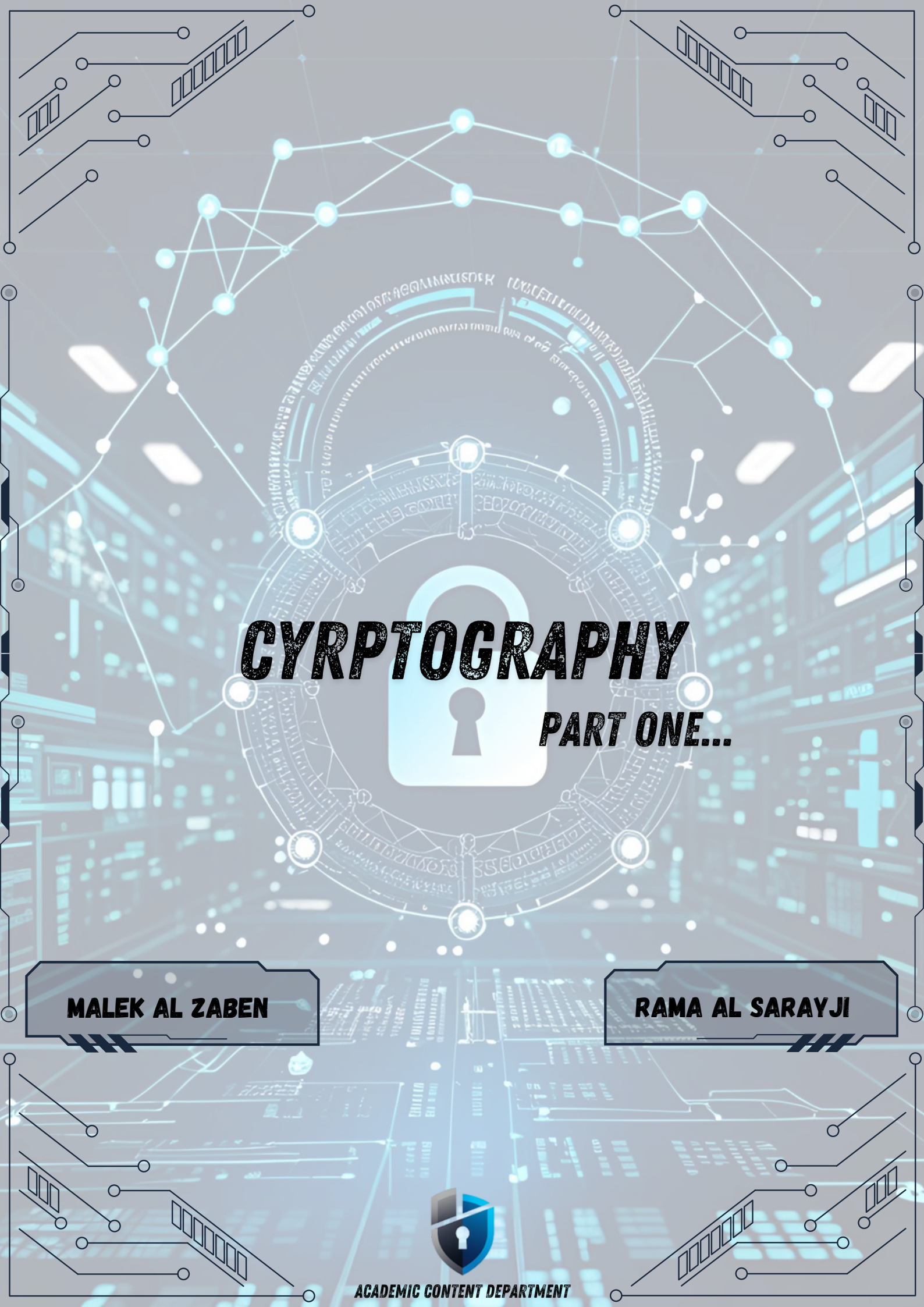


CYRPTOGRAPHY

PART ONE...

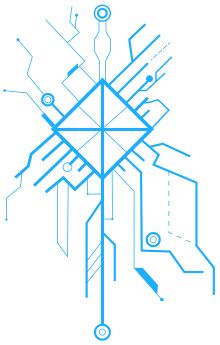
MALEK AL ZABEN

RAMA AL SARAYJI

ACADEMIC CONTENT DEPARTMENT

ERROR CATCHERS

TABLE OF CONTENT



CHAPTER ONE

INTRODUCTION TO CRYPTOGRAPHY

Computer Security: The protection to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (hardware, software, etc.]

Information security, (InfoSec) : is the practice of preventing unauthorized access, use, disclosure, of information . The information or data may take any form, electronic or physical.

1- **Cryptography**

also known as “Kryptos“ it’s Greek word means “Hidden Secrets”. practice of hiding information converting a plain text into a data which can’t be understood and to be able to convert it again to the original plain text.

2- **Steganography**

also known as “STEGANOS GRAPHIA” it’s Greek word means “Covered Writing ” is an encryption technique that can be used along with cryptography as an extra-secure method in which to protect data.

3- **Watermark**

non digital is a visible image or pattern in paper, appearing in varying shades when viewed with transmitted or reflected light, caused by differences in paper thickness.

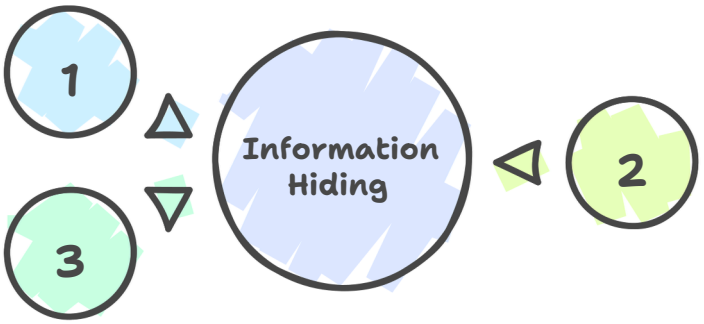
digital is an embedded signal or pattern in digital files that contains information identifying the copyright owner, creator, or authorized user.

Steganography

Methods for concealing[Hidden] data within other data

Cryptography

practice of hiding information converting a plain text into a data which can't be understood



Watermarking

Processes for embedding identifiers in content

1- Steganography

A→ Linguistic ⟶ Linguistic communication

B→Technical ⟶ Text, Audio, Video

2-Watermarking

A→ Visible

B→ Invisible (Copyright)

3-Cryptography

Cipher is a method for encrypting messages, Encryption algorithms are standardized & published,

The key which is an input to the algorithm is secret and it's a string of numbers or characters

encryption algorithm

Symmetric Algorithm

Same key is used for both encryption and decryption.

Asymmetric Algorithm

Different keys are used for encryption and decryption.

1 Symmetric Algorithms

Algorithms in which the key for encryption and decryption are the same are Symmetric

Example: Caesar Cipher

symmetric cipher Types

Block Ciphers

Suitable for encrypting single messages. encrypt data one block at a time (typically 64 bits, or 128 bits).

Stream Ciphers

Encrypt data one bit or one byte at a time. Ideal for encrypting continuous streams of data.

- Symmetric Encryption Limitations

What are the limitations of symmetric encryption?

Key Exposure Risk

Any exposure to the secret key compromises the secrecy of the ciphertext.

Key Delivery Requirement

A key needs to be delivered to the recipient for decryption.

Eavesdropping Potential

Potential for eavesdropping attacks during key transmission.

2 Asymmetric Encryption

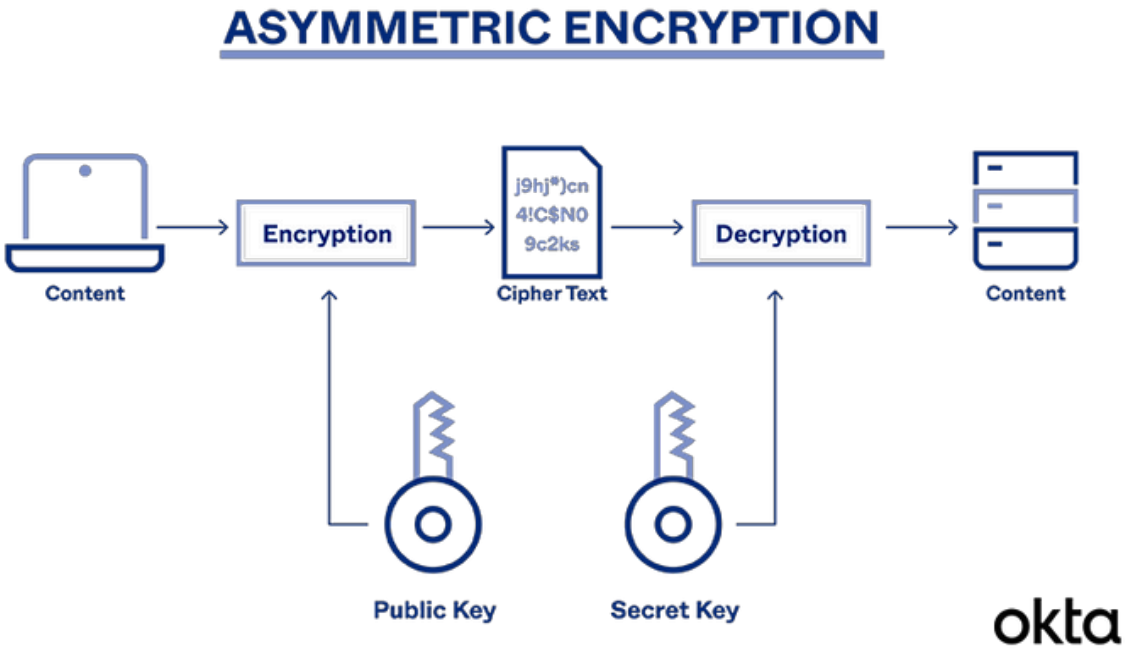
Uses a pair of keys for encryption

Public key for encryption

Private key for decryption

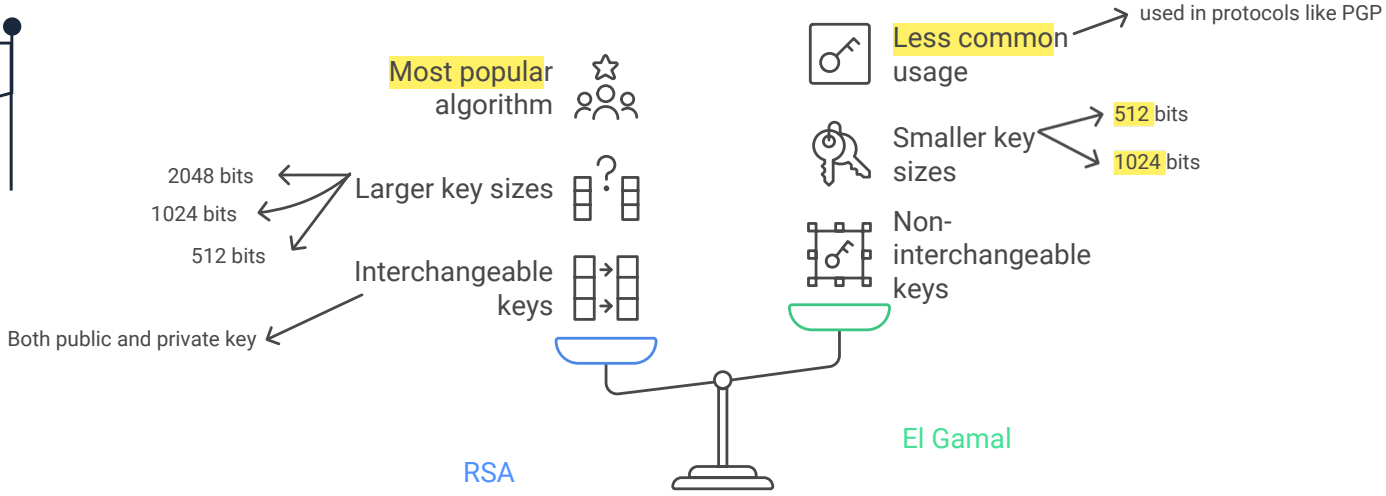
Messages encoded [encrypted] using public key decoded [decrypted] by the private key only

Secret transmission of key for decryption is not required Every entity can generate a key pair and release its public key



Asymmetric Encryption Types

Two most popular algorithms are **RSA & El Gamal**



RSA vs El Gamal

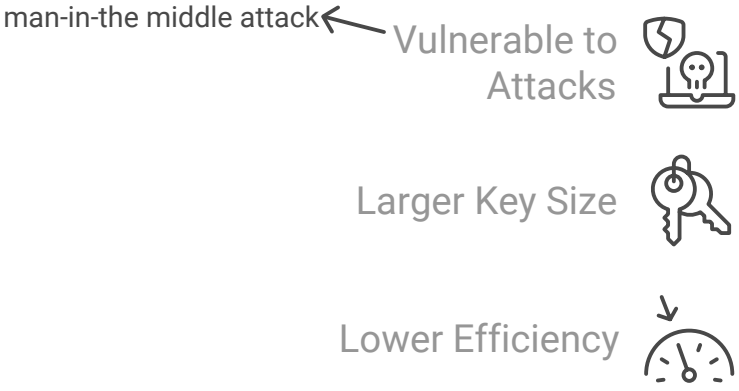
Asymmetric Encryption Weaknesses

Efficiency is lower than Symmetric Algorithms

A 1024-bit asymmetric key is equivalent to 128-bit symmetric

key Potential for man-in-the middle attack

It is problematic to get the key pair generated for the encryption



Computer Security Objectives

Confidentiality

Data Confidentiality
Ensures private or confidential information is not made available or disclosed to unauthorized individuals.

