
Decryption

	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
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
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
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
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
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

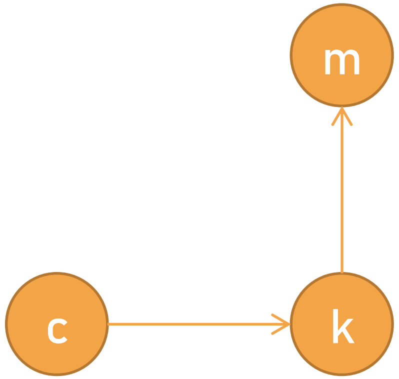
Keyword: RELATIONS

Cipher	Enciphering	Deciphering
Vigenere	$c = m + k_i$	$m = c - k_i$

2. Beaufort Cipher



Encryption



Decryption

Keyword: RELATIONSRELATIONSRELATIONSREL
Plaintext: TOBEORNOTTOBETHATISTHEQUESTION
Ciphertext: YQKWFRBZZYQKWABOUKZLEWDOKVZJQY

Cipher	Enciphering	Deciphering
Beaufort	$c = k_i - m$	$m = k_i - c$

	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

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.

3 Polygraphic

Polygram substitution ciphers encipher block of letters at the time, rather than a single letter.
This makes cryptanalysis harder, as it destroys the single letter frequency distribution.

1. Playfair Cipher
2. Hill Cipher

1. Playfair Cipher

To encipher a message in Playfair,

- **Pick** a keyword.
- **Omit** the repeated letters.
- **Follow** the keyword with the rest of the alphabet.
- **Write** it into a 5X5 Square.
- **Combine** I and J in one cell.

1. Playfair Cipher

Example

If we **pick** the keyword

MANCHESTER

1. Playfair Cipher

Example

If we **pick** the keyword

MANCHESTER

1. Playfair Cipher

Example

MANCHEST R

Omit

1. Playfair Cipher

Example

MANCHESTR

Omit

1. Playfair Cipher

Example

MANCHESTRBDFGIJKLOPQUVWXYZ

Follow

1. Playfair Cipher

Example

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

Write

1. Playfair Cipher

Example

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

Combine

1. Playfair Cipher

Example

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

This is the **key** that we will use to encipher and decipher our message.

1. Playfair Cipher

Enciphering

To encrypt

“THIS SECRET MESSAGE IS ENCRYPTED”

We need to prepare the plaintext message by break it up into two-letter groups.

1. Playfair Cipher

Enciphering

If both letters in a pair are the same, insert an X between them.

If there is only one letter in the last group, add an X to it.

THIS SECRET MESSAGE IS ENCRYPTED

TH IS SE CR ET ME SX SA GE IS EN CR YP TE D

1. Playfair Cipher

Enciphering

If both letters in a pair are the same, insert an X between them.

If there is only one letter in the last group, add an X to it.

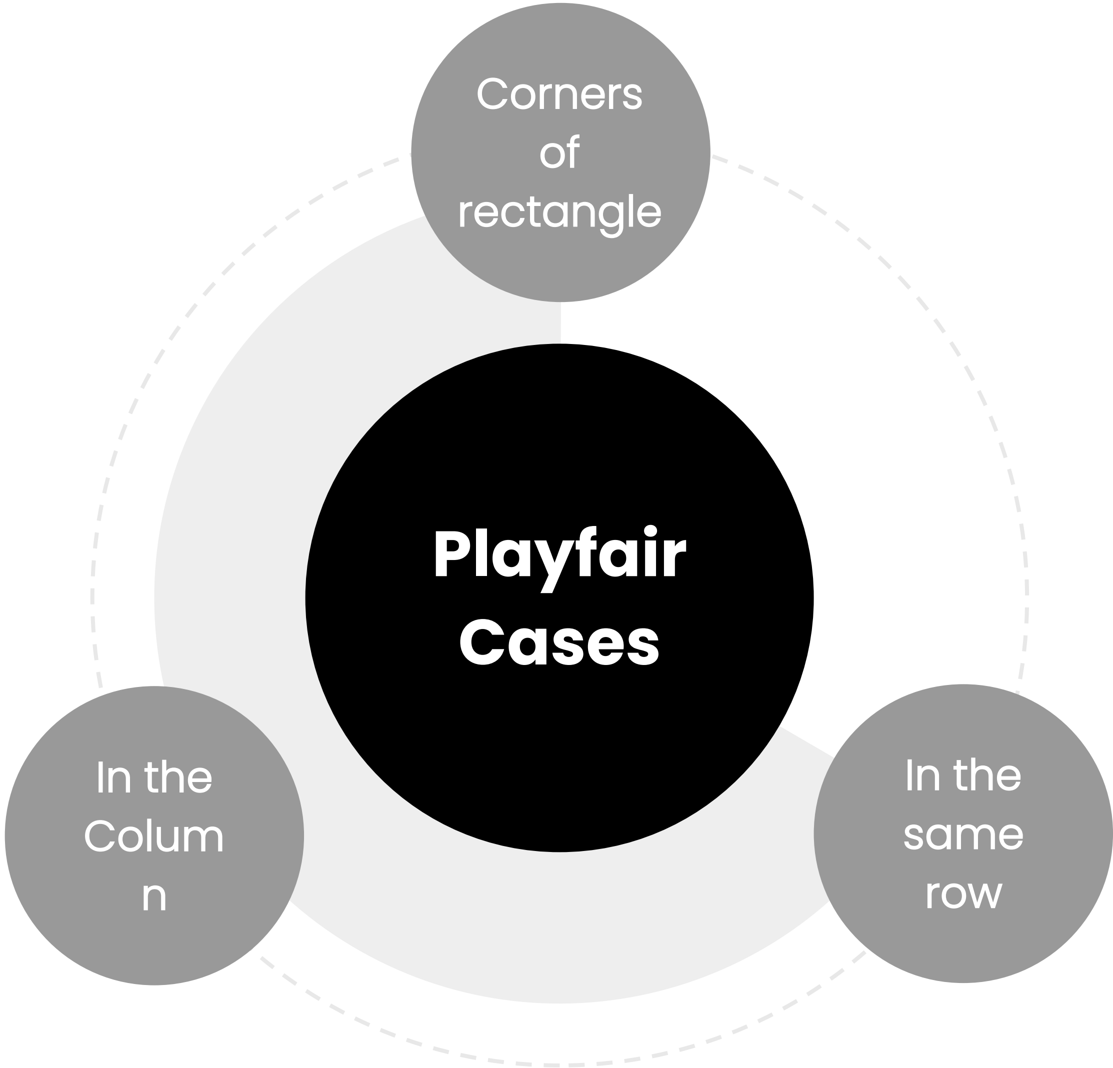
THIS SECRET MESSAGE IS ENCRYPTED

TH IS SE CR ET ME SX SA GE IS EN CR YP TE DX

1. Playfair Cipher

Enciphering

There are **three** possible cases for the letters of the pair



1. Playfair Cipher

Enciphering

.	.	N	.	H
.	.	T	.	B
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.

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

TH IS SE CR ET ME SX SA GE IS EN CR YP TE DX

BN

1. Playfair Cipher

Enciphering

.	.	.	.	.
.	S	.	R	.
.	F	.	I/J	.
.	.	.	.	.
.	.	.	.	.

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

TH IS SE CR ET ME SX SA GE IS EN CR YP TE DX

BN FR

1. Playfair Cipher

Enciphering

.	.	.	.	.
E	S	T	.	.
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.

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

TH IS SE CR ET ME SX SA GE IS EN CR YP TE DX

BN FR TS

1. Playfair Cipher

Enciphering

.	.	.	C	.
.	.	.	R	.
.	.	.	I/J	.
.	.	.	.	.
.	.	.	.	.

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

TH IS SE CR ET ME SX SA GE IS EN CR YP TE DX

BN FR TS RI

1. Playfair Cipher

Enciphering

Plaintext

TH IS SE CR ET ME SX SA GE IS EN CR YP TE DX

Ciphertext

BN FR TS RI SR ED TW FS DT FR TM RI XQ RS GV

1. Playfair Cipher

Deciphering

To decrypt the message, simply reverse the process:

- If the two letters are in different rows and columns, take the letters in the opposite corners of their rectangle.
- In the same row, take the letters to the left.
- In the same column, take the letters above each of them.

2. Hill Cipher

- The message divided onto a number of blocks M, each block contains d letters.
- Then rearranges it in matrix of one column and d rows.
- And we use a matrix K with the size dXd that contains numbers from the range between 0 and 25, then

$$C=KM \bmod 26$$

For example, if

$$K=\begin{bmatrix}3 & 3\\2 & 5\end{bmatrix} \Rightarrow K^{-1}=\begin{bmatrix}15 & 17\\20 & 9\end{bmatrix}$$

2. Hill Cipher

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	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

and we want to encipher the message HELP, then

$$M_1 = \begin{bmatrix} H \\ E \end{bmatrix} = \begin{bmatrix} 7 \\ 4 \end{bmatrix} \qquad M_2 = \begin{bmatrix} L \\ P \end{bmatrix} = \begin{bmatrix} 11 \\ 15 \end{bmatrix}$$

$$C_1 = KM_1 = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}\begin{bmatrix} 7 \\ 4 \end{bmatrix} = \begin{bmatrix} 33 \\ 34 \end{bmatrix} = \begin{bmatrix} 7 \\ 8 \end{bmatrix} = \begin{bmatrix} H \\ I \end{bmatrix}$$

$$C_2 = KM_2 = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}\begin{bmatrix} 11 \\ 15 \end{bmatrix} = \begin{bmatrix} 78 \\ 97 \end{bmatrix} = \begin{bmatrix} 0 \\ 19 \end{bmatrix} = \begin{bmatrix} A \\ T \end{bmatrix}$$

so, the ciphertext is HIAT.

Enciphering

2. Hill Cipher

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	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Now to decipher the word HIAT

$$C_1 = \begin{bmatrix} H \\ I \end{bmatrix} = \begin{bmatrix} 7 \\ 8 \end{bmatrix} \qquad C_2 = \begin{bmatrix} A \\ T \end{bmatrix} = \begin{bmatrix} 0 \\ 19 \end{bmatrix}$$

$$M_1 = K^{-1}C_1 = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}\begin{bmatrix} 7 \\ 8 \end{bmatrix} = \begin{bmatrix} 241 \\ 212 \end{bmatrix} = \begin{bmatrix} 7 \\ 4 \end{bmatrix} = \begin{bmatrix} H \\ E \end{bmatrix}$$

$$M_2 = K^{-1}C_2 = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}\begin{bmatrix} 0 \\ 19 \end{bmatrix} = \begin{bmatrix} 323 \\ 171 \end{bmatrix} = \begin{bmatrix} 11 \\ 15 \end{bmatrix} = \begin{bmatrix} L \\ P \end{bmatrix}$$

so, the original word is HELP.

Use K in the above example to calculate K^{-1}.

Deciphering

THANK YOU

Any questions?

You can find me at:
saad.m@sc.uobaghdad.edu.iq

Introduction to Cipher Systems

6

Saad Al-Momen

CIPHER SYSTEMS

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

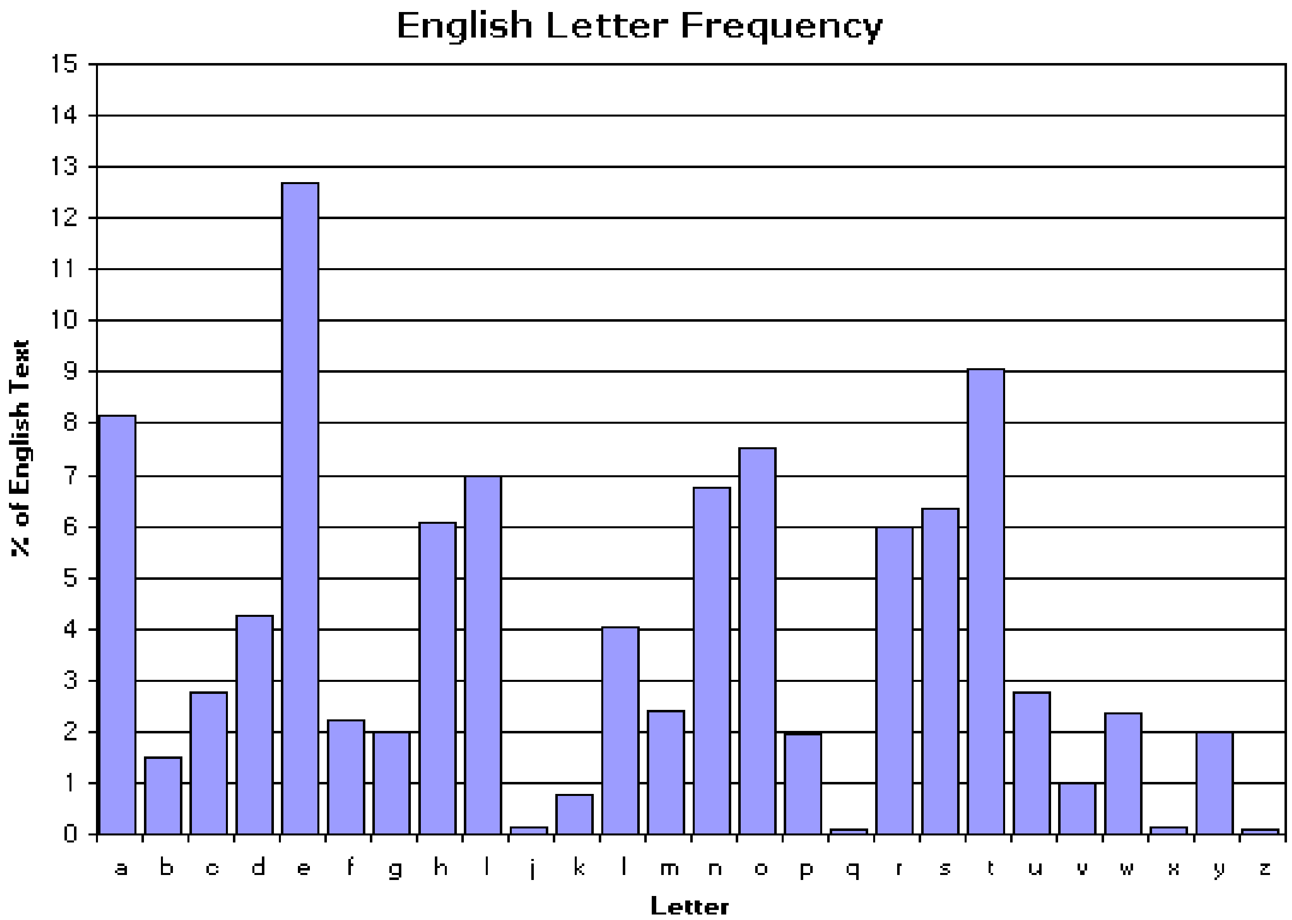
One-Time Pads

- 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.

Some Concepts on Cryptanalysis

Frequency

Number of appearance of the letter in the ciphertext, where the frequencies of the ciphertext letters are compared with the frequencies of the Language.



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

Repetition

It is the similar parts in the ciphertext that have length not less than three.

This helps us to find the length of the key (the number of alphabets that used to enciphering in the polyalphabetic systems).

Index of Coincidence (IC)

It is the probability that two letters selected from the text are identical

$$IC = \frac{\sum_{A}^{Z} f_i (f_i - 1)}{n(n-1)}$$

- The IC value differs from language to another.
- IC can be used to discover if the message were enciphered using Monoalphabetic system or polyalphabetic system.

Coincidence

It is the computing of the coincidence of the ciphertexts, where two messages put one over the other, and the purpose is to discover if the two messages were enciphered using the same key.

In the two messages

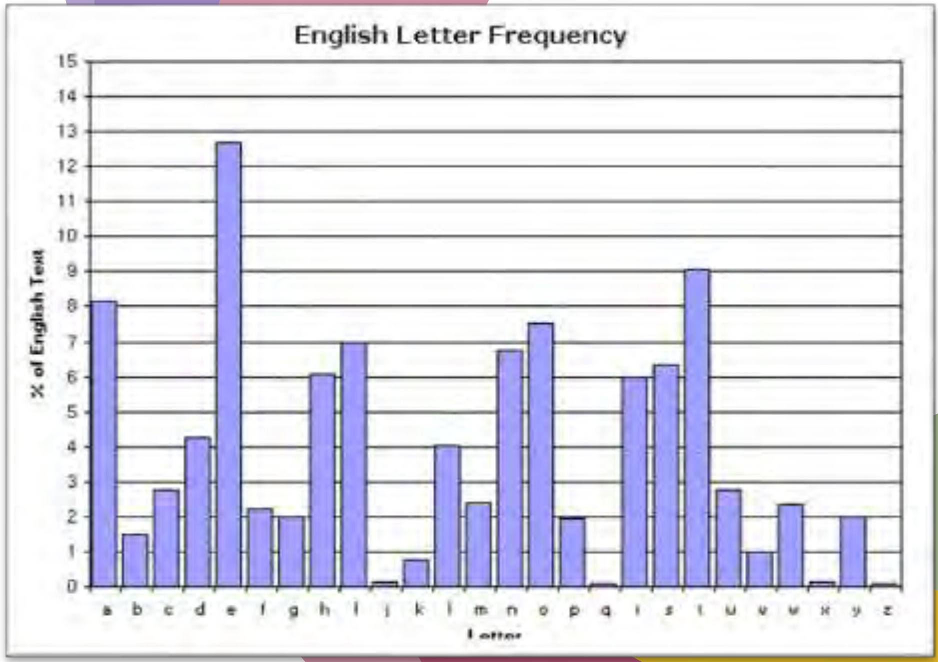
7 coincidence letters between 100 → Same key

4 coincidence letters between 100 → different keys

Cryptanalysis Examples

First of all we must specified the type of the cipher system that was used.

If the frequencies of the ciphertext are the same as the frequencies of the language then, transposition cipher system was used; otherwise a substitution cipher system was used.



Cryptanalysis of Transposition Cipher Systems

When we decide that a transposition cipher system were used, we put the cipher text in mXn matrix, m and n depends on the length of the received ciphertext, for example if the length is 500 then one of the possible sizes is 20X25. Then we rearrange the columns to get some known patterns such as (and, the, ion, that,…) in addition to some expected word in the message.

Cryptanalysis of Transposition Cipher Systems

As we know there are two types of transposition cipher system: simple and double transposition, the cryptanalysis of the last one is more complicated because we lose the ability to find the known patterns.

Columnar Transposition

1 Simple Transposition

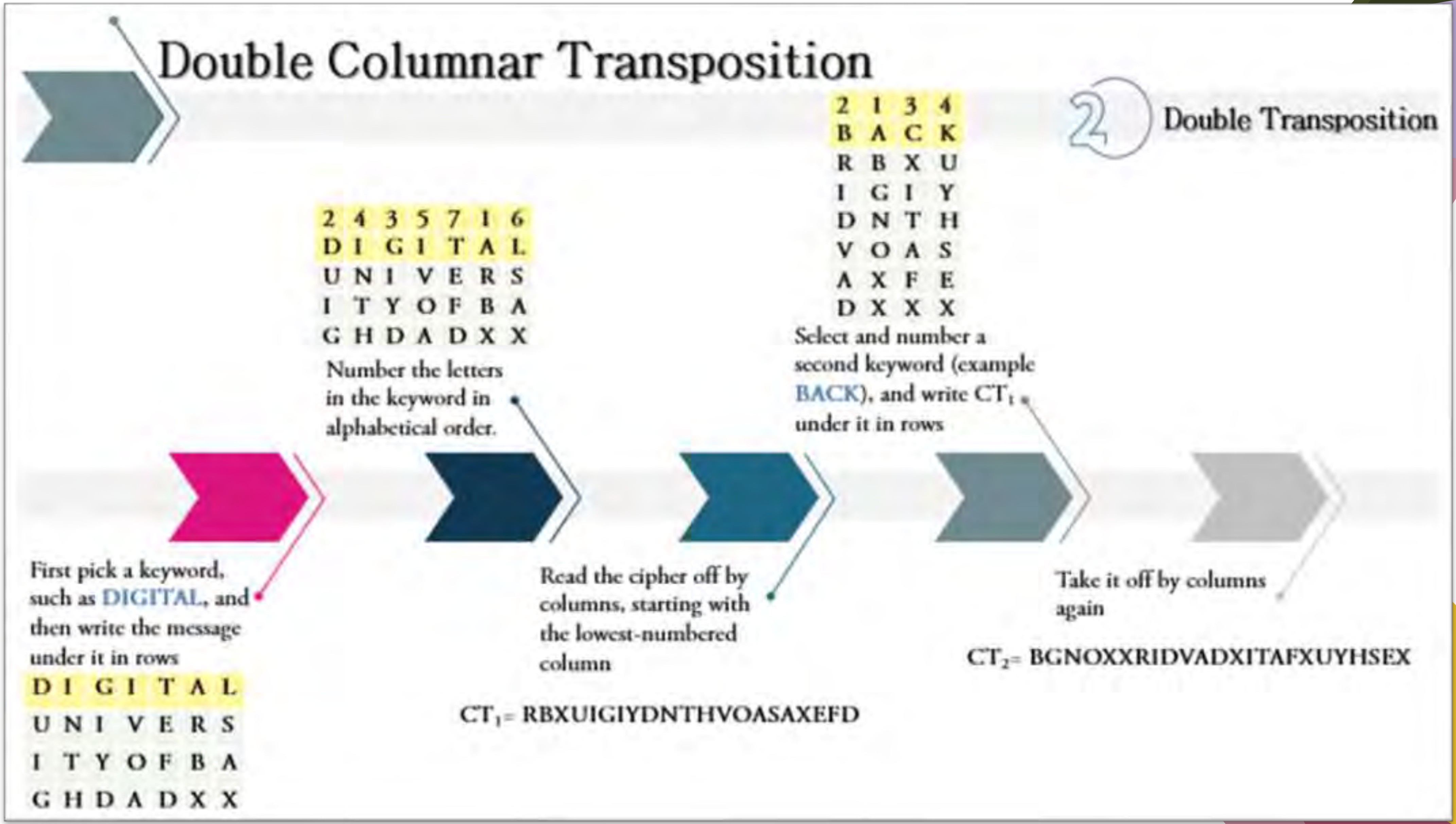
Plaintext = UNIVERSITY OF BAGHDADX

1	2	3	4	5
U	N	I	V	E
R	S	I	T	Y
O	F	B	A	G
H	D	A	D	X

If the key is (4,3,2,1,5)

4	3	2	1	5
V	I	N	U	E
T	I	S	R	Y
A	B	F	O	G
D	A	D	H	X

Ciphertext = VTADIIBANSFDUROHEYGX



Double Columnar Transposition
2 Double Transposition
First pick a keyword, such as DIGITAL, and then write the message under it in rows
D I G I T A L
U N I V E R S
I T Y O F B A
G H D A D X X
2 4 3 5 7 1 6
D I G I T A L
U N I V E R S
I T Y O F B A
G H D A D X X
Number the letters in the keyword in alphabetical order.
Read the cipher off by columns, starting with the lowest-numbered column
CT1= RBXUIGIYDNTHVOASAXEFD
2 1 3 4
B A C K
R B X U
I G I Y
D N T H
V O A S
A X F E
D X X X
Select and number a second keyword (example BACK), and write CT1 under it in rows
Take it off by columns again
CT2= BGNOXXRIDVADXITAFXUYHSEX

Cryptanalysis of Substitution Cipher Systems

$$IC = \frac{141(141-1)+36(36-1)+\ldots+23(23-1)+0(0-1)}{1679(1679-1)} = \frac{184838}{2817362} \approx 0.0656.$$

Letter	Count	Letter	count
A	141	N	119
B	36	O	132
C	36	P	28
D	103	Q	1
E	188	R	95
F	37	S	64
G	34	T	182
H	102	U	59
I	123	V	13
J	4	W	55
K	18	X	3
L	56	Y	23
M	27	Z	0

$$IC = \frac{\sum_{A}^{Z} f_i(f_i - 1)}{n(n-1)}$$

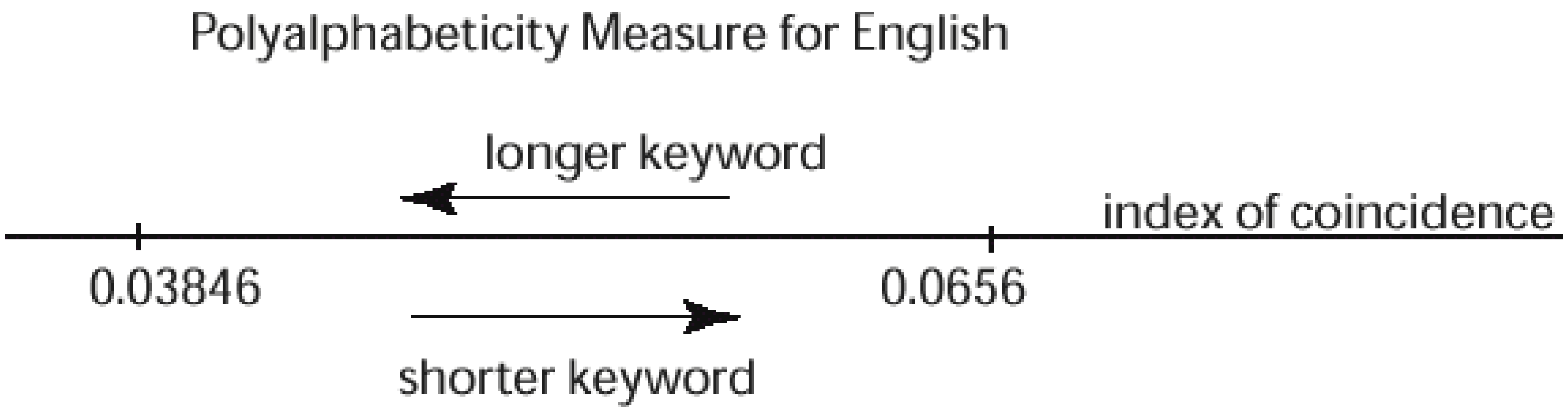
Example 1

What is the index of coincidence for a collection of 2600 letters consisting of 100 A 's,100 B 's,100 C 's,...,100 Z 's?

$$IC = \frac{100 \cdot 99 + 100 \cdot 99 + \dots + 100 \cdot 99 + 100 \cdot 99}{2600 \cdot 2599} \approx 0.0384615.$$

Example 2

Cryptanalysis of Substitution Cipher Systems



If the length of the text is n, we can quantify the connection between index of coincidence and keyword length k, (number of alphabets), where:

$$k \approx \frac{0.0265 \cdot n}{(0.065 - IC) + n(IC - 0.0385)}$$

Cryptanalysis of Substitution Cipher Systems

$$IC = \frac{60 \cdot 59 + 50 \cdot 49 + \ldots + 67 \cdot 66}{1282 \cdot 1281} = \frac{35761}{821121} \approx 0.04355.$$

Letter	Count	Letter	count
A	60	N	28
B	50	O	83
C	42	P	44
D	64	Q	69
E	51	R	13
F	63	S	29
G	19	T	66
H	48	U	87
I	56	V	63
J	67	W	19
K	23	X	43
L	45	Y	39
M	44	Z	67

Example 3

$$IC = \frac{60 \cdot 59 + 50 \cdot 49 + \ldots + 67 \cdot 66}{1282 \cdot 1281} = \frac{35761}{821121} \approx 0.04355.$$

$$K = \frac{0.0265 \cdot 1282}{(0.065 - 0.04355) + 1282(0.04355 - 0.03846)} = 5.1892.$$

Example 3

Based only on this evidence, a reasonably likely keyword length is **5**.