Privacy
Empowers individuals to control or influence how their information is collected, stored, and shared with others.

Integrity

Data Integrity
Ensures that information and programs are modified only in authorized ways.
System Integrity
Ensures a system performs its functions as expected .

Availability

System Availability Ensures systems function promptly and services are accessible to authorized users without interruption.

Threats and Attacks

threat : a possible danger that might exploit a vulnerability.

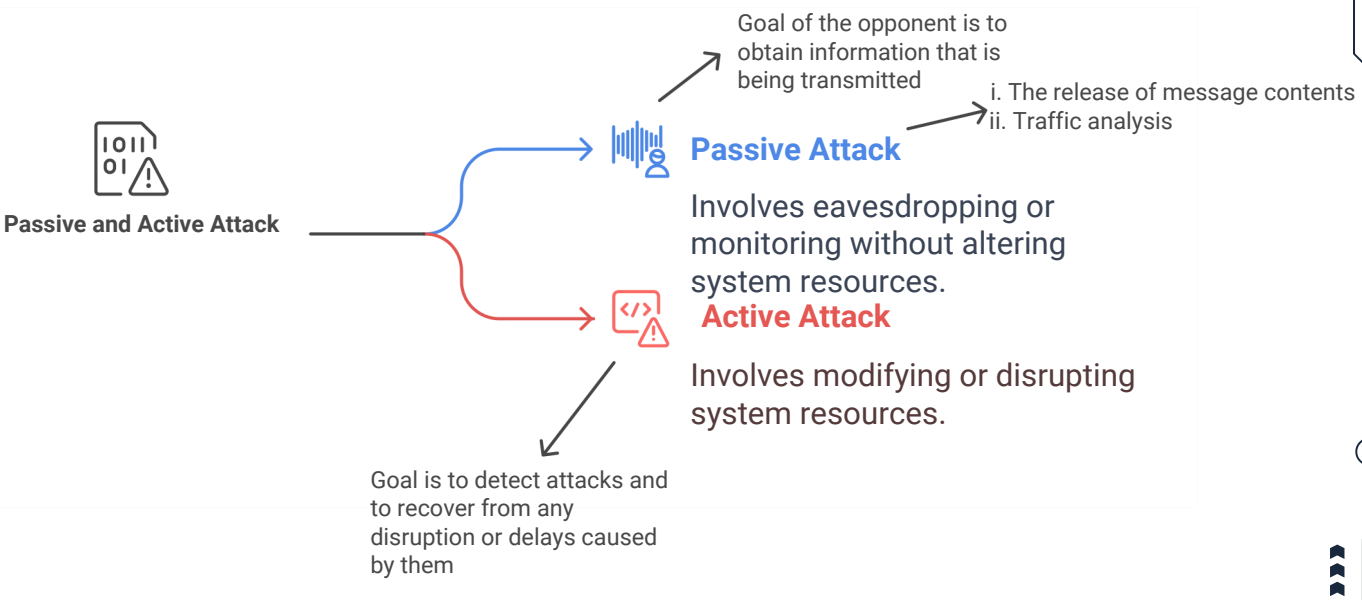
attack :is an intentional attempt to exploit system or network vulnerabilities, often for data theft or disruption.

Passive and Active Attack

A means of classifying security attacks, used both in X.800 and RFC 4949, is in terms of passive attacks and active attacks

A **passive attack** attempts to learn or make use of information from the system but does not affect system resources

An **active attack** attempts to alter system resources or affect their operation



CHAPTER TWO

CLASSICAL ENCRYPTION TECHNIQUES

Cryptography is the art and science of securing communication and information by transforming it into a format that is unreadable to unauthorized users.

Definitions for this chapter

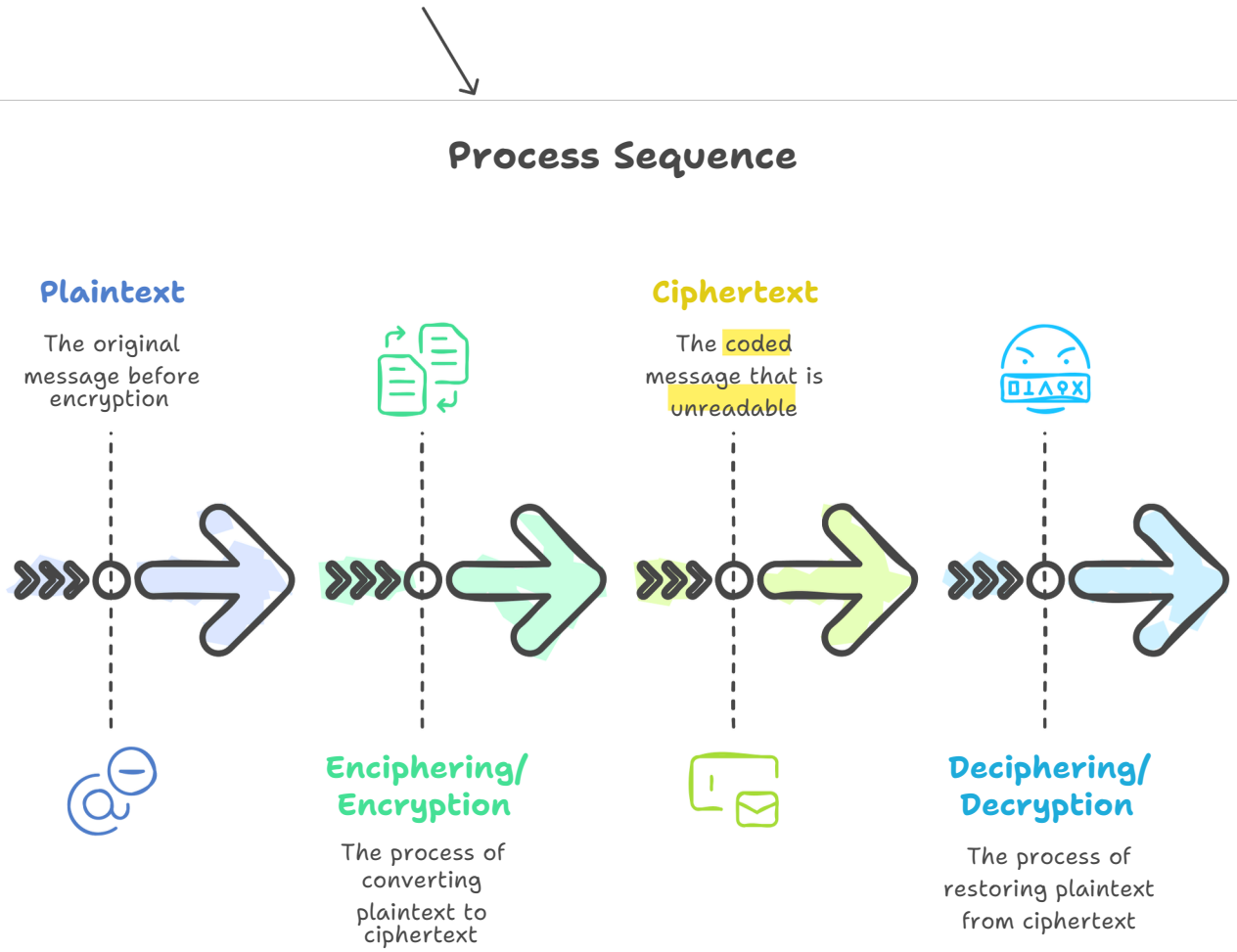
Cryptology · The areas of cryptography and cryptanalysis

Cryptography · The area of study of the many schemes used for encryption

Cryptanalysis · Techniques used to decipher messages without encryption details

Cryptographic System/Cipher · Ascheme used for encryption

The Process Sequence elements



Introduction to Cryptography

We can think of cryptography as an age-old secret language, or as an invisible shield that has grown stronger over time.

How Does It Work?

It's much like leaning in to whisper a secret to your best friend; no one else can understand what you said because there's an extra layer, which we can call the "encryption method."

Why can only your friend understand the message?

Because they have what it takes to decode it: "the secret key."

But what's the problem with this simple method?

It's not a very secure way to share a secret. Imagine that another person gets ahold of the "secret key." They could easily understand the message. We can think of this person as a third party who has everything they need to decrypt and read the message.

This is where modern cryptography comes in. It allows your phone to whisper securely to your bank's computer. Whenever you send an encrypted text message or read your email, far more complex mathematical operations are happening under the hood.

Cryptography has been used for centuries, starting from basic ciphers and evolving into the complex algorithms that scramble sensitive data in modern computing. It forms a crucial part of many fields, including finance, the military, and private communications.

Introduction to Cryptography

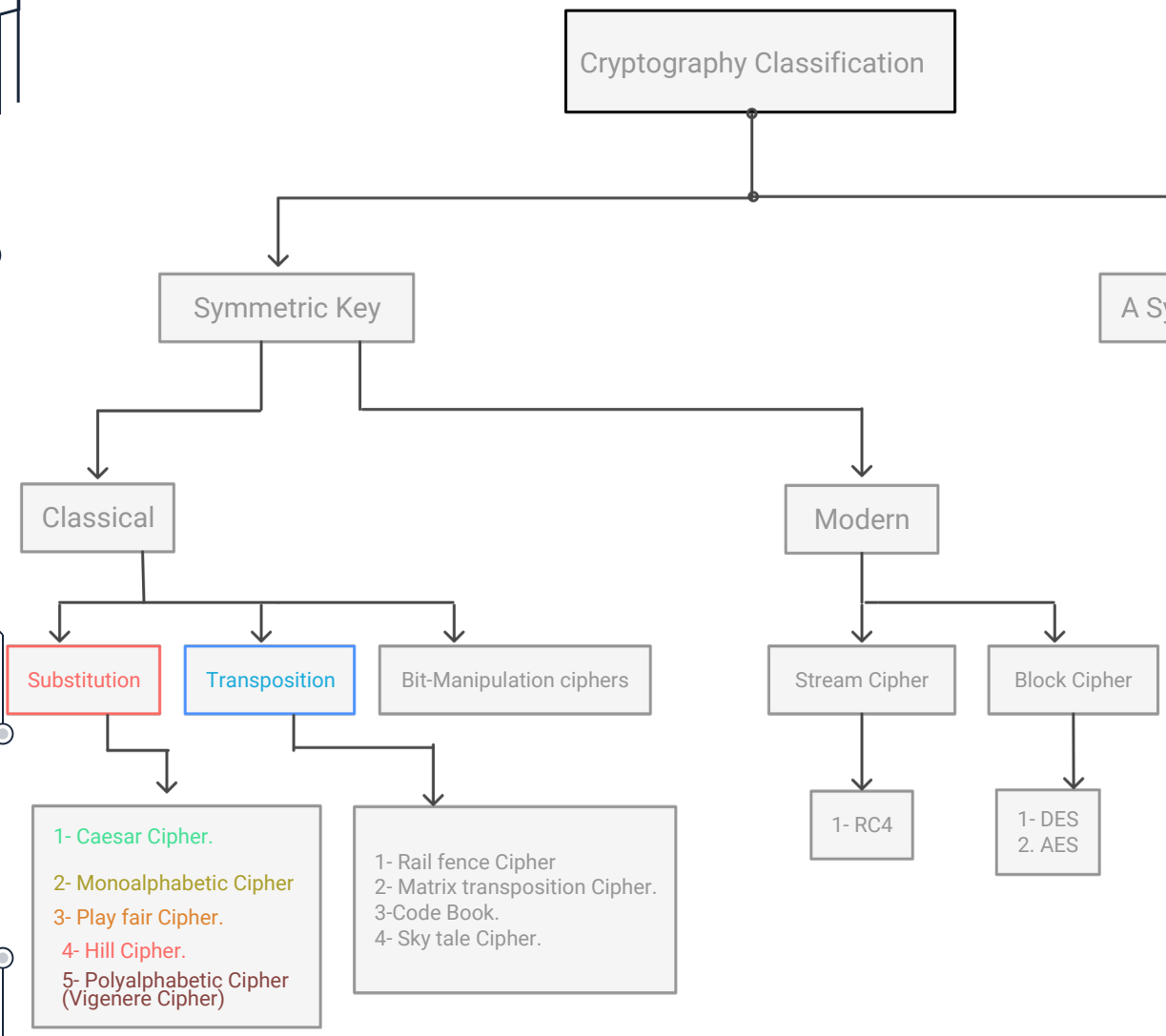
1933-1945: The Military Use of Cryptography

During WWII, the German military used the **"Enigma machine"** for secure communication. This machine encrypted messages using a combination of mechanical and electrical systems.

The Enigma's Basic Mechanism: It was a brilliant yet simple electromechanical system that worked as follows:

1. **Input**: A user presses a letter on the keyboard.
2. **Processing**: A series of rotors scrambles the electrical signal. Each time a key is pressed, the rotors shift, producing a different encryption pattern for each letter.
3. **Output**: A light bulb corresponding to the new letter lights up. This lit-up letter is the encrypted output.

Cryptography Classification diagram



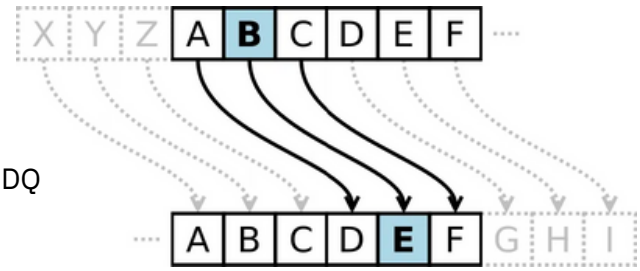
1- Caesar Cipher

The Caesar Cipher is one of the simplest and oldest methods of encrypting messages, named after Julius Caesar, who reportedly used it to protect his military communications.
The technique Involves replacing " shifting " each letter of the alphabet by a fixed number of places .
with a shift of three, the letter 'A' becomes 'D', 'B' becomes 'E', and so on. even its look so simple the Caesar Cipher formed the Foundation stone of modern cryptographic techniques.
Alphabet is wrapped around so that the letter following Z is A " as a circle "

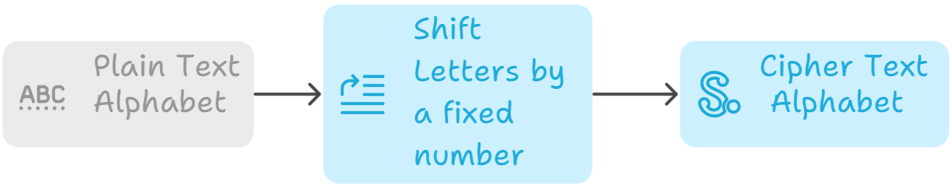
Plain Text : i am at the university of Jordan

Key :3 (1-26)

Cipher Text : L DP DW WKH XQLYHUVLWB RI MRUGDQ



Caesar Cipher Encryption Process



Plain : 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

Cipher: 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

assign a numerical equivalent to each letter “index“ :

Then the algorithm can be expressed as follows :

The general Caesar algorithm for Encryption is

C = E(k, p) = (p + k) mod 26 k takes a value in the range 1 to 25

The decryption algorithm is

p = D(k, C) = (C - k) mod 26

The Caesar cipher is a simple substitution cipher where each letter in the plaintext is "shifted" a certain number of places down the alphabet.
Step-by-Step Encryption: We will take each letter of "Malek" and shift it forward 5 places in the alphabet.

M + 5 → R
A + 5 → F
L + 5 → Q
E + 5 →J
K + 5 → P
The Result:
Plaintext: Malek
Ciphertext: RFQJP

decrypt, we do the reverse of encryption. Instead of shifting each letter forward 5 places in the alphabet, we will shift each letter backward 5 places. We will take each letter of "RFQJP" and shift it backward 5 places in the alphabet.

R - 5 →M
F - 5 →A
Q - 5 →L
J - 5 →E
P - 5 →K
The Result:
Ciphertext: RFQJP
Plaintext: MALEK

Alphabet Indexing

Indices	Letters
0	a
1	b
2	c
3	d
4	e
5	f
6	g
7	h
8	i
9	j
10	k
11	l
12	m
13	n
14	o
15	p
16	q
17	r
18	s
19	t
20	u
21	v
22	w
23	x
24	y
25	z

Disadvantages for Caesar Cipher

1. The encryption and decryption algorithms are known that's make it easy to decrypt the cipher text .

2. There are only 25 keys to try [leads to Brute-force attack], because there's a 26 letter only, if we try "ZERO" as the key we will have the same encrypted text so that's why we except zero .

3. The language of the plaintext is known and easily recognizable.

Brute-force attack

it's work by trying the 25 key possibility until you find a readable text

Cipher text : SQDYMZK

After applying the Brute-force attack the plaintext is " GERMANY"

Shifts———-	Result
0	SQDYMZK
1	TREZNAL
2	USFAOBM
3	VTGBPCN
4	WUHCQDO
5	XVIDREP
6	YWJESFQ
7	ZXKFTGR
8	AYLGUHS
9	BZMHVIT
10	CANIWJU
11	DBOJXKV
12	ECPKYLW
13	FDQLZMX
14	GERMANY
15	SQDYMZK
16	TREZNAL
17	USFAOBM
18	VTGBPCN
19	WUHCQDO
20	XVIDREP
21	SQDYMZK
22	TREZNAL
23	USFAOBM
24	VTGBPCN
25	WUHCQDO

2- Monoalphabetic Cipher

Monoalphabetic Cipher is a part of the substitution technique in which a single cipher alphabet is used per message. Monoalphabetic Cipher eliminates the brute-force techniques for cryptanalysis.

In Monoalphabetic cipher, the mapping is done randomly and the difference between the letters is not uniform.

Permutation

Of a finite set of elements S is an ordered sequence of all the elements of S , with each element appearing exactly once.

If the "cipher" line can be any permutation of the 26 alphabetic characters, then there are 26! or greater than 4×10^{26} possible keys.

Simply, a permutation is every possible way to arrange a set of items in a different order.

In other words, if you have a number of distinct [unique] items, each arrangement of those items is a "permutation."

For Example:
Let's say you have 3 letters: A, B, C

- A C B
- B A C
- B C A
- C A B
- C B A

those are permutation

Encryption

replace the letters with the corresponding in the second row

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

Plain : Cyber Security

Cipher : iALKX WKiZXTEA

Decryption

replace the letters with the corresponding in the first row. "read from the second row and replace it with the letter in the first row"

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

Cipher : iALKX WKiZXTEA

Plain : Cyber Security

Disadvantages Monoalphabetic

1- Easy to break because they reflect the frequency data of the original alphabet
2- exposure to guessing attack using the English letter frequency of occurrence of letters.

Diagram

Two-letter combination
Most common is th

Trigram

Three-letter combination
Most frequent is the (the)

A Countermeasure is to provide multiple substitutes (homophones) for a single letter

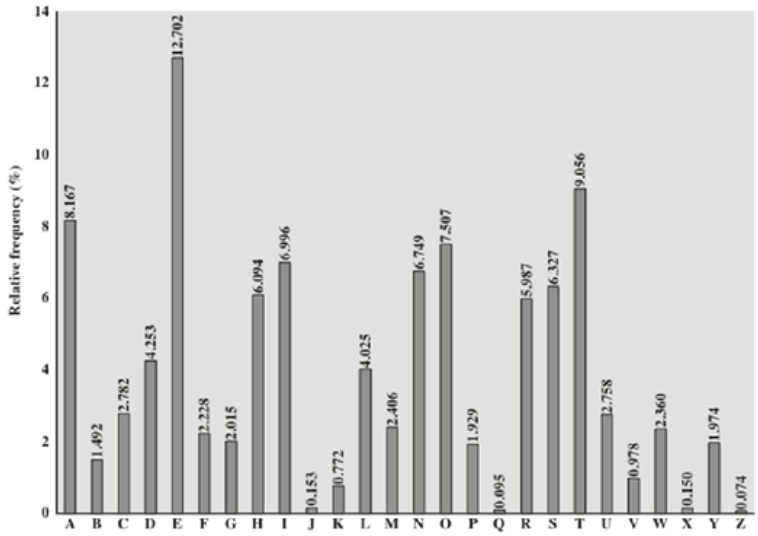
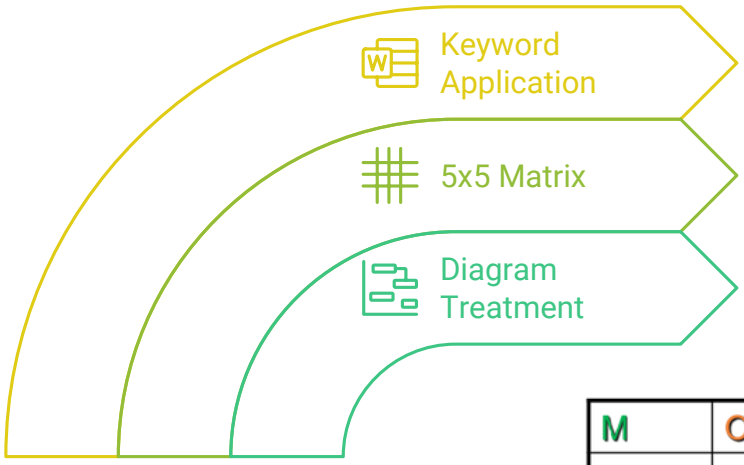


Figure 3.5 Relative Frequency of Letters in English Text

3- Play fair Cipher

Best-known multiple-letter encryption
cipher
Treats diagrams in the plaintext as single units and translates these units into
ciphertext
diagrams

5 x 5 matrix of letters constructed using a keyword (Ex :
Hello)
Invented by British scientist Sir Charles Wheatstone
in 1854
Used as the standard field system by the British Army in World War I and the U.S.
Army and
other Allied forces during World
War II



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

Steps :

Ex: The Keyword [MONARCHY] :

Fill the matrix with the keyword and complete filling the
matrix with all letters starting from A to Z but don't write
the letters again .
if you see after the last letter of the keyword we typed
B why not A ?
because we already typed A before .
and we should but the [I/J] together why ?
because we have a 5×5 Matrix that's take only 25 letter.

Rules For Encryption :

1. Diagrams → separate the plain text each 2 letters together
2. Repeating Letters Put a Filler Letter Ex. [X]
3. Same column Shift down ↓
4. Same row Shift to the right ↷

→ if the letter the last one of the column or the row WRAP AROUND "as a circle"

5. Different row and column Swap ⇄

Ex: Plain Text "JU UNIVERSITY"

JU→ Different row and column Swap J→ E U→ X = EX
UN →
IV →
ER →
SI →
TY →

Ex : Plain Text " COFFEE "
COFFEE → CO FX FE EX
→ Repeating Letters Put a Filler Letter Ex. [X]

CO → Different row and column Swap C→ H O→ M = HM
FX →
FE→
EX→

Try to solve :"The key is [Jordan] "
MOSQUE
ATTACK
YOUR NAME

For Decryption

simply just reverse the steps
1.Same column Shift Up↑
2. Same row Shift to the Left ↶
3. Different row and column Swap ⇄

Ex:
Cipher Text : ga tl mz cl rq tx
G and A not at the same row or column so
G=i/j
A=N

While CL at the same column
So move from down to up only one step
C will be M
L will be E

Plain Text: "in st ru me nt sz"

4- Hill Cipher

Developed by Lester Hill in 1929
Strength is that it completely hides single-letter frequencies
The use of a larger matrix hides more frequency information
A 3 x 3 Hill cipher hides not only single-letter but also two-letter frequency information
Strong against a ciphertext-only attack but easily broken with a known plaintext attack