Cryptanalysis Process

Cryptanalysis Process

Now, after the above tests if we conclude that a monoalphabetic cipher system was used, then:

❶ If a direct standard or reversed system were used, we compare the frequencies of the ciphertext with the frequencies of the English language, start by putting E against the letter with the higher frequency in the ciphertext, then we put the other letters sequentially.

❷ If a mixed cipher system was used (Random) then we compare the frequencies of the ciphertext with that frequency table of the language.

Cryptanalysis Process

1. Direct Standard

Plaintext alpha.:

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	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Ciphertext alpha.:

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
3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2

As an example, if the message is: UNIVERSITY OF BAGHDAD, then

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

As we see, in Caesar cipher the key is k=3

We can choose a different value to the key in the range between 0 and 25.

$$c=E_k(m)=(m+k) \bmod 26$$

Cryptanalysis Process

2. Standard Reverse

- This method is similar to the Direct standard, except that the ciphertext alphabet are written in reversed order from Z to A.

$$\text{Encipher: } c=E_k(m)=(25-m+k) \bmod 26$$

For example if k=0 then,

Plaintext alpha.:

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	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Ciphertext alpha.:

25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
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

Cryptanalysis Process

2. Standard Reverse

- This method is similar to the Direct standard, except that the ciphertext alphabet are written in reversed order from Z to A.

Encipher: $c=E_k(m)=(25-m+k) \bmod 26$

For example if k=0 then,

Plaintext alpha.:

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	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Ciphertext alpha.:

25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
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

Cryptanalysis Process

3. Multiplicative Cipher

- Ciphers based on multiply each character by a key k; that

  Encipher: $c = E_k(m) = (m^*k) \bmod 26$

- Where k and 26 are relatively prime (GCD(k,26)=1), so that the letters of the alphabet produce a complete set of residues, so that in this case the key must be an odd number and not equal to 13.

  For example if k=9 then,

Plaintext alpha.:

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	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Ciphertext alpha.:

0	9	18	1	10	19	2	11	20	3	12	21	4	13	22	5	14	23	6	15	24	7	16	25	8	17
A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R

Monoalphabetic

Cryptanalysis Process

For advanced analysis we can use in addition to single letter frequencies, a table of double letter frequencies TH, HE, IN, ER, RE, ON, AN, EN,…, and triple letter frequencies THE, AND, TIO, ATI, FOR, THA, TER, RES,… and so on.

Cryptanalysis Process

If a polyalphabetic cipher system was used then we will use the Kasiski method to find the length of the key k (number of alphabets). Then we divide the ciphertext into k parts, each part will analyze as in ❷ above.

Cryptanalysis Process

K=	H	A	M	H	A	M	H	A	M	H	A	M	H
M=	T	O	B	E	O	R	N	O	T	T	O	B	E
C=	A	O	N	L	O	D	U	O	F	A	O	N	L

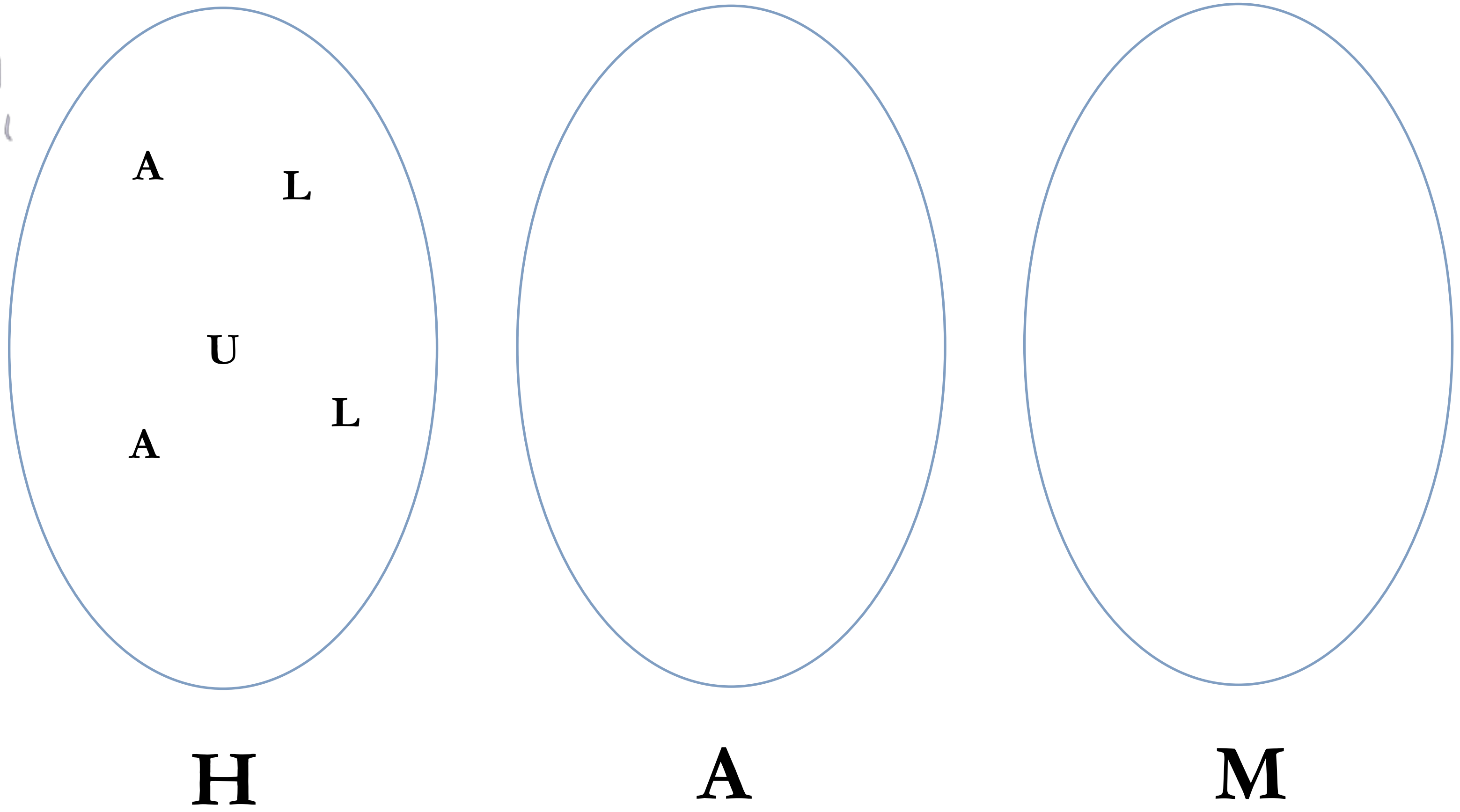
H

A

M

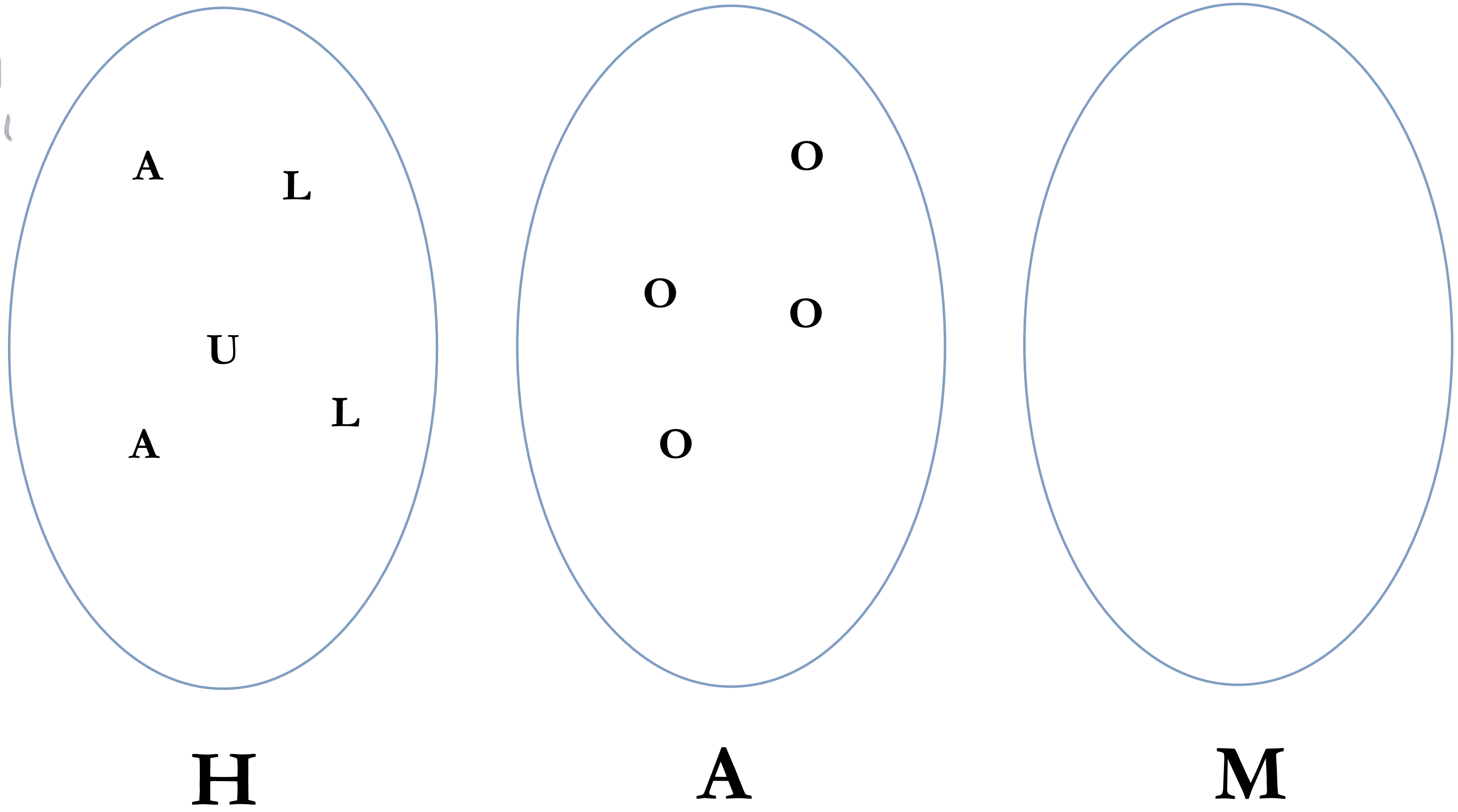
Cryptanalysis Process

K=	H	A	M	H	A	M	H	A	M	H	A	M	H
M=	T	O	B	E	O	R	N	O	T	T	O	B	E
C=		O	N		O	D		O	F		O	N	



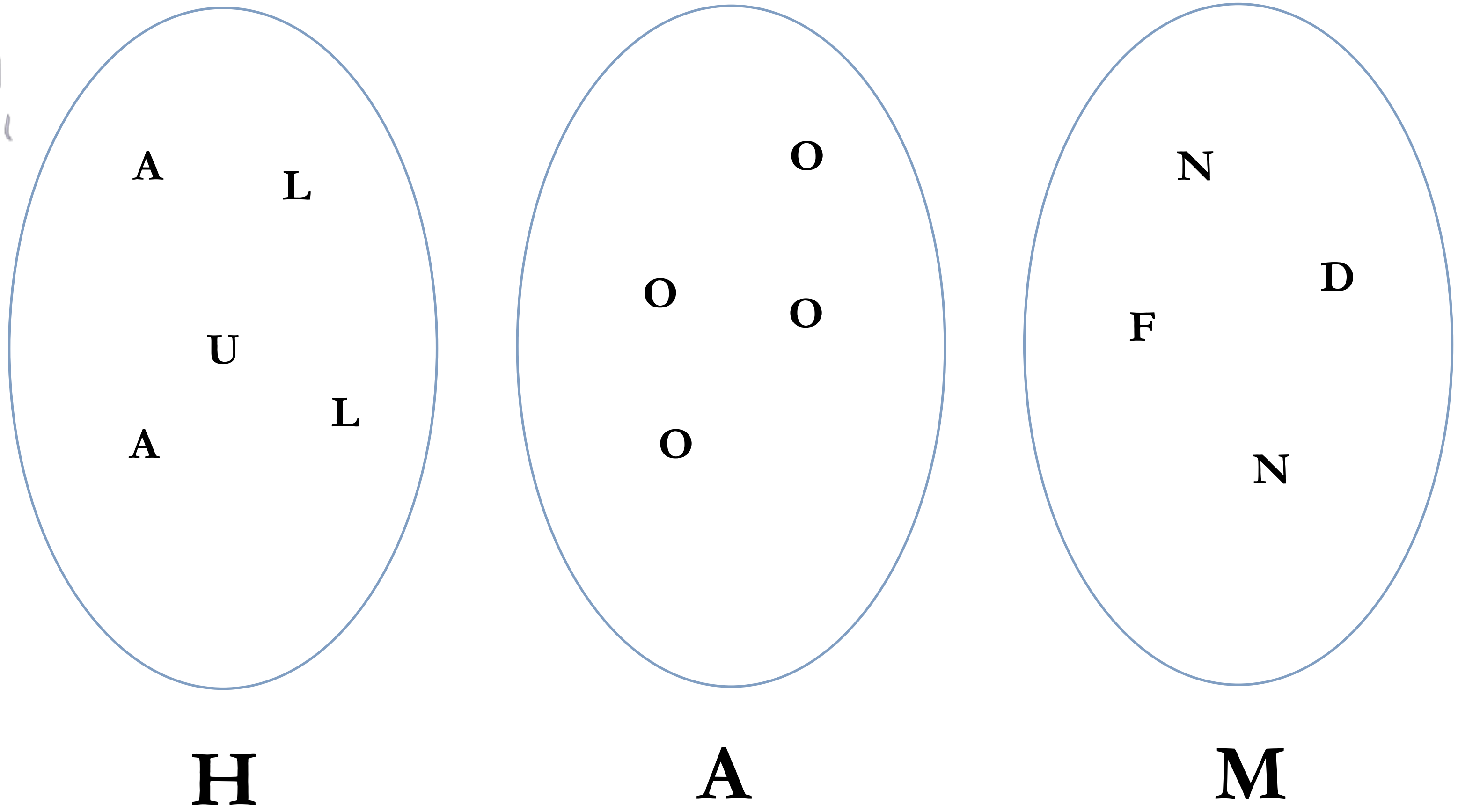
Cryptanalysis Process

K=	H	A	M	H	A	M	H	A	M	H	A	M	H
M=	T	O	B	E	O	R	N	O	T	T	O	B	E
C=			N			D			F			N	



Cryptanalysis Process

K=	H	A	M	H	A	M	H	A	M	H	A	M	H
M=	T	O	B	E	O	R	N	O	T	T	O	B	E
C=													



Kasiski Method

Kasiski Method

The Kasiski method was introduced in 1863 by the Prussian military officer Friedrich W. Kasiski. The method analysis repetitions in the ciphertext to determine the period.

For example, consider the plaintext TO BE OR NOT TO BE enciphered with a Vigenere cipher with key HAM:

K=	H	A	M	H	A	M	H	A	M	H	A	M	H
M=	T	O	B	E	O	R	N	O	T	T	O	B	E
C=	A	O	N	L	O	D	U	O	F	A	O	N	L

Kasiski Method

The Kasiski method was introduced in 1863 by the Prussian military officer Friedrich W. Kasiski. The method analysis repetitions in the ciphertext to determine the period.

For example, consider the plaintext TO BE OR NOT TO BE enciphered with a Vigenere cipher with key HAM:

K=	**H**	**A**	**M**	**H**	**A**	**M**	**H**	**A**	**M**	**H**	**A**	**M**	**H**
M=	**T**	**O**	**B**	**E**	**O**	**R**	**N**	**O**	**T**	**T**	**O**	**B**	**E**
C=	**A**	**O**	**N**	**L**	**O**	**D**	**U**	**O**	**F**	**A**	**O**	**N**	**L**

9

The ciphertext contains two occurrences of the sequence AONL 9 characters apart, and the period could be 1,3 or 9 (we know it's 3).

Repetitions in the ciphertext more than two characters long are unlikely to occur by chance. They occur when the plaintext pattern repeats at a distance equal to a multiple of the period.

Kasiski Method

Example 1

If there are m ciphertext repetitions that occur at intervals I j (1≤j≤m) the period is likely to be some number that divides most of the m intervals.

We shall use IC and Kasiski method to analyze the following ciphertext.

ZHYME	ZVELK	OJUBW	CEYIN	CUSML	RAVSR	YARNH	CEARI	UJPGP	VARDU
QZCGR	NNCAW	JALUH	GJPJR	YGEGQ	FULUS	QFFPV	EYEDQ	GOLKA	LVOSJ
TFRTR	YEJZS	RVNCI	HYJNM	ZDCRO	DKHCR	MMLNR	FFLFN	QGOLK	ALVOS
JWMIK	QKUBP	SAYOJ	RRQYI	NRNYC	YQZSY	EDNCA	LEILX	RCHUG	IEBKO
YTHGV	VCKHC	JEQGO	LKALV	OSJED	WEAKS	GJHYC	LLFTY	IGSVT	FVPMZ
NRZOL	CYUZS	FKOQR	YRTAR	ZFGKI	QKRSV	IRCEY	USKVT	MKHCR	MYQIL
XRCRL	GQARZ	OLKHY	KSNFN	RRNCZ	TWUOC	JNMKC	MDEZP	IRJEJ	W

When we calculate the frequency distribution, we will find that the IC=0.04343, n=346

$$k = \frac{0.0265 \cdot 346}{(0.065 - 0.04343) + 346(0.04343 - 0.03846)} = 5.2659$$

The IC indicates that this is a polyalphabetic cipher with a period of about **5**.

Kasiski Method

Example 1

If there are m ciphertext repetitions that occur at intervals I j (1≤j≤m) the period is likely to be some number that divides most of the m intervals.

We shall use IC and Kasiski method to analyze the following ciphertext.

ZHYME	ZVELK	OJUBW	CEYIN	CUSML	RAVSR	YARNH	CEARI	UJPGP	VARDU
QZCGR	NNCAW	JALUH	GJPJR	YGEGQ	FULUS	QFFPV	EYEDQ	GOLKA	LVOSJ
TFRTR	YEJZS	RVNCI	HYJNM	ZDCRO	DKHCR	MMLNR	FFLFN	QGOLK	ALVOS
JWMIK	QKUBP	SAYOJ	RRQYI	NRNYC	YQZSY	EDNCA	LEILX	RCHUG	IEBKO
YTHGV	VCKHC	JEQGO	LKALV	OSJED	WEAKS	GJHYC	LLFTY	IGSVT	FVPMZ
NRZOL	CYUZS	FKOQR	YRTAR	ZFGKI	QKRSV	IRCEY	USKVT	MKHCR	MYQIL
XRCRL	GQARZ	OLKHY	KSNFN	RRNCZ	TWUOC	JNMKC	MDEZP	IRJEJ	W

We observe that there are 3 occurrences of the sequence QGOLKALVOSJ, the first two occurrences are separated by **51** and the last two by **72** characters (start to start); the only common divisor of 51 and 72 is **3** - the period is almost certainly 3.

Kasiski Method

When we calculate the **IC** of some ciphertext, we find that **k=9.34**. Also we observe that there is **NYX** appearance many times in the ciphertext and the distance between them are **30**, **50**, **90**, **110**, and **33**.

30=2X3X5
50=2X5X5
90=2X3X3X5
110=2X5X11
33=3X11

- There are a number of candidates for key length.
- 2 and 5 are popular factors among these distance followed by 3 and 11.
- Note that all but 33 have 2X5=10 as a factor.
- The cryptanalyst might then disregard 33 as a pure coincidence.
- Discard that data in favor of conjecture that the key length is a multiple of 2 and/or 5.
- Combining this with data from the Friedman test that the key approximately 9 letters long, the cryptanalyst guesses that the key is 10 letters long, and not 2 or 5 letters long.

Example 2

THANK YOU

Any questions?

You can find me at:
saad.m@sc.uobaghdad.edu.iq

Saad Al-Momen

Practical Security

7.

CIPHER SYSTEMS

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

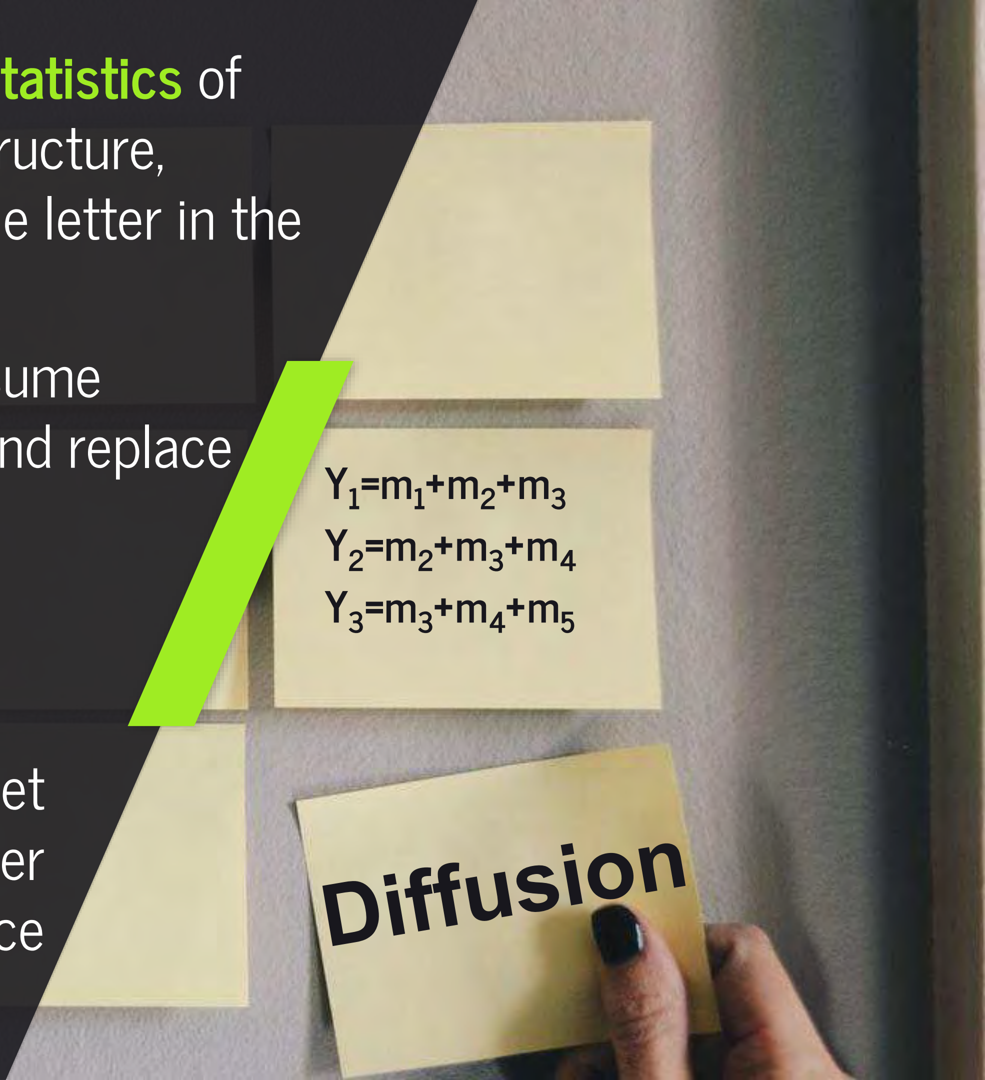
Shannon suggests that the cryptographer uses two techniques which he calls **Diffusion** and **Confusion**.