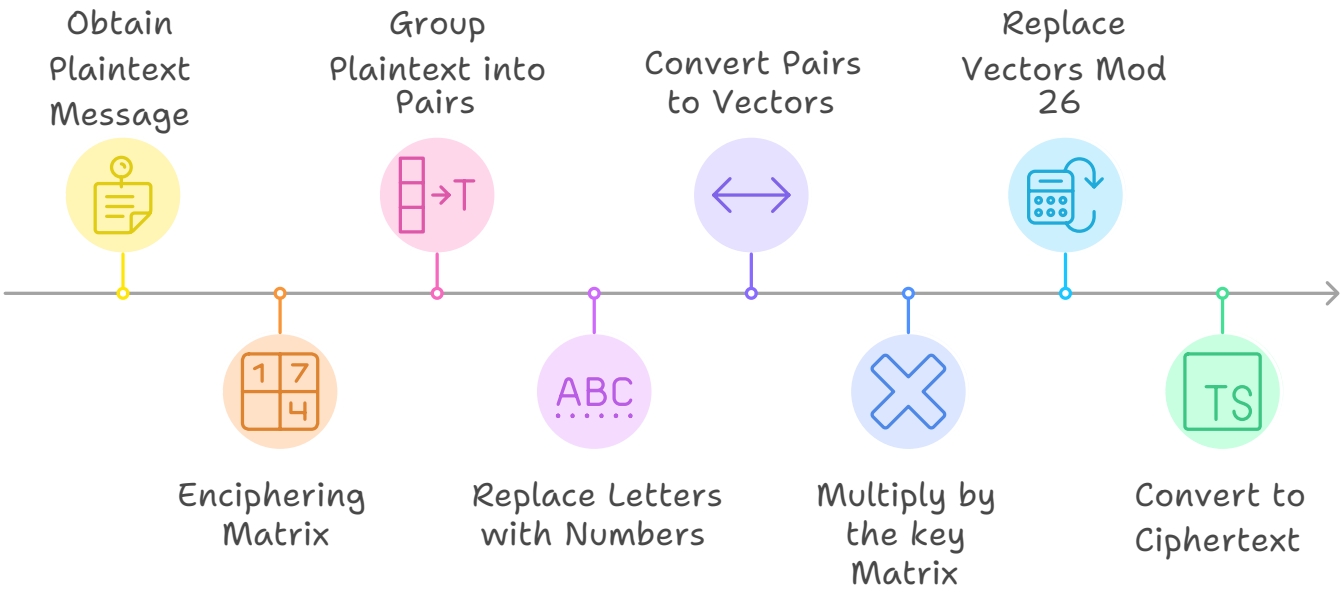
Encryption:
1. Obtain a plaintext message to encode in Standard English with no punctuation.
2. Create an enciphering matrix.
a. Form a square 2x2 or 3x3 matrix with nonnegative integers each less than 26.
b. Check that its determinant does NOT factor by 2 or 13. If this is so, return to Step a
3. Group the plaintext into pairs. If you have an odd number of letters, repeat the last letter.
4. Replace each letter by the number corresponding to its position in the alphabet i.e. A=0, B=1, C=2...Z=25.
5. Convert each pair of letters into plaintext vectors.
6. Multiply the enciphering matrix by each plaintext vector.
7. Replace each new vector by its residue modulo 26 if possible
8. Convert each entry in the cipher text vector into its corresponding position in the alphabet.
9. Align the letters in a single line without spaces. The message is now enciphered.
Cipher text = K*P mod 26
Where k is a key matrix that should not a singular matrix and P= plaintext

Encryption

Cipher text = (K*P) mod 26

Determinant	1	3	5	7	9	11	15	17	19	21	23	25
Reciprocal Modulo 26	1	9	21	15	3	19	7	23	11	5	17	25

Encryption Process



Ex:

Consider the message 'ACT', and the key below (or GYB/NQK/URP in letters):

Plaintext : 'ACT'

key=GYB/NQK/URP $= \begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$

ACT $= \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix}$

Now apply the Encryption algorithm
Cipher text = (K*P) mod 26

Cipher = $\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} = \begin{pmatrix} 67 \\ 222 \\ 319 \end{pmatrix} \equiv \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} \pmod{26}$

Cipher = 15→P,14→O,7→H which corresponds to ciphertext of 'POH'

Try to encrypt :

Network:

sara:

Cat:

The Key : 3 10 20
20 9 17
9 4 17

Note: the matrix is 3 × 3 so , the plain text should be chopped each 3 letters together.

Decryption :

To decrypt a ciphertext encoded using the Hill Cipher, we must find the inverse matrix.

Once we have the inverse matrix, the process is the same as encrypting. That is we multiply the inverse key matrix by the column vectors that the ciphertext is split into, take the results

modulo the length of the alphabet, and finally convert the numbers back to letters.

Plain text = $(K^{-1} * C) \bmod 26$

finding the inverse key matrix

$K^{-1} = (d^{-1} * adj\ (K)) \bmod 26$

Example 2 × 2 Matrix :

The keyword hill and our ciphertext is "APADJ TFTWLFJ". We start by writing out the keyword as a matrix and converting this into a key matrix as for encryption. Now we must convert this to the inverse key matrix, for which there are several steps.

$$\begin{pmatrix} H & I \\ L & L \end{pmatrix} = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}$$

Step 1 - Find the Multiplicative Inverse of the DeterminantThe determinant is a number that relates directly to the entries of the matrix.

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc \mod 26$$

Note : when calculating the mod if the value negative we need to add 26 to the negative values to get a number between 0 and 25 .

$$\begin{vmatrix} 7 & 8 \\ 11 & 11 \end{vmatrix} = 7 \times 11 - 8 \times 11 = -11 = 15\ mod\ 26 = 15$$

Determinant	1	3	5	7	9	11	15	17	19	21	23	25
Reciprocal Modulo 26	1	9	21	15	3	19	7	23	11	5	17	25

Determinant(K)=15 = Inverse= 7

So the multiplicative inverse of the determinant modulo 26 is 7. We need this number later.

Step 2 - Find the Adjugate [adjoint] Matrix

The adjoint matrix is a matrix of the same size as the original. For a 2 x 2 matrix, it is just moving the elements to different positions and changing a couple of signs. Algebraically this is given below.

$$adj\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

once we have these values we will need to take each of them modulo 26 .
we get the matrix below.

$$adj\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} = \begin{pmatrix} 11 & -8 \\ -11 & 7 \end{pmatrix} = \begin{pmatrix} 11 & 18 \\ 15 & 7 \end{pmatrix}$$

Step 3 - Multiply the Multiplicative Inverse of the Determinant by the adjoint Matrixwe now multiply the inverse determinant from step 1 by each of the elements of the adjoint matrix from step 2. Then we take each of these answers modulo 26.

$$7 \times \begin{pmatrix} 11 & 18 \\ 15 & 7 \end{pmatrix} = \begin{pmatrix} 77 & 126 \\ 105 & 49 \end{pmatrix} = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \ mod\ 26$$

$$K^{-1} = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}$$

After finding the inverse key matrix, we have to convert the ciphertext into column vectors and multiply the inverse matrix by each column vector in turn, take the results modulo 26 and convert these back into letters to get the plaintext.

ciphertext is "APADJ TFTWLFJ"

$$\begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}\begin{pmatrix} A \\ P \end{pmatrix} = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}\begin{pmatrix} 0 \\ 15 \end{pmatrix} = \begin{pmatrix} 25 \times 0 + 22 \times 15 \\ 1 \times 0 + 23 \times 15 \end{pmatrix} = \begin{pmatrix} 330 \\ 345 \end{pmatrix} = \begin{pmatrix} 18 \\ 7 \end{pmatrix} mod\ 26 = \begin{pmatrix} s \\ h \end{pmatrix}$$

$$\begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}\begin{pmatrix} A \\ D \end{pmatrix} = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}\begin{pmatrix} 0 \\ 3 \end{pmatrix} = \begin{pmatrix} 25 \times 0 + 22 \times 3 \\ 1 \times 0 + 23 \times 3 \end{pmatrix} = \begin{pmatrix} 66 \\ 69 \end{pmatrix} = \begin{pmatrix} 14 \\ 17 \end{pmatrix} mod\ 26 = \begin{pmatrix} o \\ r \end{pmatrix}$$

$$\begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}\begin{pmatrix} J \\ T \end{pmatrix} = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}\begin{pmatrix} 9 \\ 19 \end{pmatrix} = \begin{pmatrix} 25 \times 9 + 22 \times 19 \\ 1 \times 9 + 23 \times 19 \end{pmatrix} = \begin{pmatrix} 643 \\ 446 \end{pmatrix} = \begin{pmatrix} 19 \\ 4 \end{pmatrix} mod\ 26 = \begin{pmatrix} t \\ e \end{pmatrix}$$

$$\begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}\begin{pmatrix} F \\ T \end{pmatrix} = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}\begin{pmatrix} 5 \\ 19 \end{pmatrix} = \begin{pmatrix} 25 \times 5 + 22 \times 19 \\ 1 \times 5 + 23 \times 19 \end{pmatrix} = \begin{pmatrix} 543 \\ 442 \end{pmatrix} = \begin{pmatrix} 23 \\ 0 \end{pmatrix} mod\ 26 = \begin{pmatrix} x \\ a \end{pmatrix}$$

$$\begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}\begin{pmatrix} W \\ L \end{pmatrix} = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}\begin{pmatrix} 22 \\ 11 \end{pmatrix} = \begin{pmatrix} 25 \times 22 + 22 \times 11 \\ 1 \times 22 + 23 \times 11 \end{pmatrix} = \begin{pmatrix} 792 \\ 275 \end{pmatrix} = \begin{pmatrix} 12 \\ 15 \end{pmatrix} mod\ 26 = \begin{pmatrix} m \\ p \end{pmatrix}$$

$$\begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}\begin{pmatrix} F \\ J \end{pmatrix} = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}\begin{pmatrix} 5 \\ 9 \end{pmatrix} = \begin{pmatrix} 25 \times 5 + 22 \times 9 \\ 1 \times 5 + 23 \times 9 \end{pmatrix} = \begin{pmatrix} 323 \\ 212 \end{pmatrix} = \begin{pmatrix} 11 \\ 4 \end{pmatrix} mod\ 26 = \begin{pmatrix} l \\ e \end{pmatrix}$$

The Plain Text Will Be “short example”

3 × 3 Matrix :

Step 1 - Find the Multiplicative Inverse of the Determinant

For a 3 x 3 matrix it is found by multiplying the top left entry by the determinant of the 2 x 2 matrix formed by the entries that are not in the same row or column as that entry ignore [b ,c andd,g], then multiply b with d and i minus g and f [ignore [a , c] and [e , h] ignore [a , b] and [f , i] etc .

This is shown more clearly in the algebraic version below.

$$\begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} = a\begin{vmatrix} e & f \\ h & i \end{vmatrix} - b\begin{vmatrix} d & f \\ g & i \end{vmatrix} + c\begin{vmatrix} d & e \\ g & h \end{vmatrix}$$

$$= a(ei - fh) - b(di - fg) - c(dh - eg)$$

Once we have calculated this value, we take it modulo 26.

Example :

ciphertext message "**SYICHOLER**" using the keyword **alphabet**

$$\begin{pmatrix} A & L & P \\ H & A & B \\ E & T & A \end{pmatrix} = \begin{pmatrix} 0 & 11 & 15 \\ 7 & 0 & 1 \\ 4 & 19 & 0 \end{pmatrix}$$

Step 1 - Find the Multiplicative Inverse of the Determinant

$$\begin{vmatrix} 0 & 11 & 15 \\ 7 & 0 & 1 \\ 4 & 19 & 0 \end{vmatrix} = 0\begin{vmatrix} 0 & 1 \\ 19 & 0 \end{vmatrix} - 11\begin{vmatrix} 7 & 1 \\ 4 & 0 \end{vmatrix} + 15\begin{vmatrix} 7 & 0 \\ 4 & 19 \end{vmatrix}$$

$$= 0(0 - 19) - 11(0 - 4) + 15(133 - 0)$$

$$= 0 + 44 + 1995$$

$$= 2039$$

$$= 11 \bmod 26$$

Determinant	1	3	5	7	9	11	15	17	19	21	23	25
Reciprocal Modulo 26	1	9	21	15	3	19	7	23	11	5	17	25

Determinant (K) = 11 = Inverse = 19

Step 2 - Find the adjoint Matrix

$$\begin{vmatrix} 0 & 11 & 15 \\ 7 & 0 & 1 \\ 4 & 19 & 0 \end{vmatrix}$$

repeat the first two columns then repeat the first two rows again now I'm going to repeat the first two columns

0 11 15 0 11
7 0 1 7 0
4 19 0 4 19

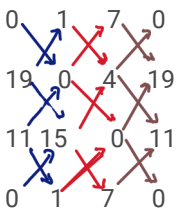
here I have completed repeating the first two columns

now let's repeat the first two rows so
these two are the first two rows we have after repeat the first two columns
now we will have a 5 x 5 matrix

0 11 15 0 11
7 0 1 7 0
4 19 0 4 19
0 11 15 0 11
7 0 1 7 0

then just ignore the first row and the first Column
now we will have a 4 × 4 matrix

0 1 7 0
19 0 4 19
11 15 0 11
0 1 7 0



then to get the value of first row first column multiply 0 × 0 - 19 × 1

to get the value of first row 2nd column multiply 19 × 15 - 11 × 0
etc.

adj = [-19 285 11 ; ,, ,, ,, ; ,, ,, ,,]

then complete all steps like 2 × 2 matrix

5- Polyalphabetic Cipher (Vigenere Cipher)

The Polyalphabetic cipher is an extension of monoalphabetic ciphers since the encryption cycles through the plaintext with greater than one substitution alphabet. An example is the Vigenère cipher, created by Blaise de Vigenère in the 16th century. It encrypts messages through a series of Caesar ciphers where each plaintext letter is shifted over a repeated secret key phrase. The cipher uses shifts of 1 to 26 and employs a number of mixed alphabets, making it more secure than simple monoalphabetic encryption. While used during the American Civil War and once thought to be unbreakable, it has since been demonstrated to be vulnerable to modern cryptanalysis.

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

EncryptionThe plaintext(P) and key(K) are added modulo 26.Ei = (P i + K i) mod 26

Example:
find the cipher text for the plaintext “she is listening ” using the word “PASCAL” as the key
Ciphertext :hhwkswxslgntcg

Plaintext	S	h	e	i	s	l	i	s	t	e	n	i	n	g
Key	p	a	s	C	a	l	p	a	s	c	a	l	p	a
(P+K)mod26	(18+15) mod26	(7+0) mod26	(4+18) mod26	(8+2) mod26	(18+0) mod26	(11+11) mod26	(8+15) mod26	(18+0) mod26	(19+18) mod26	(4+2) mod26	(13+0) mod26	(8+11) mod26	(13+15) mod26	(6+0) mod26
result	7	7	22	10	18	22	23	18	11	6	13	19	2	6
ciphertext	h	h	w	k	S	w	x	s	l	g	n	t	c	g

Try to encrypt :
“ [your name] wants to go to the University ”
the key ’‘ Cryptography ’

DecryptionDi = (Ei - Ki) mod 26

Example:
find the plain text for the ciphertext “hhwkswxslgntcg” using the word “PASCAL” as the key

ciphertext	h	h	w	k	S	w	x	s	l	g	n	t	c	g
Key	p	a	s	C	a	l	p	a	s	c	a	l	p	a
(C-K)mod26	(7-15+26) mod26	(7-0) mod26	(22-18) mod26	(10-2) mod26	(18-0) mod26	(22-11) mod26	(23-15) mod26	(18-0) mod26	(11-18+26) mod26	(6-2) mod26	(13-0) mod26	(19-11) mod26	(2-15+26) mod26	(6-0) mod26
result	18	7	4	8	18	11	8	18	19	4	13	8	13	6
plaintext	s	h	e	i	s	l	i	s	t	e	n	i	n	g

2. 2 Transposition

Transposition Ciphers are ciphers in which the plaintext message is rearranged by some means agree upon by the sender and receiver.

1- Rail fence Cipher

Simplest transposition cipher Plaintext is written down as a sequence of diagonals and then read off as a sequence of rows

Example :

the message “meet me after the Cryptography class”

with a rail fence of depth 3, we would write:

M				m				t				h				y				g				h				a		
	e		t		e		f		e		t		e		r		p		o		r		p		y		l		s	
		e				a				r				c				t				a				c				s	

now read the table row by row

Encrypted message is: mmthyghaetefeterporpylsearctacs

For Decryption

Create an empty table depends on the depth [KEY] and number of characters.

Rows = key, Columns = length of the ciphertext.

Mark the zig-zag path: Place a marker (*) in the grid where the letters should go, moving down and then up diagonally. ↘ ↗ ↘ ↗ ↘ ↗

Fill the grid: Place the ciphertext letters onto the markers, filling each row completely from left to right before moving to the next row.

Read the plaintext: Read the letters from the grid by following the zig-zag path from the top-left corner.

*				*				*				*				*				*				*				*		
	*		*		*		*		*		*		*		*		*		*		*		*		*		*		*	
		*				*				*				*				*				*				*				*	

after filling the Encrypted message : mmthyghaetefeterporpylsearctacs

M				m				t				h				y				g				h				a		
	e		t		e		f		e		t		e		r		p		o		r		p		y		l		s	
		e				a				r				c				t				a				c				s	

read it zigzag ↘ ↗ ↘ ↗ ↘ ↗

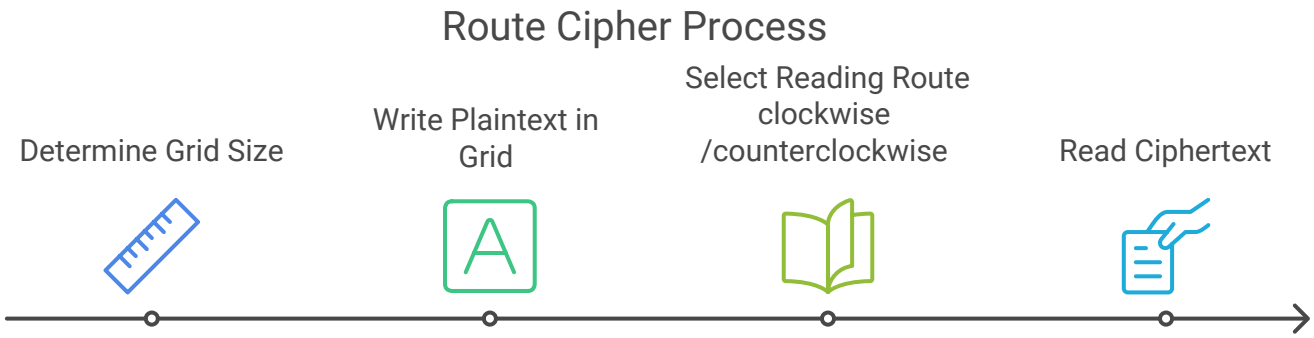
The message will be “meet me after the Cryptography class”

2- The Route Cipher

the key is which route to follow when reading the ciphertext from the block created with the plaintext. The plaintext is written in a grid, and then read off following the route chosen First we write the plaintext in a block of reasonable size for the plaintext.

Part of your key is the size of this grid, so you need to decide on either a number of columns or number of rows in the grid before starting. Once the plaintext is written out in the grid, you use the Route assigned.

1. From top-right corner clockwise to the center
2. From top-right corner counterclockwise to the center



Encryption

The Key size means the number of columns

Example :

Plain text: our cryptography exam will be tomorrow

Key size =5

1. From top-right corner clockwise to the center

o	u	r	c	r
y	p	t	O	g
r	a	p	h	Y
e	x	a	m	W
i	l	l	b	E
t	o	m	o	R
r	o	w	x	x

clockwise

o	u	r	c	r
y	p	t	O	g
r	a	p	h	Y
e	x	a	m	W
i	l	l	b	E
t	o	m	o	R
r	o	w	x	x

counterclockwise

The cipher text ‘clockwise’ : rgywerxxwortieryourcohmbomolxaptpal

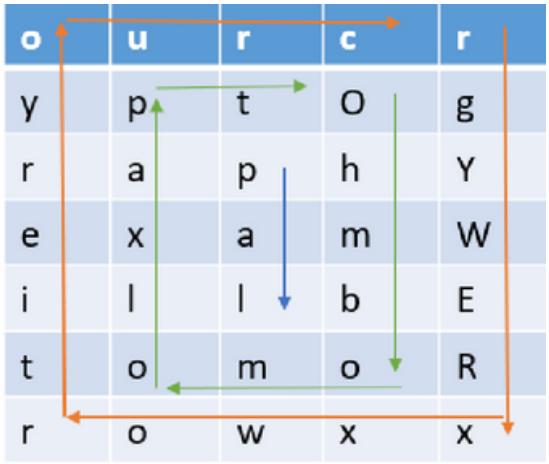
NOTE : you can add rows only, if there's an empty cell you can add X
remember that you can't add column WHY ?
because the number of columns means the Key so we can't edit the key

Example:
The cipher text 'clockwise' : rgywerxxwortieryourcohmbomolxaptpal
The Key =5

The number of rows = characters of the cipher text / key size
Rows = 35 / 5 = 7 rows

then make a 7 × 5 matrix and then fill the matrix with the cipher text depends on the Reading Route clockwise or counterclockwise
then read the matrix row by row

The cipher text 'clockwise'



Plain text: our cryptography exam will be tomorrow

CHAPTER THREE

MODERN ENCRYPTION TECHNIQUES

1. Stream Ciphers

- Stream ciphers encrypt digital data in one bit or one byte at a time, as the plaintext is combined with a **keystream** (a series of bits/bytes), often using the XOR operation. This contrasts with block ciphers that encrypt data in fixed-length blocks of bytes.
- Ex:

  Autokeyed Vigenère cipher

  Vernam cipher

- **One-Time Pad:** An ideal stream cipher, it takes a keystream of the same size as the message consisting of truly random values and employed only once. if truly random, it's provably unbreakable mathematically.

- For **practical reasons** the bit stream generator must be implemented as an algorithmic procedure so that the cryptographic bit stream can be produced by both users The two users need only share the generating key and each can produce the keystream

Vernam Cipher

Uses the XOR operation between the plaintext and the keystream. Both encryption and decryption are achieved by performing XOR with the same keystream.

Figure 7.7 is a representative diagram of stream cipher structure. In this structure, a key is input to a pseudorandom bit generator that produces a stream of 8-bit numbers that are apparently random. The output of the generator, called a keystream, is combined one byte at a time with the plaintext stream using the bitwise exclusive-OR (XOR) operation. For example, if the next byte generated by the generator is 01101100 and the next plaintext byte is 11001100, then the resulting ciphertext byte is

- 11001100 plaintext
- 01101100 key stream
- 10100000 ciphertext

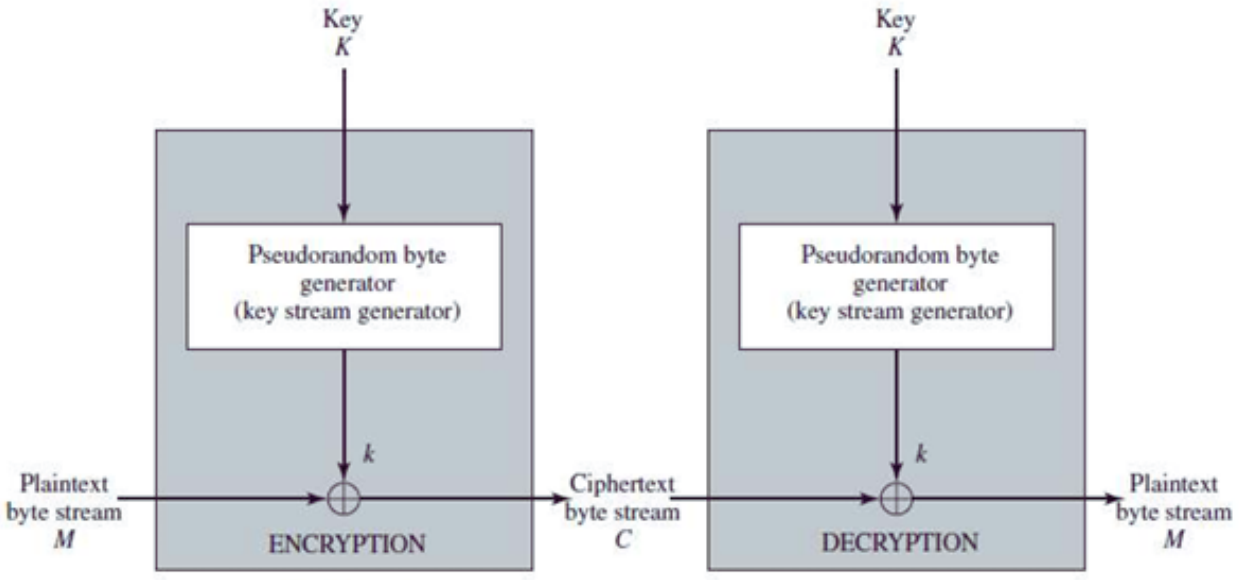


Figure 7.7 Stream Cipher Diagram

Encryption

```
  11001100 plaintext
⊕ 01101100 key stream
  10100000 ciphertext
```

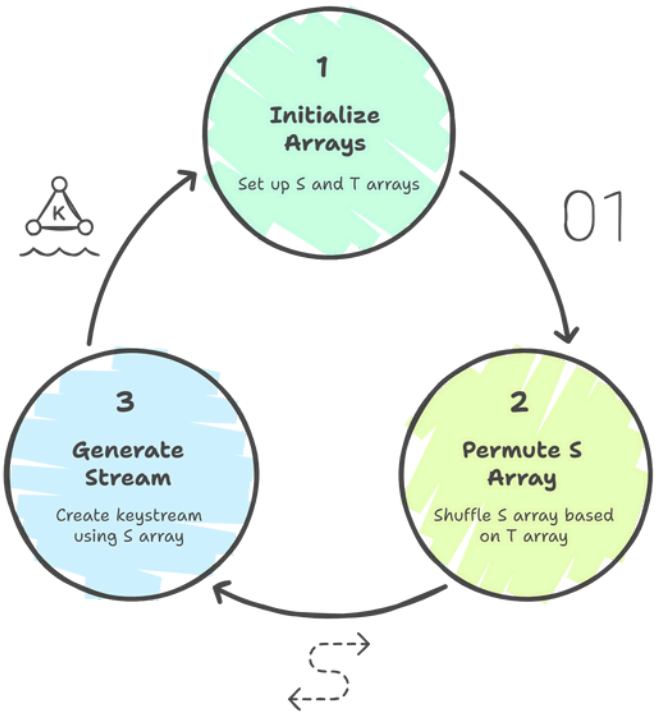
Decryption

```
⊕ 10100000 ciphertext
  01101100 key stream
  11001100 plaintext
```

RC4 Stream Cipher

·RC4 is a stream cipher designed in 1987 by Ron Rivest for RSA Security.

It is a variable key size stream cipher with byte-oriented operations.
The algorithm is based on the use of a random permutation.
Analysis shows that the period of the cipher is overwhelmingly likely to be greater than 10 100
RC4 is used in the Secure Sockets Layer/Transport Layer Security (SSL/TLS) standards that have been defined for communication between Web browsers and servers.
It is also used in the Wired Equivalent Privacy (WEP) protocol and the newer WiFi Protected Access (WPA) protocol that are part of the IEEE 802.11 wireless LAN standard.