The idea of diffusion is to **spread the statistics** of the message space into a statistical structure, which involves long combinations of the letter in the ciphertext.

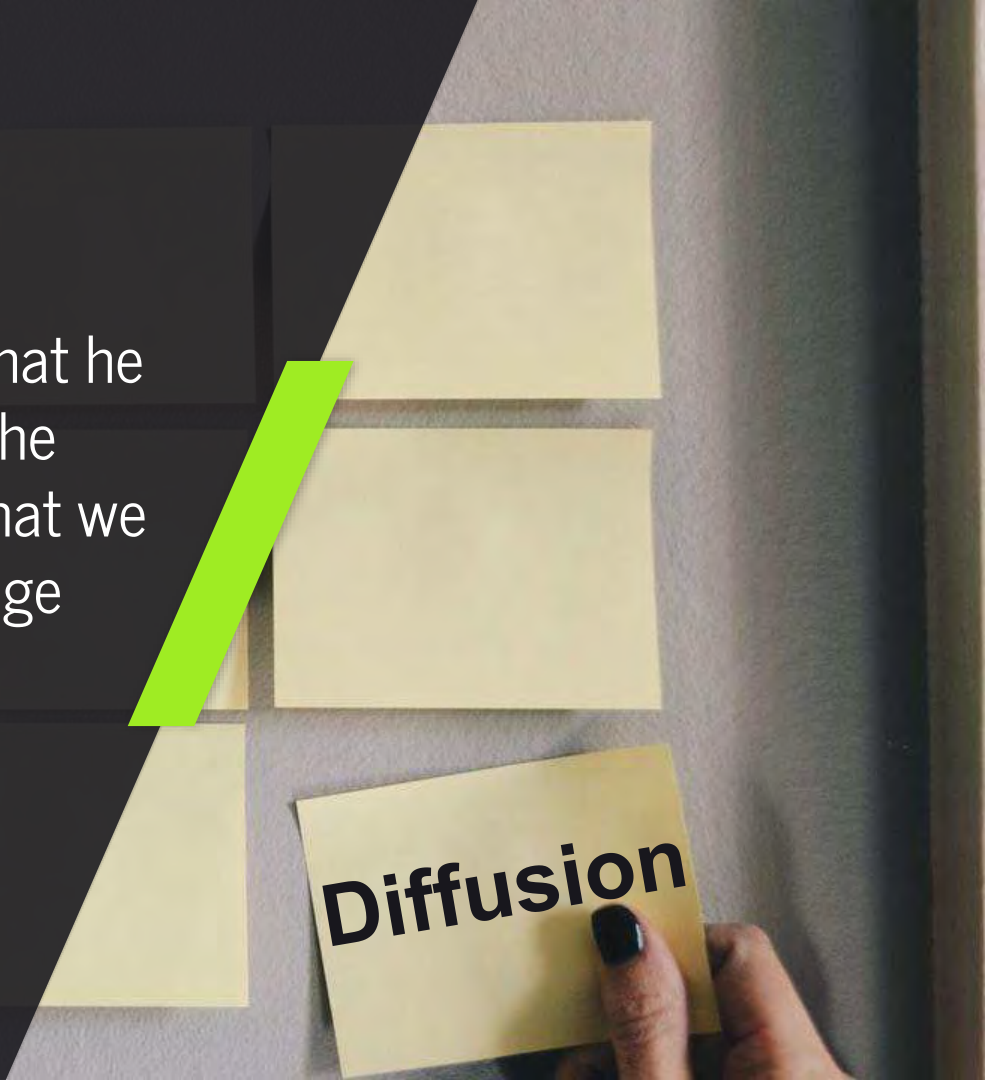
To understand the idea of diffusion assume $M=m_1\ m_2\ldots$, then we pick an integer s and replace m by the sequence $y_1\ y_2\ldots$ where

$$y_n = \sum_{i=0}^{s-1} m_{n+i} \mod 26$$

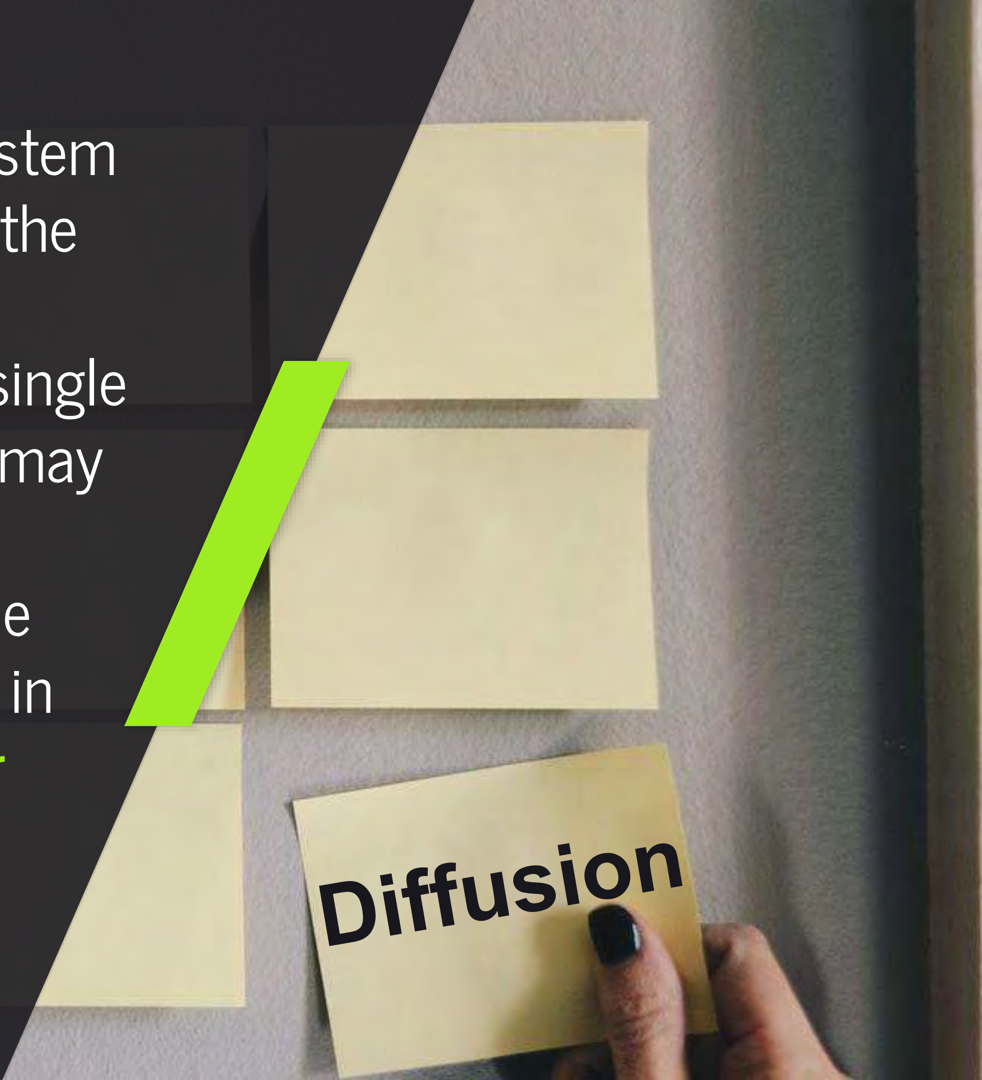
Where n=1, 2, 3,... By doing this we'll get the message space with letter frequencies of the new message space Y will become more equal than in M.



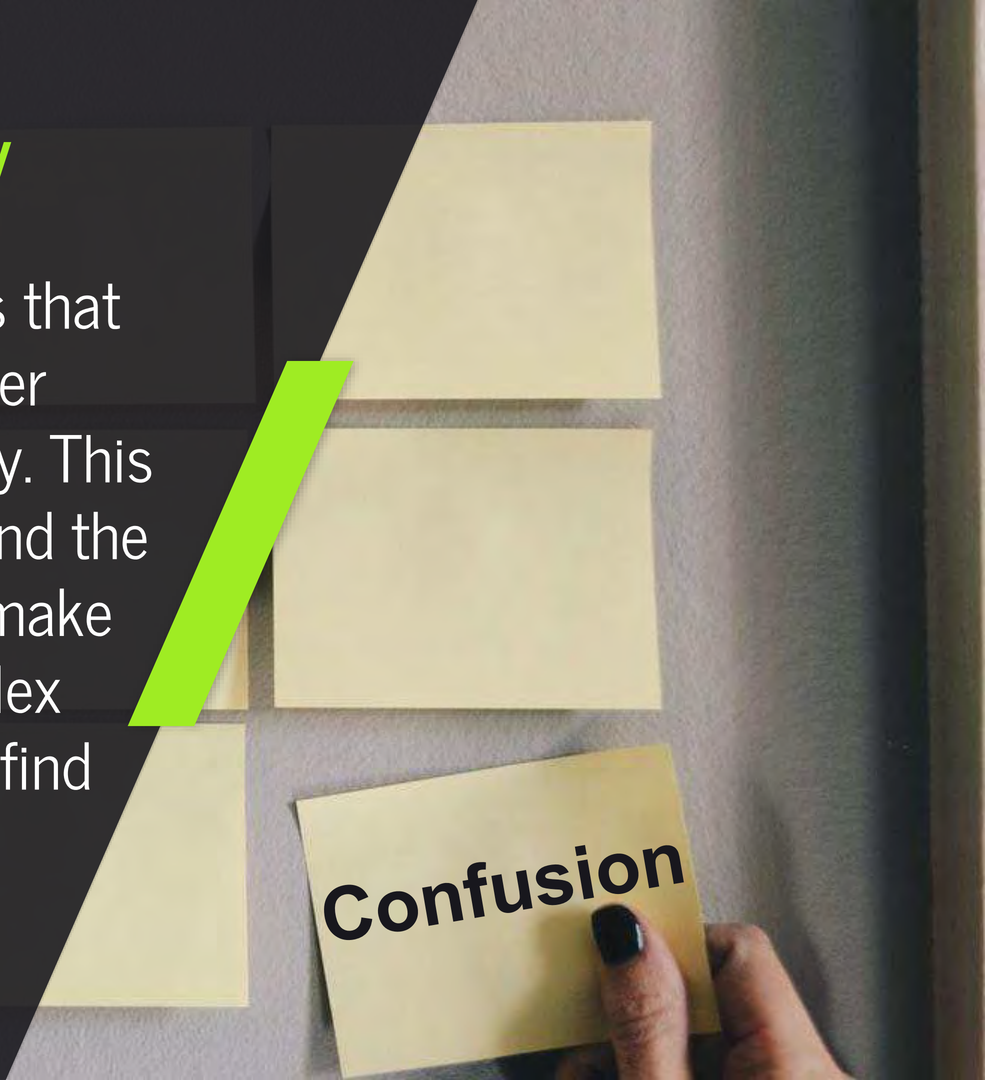
The effect of all this is that the **cryptanalyst needs along time** so that he can find a certain way to decipher the ciphertext. In practice this means that we are enciphering a number of message characters **simultaneously and dependently**.



The disadvantage of this type of system is that, at the receiver, each part of the message depends on a number of ciphertext characters. Thus, if one single ciphertext is error transmitted, this may cause many errors in the received message. This diffusing effect of one error in transmission causing many in decipherment is usually called error propagation.



The idea of confusion is to **hide any relationship between the plaintext, ciphertext and the key**. This implies that the message characters will encipher depending on virtually the entire key. This idea will force the cryptanalyst to find the whole key simultaneously and will make him solve considerably more complex equation than when he was able to find the key piece by piece.



Shannon’s Five Criteria

Shannon suggests five important criteria to evaluate the cipher systems, which are:

The amount of secrecy offered

It is clear that any system has a higher security will be superior than any other system. If the system theoretically can be broken, it might, practically impossible to do so; because there might not be a certain way to analyze the code so that an intruder can't take the original plaintext from the ciphertext.

1

The size of the key

Some of cipher systems generate a key space i.e. it take all the possibilities of the keys that may solve the problem.

2

The simplicity of the enciphering and deciphering operations

A good cipher system has to have a simple encipher and decipher algorithms but the analysis of the key has to be a very complicated one;

i.e. the time taken to encipher and decipher the message must be a polynomial time while the time taken by the cryptanalyst to break the message must be an exponential time.

3

In many ciphering systems, the error might be propagate and damage or garbled the information, hence we have cut this propagation of errors

The propagation of errors

4

If the message being a very long, it might be broken, hence the cipher system has to be unbreakable in spite of the massage is long.

Extension of the message

5

Concept of Randomness

Let $S = s_0, s_1, s_2, \ldots$ be an infinite sequence. The subsequence consisting of the first n terms of s is denoted by $S^n = s_0, s_1, \ldots, s_{n-1}$.

Example:

S=afrsgwfsvdsw...

S^5=afrsg

S^7=afrsgwf

Sequences

Let $S = s_0, s_1, s_2, \ldots$ be an infinite sequence. The subsequence consisting of the first n terms of s is denoted by $S^n = s_0, s_1, \ldots, s_n$.

Example:

$S=0110101100101\ldots$

$S^3=011$

$S^6=011010$

Sequences

The sequence $s = s_0, s_1, s_2, \ldots$ is said to be ***N-periodic*** if $s_i = s_{i+N}$ for all $i \geq 0$.

1001010010100101001010...

Periodic Sequences

The sequence $s = s_0, s_1, s_2, \ldots$ is said to be ***N-periodic*** if $s_i = s_{i+N}$ for all $i \geq 0$.

5-periodic **period=5**

1001010010100101001010...

The sequence s is periodic if it is N-periodic for some positive integer N.

The period of a periodic sequence s is the smallest positive integer N for which s is N-periodic.

Periodic Sequences

The sequence $s = s_0, s_1, s_2, \ldots$ is said to be ***N-periodic*** if $s_i = s_{i+N}$ for all $i \geq 0$.

5-periodic **period=5**

1001010010100101001010...

If s is a periodic sequence of period N, then the cycle of s is the subsequence s^N .

10010

Periodic Sequences

Run , Gap & Block

11011001000100000011

Run

11 0 11 00 1 000 1 0000 11

Gap

11 0 11 00 1 000 1 0000 11

Block

11 0 11 00 1 000 1 0000 11

Autocorrelation function

$$C(t) = \frac{1}{N}\sum_{i=0}^{N-1}(2s_i - 1)\cdot(2s_{i+t} - 1), \quad \text{for } 0 \le t \le N-1.$$

Example:

Consider the following sequence: 0101101011010110101101011

As we see N=5, s^N=01011

S_0= 0 1 0 1 1

S_1= 1 0 1 1 0

S_2= 0 1 1 0 1

S_3= 1 1 0 1 0

S_4= 1 0 1 0 1

$$C(t) = \frac{1}{N}\sum_{i=0}^{N-1}(2s_i - 1)\cdot(2s_{i+t} - 1), \quad \text{for } 0 \le t \le N-1.$$

$$c(t) = \frac{1}{5}\sum_{i=0}^{4}(2s_i - 1)(2s_{i+t} - 1)$$

$$c(t) = \frac{1}{5}[(2s_0 - 1)(2s_{0+t} - 1) + (2s_1 - 1)(2s_{1+t} - 1) +$$
$$(2s_2 - 1)(2s_{2+t} - 1) + (2s_3 - 1)(2s_{3+t} - 1) +$$
$$(2s_4 - 1)(2s_{4+t} - 1)]$$

$$\boxed{C(t) = \frac{A-D}{N}, \quad 0 \le t \le N-1}$$

Autocorrelation function

$$C(t)=\frac{1}{N}\sum_{i=0}^{N-1}(2s_i-1)\cdot(2s_{i+t}-1),\quad \text{for } 0\le t\le N-1.$$

Example:

Consider the following sequence: 0101101011010110101101011

As we see N=5, s^N=01011

S_0= 0 1 0 1 1

S_1= 1 0 1 1 0

S_2= 0 1 1 0 1

S_3= 1 1 0 1 0

S_4= 1 0 1 0 1

(1)

S = 0 1 0 1 1

S_0= 0 1 0 1 1

A=5, D=0

$$\Rightarrow c(0)=\frac{5-0}{5}=1$$

Autocorrelation
function

$$C(t) = \frac{1}{N}\sum_{i=0}^{N-1}(2s_i - 1)\cdot(2s_{i+t} - 1), \quad \text{for } 0 \le t \le N-1.$$

Example:

Consider the following sequence: 0101101011010110101101011

As we see N=5, s^N=01011

S_0= 0 1 0 1 1

S_1= 1 0 1 1 0

S_2= 0 1 1 0 1

S_3= 1 1 0 1 0

S_4= 1 0 1 0 1

(2)

S = 0 1 0 1 1

S_1= 1 0 1 1 0

A=1, D=4

$$\Rightarrow c(1) = \frac{1-4}{5} = -\frac{3}{5}$$

Autocorrelation function

$$C(t)=\frac{1}{N}\sum_{i=0}^{N-1}(2s_i-1)\cdot(2s_{i+t}-1),\quad \text{for } 0\le t\le N-1.$$

Example:

Consider the following sequence: 0101101011010110101101011

As we see N=5, s^N=01011

S_0= 0 1 0 1 1

S_1= 1 0 1 1 0

S_2= 0 1 1 0 1

S_3= 1 1 0 1 0

S_4= 1 0 1 0 1

(3)

S = 0 1 0 1 1

S_2= 0 1 1 0 1

A=3, D=2

$$\Rightarrow c(2)=\frac{3-2}{5}=\frac{1}{5}$$

Autocorrelation function

$$C(t) = \frac{1}{N}\sum_{i=0}^{N-1}(2s_i - 1)\cdot(2s_{i+t} - 1), \quad \text{for } 0 \le t \le N-1.$$

Example:

Consider the following sequence: **0101101011010110101101011**

As we see N=5, s^N=01011

S_0= 0 1 0 1 1

S_1= 1 0 1 1 0

S_2= 0 1 1 0 1

S_3= 1 1 0 1 0

S_4= 1 0 1 0 1

(4)

S = 0 1 0 1 1

S_3= 1 1 0 1 0

A=3, D=2

$$\Rightarrow c(3) = \frac{3-2}{5} = \frac{1}{5}$$

Autocorrelation function

$$C(t)=\frac{1}{N}\sum_{i=0}^{N-1}(2s_i-1)\cdot(2s_{i+t}-1),\quad \text{for } 0\le t\le N-1.$$

Example:

Consider the following sequence: 01011010110101101011 01011

As we see N=5, s^N=01011

S_0= 0 1 0 1 1

S_1= 1 0 1 1 0

S_2= 0 1 1 0 1

S_3= 1 1 0 1 0

S_4= 1 0 1 0 1

(5)

S = 0 1 0 1 1

S_4= 1 0 1 0 1

A=1, D=4

$$\Rightarrow c(4)=\frac{1-4}{5}=-\frac{3}{5}$$

Autocorrelation function

Golomb's Randomness Postulates

Let s be a periodic sequence of period N. *Golomb's randomness postulates* are the following.

R1

In the cycle s^N of s, the number of 1's differs from the number of 0's by at most 1. In other word if N is an even number then the number of 1's and 0's are equal, while if N is an odd number, then the number of 1's either more by one or less by one than the number of 0's.

For example

if the length of the sequence is 80 then

no. of 1: 40 and no. of 0: 40

if the length of the sequence is 81 then

Either: no. of 1: 40 and no. of 0: 41

Or: no. of 1: 41 and no. of 0: 40

Let s be a periodic sequence of period N. *Golomb's randomness postulates* are the following.

R2 In the cycle s^N, at least half the runs have length 1, at least one-fourth have length 2, at least one-eighth have length 3, in general, at least $1/2^i$ have length i. Moreover, for each of these lengths, there are (almost) equally many gaps and blocks.

Length of Run	Quantity
1	$\frac{1}{2}$ Runs
2	$\frac{1}{4}$ Runs
3	$\frac{1}{8}$ Runs
⋮	⋮
n	$\frac{1}{2^n}$ Runs

Let s be a periodic sequence of period N. *Golomb's randomness postulates* are the following.

R3

The autocorrelation function C(t) is two-valued. That is for some integer K,

$$N \cdot C(t) = \sum_{i=0}^{N-1} (2s_i - 1) \cdot (2s_{i+t} - 1) = \begin{cases} N, & \text{if } t = 0, \\ K, & \text{if } 1 \le t \le N-1. \end{cases}$$

A binary sequence which satisfies Golomb's randomness postulates is called a ***pseudo-noise sequence*** or a ***pn-sequence***.

Golomb's randomness postulates are **necessary** conditions for a periodic pseudo random sequence to look random, but they are not **sufficient**.

Consider the periodic sequence s of period N = 15 with cycle

$$s^{15} = 0\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 1$$

The following shows that the sequence s satisfies Golomb's randomness postulates.

Example

pn-sequence

Consider the periodic sequence s of period N = 15 with cycle

$$s^{15} = 0\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 1$$

The following shows that the sequence s satisfies Golomb's randomness postulates.

R1: The number of 0's in s^{15} is 7, while the number of 1's is 8.

Example

pn-sequence

Consider the periodic sequence s of period N = 15 with cycle

$$s^{15} = \underline{0}\ \underline{1\ 1}\ \underline{0\ 0}\ \underline{1}\ \underline{0\ 0\ 0}\ \underline{1\ 1\ 1\ 1}\ \underline{0}\ \underline{1}$$

The following shows that the sequence s satisfies Golomb's randomness postulates.

R2: s^{15} has 8 runs. There are 4 runs of length 1 (2 gaps and 2 blocks), 2 runs of length 2 (1 gap and 1 block), 1 run of length 3 (1 gap), and 1 run of length 4 (1 block).

Example

pn-sequence

Consider the periodic sequence s of period N = 15 with cycle

$$s^{15} = \underline{0}\ 1\ 1\ 0\ 0\ \underline{1}\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ \underline{0}\ \underline{1}$$

The following shows that the sequence s satisfies Golomb's randomness postulates.

R2: s^{15} has 8 runs. There are 4 runs of length 1 (2 gaps and 2 blocks), 2 runs of length 2 (1 gap and 1 block), 1 run of length 3 (1 gap), and 1 run of length 4 (1 block).

Example
pn-sequence

Consider the periodic sequence s of period N = 15 with cycle

$$s^{15} = 0\ \underline{1\ 1}\ \underline{0\ 0}\ 1\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 1$$

The following shows that the sequence s satisfies Golomb's randomness postulates.

R2: s^{15} has 8 runs. There are 4 runs of length 1 (2 gaps and 2 blocks), 2 runs of length 2 (1 gap and 1 block), 1 run of length 3 (1 gap), and 1 run of length 4 (1 block).

Example

pn-sequence

Consider the periodic sequence s of period N = 15 with cycle

$$s^{15} = 0\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 1$$

The following shows that the sequence s satisfies Golomb's randomness postulates.

R2: s^{15} has 8 runs. There are 4 runs of length 1 (2 gaps and 2 blocks), 2 runs of length 2 (1 gap and 1 block), 1 run of length 3 (1 gap), and 1 run of length 4 (1 block).

Example
pn-sequence

Consider the periodic sequence s of period N = 15 with cycle

$$s^{15} = 0\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 0\ \underline{1\ 1\ 1\ 1}\ 0\ 1$$

The following shows that the sequence s satisfies Golomb's randomness postulates.

R2: s^{15} has 8 runs. There are 4 runs of length 1 (2 gaps and 2 blocks), 2 runs of length 2 (1 gap and 1 block), 1 run of length 3 (1 gap), and 1 run of length 4 (1 block).

Example

pn-sequence

Consider the periodic sequence s of period N = 15 with cycle

$$s^{15} = 0\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 1$$

The following shows that the sequence s satisfies Golomb's randomness postulates.

R3: The autocorrelation function C(t) takes on two values:

$$C(0)=1 \text{ and}$$
$$C(t) = -\frac{1}{15} \qquad 1 \le t \le 14.$$

Hence, s is a pn-sequence.

Example
pn-sequence

THANK YOU

Any questions?