1. Initialization

```
for i = 0 to 255 do
    S[i] = i;
T[i] = K[i mod keylen];
```

2.Permutation

```
j = 0;
for i = 0 to 255 do
j = (j + S[i] + T[i]) mod 256;
Swap (S[i], S[j]);
```

3.Stream Generation

```
i, j = 0;
while (true)
i = (i + 1) mod 256;
j = (j + S[i]) mod 256;
Swap (S[i], S[j]);
t = (S[i] + S[j]) mod 256;
k = S[t];
```

An array S is initialized with sequential values (commonly 0 to 255). A temporary array T is formed from a user-provided key (repeated if necessary).

A permutation of the array S is generated by iteratively swapping elements based on values derived from T.

Pseudorandom Generation Algorithm After initialization, the algorithm enters a loop where two counters (i and j) are updated. At each iteration, a swap operation is performed, and a new value is generated from S which is then XORed with the plaintext.

RC4 Example:

use 8 x 3-bits. the state vector S is 8 x 3-bits. We will operate on 3-bits of plaintext at a time since S can take the values 0 to 7, which can be represented as 3 bits.
we use a 4 x 3-bit key of K = [1 2 3 6].
plaintext P = [1 2 2 3]
The first step is to generate the stream. Initialize the state vector S and temporary vector T. S is initialized so the S[i] = i, and T is initialized so it is the key K (repeated as necessary).

1. Initialization

S=[01234567]

T=[12361236]

Trace this code

```
for i =0 to 8 do
s[i]=i;
 t[i]=k[i mod keylen]
```

Note :We can say the T is the reptation of the Key

2.Permutation

```
j=0;
for i= 0 to 7
 do j = (j + S[i] + T[i]) mod 8
 Swap(S[i],S[j]);
 end
```

Number of iteration8	S=[0 1 2 3 4 5 6 7]	Swap(S[i] , S[j])	i=0 , j=0
1	S = [1 0 2 3 4 5 6 7]	Swap (S[0],S[1])	i=0 , j=1
2	S = [1 3 2 0 4 5 6 7]	Swap(S[1],S[3])	i=1 , j=3
3	S = [2 3 1 0 4 5 6 7]	Swap(S[2],S[0])	i=2 , j=0
4	S = [2 3 1 6 4 5 0 7]	Swap(S[3],S[6])	i=3 , j=6
5	S = [2 3 1 4 6 5 0 7]	Swap(S[4],S[3])	i=4 , j=3
6	S = [2 3 5 4 6 1 0 7]	Swap(S[5],S[2])	i=5 , j=2
7	S = [2 3 5 4 6 0 1 7]	Swap(S[6],S[4])	i=6 , j=5
8	**S = [2 3 7 4 6 0 1 5]**	Swap(S[7],S[2])	i=7 , j=2

3.Stream Generation

i,j=0;
while (true) {
 i=(i+1)mod8;
j = (j + S[i]) mod 8;
 Swap (S[i], S[j]);
t = (S[i] + S[j]) mod 8; k = S[t]; }
The Encryption result
 plaintext stream P = [1 2 2 3]
with key K = [1 2 3 6]
using RC4
result C = [4 4 2 2].

Number of iteration	S = [2 3 7 4 6 0 1 5]	Swap(S[i] , S[j])	i=0 , j=0	T=(S[i] + S[j]) mod 8	K=S[t]	Encryption
1	S = [2, 4, 7, 3, 6, 0, 1, 5]	Swap(S[1],S[3])	i=1, j=3	T= (S[1] + S[3]) mod 8 = 7	k = S[7] = 5	first 3-bits of ciphertext is obtained by: k XOR P 5 XOR 1 = 101 XOR 001 = 100 = 4
2	S = [2, 4, 7, 3, 6, 0, 1, 5]	Swap(S[2],S[2])	i=2, j=2	T = (S[2] + S[2]) mod 8 = 6	k = S[6] = 1	Second 3-bits of ciphertext are: 1 XOR 2 = 001 XOR 010 = 011 = 3
3	S = [2, 4, 7, 0, 6, 3, 1, 5]]	Swap(S[3],S[5])	i=3, j=5	t = (S[3] + S[5]) mod 8 = 3	k = S[3] = 0	Third 3-bits of ciphertext are: 0 XOR 2 = 000 XOR 010 = 010 = 2
4	S = [2, 4, 7, 6, 0, 3, 1, 5]	Swap(S[4],S[3])	i=4,j=3	t = (S[4] + S[3]) mod 8 = 3	k = S[3] = 1	Last 3-bits of ciphertext are: 1 XOR 3 = 001 XOR 011 = 010 = 2

2. Block Ciphers

A block of plaintext is treated as a whole and used to produce a ciphertext block of equal length Typically a block size of 64 or 128 bits is used As with a stream cipher, the two users share a symmetric encryption key
The majority of network-based symmetric cryptographic applications make use of block ciphers

• Feistel Cipher Structure: Developed on ideas by Claude Shannon, the Feistel structure alternates between substitution and permutation operations to achieve both confusion and diffusion.

substitution

Each plaintext element or group of elements is uniquely replaced by a corresponding ciphertext element or group of elements.

permutation

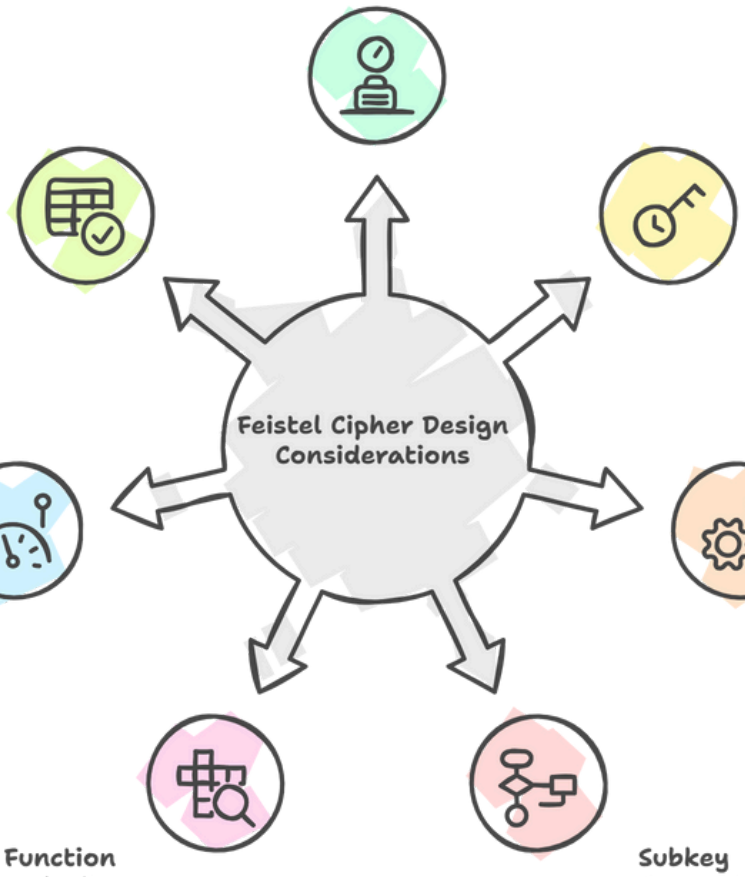
No elements are added or deleted or replaced in the sequence, rather the order in which the elements appear in the sequence is changed.

Confusion

make the relationship between the key and the ciphertext as complex as possible

Diffusion

spreads the plaintext statistics over the ciphertext, making the impact of any single bit change in the plaintext highly unpredictable.



Block Size

Larger block sizes enhance security but reduce speed.

Key Size

Larger key sizes increase security but may decrease speed.

Number of Rounds

More rounds increase security but also complexity.

Subkey Generation

Complex algorithms enhance security but increase analysis difficulty.

Round Function Complexity

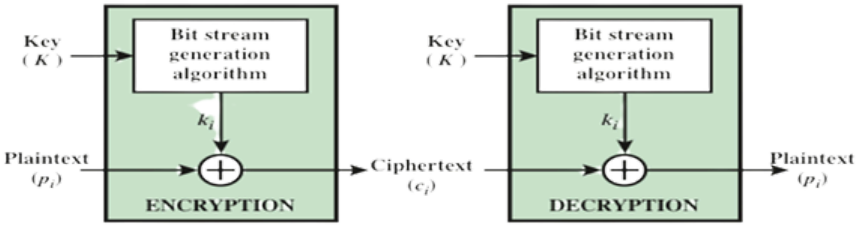
Greater complexity improves resistance to cryptanalysis.

Software Encryption Speed

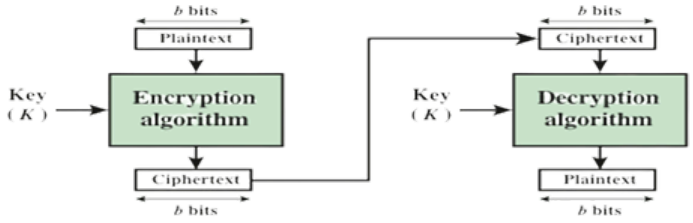
Fast software encryption is crucial for applications without hardware support.

Ease of Analysis

Clear explanations aid in identifying vulnerabilities.



(a) Stream Cipher Using Algorithmic Bit Stream Generator



(b) Block Cipher

Figure 4.1 Stream Cipher and Block Cipher

Block-wise encryption

Symmetric key sharing

Fixed block size

DES/AES

10010 01100 Bit-wise encryption

Symmetric key sharing

Variable bit stream

RC4/vernam

Block Cipher

Stream Cipher

DATA ENCRYPTION STANDARD (DES)

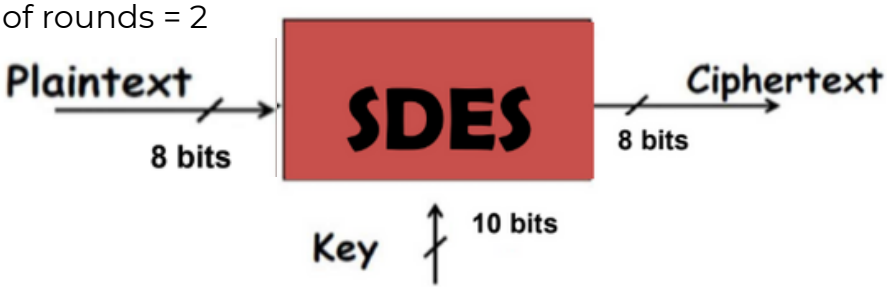
- Issued in 1977 by the National Bureau of Standards (now NIST) as Federal Information Processing Standard 46
- Was the most widely used encryption scheme until the introduction of the Advanced Encryption Standard (AES) in 2001
- Algorithm itself is referred to as the Data Encryption Algorithm (DEA)
  - Data are encrypted in 64-bit blocks using a 56-bit key
  - The algorithm transforms 64-bit input in a series of steps into a 64-bit output
  - The same steps, with the same key, are used to reverse the encryption

number of rounds = 16

هاي الارقام حفظ ممكن تجيب الدكتورة اسئلة عليها.

SIMPLIFIED DATA ENCRYPTION STANDARD (SDES)

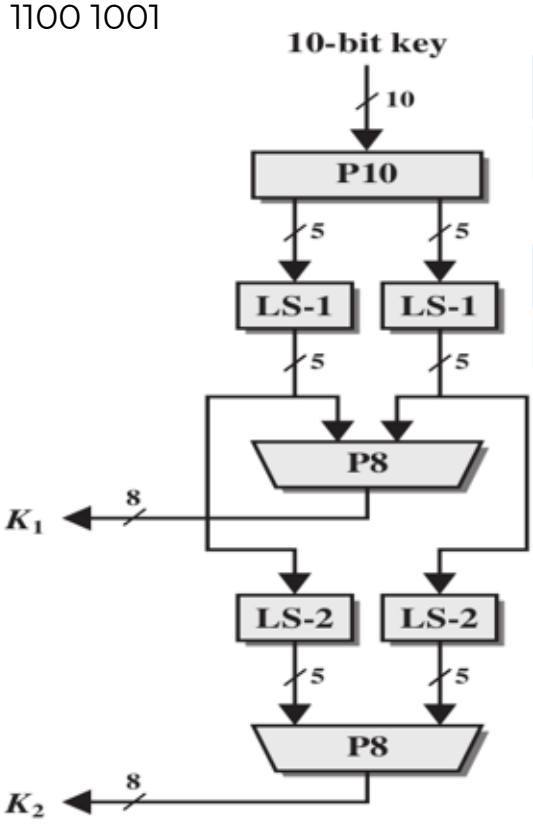
every round has a key
number of rounds = 2



- هلا حنشرح طريقة الحل ورح يكون على مرحلتين. المرحلة الاولى هي key generation حناخد النتيجة من هون ونستعملها بالمرحلة الثانية الي هي msg encryption يلي حنطلع منها المسج المشفر

- هلا حنبلش باول مثال بال SDES وحيكون في عنا رسمات هدول مش حفظ الدكتورة بتعطيكم ياهم بالامتحان
والدكتورة غالبا ما بتطلب السؤال كامل بس انتو امشو فيه من الصفر عشان تتدربو منيح على نمط السؤال، خطا واحد بدمر السؤال كامل هلا خلينا نبلش

- example: find the cipher text if the key is 00101 10011 and the message is 1100 1001

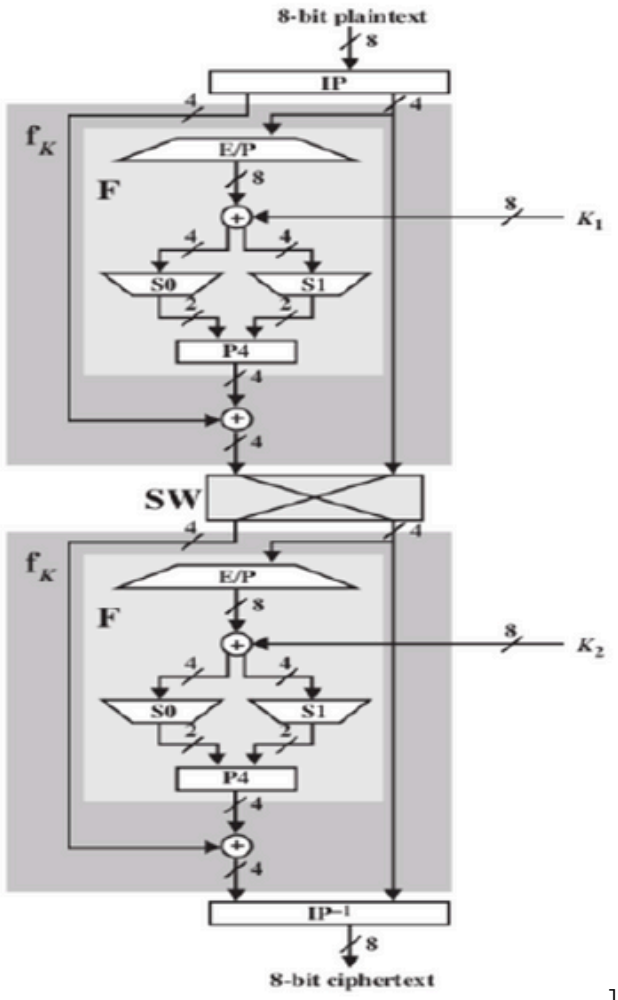


P10									
3	5	2	7	4	10	1	9	8	6

P8							
6	3	7	4	8	5	10	9

بنمشي حبه حبه بالاول بنمسك الkey وبنبلش فيه باول مرحلة (key generation)
هلا بنمشي على الرسمة اول اشي بدخل 10bits بنفووت على جدول p10 وبنعيد ترتيب المفتاح زي يلي بالجدول
1 2 3 4 5 6 7 8 9 10
k=00101 10011
بقول الجدول اول اشي بنحط 3 بعدين 5 بعدين 2 ....
بصير عنا p10=11000 10101
بعدين بنفصل كل خمسة بناخد اخر رقم على الشمال بنحطو يمين بصير 01011 10001 بعدين بندخل هاي على p8 نفس قبل شوي بس بتصير 8bits p8=k1=0010 0111 هيك بنكون اوجدنا اول خطوة هلا نفسها لp10 بعد ما حركنا اخر بت بنرجع نفصل كل خمسة بس بنحرك اخر بتين كمان على الشمال لليمين بتصير هيك 01101 00110 وبنرجه اندخلها كمان مره على جدول p8
p8=k2=0111 1010

هيك خلصنا اول مرحلة هلا ببلش الحل جد



S0	00	01	10	11
00	1	0	3	2
01	3	2	1	0
10	0	2	1	3
11	3	1	3	2

S1	00	01	10	11
00	0	1	2	3
01	2	0	1	3
10	3	0	1	0
11	2	1	0	3

IP							
2	6	3	1	4	8	5	7

P4			
2	4	3	1

E/P							
4	1	2	3	2	3	4	1

IP^{-1}							
4	1	3	5	7	2	8	6

12345678

- هلا بدنا نبلش نشفر المسج يلي كان m=1100 1001 بندخلو على جدول IP زي قبل شوي عادي وبصير عنا IP=1001 0110 وبنفصل كل اربعة بت لحال اول اربعة على الشمال ما بنلمسهم وبنزلهم بنستخدمهم بعدين،اما يلي على اليمين بدهم يدخلو على جدول E/P وبيطلع معنا E/P=0011 1100 وبنعمللها xor مع k1 يلي طلعناها من المرحلة الاولى

E/P= 0011 1100
k1= 0010 0111
xor ----------
0001 1011
s0 s1

هلا الجواب يلي طلع معنا بدنا اندخلو على s-box كل اربعة بدنا نفصلهم لثنين وانتبهو كل اربعة بفوتو جدول مختلف
اول واخر بت يلي هم 01 حيكونو عامودي البتين البنص يلي هم 00 حيكونو افقي وبتقاطعهم وبتاخد الجواب بطلع 3 وبنحولهم لباينري s0=11
بنكمل على ثاني اربعة 11 عامودي 01 افقي ينقاطعهم بطلع s1=01
بنحطهم جمب بعض وبنرقمهم وبندخلهم على جدول p4 وبصير عنا p4=1101
هلا بنرجع للقيمة يلي نزلناها لتحت المفروض من البداية وبنعمللها xor with p4

IP= 1001
p4= 1101
xor -------
0100

هلا وصلنا مرحلة swap بنقدر نقول خلصنا نص المشوار
بنبدل هلا اماكن يلي على اليمين بصير شمال ويلي على الشمال بصير على اليمين بين نص ip اليمين و ناتج xor بصير عنا sw=0110 0100 وبنرجع نعيد نفس القبل بزبط بس مع المفتاح الثاني يلي طلنا باول مرحلة حنمشي هون اسرع واذا حسيتو انكم ما فهمتو اشي اسالونا

take the left side 0100 and change it depend on E/P = 0010 1000
E/P xor k2 = 0101 0010
s0=01 s1=01 → 0101
take the result of the s-box and change it depend on p4 = 1100
p4 xor left side of SW = 1010
result of xor change it depend on IP^{-1} → cipher text = 0110 0001

SDES decryption

اما بالنسبة للdecryption فهي تقريبا نفس الاشي بس بالرسمة بنمشي من تحت لفوق
find the plain text if ip^{-1} =0110 0001 and k=00101 10011
اول اشي بنوجد المفاتيح من key generation بزبط زي الencryption (نفس السؤال عشان نثبت انو رح نرجع لنفس المسج)

take the key of 10 bits and inter it in p10 = 11000 10101
left lift bit L=10001 R=01011
now in p8 = 0010 0111 and that is k1
left the L and R two bits more L2 = 00110 R2 = 01101
in p8 again = 0111 1010 and that is k2

هلا بدنا نفوت المرحلة الثانية
هون بالعكس بدل ما اخربط ترتيب الارقام حسب الجدول بالعكس بحطهم وبرتبهم باخد الارقام بالتسلسل 1 بعدين 2 بعدين 3 ...

IP^{-1}							
4	1	3	5	7	2	8	6
0	1	1	0	0	0	0	1

بنشوف بالجدول ايش قيمة 1=1 ايش قيمة 2=0 وبنرتبهم هيك IP=1010 0100 R2=0100 هلا بنرفع R2 لفوق وبنرجع نمشي لتحت طبيعي عشان انجيب باقي المعلومات

we enter R2 in E/P=0010 1000
E/P xor k2 = 0101 0010
s-box=01 01
p4 = 1100
هلا بنرجعها لفوق عند السواب بنعكس النتائج وبنرفعها p4 xor IP (left side)= L1 = 0110
وبنعيد نفس الخطوات هاي عشان نجيب المسج
SW=0110 0100 swap the answer = 0100 0110 (R0=0110 (part of the ip))
enter R0 in E/P=0011 1100

E/P xor k1 = 0001 1011
s-box=11 01
p4 = 1101
p4 xor IP (left side)= L0 = 1001
IP = 1001 0110 بنرجع زي قبل شوي بندخلها على الجدول وبنرتبها ترتيب صح وبطلع معنا المسج
M=1100 1001 وبنلاحظ انو نفس المسج يلي كان بسؤال القبل يعني حلنا صح

ديرو بالكم عهاد الجدول بتجيب منو اسئلة

The Difference between DES and Simplified -DES

Parameters	DES	S-DES
M length	64 bits	8 bits
C length	64 bits	8 bits
K length	56 bits	10 bits
Number of Round	16 round	2 Round
Number of Sub Keys	16 keys (48 bits)	2 keys (8 bits)
S-boxes	8 boxes 6 bits -> 4 bits	2 boxes 4 bits -> 2 bits

block cipher design principles: number of rounds:
•The greater the number of rounds, the more difficult it is to perform cryptanalysis
•In general, the criterion should be that the number of rounds is chosen so that known cryptanalytic efforts require greater effort than a simple brute-force key search attack
•If DES had 15 or fewer rounds, differential cryptanalysis would require less effort than a brute-force key search

Measures of cipher strength:
1- SAC: strict avalanche criterion
•States that any output bit j of an S-box should change with probability 1/2 when any single input bit i is inverted for all i , j
يعني اذا تغير bit واحد بالinput لازم على الاقل تتغير نص الciphertext (بتنهار)

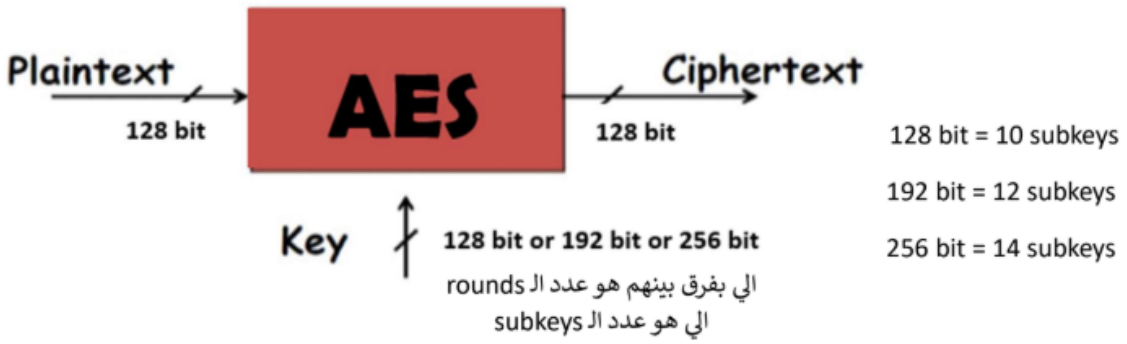
2-BIC: bit independence criterion
•States that output bits j and k should change independently when any single input bit i is inverted for all i , j , and k
هون التغير عشوائي مو شرط اذا غيرنا اشي يتغير نصها

AES

- clear a replacement for DES was needed
  - have theoretical attacks that can break it
  - have demonstrated exhaustive key search attacks
- can use Triple-DES – but slow, has small blocks
- US NIST issued call for ciphers in 1997
- 15 candidates accepted in Jun 98
- 5 were shortlisted in Aug-99
- Rijndael was selected as the AES in Oct-2000
- issued as FIPS PUB 197 standard in Nov-2001

the AES cipher-Rijndael:

- designed by Rijmen-Daemen in Belgium
- has 128/192/256 bit keys, 128 bit data
- an **iterative** rather than **Feistel** cipher
  - processes data as block of 4 columns of 4 bytes
  - operates on entire data block in every round
- designed to have:
  - resistance against known attacks
  - speed and code compactness on many CPUs
  - design simplicity



M=128 bits ,k=128 bits
every 4 bits is 1 hexa
128/4=32 hexa digit

AES encryption

هلا هون في خطوات للحل وهدول الخطوات حفظ وبالترتيب

Step1: Convert Plaintext and key into Hexadecimal (from block to state)
Step2 :- Add Round key, Round 0
Step 3: Substitution Bytes (S-box) – Round 1
Step 4: Shift Row – Round 1
Step 5: Mix column – Round 1
Step 6: Add Round Key- Round 1

032	Space	048	0	064	@	080	P	096	‘	112	p				
033	!	049	1	065	A	081	Q	097	a	113	q				
034	"	050	2	066	B	082	R	098	b	114	r				
035	#	051	3	067	C	083	S	099	c	115	s				
036	$	052	4	068	D	084	T	100	d	116	t				
037	%	053	5	069	E	085	U	101	e	117	u				
038	&	054	6	070	F	086	V	102	f	118	v				
039	’	055	7	071	G	087	W	103	g	119	w				
040	(	056	8	072	H	088	X	104	h	120	x				
041	)	057	9	073	I	089	Y	105	i	121	y				
042	*	058	:	074	J	090	Z	106	j	122	z				
043	+	059	;	075	K	091	[	107	k	123	{				
044	‘	060	<	076	L	092	\	108	l	124	|				
045	-	061	=	077	M	093	]	109	m	125	}				
046	.	062	>	078	N	094	^	110	n	126	~				
047	/	063	?	079	O	095	_	111	o	127	DEL				