You can find me at:

saad.m@sc.uobaghdad.edu.iq

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

Frequency Test

Frequency Test

1110001100010001010011101111001001001001

1110001100010001010011101111001001001001

1110001100010001010011101111001001001001

1110001100010001010011101111001001001001

$n_0=84$ $n_1=76$

Example 1

Frequency Test

$n_0=84$ $n_1=76$ $n=160$

(i) (frequency test) $n_0=84$, $n_1=76$, and the value of the statistic X_1 is 0.4.

$$X_1 = \frac{(n_0 - n_1)^2}{n}$$

$$X_1 = \frac{(84-76)^2}{160} = 0.4.$$

Example 1

χ^2 (chi-square) distribution

v	α 0.100	0.050	0.025	0.010	0.005	0.001
1	2.7055	3.8415	5.0239	6.6349	7.8794	10.8276
2	4.6052	5.9915	7.3778	9.2103	10.5966	13.8155
3	6.2514	7.8147	9.3484	11.3449	12.8382	16.2662
4	7.7794	9.4877	11.1433	13.2767	14.8603	18.4668
5	9.2364	11.0705	12.8325	15.0863	16.7496	20.5150
6	10.6446	12.5916	14.4494	16.8119	18.5476	22.4577
7	12.0170	14.0671	16.0128	18.4753	20.2777	24.3219
8	13.3616	15.5073	17.5345	20.0902	21.9550	26.1245
9	14.6837	16.9190	19.0228	21.6660	23.5894	27.8772
10	15.9872	18.3070	20.4832	23.2093	25.1882	29.5883
11	17.2750	19.6751	21.9200	24.7250	26.7568	31.2641
12						95
13						82
14						33
15						73
16	23.5418	26.2962	28.8454	31.9999	34.2672	39.2524

Frequency Test: degree of freedom *v*=1

Example 1

Serial Test

Serial Test

1110001100010001010011101111001001001001
1110001100010001010011101111001001001001
1110001100010001010011101111001001001001
1110001100010001010011101111001001001001

$n_0=84$ $n_1=76$

Example 1

Serial Test

1110001100010001010011101111001001001001

1110001100010001010011101111001001001001

1110001100010001010011101111001001001001

1110001100010001010011101111001001001001

$n_0=84$ $n_1=76$

Example 1

Serial Test

1110001100010001010011101111001001001001

1110001100010001010011101111001001001001

1110001100010001010011101111001001001001

1110001100010001010011101111001001001001

$n_0=84$ $n_1=76$

Example 1

Serial Test

1110001100010001010011101111001001001001
1110001100010001010011101111001001001001
1110001100010001010011101111001001001001
1110001100010001010011101111001001001001

$n_0=84$ $n_1=76$

Example 1

Serial Test

1110001100010001010011101111001001001001
1110001100010001010011101111001001001001
1110001100010001010011101111001001001001
1110001100010001010011101111001001001001

n_0=84 n_1=76

Example 1

Serial Test

111000011000100010100111011111001001001001

111000011000100010100111011111001001001001

111000011000100010100111011111001001001001

111000011000100010100111011111001001001001

n_0=84 n_1=76

Example 1

Serial Test

1110001100010001010011101111001001001001

1110001100010001010011101111001001001001

1110001100010001010011101111001001001001

1110001100010001010011101111001001001001

n_0=84 n_1=76

Example 1

Serial Test

111000110001000101001110111100100100 1001

1110001100010001010011101111001001001001

1110001100010001010011101111001001001001

1110001100010001010011101111001001001001

n_0=84 n_1=76

Example 1

Serial Test

1110001100010001010011101111001001001001
1110001100010001010011101111001001001001
1110001100010001010011101111001001001001
1110001100010001010011101111001001001001

$n_0=84 \quad n_1=76$

Example 1

Serial Test

1110001100010001010011101111001001001001

1110001100010001010011101111001001001001

1110001100010001010011101111001001001001

1110001100010001010011101111001001001001

n_0=84 n_1=76

Example 1

Serial Test

1110001100010001010011101111001001001001

1110001100010001010011101111001001001001

1110001100010001010011101111001001001001

1110001100010001010011101111001001001001

$n_0=84 \quad n_1=76$

Example 1

Serial Test

1110001100010001010011101111001001001001

1110001100010001010011101111001001001001

1110001100010001010011101111001001001001

1110001100010001010011101111001001001001

$n_{00}=44$

$n_0=84$ $n_1=76$

Example 1

Serial Test

11100011000100010100111011110010010010011
11100011000100010100111011110010010010011
11100011000100010100111011110010010010011
11100011000100010100111011110010010010011

$n_{00}=44$, $n_{01}=40$

$n_0=84$ $n_1=76$

Example 1

Serial Test

1110001100010001010011101111001001001001

1110001100010001010011101111001001001001

1110001100010001010011101111001001001001

1110001100010001010011101111001001001001

$n_{00}=44$, $n_{01}=40$, $n_{10}=40$

$n_0=84$ $n_1=76$

Example 1

Serial Test

1110001100010001010011101111001001001001
1110001100010001010011101111001001001001
1110001100010001010011101111001001001001
1110001100010001010011101111001001001001

$n_{00}=44$, $n_{01}=40$, $n_{10}=40$, $n_{11}=35$

$n_0=84$ $n_1=76$

Example 1

Serial Test

(ii) (serial test) n_{00}=44, n_{01}=40, n_{10}=40, n_{11}=35, and the value of the statistic X_2 is 0.6252.

$$X_2 = \frac{4}{n-1}\sum_{i=0}^{1}\sum_{j=0}^{1} n_{ij}^2 - \frac{2}{n}\sum_{i=0}^{1} n_i^2 + 1$$

$$= \frac{4}{n-1}\left(n_{00}^2 + n_{01}^2 + n_{10}^2 + n_{11}^2\right) - \frac{2}{n}\left(n_0^2 + n_1^2\right) + 1$$

$$= \frac{4}{159}\left(44^2 + 40^2 + 40^2 + 35^2\right) - \frac{2}{160}\left(84^2 + 76^2\right) + 1$$

$$= \frac{4}{159}(1936 + 1600 + 1600 + 1225) - \frac{2}{160}(7056 + 5776) + 1$$

$$= \frac{4}{159}(6361) - \frac{2}{160}(12832) + 1$$

$$= 160.0252 - 160.4 + 1 = 0.6252.$$

χ^2 (chi-square) distribution

v	α 0.100	0.050	0.025	0.010	0.005	0.001
1	2.7055	3.8415	5.0239	6.6349	7.8794	10.8276
2	4.6052	$\boxed{5.9915}$	7.3778	9.2103	10.5966	13.8155
3	6.2514	7.8147	9.3484	11.3449	12.8382	16.2662
4	7.7794	9.4877	11.1433	13.2767	14.8603	18.4668
5	9.2364	11.0705	12.8325	15.0863	16.7496	20.5150
6	10.6446	12.5916	14.4494	16.8119	18.5476	22.4577
7	12.0170	14.0671	16.0128	18.4753	20.2777	24.3219
8	13.3616	15.5073	17.5345	20.0902	21.9550	26.1245
9	14.6837	16.9190	19.0228	21.6660	23.5894	27.8772
10	15.9872	18.3070	20.4832	23.2093	25.1882	29.5883
11	17.2750	19.6751	21.9200	24.7250	26.7568	31.2641
12						95
13						82
14						33
15						73
16	23.5418	26.2962	28.8454	31.9999	34.2672	39.2524

Serial Test: degree of freedom *v*=2

Example 1

Poker Test

Poker Test

Let m be a positive integer such that $\left\lfloor \frac{n}{m} \right\rfloor \geq 5 \cdot 2^m$, and let $k = \left\lfloor \frac{n}{m} \right\rfloor$.

$\lfloor 10.5 \rfloor = 10$

$\lfloor 0.4 \rfloor = 0$

$\lfloor 8.9 \rfloor = 8$

$\lfloor 12.9999999999999999 \rfloor = 12$

Example 1

Poker Test

$$\left\lfloor \frac{n}{m} \right\rfloor \geq 5 \cdot 2^m$$

m=1	$\left\lfloor \frac{160}{1} \right\rfloor$=160	>	$5 \cdot 2^1$=10
m=2	$\left\lfloor \frac{160}{2} \right\rfloor$=80	>	$5 \cdot 2^2$=20
m=3	$\left\lfloor \frac{160}{3} \right\rfloor$=53	>	$5 \cdot 2^3$=40
m=4	$\left\lfloor \frac{160}{4} \right\rfloor$=40	<	$5 \cdot 2^4$=80

Example 1

Poker Test

Type of blocks of length 3

$$2^m$$

Example 1

Poker Test

Type of blocks of length 3

$$2^3$$

Example 1

Poker Test

Type of blocks of length 3

000
001
010
011
100
101
110
111

8

Example 1

Poker Test

111-000-110-001-000-101-001-110-111-100-100-100-100-1
11-100-011-000-100-010-100-111-011-110-010-010-010-01
1-110-001-100-010-001-010-011-101-111-001-001-001-001
-111-000-110-001-000-101-001-110-111-100-100-100-100-1

Example 1

Poker Test

111-000-110-001-000-101-001-110-111-100-100-100-100-1

11-100-011-000-100-010-100-111-011-110-010-010-010-01

1-110-001-100-010-001-010-011-101-111-001-001-001-001

-111-000-110-001-000-101-001-110-111-100-100-100-100-1

Example 1

Poker Test

111-000-110-001-000-101-001-110-111-100-100-100-100-1

11-100-011-000-100-010-100-111-011-110-010-010-010-01

1-110-001-100-010-001-010-011-101-111-001-001-001-001

-111-000-110-001-000-101-001-110-111-100-100-100-100-1

Example 1

Poker Test

Type of blocks of length 3

$n_{000} = 5$
$n_{001} = 10$
$n_{010} = 6$
$n_{011} = 4$
$n_{100} = 12$
$n_{101} = 3$
$n_{110} = 6$
$n_{111} = 7$

Example 1

Poker Test

Here m=3 and k=53. The blocks 000, 001, 010, 011, 100, 101, 110, 111 appear 5, 10, 6, 4, 12, 3, 6,and 7 times, respectively, and the value of the statistic X_3 is 9.6415.

$$X_3 = \frac{2^m}{k}\left(\sum_{i=1}^{2^m} n_i^2\right) - k$$

$$X_3 = \frac{2^3}{53}(5^2 + 10^2 + 6^2 + 4^2 + 12^2 + 3^2 + 6^2 + 7^2) - 53$$

$$= \frac{8}{53}(25 + 100 + 36 + 16 + 144 + 9 + 36 + 49) - 53 = 9.6415$$

Example 1

χ^2 (chi-square) distribution

v	α 0.100	0.050	0.025	0.010	0.005	0.001
1	2.7055	3.8415	5.0239	6.6349	7.8794	10.8276
2	4.6052	5.9915	7.3778	9.2103	10.5966	13.8155
3	6.2514	7.8147	9.3484	11.3449	12.8382	16.2662
4	7.7794	9.4877	11.1433	13.2767	14.8603	18.4668
5	9.2364	11.0705	12.8325	15.0863	16.7496	20.5150
6	10.6446	12.5916	14.4494	16.8119	18.5476	22.4577
7	12.0170	14.0671	16.0128	18.4753	20.2777	24.3219
8	13.3616	15.5073	17.5345	20.0902	21.9550	26.1245
9	14.6837	16.9190	19.0228	21.6660	23.5894	27.8772
10	15.9872	18.3070	20.4832	23.2093	25.1882	29.5883
11	17.2750	19.6751	21.9200	24.7250	26.7568	31.2641
12	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]95
13	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]82
14	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]33
15	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]73
16	23.5418	26.2962	28.8454	31.9999	34.2672	39.2524

Poker Test: degree of freedom $v=2^m-1$

Example 1

Runs Test

Runs Test

$$X_4 = \sum_{i=1}^{k} \frac{(B_i - e_i)^2}{e_i} + \sum_{i=1}^{k} \frac{(G_i - e_i)^2}{e_i}$$

$$e_i = \frac{(n - i + 3)}{2^{i+2}} \geq 5$$

Example 1

Runs Test

i	$e_i=(n-i+3)/2^{i+2}$		
1	$(160-1+3)/2^3=\frac{162}{8}=20.25$	>	5
2	$(160-2+3)/2^4=\frac{161}{16}=10.0625$	>	5
3	$(160-3+3)/2^5=\frac{160}{32}=5$	=	5
4	$(160-4+3)/2^6=\frac{159}{64}=2.4843$	<	5

Example 1

Runs Test

11100001100010001010011101111001001001001

11100001100010001010011101111001001001001

11100001100010001010011101111001001001001

11100001100010001010011101111001001001001

$B_1=25$

Example 1

Runs Test

1110001100010001010011101111001001001001

1110001100010001010011101111001001001001

1110001100010001010011101111001001001001

1110001100010001010011101111001001001001

$B_1=25$ $B_2=4$

Example 1

Runs Test

111000110001000101001110111100100100 1001

1110001100010001010011101111001001001001

1110001100010001010011101111001001001001

1110001100010001010011101111001001001001

B_1=25 B_2=4 B_3=5

Example 1

Runs Test

1110001100010001010011101111001001001001

1110001100010001010011101111001001001001

1110001100010001010011101111001001001001

1110001100010001010011101111001001001001

B_1=25 B_2=4 B_3=5

G_1=8

Example 1

Runs Test

11100011000100010100111011110010010011001

11100011000100010100111011110010010011001

11100011000100010100111011110010010011001

11100011000100010100111011110010010011001

$B_1=25$ $B_2=4$ $B_3=5$

$G_1=8$ $G_2=20$

Example 1

Runs Test

111000110001000101001110111100100100100

111000110001000101001110111100100100100

111000110001000101001110111100100100100

111000110001000101001110111100100100100

B_1=25 B_2=4 B_3=5

G_1=8 G_2=20 G_3=12

Example 1

Runs Test

Here k=3. There are 25, 4, 5 blocks of lengths 1, 2, 3, respectively, and 8, 20, 12 gaps of lengths 1, 2, 3, respectively. The value of the statistic X_4 is 31.7913.

$$X_4 = \sum_{i=1}^{k} \frac{(B_i - e_i)^2}{e_i} + \sum_{i=1}^{k} \frac{(G_i - e_i)^2}{e_i}$$

$$X_4 = \frac{(B_1 - e_1)^2}{e_1} + \frac{(B_2 - e_2)^2}{e_2} + \frac{(B_3 - e_3)^2}{e_3} + \frac{(G_1 - e_1)^2}{e_1} + \frac{(G_2 - e_2)^2}{e_2} + \frac{(G_3 - e_3)^2}{e_3}$$

$$X_4 = \frac{(25 - 20.25)^2}{20.25} + \frac{(4 - 10.0625)^2}{10.0625} + \frac{(5 - 5)^2}{5} + \frac{(8 - 20.25)^2}{20.25} + \frac{(20 - 10.0625)^2}{10.0625} + \frac{(12 - 5)^2}{5}$$

$$X_4 = 31.7913.$$

Example 1

χ^2 (chi-square) distribution

v	α = 0.100	0.050	0.025	0.010	0.005	0.001
1	2.7055	3.8415	5.0239	6.6349	7.8794	10.8276
2	4.6052	5.9915	7.3778	9.2103	10.5966	13.8155
3	6.2514	7.8147	9.3484	11.3449	12.8382	16.2662
4	7.7794	9.4877	11.1433	13.2767	14.8603	18.4668
5	9.2364	11.0705	12.8325	15.0863	16.7496	20.5150
6	10.6446	12.5916	14.4494	16.8119	18.5476	22.4577
7	12.0170	14.0671	16.0128	18.4753	20.2777	24.3219
8	13.3616	15.5073	17.5345	20.0902	21.9550	26.1245
9	14.6837	16.9190	19.0228	21.6660	23.5894	27.8772
10	15.9872	18.3070	20.4832	23.2093	25.1882	29.5883
11	17.2750	19.6751	21.9200	24.7250	26.7568	31.2641
12	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]95
13	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]82
14	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]33
15	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]73
16	23.5418	26.2962	28.8454	31.9999	34.2672	39.2524

Runs Test: degree of freedom *v*=2k-2

Example 1

Results Discussion

χ^2 (chi-square) distribution

	α					
v	0.100	0.050	0.025	0.010	0.005	0.001
1	2.7055	3.8415	5.0239	6.6349	7.8794	10.8276
2	4.6052	5.9915	7.3778	9.2103	10.5966	13.8155
3	6.2514	7.8147	9.3484	11.3449	12.8382	16.2662
4	7.7794	9.4877	11.1433	13.2767	14.8603	18.4668
5	9.2364	11.0705	12.8325	15.0863	16.7496	20.5150
6	10.6446	12.5916	14.4494	16.8119	18.5476	22.4577
7	12.0170	14.0671	16.0128	18.4753	20.2777	24.3219
8	13.3616	15.5073	17.5345	20.0902	21.9550	26.1245
9	14.6837	16.9190	19.0228	21.6660	23.5894	27.8772
10	15.9872	18.3070	20.4832	23.2093	25.1882	29.5883

- 3.8415 (for one degree of freedom)
- 5.9915 (for two degree of freedom)
- 14.0671 (for seven degree of freedom, since $2^m-1=2^3-1=7$)
- 9.4877 (for four degree of freedom, since $2k-2=2(3)-2=4$

Example 1

Results Discussion

For a significance level of α =0.05, the threshold values for X_1, X_2, X_3, and X_4 are:

X_1=0.4 < 3.8415

X_2=0.6252 < 5.9915

X_3=9.6415 < 14.0671

X_4=31.7913 > 9.4877

Example 1

Results Discussion

Hence, the given sequence s passes the **frequency**, **serial**, and **poker** tests, but fails the **runs** test.

So, s is **not a pn-sequence** i.e. it is not random sequence

Example 1

Example 2

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

n=124

Example 2

Frequency Test

Frequency Test

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

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

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

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

$n=124$

$n_0=60$

Example 2

Frequency Test

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

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

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

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

$n=124$

$n_0=60$ $n_1=64$

Example 2

Frequency Test

(i) (frequency test) n_0=60, n_1=64, and the value of the statistic X_1 is 0.1290.

$$X_1 = \frac{(60-64)^2}{124} = 0.1290 < 3.84,$$

so the sequence pass this test.

Example 2

Serial Test

Serial Test

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

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

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

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

$n=124$

$n_0=60$ $n_1=64$

$n_{00}=27$

Example 2

Serial Test

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

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

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

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

$n=124$

$n_0=60$ $n_1=64$

$n_{00}=27$, $n_{01}=32$

Example 2

Serial Test

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

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

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

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

$n=124$

$n_0=60 \quad n_1=64$

$n_{00}=27$, $n_{01}=32$, $n_{10}=32$

Example 2

Serial Test

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

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

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

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

$n=124$

$n_0=60$ $n_1=64$

$n_{00}=27$, $n_{01}=32$, $n_{10}=32$, $n_{11}=32$

Example 2

Serial Test

$$X_2 = \frac{4}{n-1}\sum_{i=0}^{1}\sum_{j=0}^{1} n_{ij}^2 - \frac{2}{n}\sum_{i=0}^{1} n_i^2 + 1$$

(ii) (serial test) $n_{00}=27$, $n_{01}=32$, $n_{10}=32$, $n_{11}=32$, and the value of the statistic X_2 is

$$X_2 = \frac{4}{123}\left(27^2+32^2+32^2+32^2\right) - \frac{2}{124}\left(60^2+64^2\right)+1$$

$$= \frac{4}{123}(3801) - \frac{2}{124}(7696)+1$$

$$= 123.6097 - 124.1290 + 1 = 0.4807 < 5.99,$$

so the sequence pass this test also.

Example 2

Poker Test

Poker Test

m=1	$\left\lfloor \frac{124}{1} \right\rfloor = 124$	>	$5 \cdot 2^1 = 10$
m=2	$\left\lfloor \frac{124}{2} \right\rfloor = 62$	>	$5 \cdot 2^2 = 20$
m=3	$\left\lfloor \frac{124}{3} \right\rfloor = 41$	>	$5 \cdot 2^3 = 40$
m=4	$\left\lfloor \frac{124}{4} \right\rfloor = 31$	<	$5 \cdot 2^4 = 80$

Example 2

Poker Test

$$X_3 = \frac{2^m}{k}\left(\sum_{i=1}^{2^m} n_i^2\right) - k$$

Here m=3 and k=41.

010	101	110	110	001	111	100	110	100	100
001	010	111	011	000	111	110	011	010	010
000	101	011	101	100	011	111	001	101	001
000	010	101	110	110	001	111	100	110	100
100	0								

The blocks 000, 001, 010, 011, 100, 101, 110, 111 appear 3, 5, 5, 4, 7, 5, 7,and 5 times, respectively, and the value of the statistic X_3 is

$$X_3 = \frac{2^3}{41}(3^2+5^2+5^2+4^2+7^2+5^2+7^2+5^2)-41$$
$$= \frac{8}{41}(9+25+25+16+49+25+49+25)-41 = 2.5122$$

The degree of freedom here is 2^3-1=7, so χ^2=14.0671. And since 2.5122<14.0671, so the sequence pass this test also.

Example 2

Runs Test

Runs Test

i	$e_i=(n-i+3)/2^{i+2}$		
1	$(124-1+3)/2^3=\frac{126}{8}=15.75$	$>$	5
2	$(124-2+3)/2^4=\frac{125}{16}=7.8125$	$>$	5
3	$(124-3+3)/2^5=\frac{124}{32}=3.875$	$<$	5

Example 2

Runs Test

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

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

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

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

G_1=17

Example 2

Runs Test

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

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

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

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

$G_1=17$ $G_2=8$

Example 2

Runs Test

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

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

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

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

$G_1=17$ $G_2=8$

$B_1=16$

Example 2

Runs Test

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

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

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

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

$G_1=17$ $G_2=8$

$B_1=16$ $B_2=8$

Example 2

Runs Test

Here k=2.

i	B_i	G_i
1	16	17
2	8	8

There are 16, 8 blocks of lengths 1, 2, respectively, and 17, 8 gaps of lengths 1, 2, respectively. The value of the statistic X_4 is

$$X_4 = \frac{(B_1-e_1)^2}{e_1} + \frac{(B_2-e_2)^2}{e_2} + \frac{(G_1-e_1)^2}{e_1} + \frac{(G_2-e_2)^2}{e_2}$$

$$X_4 = \frac{(16-15.75)^2}{15.75} + \frac{(8-7.8125)^2}{7.8125} + \frac{(17-15.75)^2}{15.75} + \frac{(8-7.8125)^2}{7.8125}$$

$$X_4 = 0.11213.$$

The degree of freedom here is 2(2)-2=2, so χ^2=5.99. And since 0.11213<5.99, so the sequence pass this test also.

Example 2

Results Discussion

Results Discussion

Hence, the given sequence s passes the **frequency**, **serial**, **poker** and **runs** test.

So, s is **a pn-sequence** i.e. it is not random sequence

Example 1

THANK YOU

Any questions?

You can find me at:

saad.m@sc.uobaghdad.edu.iq

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

Unconditional Security

A cryptosystem is unconditionally secure if it cannot be broken even with infinite computational resources.

OTP

$|M| = |C| = |K|$

$m_i\,;\, c_i\,;\, z_i \in \{0,1\}$

Encryption: $c_i = e_{z_i}(m_i) = m_i \oplus z_i$

Decryption: $m_i = d_{z_i}(c_i) = c_i \oplus z_i$

XOR

a	b	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

Encryption and decryption are the same operation (XOR)

Decryption:

$c_i \oplus z_i$

Encryption and decryption are the same operation (XOR)

Decryption:

$$c_i \oplus z_i = (m_i \oplus z_i) \oplus z_i$$

Encryption and decryption are the same operation (XOR)

Decryption:

$c_i \oplus z_i = (m_i \oplus z_i) \oplus z_i = m_i \oplus (z_i \oplus z_i)$

Encryption and decryption are the same operation (XOR)

Decryption:

$$c_i \oplus z_i = (m_i \oplus z_i) \oplus z_i = m_i \oplus \overbrace{(z_i \oplus z_i)}^{0}$$

Since, $z_i \oplus z_i = 0$ for $z_i = 0$ and for $z_i = 1$

Encryption and decryption are the same operation (XOR)

Decryption:

$$c_i \oplus z_i = (m_i \oplus z_i) \oplus z_i = m_i \oplus \overbrace{(z_i \oplus z_i)}^{0} = m_i$$

Since, $z_i \oplus z_i = 0$ for $z_i = 0$ and for $z_i = 1$

Example

Example

Encryption of the letter A by Alice.

A is given in ASCII code as $65_{10} = 1000001_2$.

Let's assume that the first key stream bits are

$z_1, \ldots, z_7 = 0101101$

Decimal to Binary

65	
32	1
16	0
8	0
4	0
2	0
1	0

1000001

Example

Encryption by Alice:

Plaintext m_i : $\boxed{1}\boxed{0}\boxed{0}\boxed{0}\boxed{0}\boxed{0}\boxed{1}$ = A (ASCII symbol)

Key stream z_i: $\boxed{0}\boxed{1}\boxed{0}\boxed{1}\boxed{1}\boxed{0}\boxed{1}$

Ciphertext c_i : $\boxed{1}\boxed{1}\boxed{0}\boxed{1}\boxed{1}\boxed{0}\boxed{0}$ = ℓ (ASCII symbol)

Binary to Decimal

Remember:

$$5632$$

$$5000+600+30+2$$

$$5*1000+6*100+3*10+2*1$$

$$5*10^3+6*10^2+3*10^1+2*10^0$$

Binary to Decimal

In Binary System

1	1	0	1	1	0	0
2^6	2^5	2^4	2^3	2^2	2^1	2^0
64	32	16	8	4	2	1

Binary to Decimal

In Binary System

1	1	0	1	1	0	0

64	32	16	8	4	2	1

$$64 + 32 + 8 + 4 = 108$$

ASCII - Binary Character Table

Letter	ASCII Code	Binary	Letter	ASCII Code	Binary
a	097	01100001	A	065	01000001
b	098	01100010	B	066	01000010
c	099	01100011	C	067	01000011
d	100	01100100	D	068	01000100
e	101	01100101	E	069	01000101
f	102	01100110	F	070	01000110
g	103	01100111	G	071	01000111
h	104	01101000	H	072	01001000
i	105	01101001	I	073	01001001
j	106	01101010	J	074	01001010
k	107	01101011	K	075	01001011
l	108	01101100	L	076	01001100
m	109	01101101	M	077	01001101
n	110	01101110	N	078	01001110
o	111	01101111	O	079	01001111
p	112	01110000	P	080	01010000
q	113	01110001	Q	081	01010001
r	114	01110010	R	082	01010010
s	115	01110011	S	083	01010011
t	116	01110100	T	084	01010100
u	117	01110101	U	085	01010101
v	118	01110110	V	086	01010110
w	119	01110111	W	087	01010111
x	120	01111000	X	088	01011000
y	121	01111001	Y	089	01011001
z	122	01111010	Z	090	01011010

Example

Decryption by Bob:

Ciphertext c_i:

1	1	0	1	1	0	0

= ℓ (ASCII symbol)

Key stream z_i:

0	1	0	1	1	0	1

Plaintext m_i :

1	0	0	0	0	0	1

= A (ASCII symbol)

“

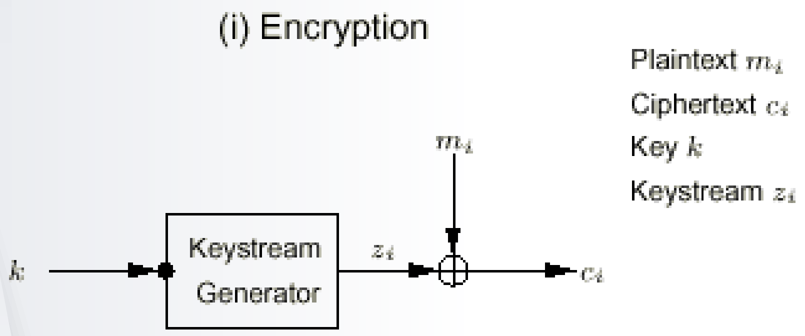
The OTP is unconditionally secure if keys are only used once.

1.

Synchronous Stream Ciphers

***Synchronous* Stream**

Cipher in which the **keystream** is generated **independently** of the **plaintext** and of the **ciphertext**.



General model of a binary additive synchronous stream cipher

Properties of synchronous stream ciphers

Synchronization requirements
Both the sender and receiver must be *synchronized* – using the same key and operating at the same position (state) within that key – to allow for proper decryption.

If synchronization is lost due to ciphertext digits being inserted or deleted during transmission, then decryption fails and can only be restored through additional techniques for re-synchronization.

Encryption

m_1	m_2	m_3	m_4	m_5	m_6	m_7	m_8	m_9	m_{10}

k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	k_9	k_{10}

c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9	c_{10}

Decryption

c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9	c_{10}

Encryption

m_1	m_2	m_3	m_4	m_5	m_6	m_7	m_8	m_9	m_{10}

k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	k_9	k_{10}

c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9	c_{10}

Decryption

c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9	c_{10}

Encryption

m_1	m_2	m_3	m_4	m_5	m_6	m_7	m_8	m_9	m_{10}
k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	k_9	k_{10}
c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9	c_{10}

Decryption

c_1	c_2	c_3	c_7	c_8	c_9	c_{10}	c_{11}	c_{12}	c_{13}
k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	k_9	k_{10}
m_1	m_2	m_3	x	x	x	x	x	x	x

Encryption

m_1	m_2	m_3	m_4	m_5	m_6	m_7	m_8	m_9	m_{10}

k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	k_9	k_{10}

c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9	c_{10}

Decryption

c_1	c_2	c_3	x	c_7	c_8	c_9	c_{10}	c_{11}	c_{12}

k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	k_9	k_{10}

m_1	m_2	m_3	x	x	x	x	x	x	x

Encryption

m_1	m_2	m_3	m_4	m_5	m_6	m_7	m_8	m_9	m_{10}
k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	k_9	k_{10}
c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9	c_{10}

Decryption

c_1	c_2	c_3	x	x	c_7	c_8	c_9	c_{10}	c_{11}
k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	k_9	k_{10}
m_1	m_2	m_3	x	x	x	x	x	x	x

Encryption

m_1	m_2	m_3	m_4	m_5	m_6	m_7	m_8	m_9	m_{10}
k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	k_9	k_{10}
c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9	c_{10}

Decryption

c_1	c_2	c_3	x	x	x	c_7	c_8	c_9	c_{10}
k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	k_9	k_{10}
m_1	m_2	m_3	x	x	x	x	x	x	x

Properties of synchronous stream ciphers

No error propagation
A ciphertext digit that is modified (but not deleted) during transmission does not affect the decryption of other ciphertext digits.

Encryption

m_1	m_2	m_3	m_4	m_5	m_6	m_7	m_8	m_9	m_{10}
k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	k_9	k_{10}
c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9	c_{10}

Decryption

c_1	c_2	c_3	c_4	x	c_6	c_7	c_8	c_9	c_{10}
k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	k_9	k_{10}
m_1	m_2	m_3	m_4	x	m_6	m_7	m_8	m_9	m_{10}

Properties of synchronous stream ciphers

Active attacks

Insertion, deletion, or replay of ciphertext digits by an active adversary causes immediate loss of synchronization, and hence might possibly be detected by the decryptor.

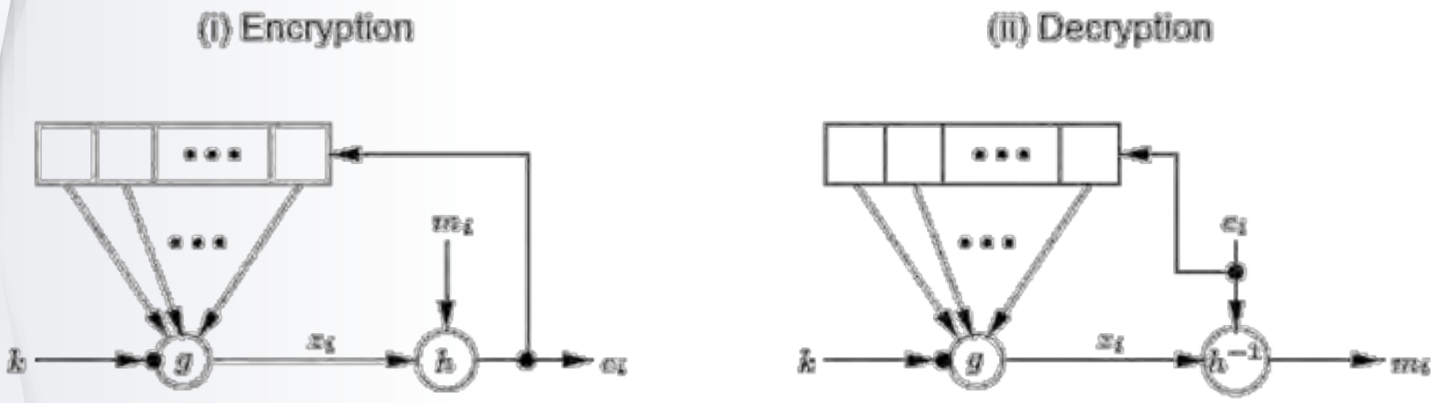
because the decryption mapping depends only on a fixed number of preceding ciphertext characters.

2. Asynchronous Stream Ciphers

Self-Synchronizing Stream Cipher

Asynchronous Stream

Cipher in which the **keystream** is generated as a function of the key and a fixed number of previous ciphertext digits.



General model of a self-synchronizing stream cipher

Properties of asynchronous stream ciphers

self-synchronization

Its capable of re-establishing proper decryption automatically after loss of synchronization, with only a fixed number of plaintext characters unrecoverable.

Properties of asynchronous stream ciphers

Limited error propagation
If a single ciphertext digit is modified (or even deleted or inserted) during transmission, then decryption of up to t subsequent ciphertext digits may be incorrect.

After which correct decryption resumes.

Properties of asynchronous stream ciphers

Active attacks

Modification of ciphertext digits by an active adversary causes several other ciphertext digits to be decrypted incorrectly. It is likelihood of being detected by the decryptor.

It is more difficult to detect insertion, deletion, or replay of ciphertext digits by an active adversary.

Properties of asynchronous stream ciphers

Diffusion of plaintext statistics

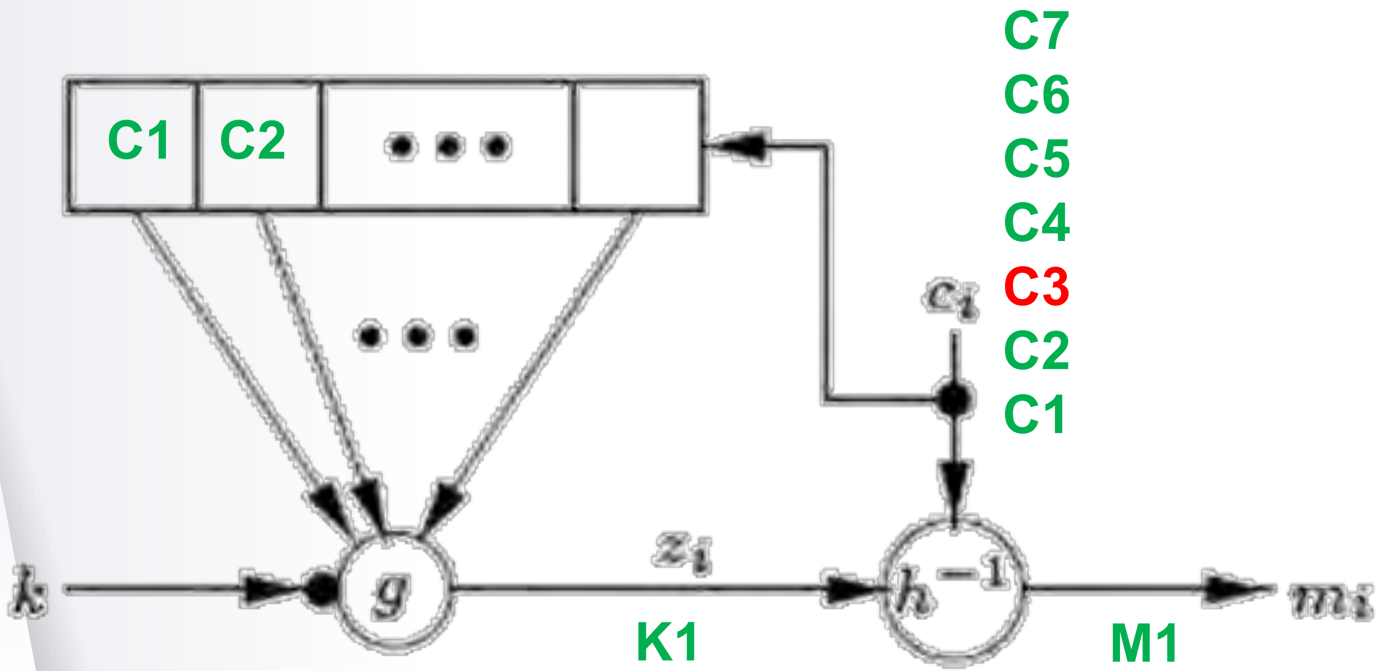
The statistical properties of the plaintext are dispersed through the ciphertext.

self-synchronizing stream ciphers may be more resistant than synchronous stream ciphers against attacks based on plaintext redundancy.

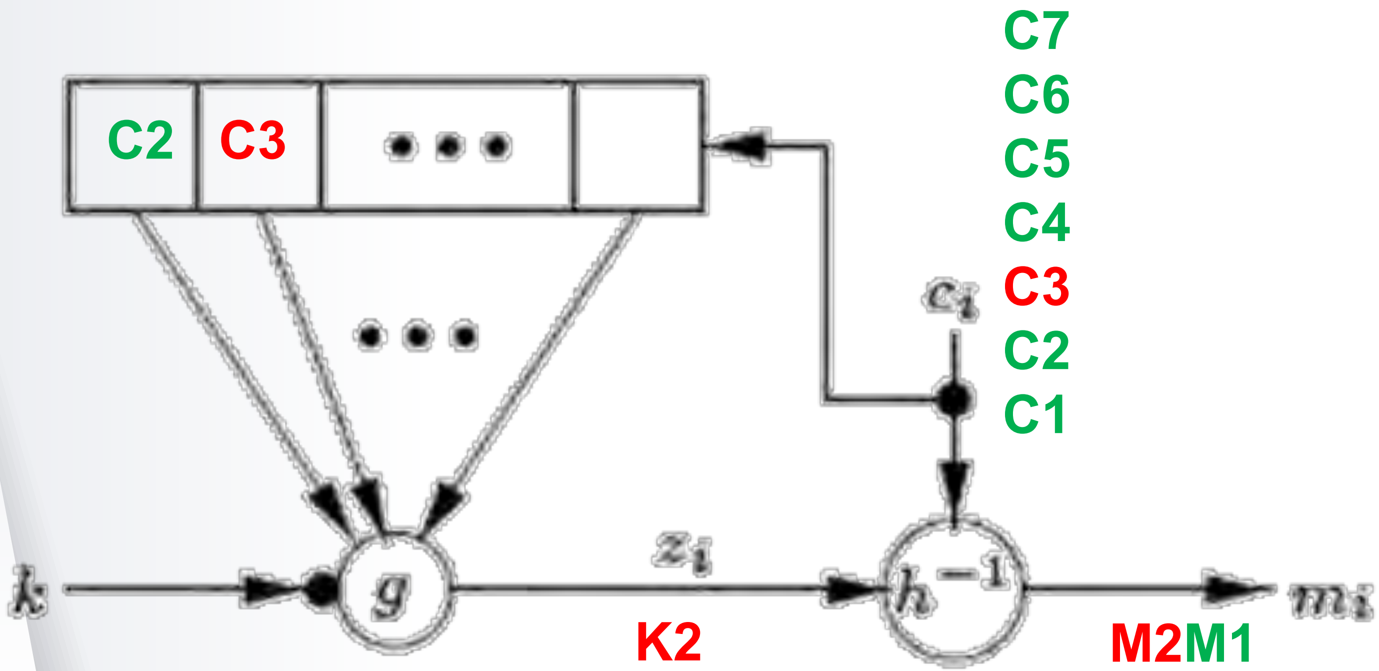
Decleration

for Asynchronous cipher

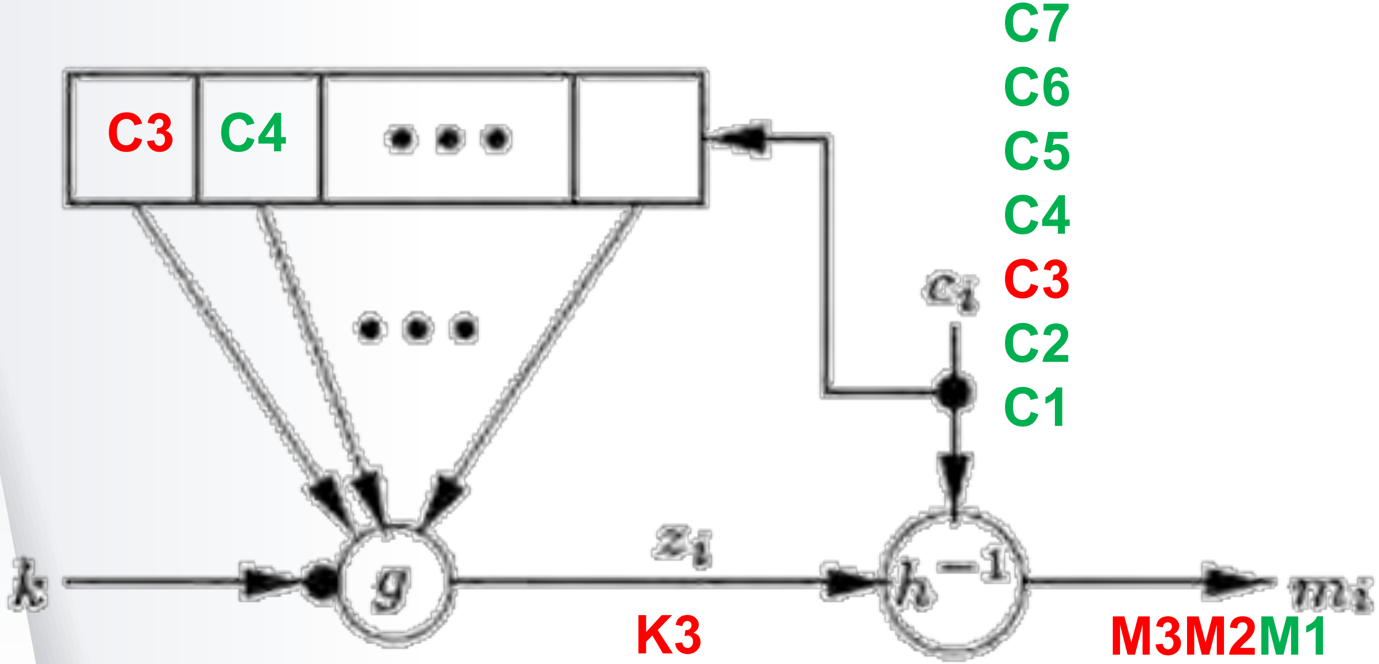
Decleration



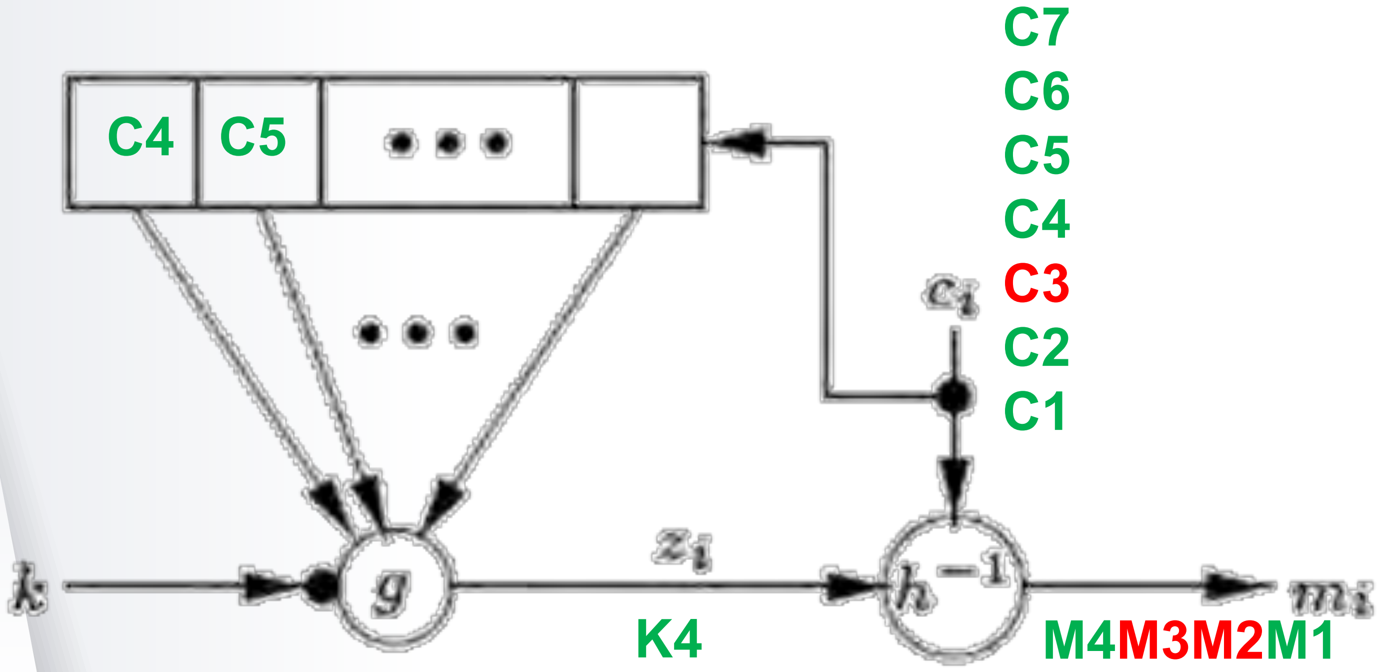
Decleration



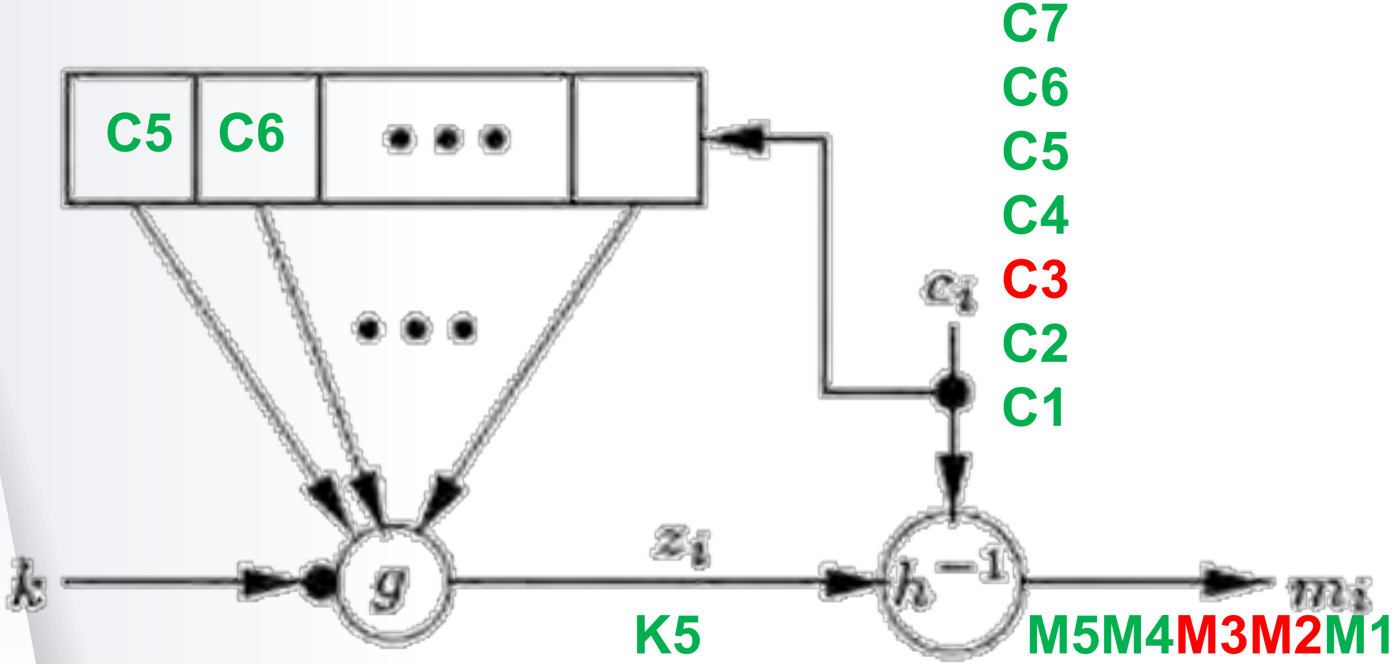
Decleration



Decleration



Decleration



THANK YOU

Any questions?

You can find me at:
saad.m@sc.uobaghdad.edu.iq

Saad Al-Momen

Stream Ciphers

10.

CIPHER SYSTEMS

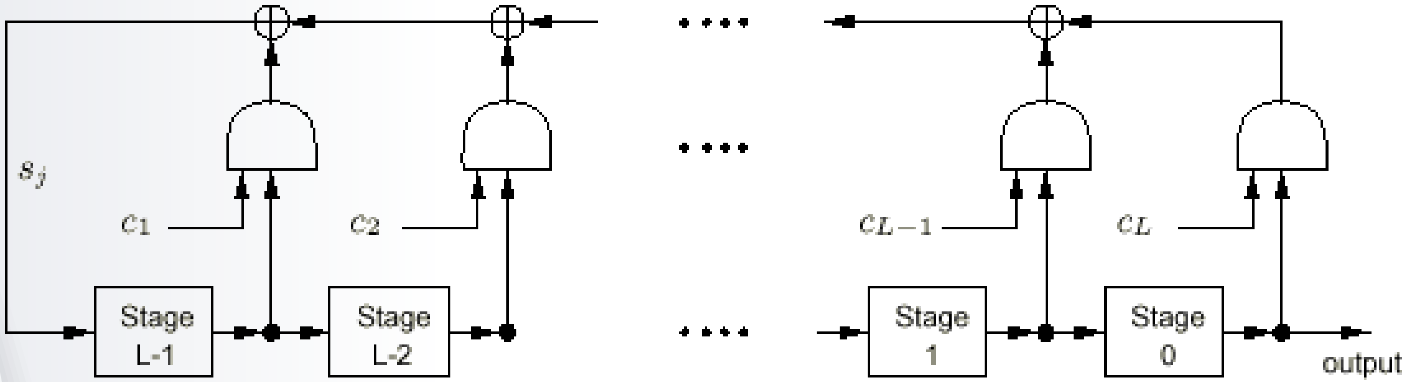
Fourth Class
Department of Mathematics
College of Science - University of Baghdad

Linear Feedback Shift Register (LFSR)

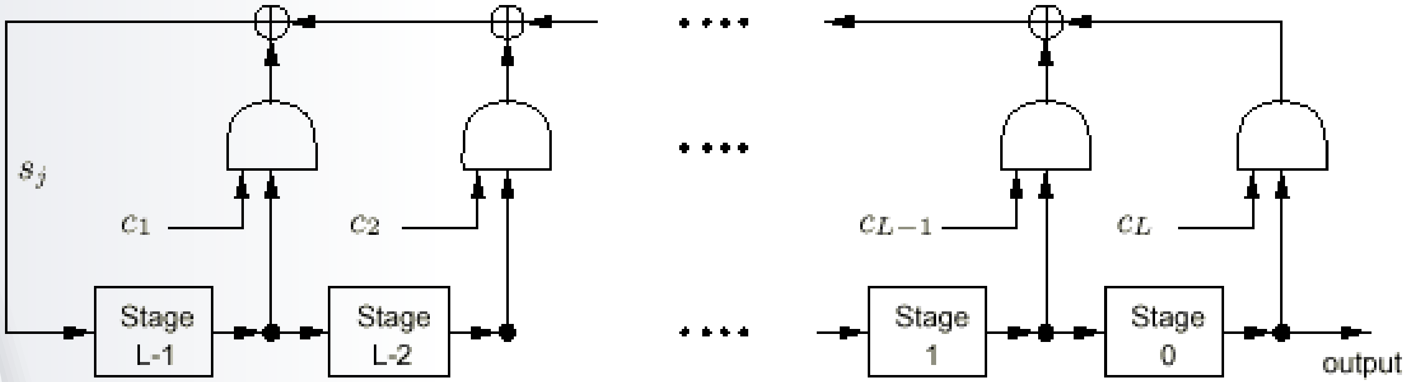
Linear Feedback Shift Register

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.