Hexa Decimal Value

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
2	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
3	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
4	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
5	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
6	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
7	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
8	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143
9	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
A	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175
B	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
C	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207
D	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
E	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239
F	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

AES S-Box Lookup Table

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

AES encryption

يلا نحل اول سؤال

find the cipher text of m= Hello Students L and the k=Go to the GYM $?
using AES cipher

بنبلش باول خطوة من الخطوات يلي المفروض حفظتوهم بتحكيلنا لازم نحول النص لهيكسا
بنحولهم من الصورتين هدول بتعطينا ياهم الدكتورة
اول اشي بنروح على جدول ASCII بنشوف الحرف او الرمز شو رقمو بناخد الرقم وبنروح على جدول الهيكسا بندور على الرقم وبناخد العامود بعدين السطر

H	e	l	l	o		S	t	u	d	e	n	t	s		L
72	101	108	108	111	32	83	116	117	100	101	110	116	115	32	76
48	65	6C	6C	6F	20	53	74	75	64	65	6E	74	73	20	4C

G	o		t	o		T	h	e		G	Y	M		$	?
71	111	32	116	111	32	84	104	101	32	71	89	77	32	36	63
47	6F	20	74	6F	20	74	68	65	20	47	59	4D	20	24	3F

هلا بناخد كل اربعة بنحطهم فوق بعض عشان نعمل ماتريكس

$$\text{Plaintext=}\begin{pmatrix} 48 & 6F & 75 & 74 \\ 65 & 20 & 64 & 73 \\ 6C & 53 & 65 & 20 \\ 6C & 74 & 6E & 4C \end{pmatrix} \qquad \text{Key=}\begin{pmatrix} 47 & 6F & 65 & 4D \\ 6F & 20 & 20 & 20 \\ 20 & 74 & 47 & 24 \\ 74 & 68 & 59 & 3F \end{pmatrix}$$

هيك بنكون خلصنا المرحلة الاولى عنا المرحلة الثانية يلي هي نجيب state matrix
هي طويلة بس سهلة بدنا نعمل xor لكل رقمين مع بعض حنحل مع بعض اكم مثال وانتو كملو

48 xor 47 = 0100 1000 xor 0100 0111 = 0000 1111 = 0F
65 xor 6F = 0110 0101 xor 0110 1111 = 0000 1010 = 0A
6C xor 20 = 0110 1100 xor 0010 0000 = 0100 1100 = 4C

$$\text{State Matrix=}\begin{pmatrix} 0F & 00 & 10 & 39 \\ 0A & 00 & 44 & 53 \\ 4C & 27 & 22 & 04 \\ 18 & 1C & 37 & 73 \end{pmatrix}$$

AES encryption

بناخد الجواب وبنروح على الجدول الثالث كل رقم بالماتريكس متكون من منزلتين مثلا اول وحدة 0F بناخد ال0 بنحطها عامودي و F بنحطها افقي وبناخد التقاطع بطلع معنا 76 وبنكمل على كل الارقام وبطلع معنا هيك

$$\text{New State Matrix} = \begin{pmatrix} 76 & 63 & CA & 12 \\ 67 & 63 & 1B & ED \\ 29 & CC & 93 & F2 \\ AD & 9C & 9A & 8F \end{pmatrix}$$

اما بالنسبة للخطوة الرابعة shift row اول سطر ما بنلمسو ثاني سطر بس اول وحدة بتصير اخر وحدة ثالث سطر بنحرك ثنتين الرابع بنحرك ثلاث وهكذا بتصير عنا هيك

$$\text{New Shifted State Matrix} = \begin{pmatrix} 76 & 63 & CA & 12 \\ 63 & 1B & ED & 67 \\ 93 & F2 & 29 & CC \\ 8F & AD & 9C & 9A \end{pmatrix}$$

والخطوة الخامسة mix columns في عنا ماتريكس حفظ بنضربها باخر ماتريكس طلعت معنا السطر بالعامود والضرب هون حفلة مرتبة

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} * \begin{pmatrix} 76 & 63 & CA & 12 \\ 63 & 1B & ED & 67 \\ 93 & F2 & 29 & CC \\ 8F & AD & 9C & 9A \end{pmatrix}$$

طريقة الضرب ححل بس هاي والباقي عليكم نفس الطريقة كلهم بس قبل ما ابلش فيها لازم نراجع شغلة سريعة بالضرب

لما نضرب بواحد بضل الرقم نفسو

لما نضرب بثنين بنفرط اول اشي لباينري وبنطلع على اقصى اليسار للرقم اذا كان 0 بننقلو من اقصى اليسار الى اقصى اليمين

اما اذا كان 1 بنمحي الواحد وبنحط صفر باقصى اليمين وبنعملها xor with 1B

ولما نضرب بثلاث بنفكها ضرب اثنين وضرب واحد وبنرجع للطريقة القبل وبنكمل

AES encryption

هاد كلو بكون بس اول نقطة بالناتج (2 * 76)ب xor (63 * 3) xor (93 * 1) xor (8F * 1)
هلا خلينا نبلش

76 * 2 = **0**111 0110 * 2 = 1110 110**0**
63 * 3 = (63*2) xor (63*1) = 0110 0011 *2 xor 0110 0011*1
= 11000110 xor 0110 0011 = 1010 0101
93 * 1 = 1001 0011
8F * 1 = 1000 1111

هلا كل الاجوبة يلي طلعت معنا بنعمللها xor مع بعض
1110 1100 xor 1010 0101 xor 1001 0011 xor 1000 1111 = 0101 0101 = 55

$$\text{Result=}\begin{pmatrix} 55 & B4 & 16 & DB \\ 91 & F5 & EC & 09 \\ A2 & 6B & CA & 43 \\ 6F & 0D & A2 & B2 \end{pmatrix}$$

هيك بطلع الجواب النهائي

وبالمناسبة الدكتورة ما بتطلب كل هاد بالعادة بس بتطلب خطوة او خطوتين

SAES key expansion

يلا نبلش دغري والحل هون بعتمد على الصور يلي استخدمناهم فوق

k= Thats my Kung Fu
k in hex = = 54 68 61 74 73 20 6D 79 20 4B 75 6E 67 20 46 75 (128bit)
حولناهم لهيكسا زي فوق بنشوف الجدول الاول شو مقابل كل حرف رقم بعدين بنقاطلعهم على الجدول الثاني

w0= 54 68 61 74
w1= 73 20 6D 79
w2= 20 4B 75 6E
w3= 67 20 46 75

Round	Constant (RCon)	Round	Constant (RCon)
1	$(01\ 00\ 00\ 00)_{16}$	6	$(20\ 00\ 00\ 00)_{16}$
2	$(02\ 00\ 00\ 00)_{16}$	7	$(40\ 00\ 00\ 00)_{16}$
3	$(04\ 00\ 00\ 00)_{16}$	8	$(80\ 00\ 00\ 00)_{16}$
4	$(08\ 00\ 00\ 00)_{16}$	9	$(1B\ 00\ 00\ 00)_{16}$
5	$(10\ 00\ 00\ 00)_{16}$	10	$(36\ 00\ 00\ 00)_{16}$

قسمنا كل اربعة لword كل وحدة بتتكون من (bit 32)
حنستخدم كل جزء بمعادلة مختلفة عشان نوجد باقي الsubkeys عددهم 10 لان 128 key فكل اربع مقاطع حنحطهم بمفتاح مختلف
k1= w4 w5 w6 w7
k2 = w8 w9 w10 w11
وهكذاااا

AES key expansion

عشان انبلش هون برضو عنا قوانين ولازم نحفظهم عشان نوجد كل word
اول word بكل key هيك بنوجدو

1. circular byte left shift of w[3]: (20; 46; 75; 67)

بنخلي اول رقم اخر رقم

2. Byte Substitution (S-Box): (B7; 5A; 9D; 85)

بنروح على الجدول الثالث يلي هو AES s-box وبنقاطع 20 بطلع الجواب B7 وهكذا

3. Adding round constant (01; 00; 00; 00) gives: g(w[3]) = (B6; 5A; 9D; 85)

هون حقلكم طريقة سريعة اول رقمين الخانة الثانية بتطرحو منها واحد والباقي بنزل عادي

w[4] = w[0] ⊕ g(w[3]) = (E2; 32; FC; F1)

بعدين بنعمل xor الجواب مع يلي بتقابلها بالمفتاح القبل وهيك طلعنا اول word

اما الثلاث الباقيين فهم بس بنعمل xor مع القبلها ويلي بتقابلها بالمفتاح يلي قبلها يعني

w[5] = w[4] ⊕ w[1] = (91; 12; 91; 88)
w[6] = w[5] ⊕ w[2] = (B1; 59;E4;E6)
w[7] = w[6] ⊕ w[3] = (D6; 79;A2; 93)
first round key :k2 = E2 32 FC F1 91 12 91 88 B1 59 E4 E6 D6 79 A2 93

اما هلا نوجد k2 مهمممم اجا بالفاينل

k2 = w8 w9 w10 w11
w8 = G(w7) xor w4
w9 = w8 xor w5
w10 = w9 xor w6
w11 = w10 xor w7

1. circular byte left shift of w[7]: (79 A2 93 D6)

زي اول مفتاح ما اختلف اشي اول رقم بصير اخر رقم

2. Byte Substitution (S-Box): (B6 3A DC F6)

بنروح على جدول وبنقاطع الارقام

3. Adding round constant (02; 00; 00; 00) gives: g(w[7]) = (B4; 5A; 9D; 85)

هون نفس الاشي بس عشان صرنا بالدورة الثانية بنطرح اثنين بدل واحد

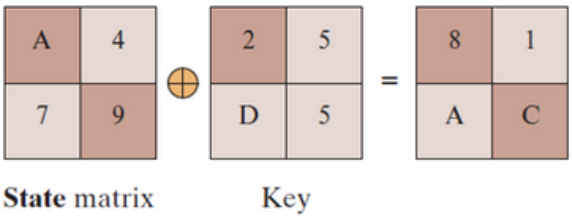
w[8] = w[4] ⊕ g(w[7]) = (56 68 61 74):

w[9] = w[8] ⊕ w[5] = (C7 7A F0 FC),
w[10] = w[9] ⊕ w[6] = (76 2314 1A),
w[11] = w[10] ⊕ w[7] = (A0 5A B6 89)
second roundkey: 56 68 61 74 C7 7A F0 FC 76 23 14 1A A0 5A B6 89

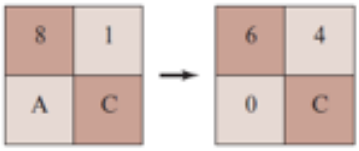
SAES encryption

three step :

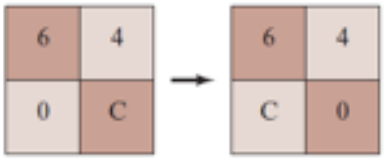
1- add key



2- nibble substitution



3- shift row



4- mix column

$$\begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix} \begin{bmatrix} s_{0,0} & s_{0,1} \\ s_{1,0} & s_{1,1} \end{bmatrix} = \begin{bmatrix} s'_{0,0} & s'_{0,1} \\ s'_{1,0} & s'_{1,1} \end{bmatrix}$$

let know that the first sub key is 6F 32 determine the second sub key

w0 = 6F

w1 = 32

w2 = x0 xor 80 xor subNib(RotNib(w1))

هاد القانون حفظ كمان

w2 = 0110 1111 xor 1000 0000 xor subNib(RotNib(0011 0010))

عوضنا هون القيم

w2 = 0110 1111 xor 1000 0000 xor subNib(0010 0011)

اول اشي RotNib نقلب اليمين يسار واليسار يمين

w2 = 0110 1111 xor 1000 0000 xor 1010 1011

هون SubNib من الجدول كل اربع ارقام قبالها ارقام

w2 = 0100 0100

بنعمل xor عادي

w3 = w2 xor w1

w3 = 0100 0100 xor 0011 0010

w3 = 0111 0110

nibble	S-box(nibble)	nibble	S-box(nibble)
0000	1001	1000	0110
0001	0100	1001	0010
0010	1010	1010	0000
0011	1011	1011	0011
0100	1101	1100	1100
0101	0001	1101	1110
0110	1000	1110	1111
0111	0101	1111	0111

CHAPTER FOUR

COMING SOON !!!

CHAPTER FOUR

IDENTIFYING AND ANALYZING THREATS, VULNERABILITIES, AND EXPLOITS

CHAPTER FIVE

DATA INTEGRITY ALGORITHM

CHAPTER SEVEN

BLOCK CIPHER OPERATION

QUESTIONS

SUGGESTED AND PAST QUESTIONS

ERROR CATCHERS

WE CATCH WHAT OTHERS MISS !

MORE ABOUT US !