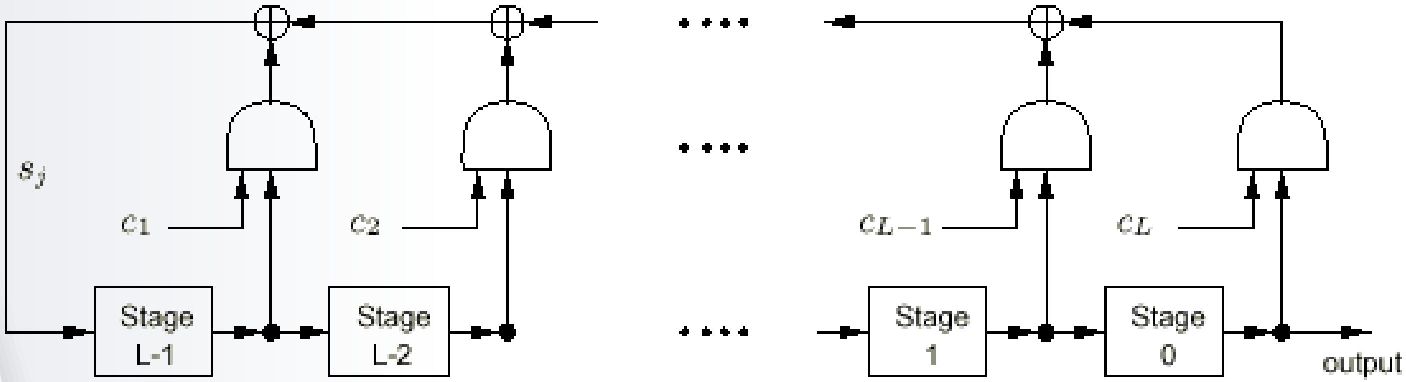
(i) The content of stage 0 is **output** and forms part of the *output sequence*.



(ii) The content of stage **i** is **moved** to stage **i-1** for each i. $1 \leq i \leq L-1$



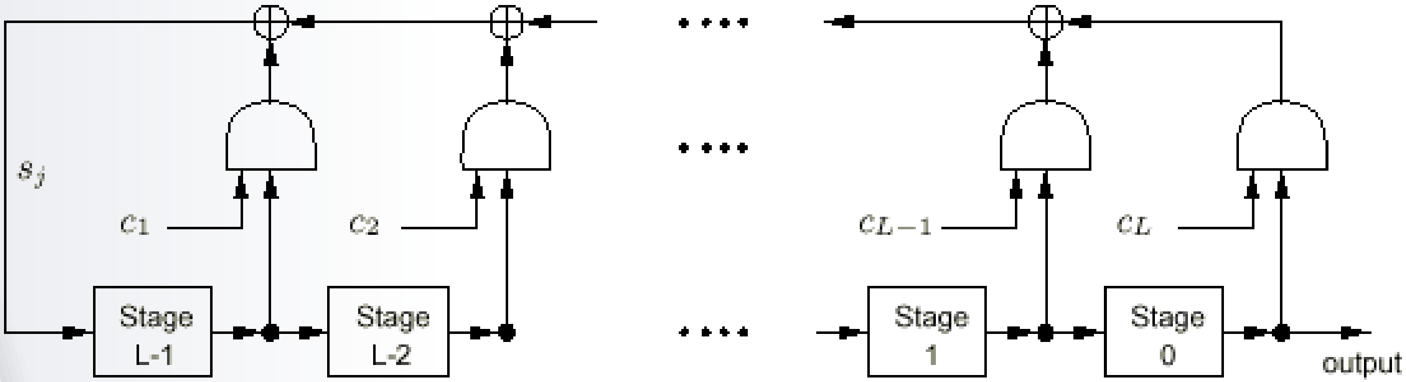
(iii) The new content of stage **L-1** is the *feedback bit* $\mathbf{s}_j$ which is **calculated** by adding together modulo 2 the previous contents of **a fixed subset of stages 0,1, ... ,L-1**.



The LFSR is denoted <L,C(D)>, where

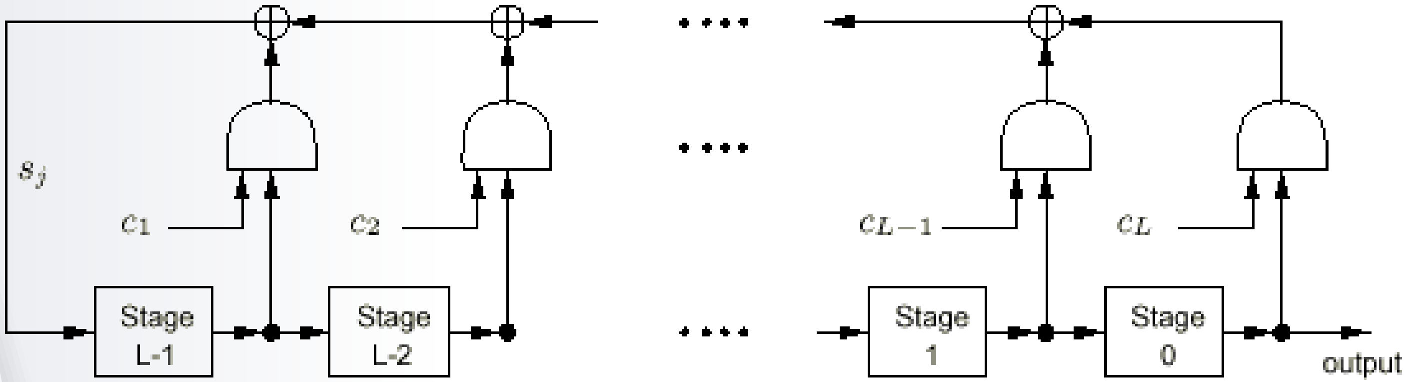
$$C(D) = 1 + c_1 D + c_2 D^2 + \ldots + c_L D^L \in Z_2[D]$$

is the ***connection polynomial***.

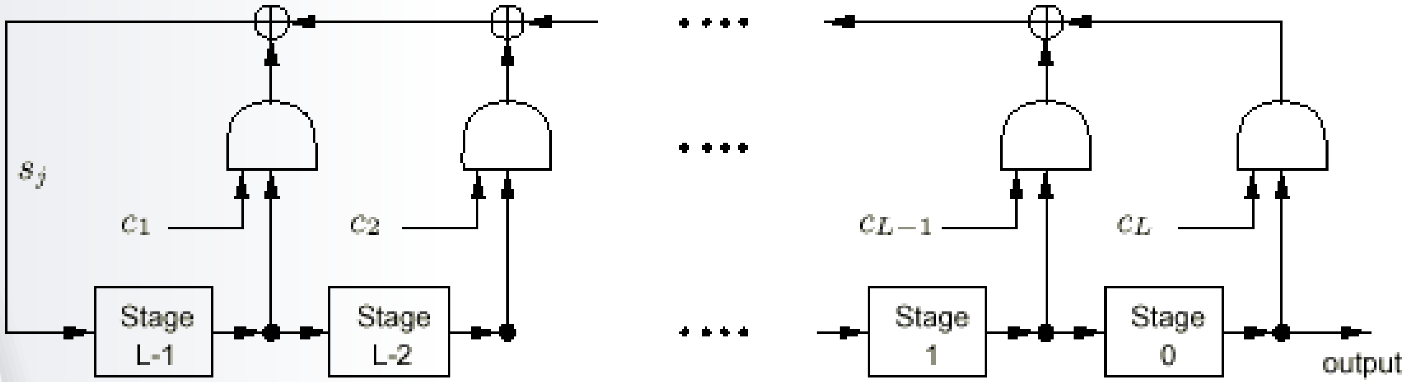


The LFSR is said to be **non-singular** if the degree of C(D) is L (that is $\mathbf{c_L=1}$).

$$C(D) = 1 + c_1 D + c_2 D^2 + \ldots + c_L D^L \in Z_2[D]$$

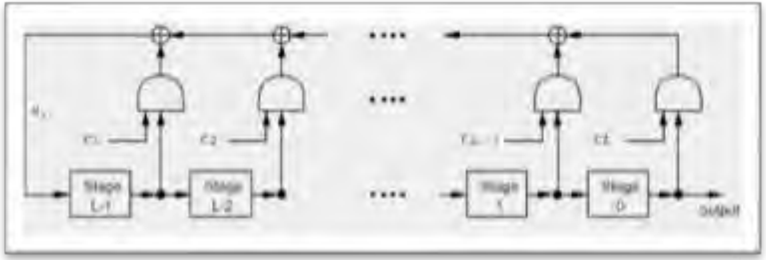


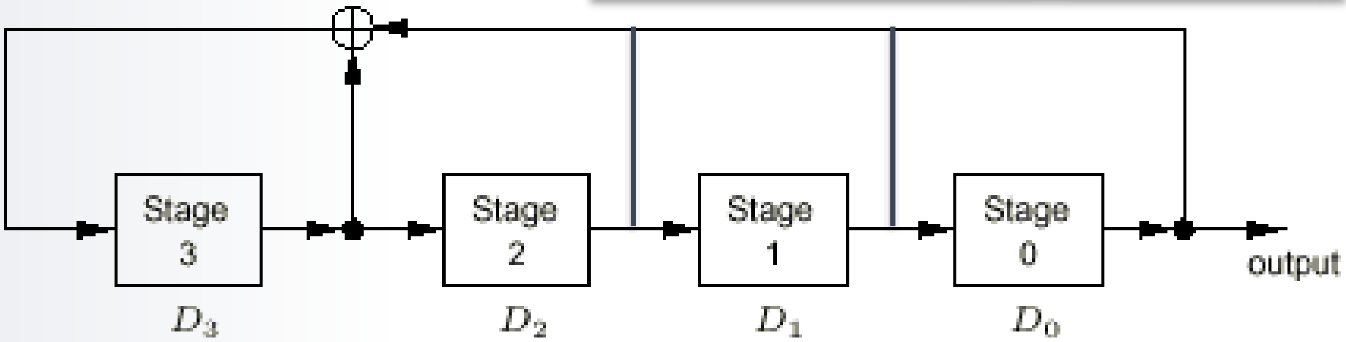
If the initial content of stage **i** is $\mathbf{s_i} \in \mathbf{\{0,1\}}$ for each **i**, $0 \leq i \leq L-1$, then $\mathbf{[s_{L-1}, \ldots, s_1, s_0]}$ is called the ***initial state*** of the LFSR.



Example

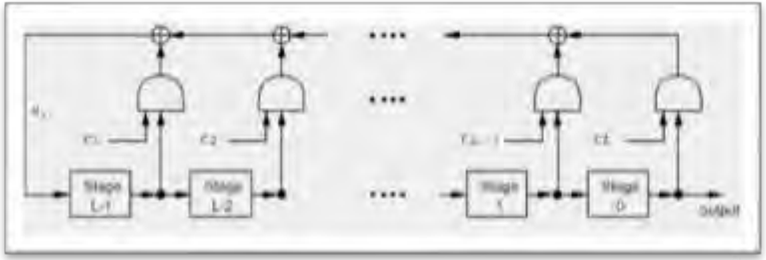
Consider the LFSR <4,1+D+D⁴>, depicted in the figure below.

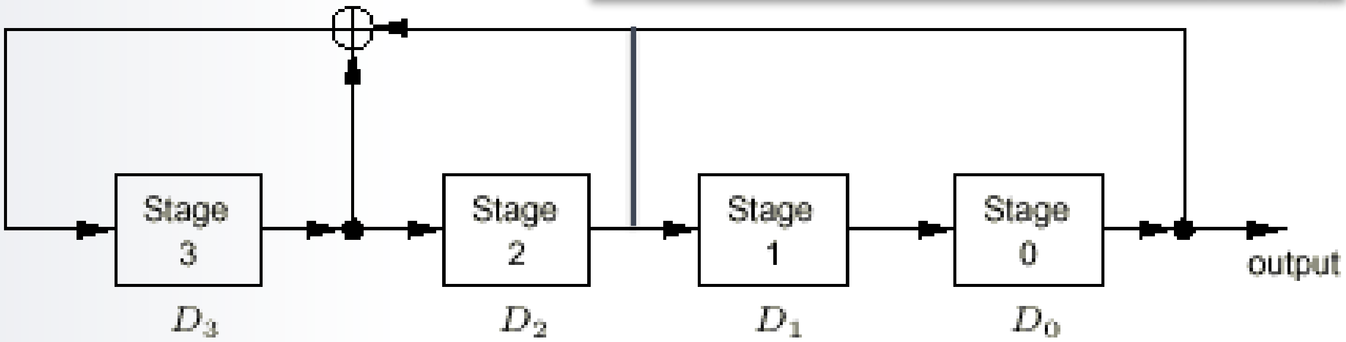




Example

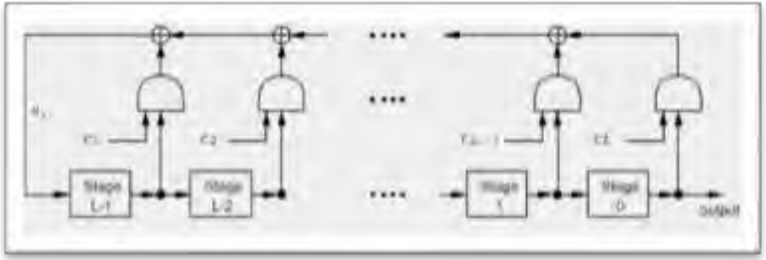
Consider the LFSR <4,1+D+D^4>, depicted in the figure below.

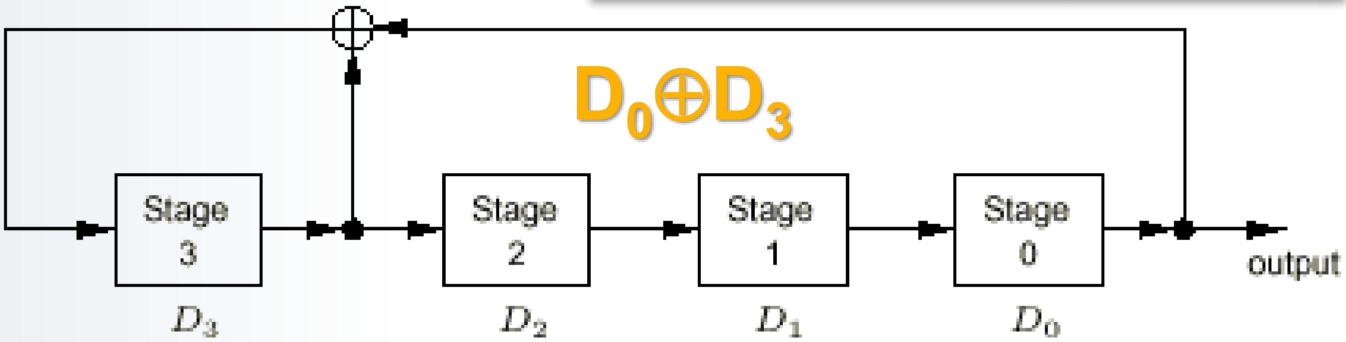




Example

Consider the LFSR <4,1+D+D⁴>, depicted in the figure below.





If the initial state of the LFSR is [0, 0, 0, 0], the output sequence is the zero sequence.

Example

If the initial state of the LFSR is [0, 1, 1, 0], The output sequence is

$$s = 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, \ldots,$$

and is periodic with period 15.

t	D3	D2	D1	D0
0	0	1	1	0

1
3

Example

If the initial state of the LFSR is [0, 1, 1, 0], The output sequence is

$$s = 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, \ldots ,$$

and is periodic with period 15.

t	D3	D2	D1	D0
0	0	1	1	0
1		0	1	1

Example

If the initial state of the LFSR is [0, 1, 1, 0], The output sequence is

$$s = 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, \ldots,$$

and is periodic with period 15.

t	D3	D2	D1	D0
0	0	1	1	0
1	0	0	1	1

Example

If the initial state of the LFSR is [0, 1, 1, 0], The output sequence is

$$s = 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, \ldots,$$

and is periodic with period 15.

t	D3	D2	D1	D0
0	0	1	1	0
1	0	0	1	1
2		0	0	1

Example

If the initial state of the LFSR is [0, 1, 1, 0], The output sequence is

$$s = 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, \dots ,$$

and is periodic with period 15.

t	D3	D2	D1	D0
0	0	1	1	0
1	0	0	1	1
2	1	0	0	1

Example

If the initial state of the LFSR is [0, 1, 1, 0], The output sequence is

$$s = 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, \ldots ,$$

and is periodic with period 15.

t	D3	D2	D1	D0
0	0	1	1	0
1	0	0	1	1
2	1	0	0	1
3	0	1	0	0
4	0	0	1	0
5	0	0	0	1
6	1	0	0	0
7	1	1	0	0

t	D3	D2	D1	D0
8	1	1	1	0
9	1	1	1	1
10	0	1	1	1
11	1	0	1	1
12	0	1	0	1
13	1	0	1	0
14	1	1	0	1
15	0	1	1	0

Facts

Facts

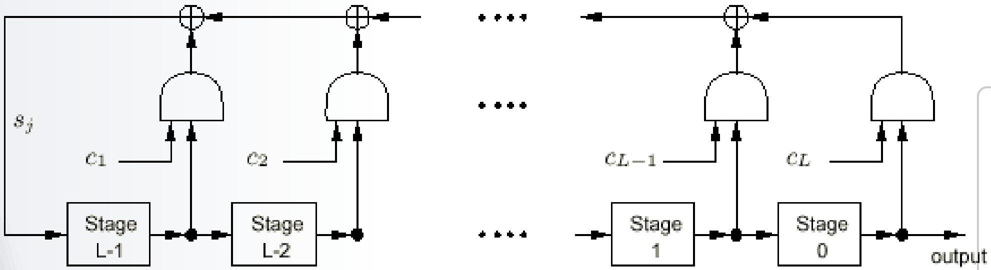
Every output sequence (i.e., for all possible initial states) of an LFSR is **periodic if and only** if the connection polynomial C(D) has **degree L**.

Facts

If an LFSR is *singular* (i.e., C(D) has degree less than L), then **not all output** sequences are **periodic**.

Facts

For the remainder of this chapter, it will be **assumed** that all LFSRs are **non-singular**.



$$C(D) = 1 + c_1 D + c_2 D^2 + \ldots + c_L D^L$$

Facts

Periods of LFSR output sequences. Let $C(D) \in \mathbb{Z}_2[D]$ be a connection polynomial of degree L.

(i) If $C(D)$ is **irreducible** over $\mathbb{Z}_2$, then each of the **2^L-1** non-zero initial states of the **non-singular** LFSR $\langle L, C(D) \rangle$ produces an output sequence with period equal to the **least positive integer N** such that **$C(D)$ divides $1+D^N$** in $\mathbb{Z}_2[D]$.
Note: **it is always the case that this N is a divisor of 2^L-1**

Facts

Periods of LFSR output sequences. Let $C(D) \in \mathbb{Z}_2[D]$ be a connection polynomial of degree L.

(ii) If $C(D)$ is a **primitive** polynomial, then each of the **2^L-1** non-zero initial states of the **non-singular** LFSR <L,C(D)> produces an output sequence with **maximum possible period 2^L-1**.

Definition

If $C(D) \in Z_2[D]$ is a primitive polynomial of degree L, then $<L,C(D)>$ is called a ***maximum-length LFSR***.

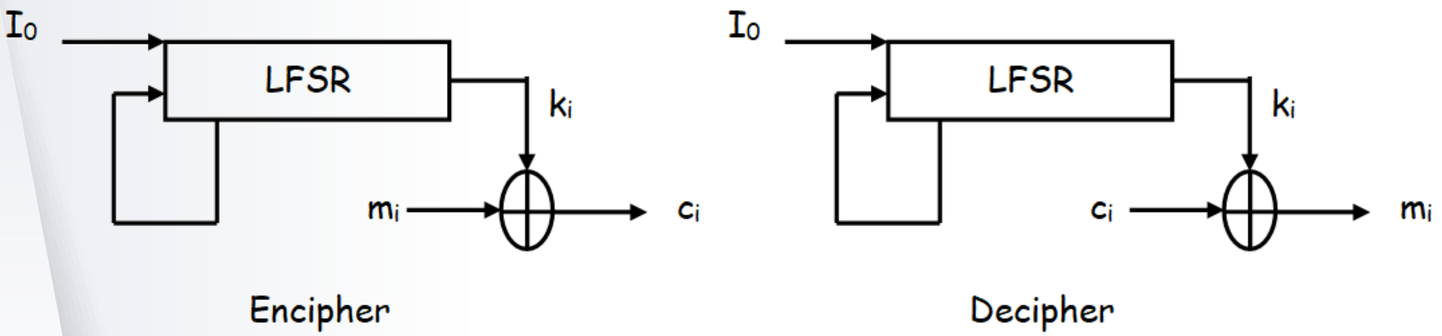
The output of a maximum-length LFSR with non-zero initial state is called an ***m-sequence***.

Facts

A binary message stream M=m1 m2... is enciphered by computing:

$$c_i = m_i \oplus k_i$$

As the bits of the key stream are generated as shown in the following figure:



Encryption with LFSR

THANK YOU

Any questions?

You can find me at:

saad.m@sc.uobaghdad.edu.iq

Saad Al-Momen

Stream Ciphers

CIPHER SYSTEMS

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

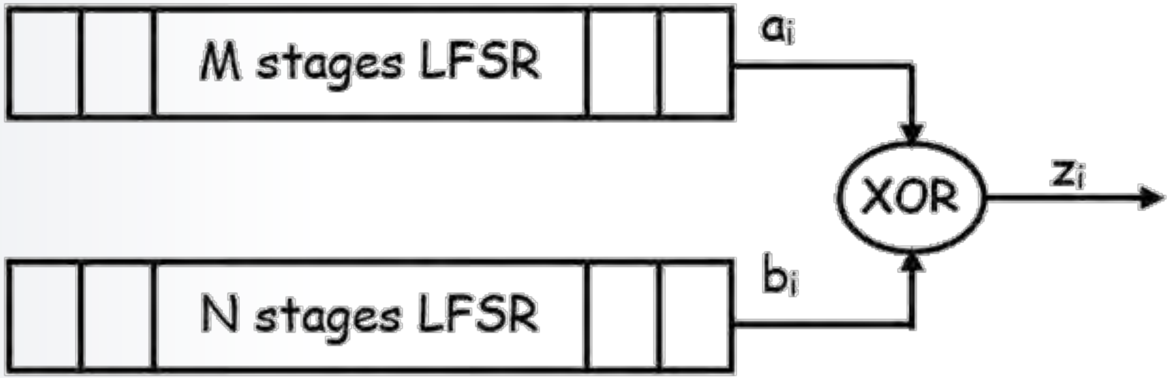
11.

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.

1. Exclusive-OR Algorithm



$$z_i = a_i \oplus b_i$$

$$Z = A \oplus B = \overline{A}B + A\overline{B}$$

When the **gcd(M,N)=1**, the period length of the final sequence is **$(2^M-1)(2^N-1)$**, which is the **maximum period**.

A	B	$A \oplus B$	$\bar{A}$	$\bar{B}$	$\bar{A}\mathrm{B}$	$A\bar{B}$	$\bar{A}\mathrm{B} + A\bar{B}$

A	B	$A \oplus B$	$\overline{A}$	$\overline{B}$	$\overline{A}\mathrm{B}$	$A\overline{B}$	$\overline{A}\mathrm{B} + A\overline{B}$
0							
0							
1							
1							

A	B	$A \oplus B$	$\bar{A}$	$\bar{B}$	$\bar{A}\mathrm{B}$	$A\bar{B}$	$\bar{A}\mathrm{B} + A\bar{B}$
0	0						
0	1						
1	0						
1	1						

A	B	$A \oplus B$	$\bar{A}$	$\bar{B}$	$\bar{A}\mathrm{B}$	$A\bar{B}$	$\bar{A}\mathrm{B} + A\bar{B}$
0	0	0					
0	1	1					
1	0	1					
1	1	0					

A	B	$A \oplus B$	$\overline{A}$	$\overline{B}$	$\overline{A}\mathrm{B}$	$A\overline{B}$	$\overline{A}\mathrm{B} + A\overline{B}$
0	0	0	1				
0	1	1	1				
1	0	1	0				
1	1	0	0				

A	B	$A\oplus B$	$\bar{A}$	$\bar{B}$	$\bar{A}\mathrm{B}$	$A\bar{B}$	$\bar{A}\mathrm{B}+A\bar{B}$
0	0	0	1	1			
0	1	1	1	0			
1	0	1	0	1			
1	1	0	0	0			

A	B	$A \oplus B$	$\bar{A}$	$\bar{B}$	$\bar{A}B$	$A\bar{B}$	$\bar{A}B + A\bar{B}$
0	0	0	1	1	0		
0	1	1	1	0	1		
1	0	1	0	1	0		
1	1	0	0	0	0		

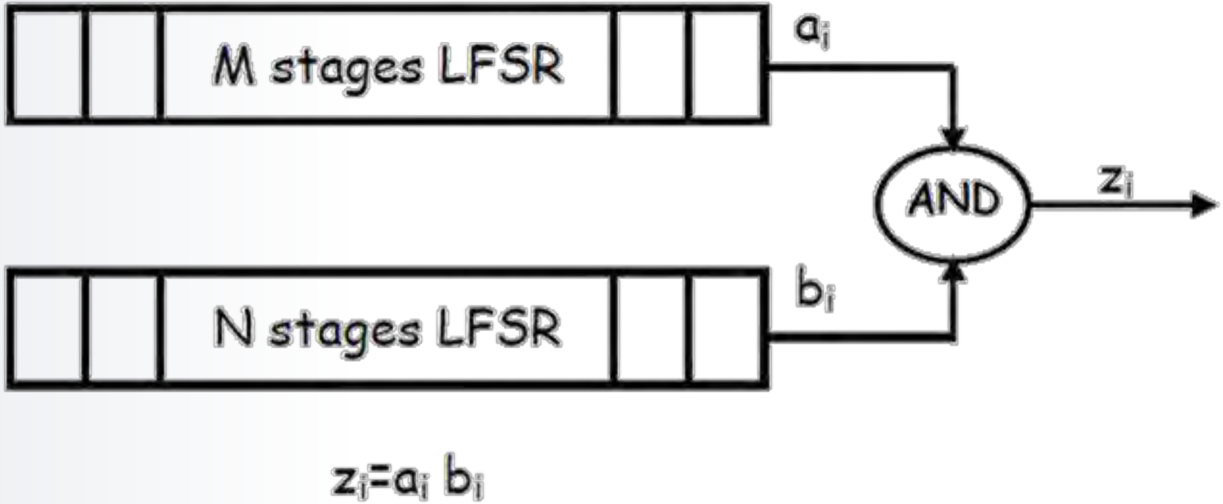
A	B	$A \oplus B$	$\bar{A}$	$\bar{B}$	$\bar{A}\mathrm{B}$	$A\bar{B}$	$\bar{A}\mathrm{B} + A\bar{B}$
0	0	0	1	1	0	0	
0	1	1	1	0	1	0	
1	0	1	0	1	0	1	
1	1	0	0	0	0	0	

A	B	$A \oplus B$	$\bar{A}$	$\bar{B}$	$\bar{A}\mathrm{B}$	$A\bar{B}$	$\bar{A}\mathrm{B} + A\bar{B}$
0	0	0	1	1	0	0	0
0	1	1	1	0	1	0	1
1	0	1	0	1	0	1	1
1	1	0	0	0	0	0	0

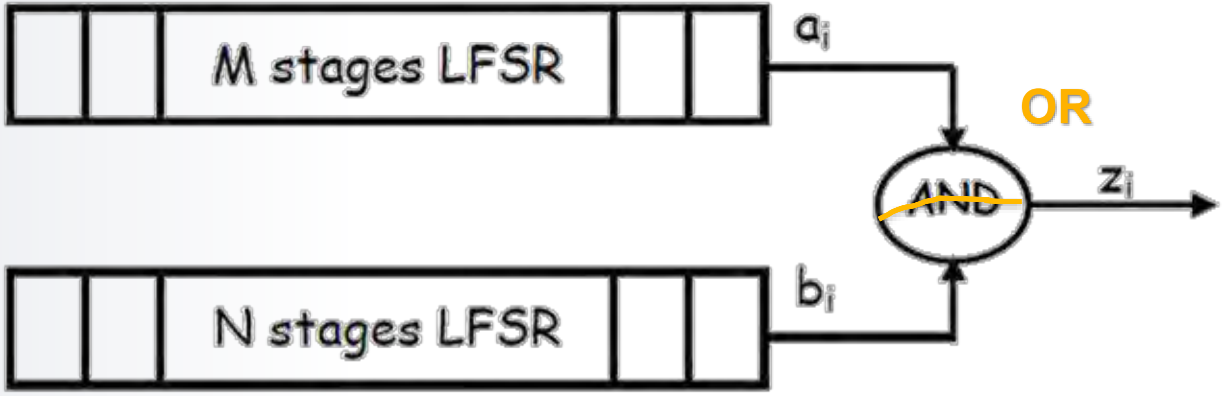
A	B	$A \oplus B$	$\bar{A}$	$\bar{B}$	$\bar{A}$B	$A\bar{B}$	$\bar{A}$B + $A\bar{B}$
0	0	0	1	1	0	0	0
0	1	1	1	0	1	0	1
1	0	1	0	1	0	1	1
1	1	0	0	0	0	0	0

$$Z = A \oplus B = \bar{A}B + A\bar{B}$$

2. Hadamard Algorithm



When the **gcd(M,N)=1**, the period length of the final sequence is **$(2^M-1)(2^N-1)$**, which is the **maximum period**.



$\cancel{z_i = a_i\, b_i}$ $\quad z_i = a_i + b_i + a_i\, b_i$

Prove that

When the **gcd(M,N)=1**, the period length of the final sequence is **$(2^M-1)(2^N-1)$**, which is the **maximum period**.

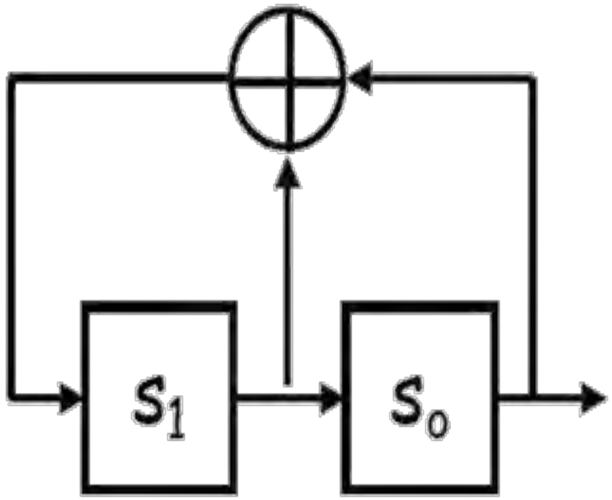
Example

We have two linear feedback shift registers with 2 and 3 stages respectively, and the corresponding connection polynomials are
$C_1(D)=1+D+D^2$ and $C_2(D)=1+D^2+D^3$,

With initial states [1,1] and [1,1,1] respectively.
Apply the Hadamard algorithm to find the resulting sequence.

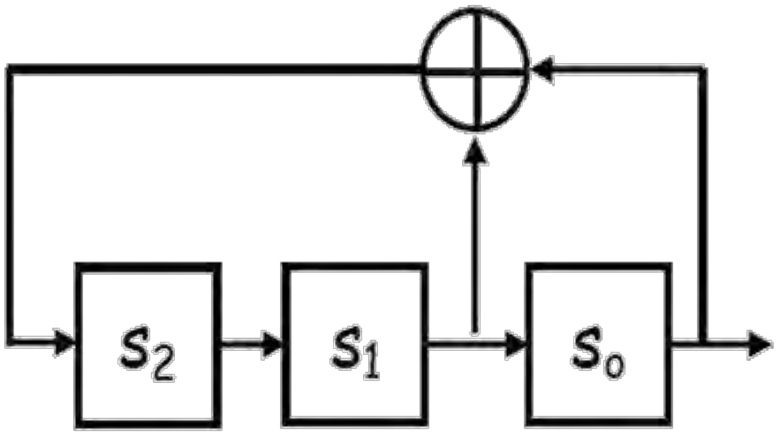
Example

$C_1(D)=1+D+D^2 \Rightarrow s_0+s_1.$



Example

$C_2(D)=1+D^2+D^3 \Rightarrow s_0+s_1.$



	LFSR 1 s_0+s_1		
T	S_1	S_0	a_i
0	1	1	
1	0	1	1
2	1	0	1
3	1	1	0
4			
5			
6			
7			
Max per.	$2^2-1=3$		
Output	110110110110...		

	LFSR 1		s_0+s_1
T	S_1	S_0	a_i
0	1	1	
1	0	1	1
2	1	0	1
3	1	1	0
4			
5			
6			
7			
Max per.	$2^2-1=3$		
Output	110110110110...		

LFSR 2			s_0+s_1
S_2	S_1	S_0	b_i
1	1	1	
0	1	1	1
0	0	1	1
1	0	0	1
0	1	0	0
1	0	1	0
1	1	0	1
1	1	1	0
$2^3-1=7$			
11100101110010...			

	LFSR 1		s_0+s_1
T	S_1	S_0	a_i
0	1	1	
1	0	1	1
2	1	0	1
3	1	1	0
4			
5			
6			
7			
Max per.	$2^2-1=3$		
Output	110110110110…		

LFSR 2			s_0+s_1
S_2	S_1	S_0	b_i
1	1	1	
0	1	1	1
0	0	1	1
1	0	0	1
0	1	0	0
1	0	1	0
1	1	0	1
1	1	1	0
$2^3-1=7$			
11100101110010…			

Since gcd(3,7)=1, hence the period of the resulting sequence =3X7=21.

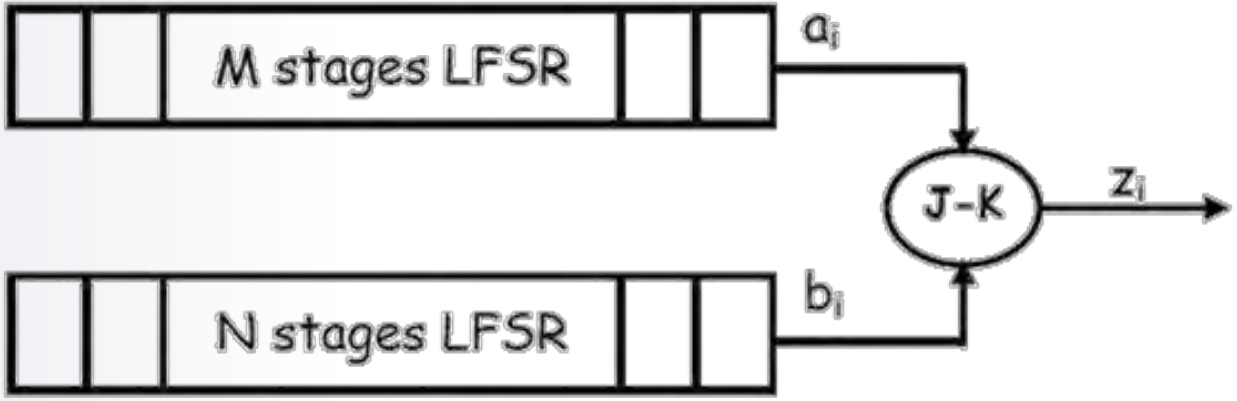
A=	$\boxed{1\ 1\ 0}$			$\boxed{1\ 1\ 0}$			$\boxed{1\ 1\ 0}$			$\boxed{1\ 1\ 0}$			$\boxed{1\ 1\ 0}$			$\boxed{1\ 1\ 0}$			$\boxed{1\ 1\ 0}$		
B=	$\boxed{1\ 1\ 1\ 0\ 0\ 1\ 0}$							$\boxed{1\ 1\ 1\ 0\ 0\ 1\ 0}$							$\boxed{1\ 1\ 1\ 0\ 0\ 1\ 0}$						
Z=	1	1	0	0	0	0	0	1	0	1	0	0	1	0	0	1	1	0	0	1	0

NOTE:

Approximately, three to four from the results are zeros, because of the AND operation.

So, the result of the algorithm does not satisfy the first randomness postulate.

3. J-K flip-flop Algorithm



$$z_i = (a_i + b_i + 1)\, z_{i-1} + a_i$$

When the **gcd(M,N)=1**, the period length of the final sequence is **$(2^M-1)(2^N-1)$**, which is the **maximum period**.

Prove that

The truth table for J-K flip flop ($z_i = (a_i + b_i + 1)\, z_{i-1} + a_i$) is:

J	K	z_{i+1}
0	0	z_i
0	1	0
1	0	1
1	1	$\bar{z}_i$

HW:

You have **two** linear feedback shift registers with **3** and **5** stages respectively, and the corresponding connection polynomials are $C_1(D)=1+D+D^3$ and $C_2(D)=1+D^3+D^5$, with initial states [1,0,1] and [1,0,0,1,1] respectively. Apply the **J-K flip-flop** algorithm to find the first 35 digits of the resulting sequence.

THANK YOU

Any questions?

You can find me at:

saad.m@sc.uobaghdad.edu.iq

Saad Al-Momen

Stream Ciphers

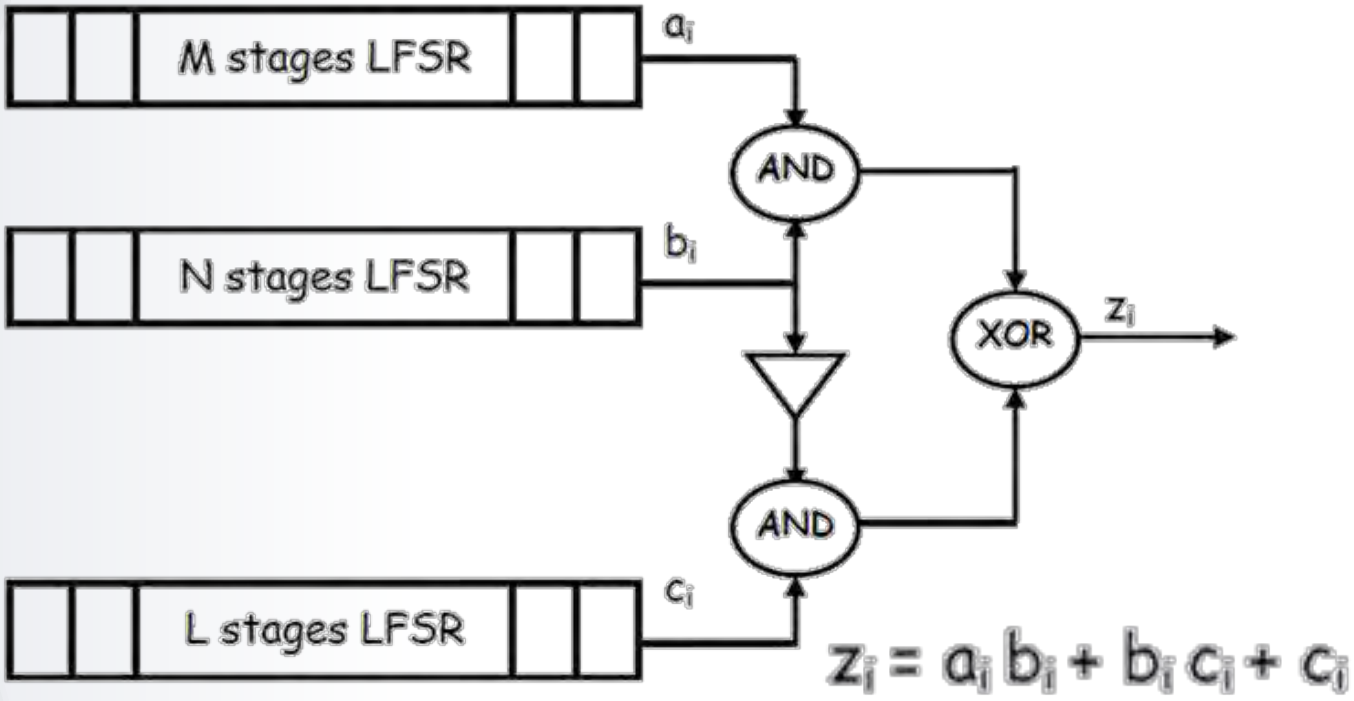
12.

CIPHER SYSTEMS

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

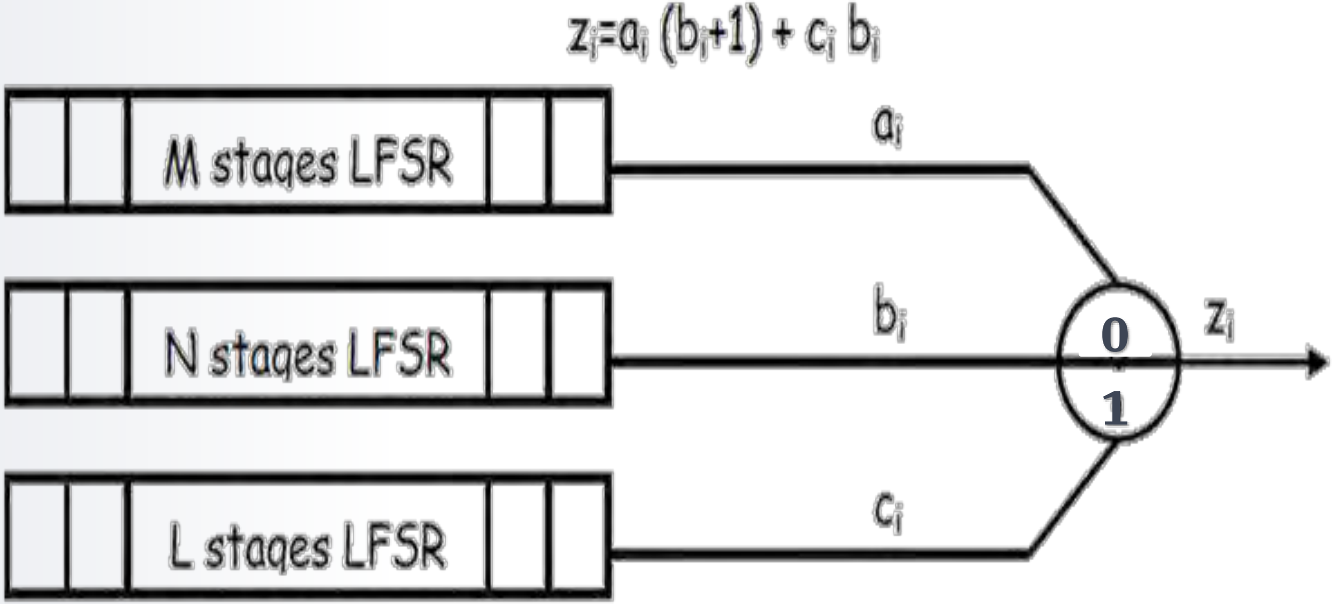
Stream Cipher Algorithms

4. Geffe's Algorithm



When the **gcd(M,N,L)=1**, the period length of the final sequence is **$(2^M-1)(2^N-1)(2^L-1)$**, which is the **maximum period**.

5. Police Algorithm



If b_i=0 then z_i=a_i, and if b_i=1 then z_i=c_i

When the **gcd(M,N,L)=1**, the period length of the final sequence is **$(2^M-1)(2^N-1)(2^L-1)$**, which is the **maximum period**.

$$z_i = a_i\,(b_i + 1) + c_i\, b_i$$

If $b_i = 0$ then $z_i = a_i$

Let $b_i = 0$

$$z_i = a_i(0+1) + c_i(0)$$
$$= a_i(1) = a_i$$

✓

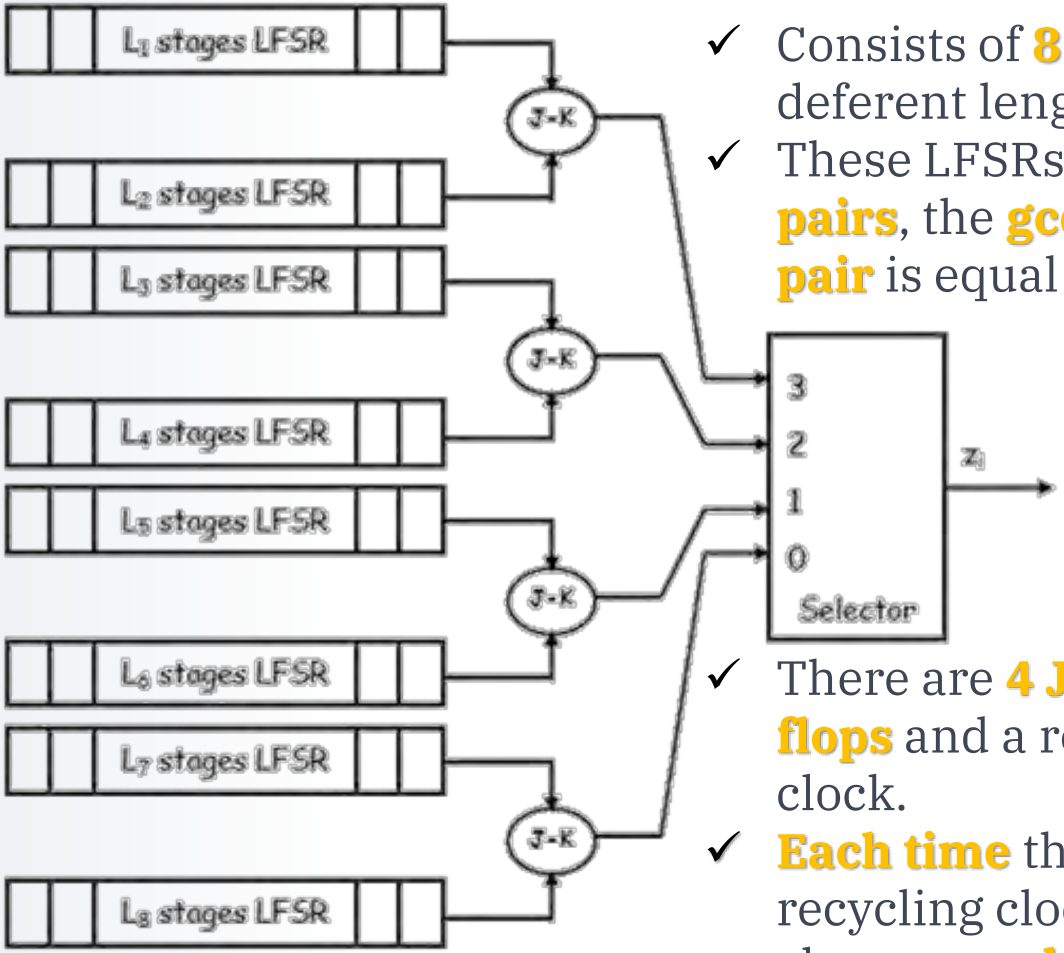
If $b_i = 1$ then $z_i = c_i$

Let $b_i = 1$

$$z_i = a_i(1+1) + c_i(1)$$
$$= a_i(0) + c_i = c_i$$

✓

6. Pless's Algorithm



- ✓ Consists of **8 LFSRs** of deferent lengths.
- ✓ These LFSRs put in **4 pairs**, the **gcd of each pair** is equal to **one**.
- ✓ There are **4 J-K flip-flops** and a recycling clock.
- ✓ **Each time** the recycling clock will choose **one bit** from the four arrival bits

Example

In Pless's algorithm, there are 4 shift registers pairs with the following output:

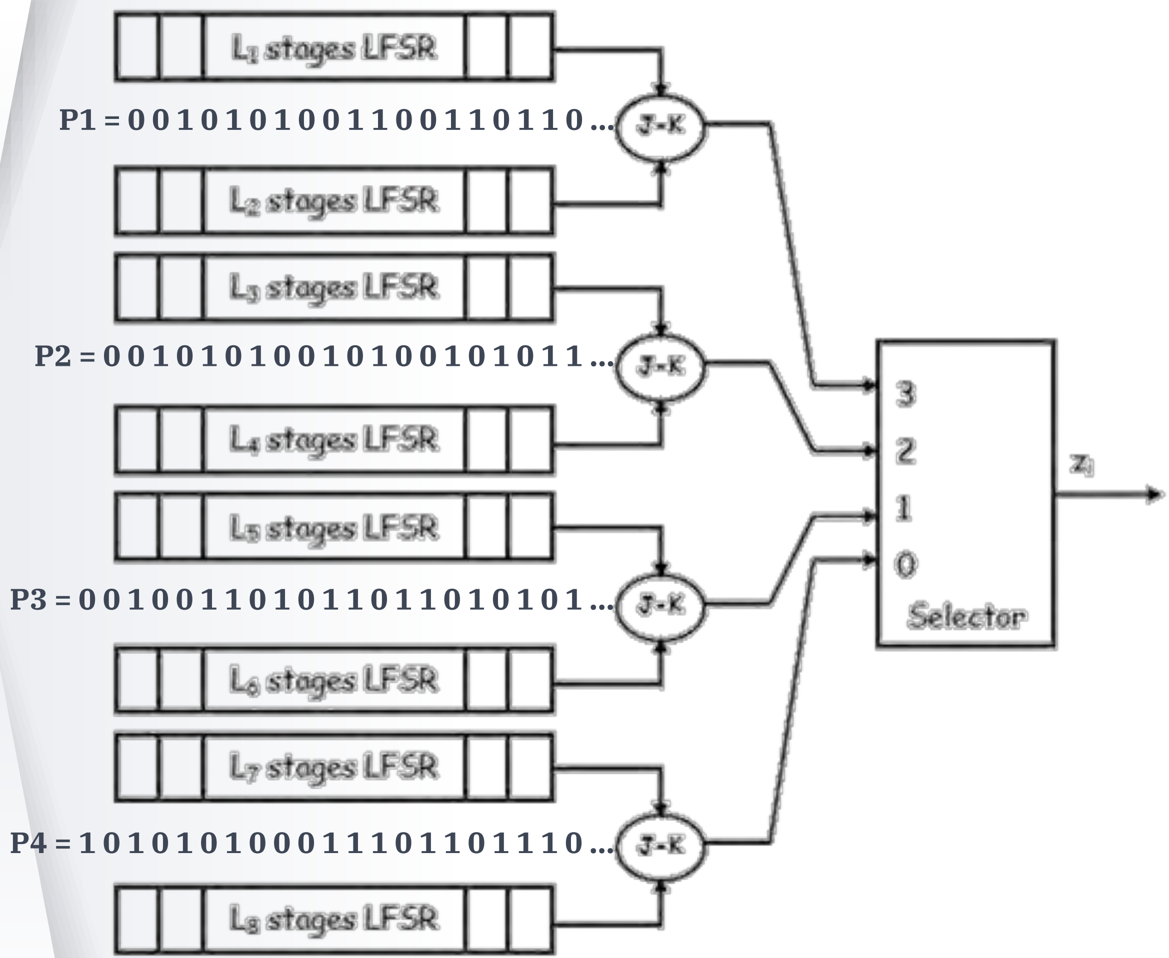
P1 = 0 0 1 0 1 0 1 0 0 1 1 0 0 1 1 0 1 1 0 …

P2 = 0 0 1 0 1 0 1 0 0 1 0 1 0 0 1 0 1 0 1 1 …

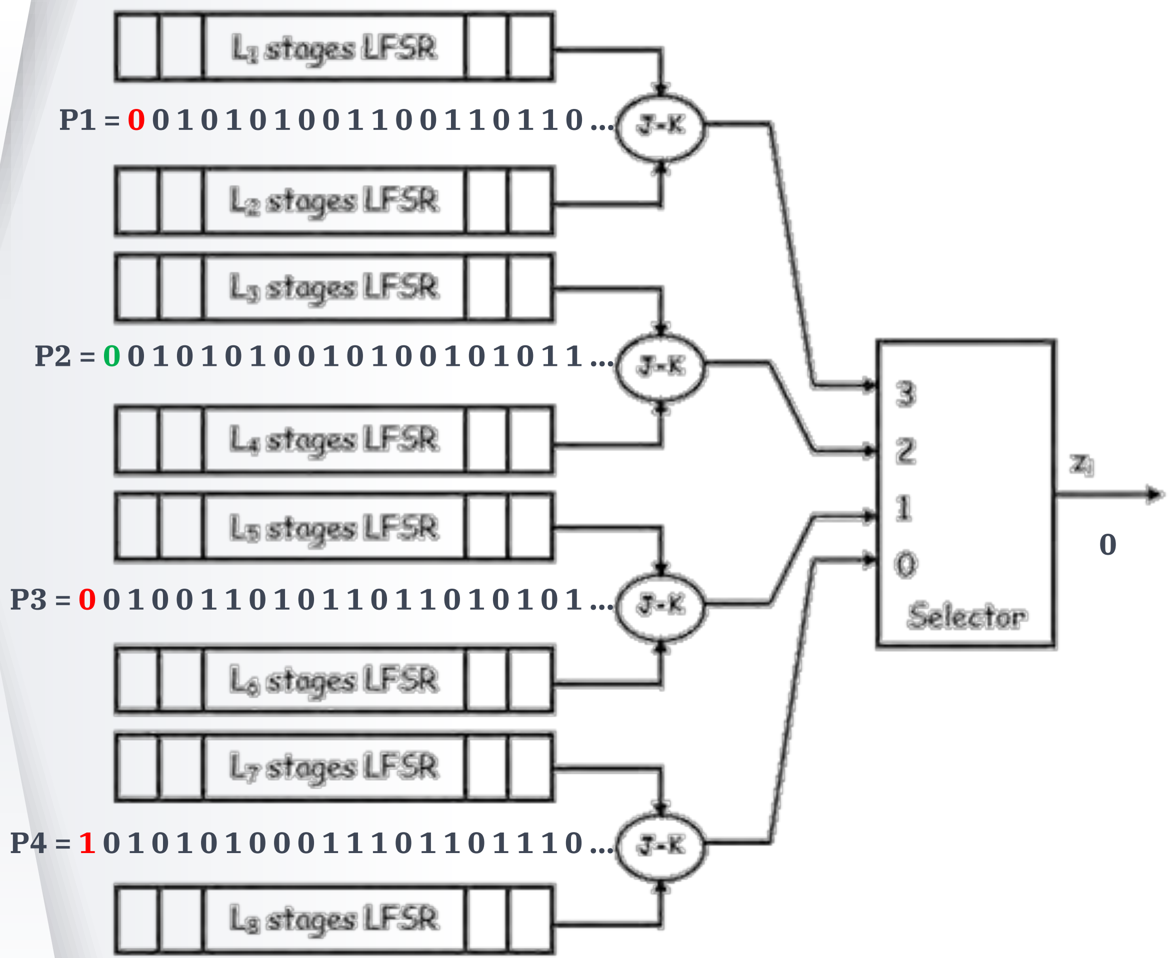
P3 = 0 0 1 0 0 1 1 0 1 0 1 1 0 1 1 0 1 0 1 0 1 …

P4 = 1 0 1 0 1 0 1 0 0 0 1 1 1 0 1 1 0 1 1 1 0 …

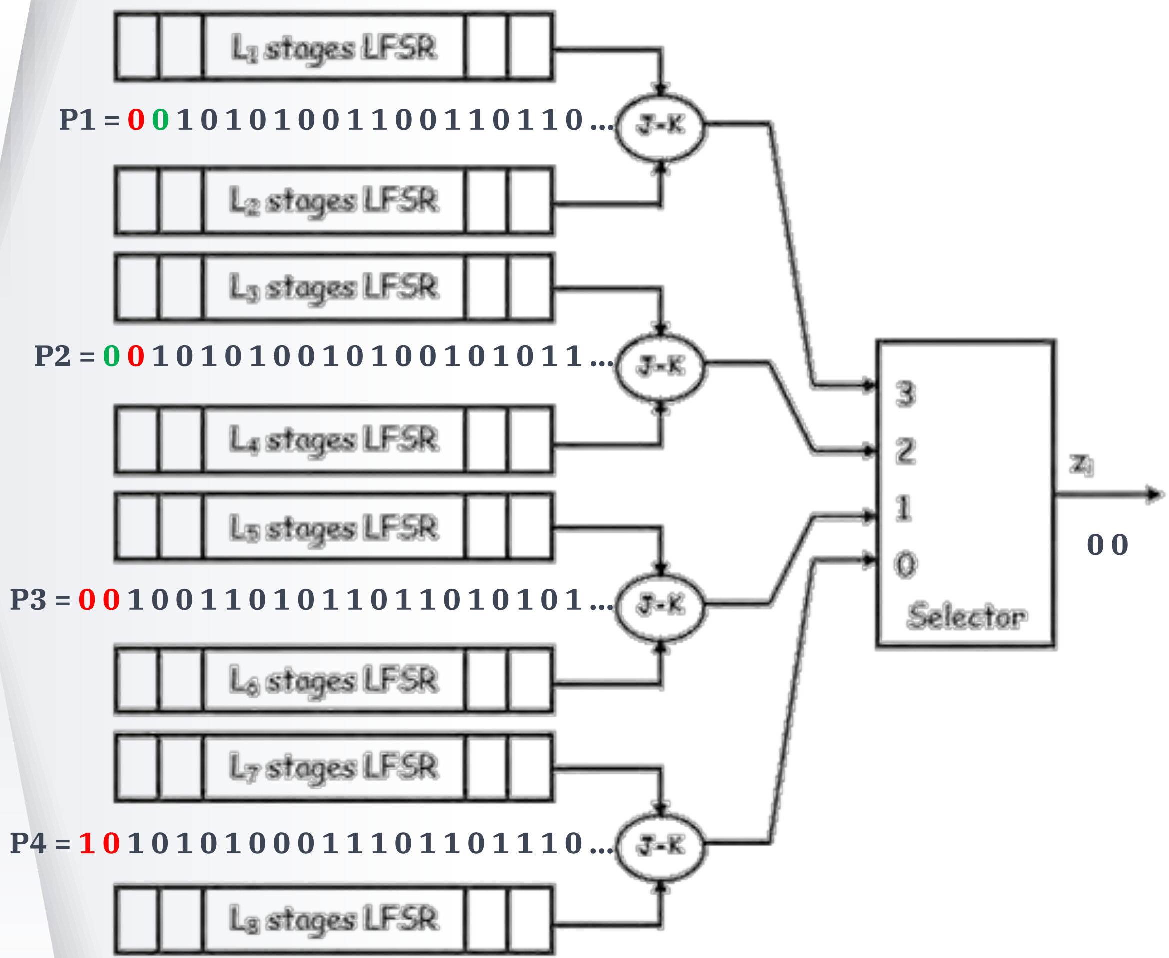
If the initial of the recycling clock is 2, what are the first 10 bits of the resulting sequence?

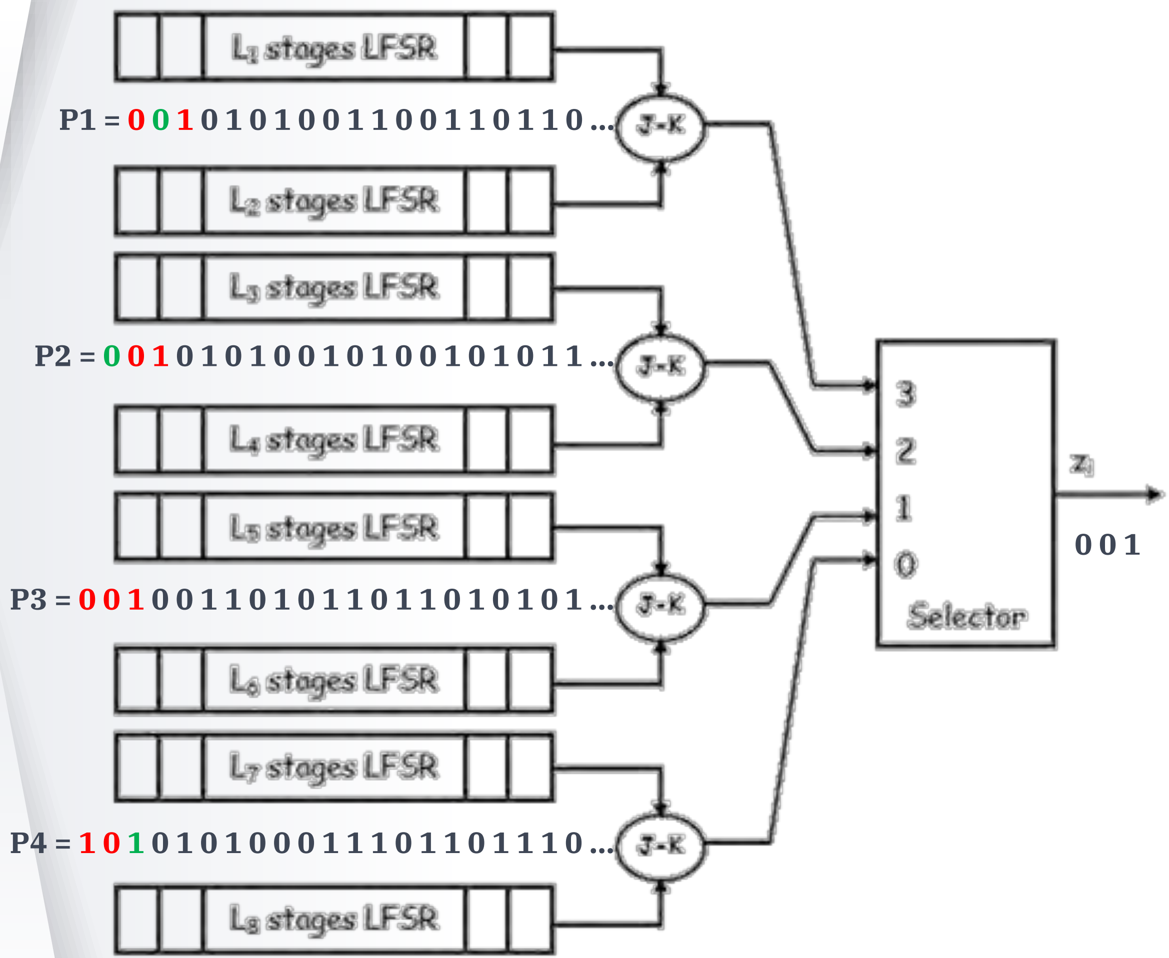


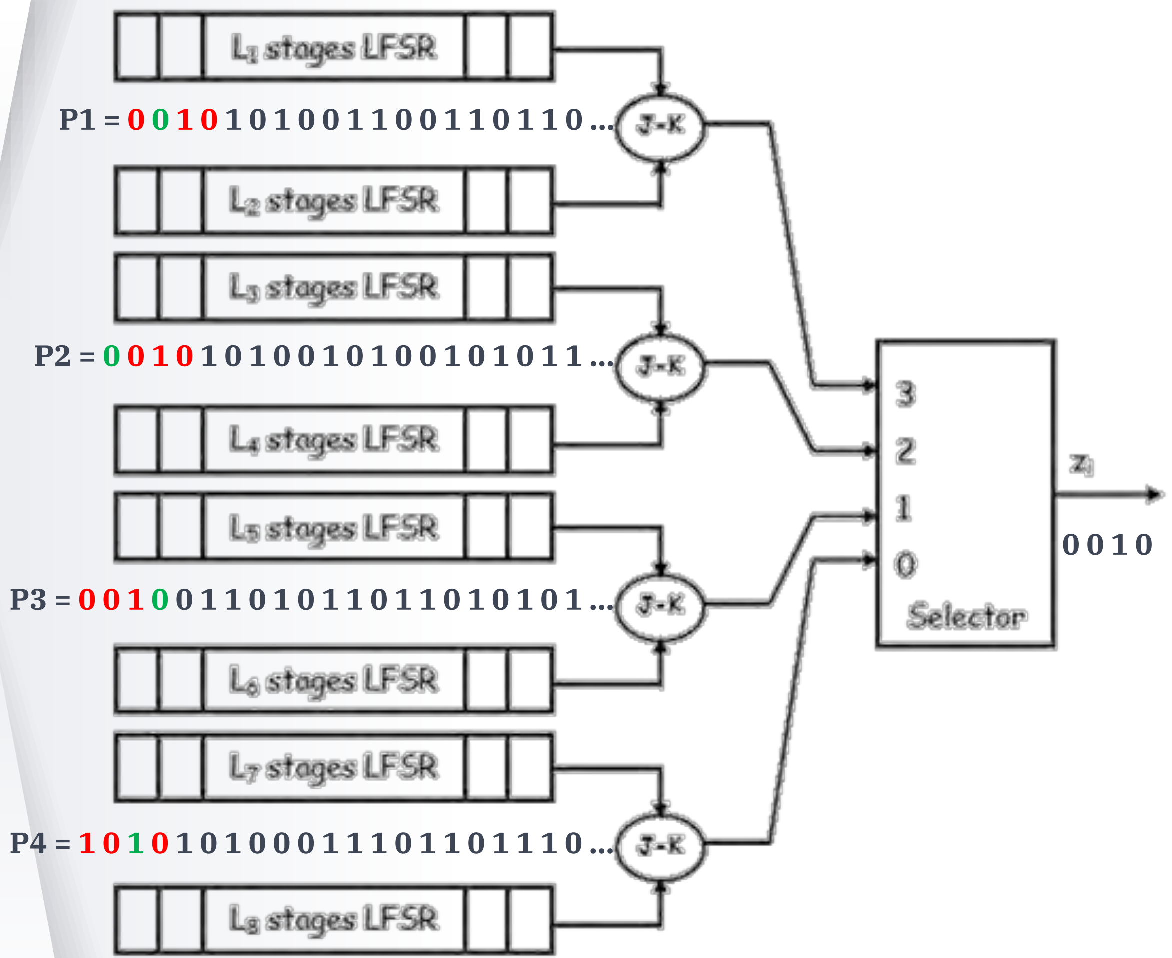
L_1 stages LFSR
P1 = 0 0 1 0 1 0 1 0 0 1 1 0 0 1 1 0 1 1 0 ...
J-K
L_2 stages LFSR
L_3 stages LFSR
P2 = 0 0 1 0 1 0 1 0 0 1 0 1 0 0 1 0 1 0 1 1 ...
J-K
L_4 stages LFSR
L_5 stages LFSR
P3 = 0 0 1 0 0 1 1 0 1 0 1 1 0 1 1 0 1 0 1 0 1 ...
J-K
L_6 stages LFSR
L_7 stages LFSR
P4 = 1 0 1 0 1 0 1 0 0 0 1 1 1 0 1 1 0 1 1 1 0 ...
J-K
L_8 stages LFSR
3
2
1
0
Selector
z_j



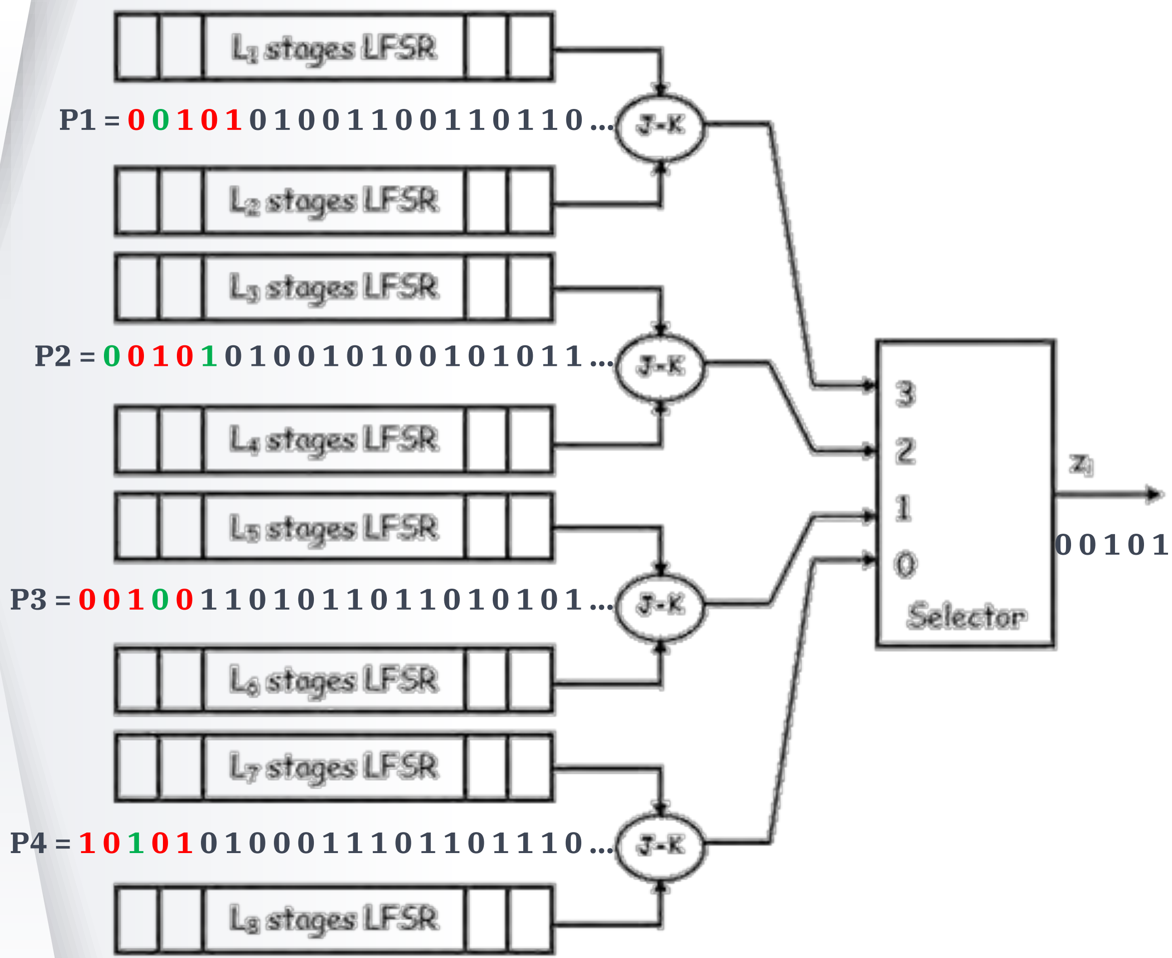
L1 stages LFSR
P1 = 0 0 1 0 1 0 1 0 0 1 1 0 0 1 1 0 1 1 0 ...
J-K
L2 stages LFSR
L3 stages LFSR
P2 = 0 0 1 0 1 0 1 0 0 1 0 1 0 0 1 0 1 0 1 1 ...
J-K
L4 stages LFSR
L5 stages LFSR
P3 = 0 0 1 0 0 1 1 0 1 0 1 1 0 1 1 0 1 0 1 0 1 ...
J-K
L6 stages LFSR
L7 stages LFSR
P4 = 1 0 1 0 1 0 1 0 0 0 1 1 1 0 1 1 0 1 1 1 0 ...
J-K
L8 stages LFSR
3
2
1
0
Selector
zj
0


L1 stages LFSR
P1 = 0 0 1 0 1 0 1 0 0 1 1 0 0 1 1 0 1 1 0 ...
J-K
L2 stages LFSR
L3 stages LFSR
P2 = 0 0 1 0 1 0 1 0 0 1 0 1 0 0 1 0 1 0 1 1 ...
J-K
L4 stages LFSR
L5 stages LFSR
P3 = 0 0 1 0 0 1 1 0 1 0 1 1 0 1 1 0 1 0 1 0 1 ...
J-K
L6 stages LFSR
L7 stages LFSR
P4 = 1 0 1 0 1 0 1 0 0 0 1 1 1 0 1 1 0 1 1 1 0 ...
J-K
L8 stages LFSR
3
2
1
0
Selector
zj
0 0


L1 stages LFSR
P1 = 0 0 1 0 1 0 1 0 0 1 1 0 0 1 1 0 1 1 0 ...
J-K
L2 stages LFSR
L3 stages LFSR
P2 = 0 0 1 0 1 0 1 0 0 1 0 1 0 0 1 0 1 0 1 1 ...
J-K
L4 stages LFSR
L5 stages LFSR
P3 = 0 0 1 0 0 1 1 0 1 0 1 1 0 1 1 0 1 0 1 0 1 ...
J-K
L6 stages LFSR
L7 stages LFSR
P4 = 1 0 1 0 1 0 1 0 0 0 1 1 1 0 1 1 0 1 1 1 0 ...
J-K
L8 stages LFSR
3
2
1
0
Selector
zj
0 0 1



L1 stages LFSR
P1 = 0 0 1 0 1 0 1 0 0 1 1 0 0 1 1 0 1 1 0 ...
J-K
L2 stages LFSR
L3 stages LFSR
P2 = 0 0 1 0 1 0 1 0 0 1 0 1 0 0 1 0 1 0 1 1 ...
J-K
L4 stages LFSR
L5 stages LFSR
P3 = 0 0 1 0 0 1 1 0 1 0 1 1 0 1 1 0 1 0 1 0 1 ...
J-K
L6 stages LFSR
L7 stages LFSR
P4 = 1 0 1 0 1 0 1 0 0 0 1 1 1 0 1 1 0 1 1 1 0 ...
J-K
L8 stages LFSR
3
2
1
0
Selector
zi
0 0 1 0



L1 stages LFSR
P1 = 0 0 1 0 1 0 1 0 0 1 1 0 0 1 1 0 1 1 0 ...
J-K
L2 stages LFSR
L3 stages LFSR
P2 = 0 0 1 0 1 0 1 0 0 1 0 1 0 0 1 0 1 0 1 1 ...
J-K
L4 stages LFSR
L5 stages LFSR
P3 = 0 0 1 0 0 1 1 0 1 0 1 1 0 1 1 0 1 0 1 0 1 ...
J-K
L6 stages LFSR
L7 stages LFSR
P4 = 1 0 1 0 1 0 1 0 0 0 1 1 1 0 1 1 0 1 1 1 0 ...
J-K
L8 stages LFSR
3
2
1
0
Selector
zi
0 0 1 0 1

THANK YOU

Any questions?

You can find me at:

saad.m@sc.uobaghdad.edu.iq