كلية العلوم

قســـم الانظمة الطبية الذكية

Lecture: (4)

Information Security in Healthcare

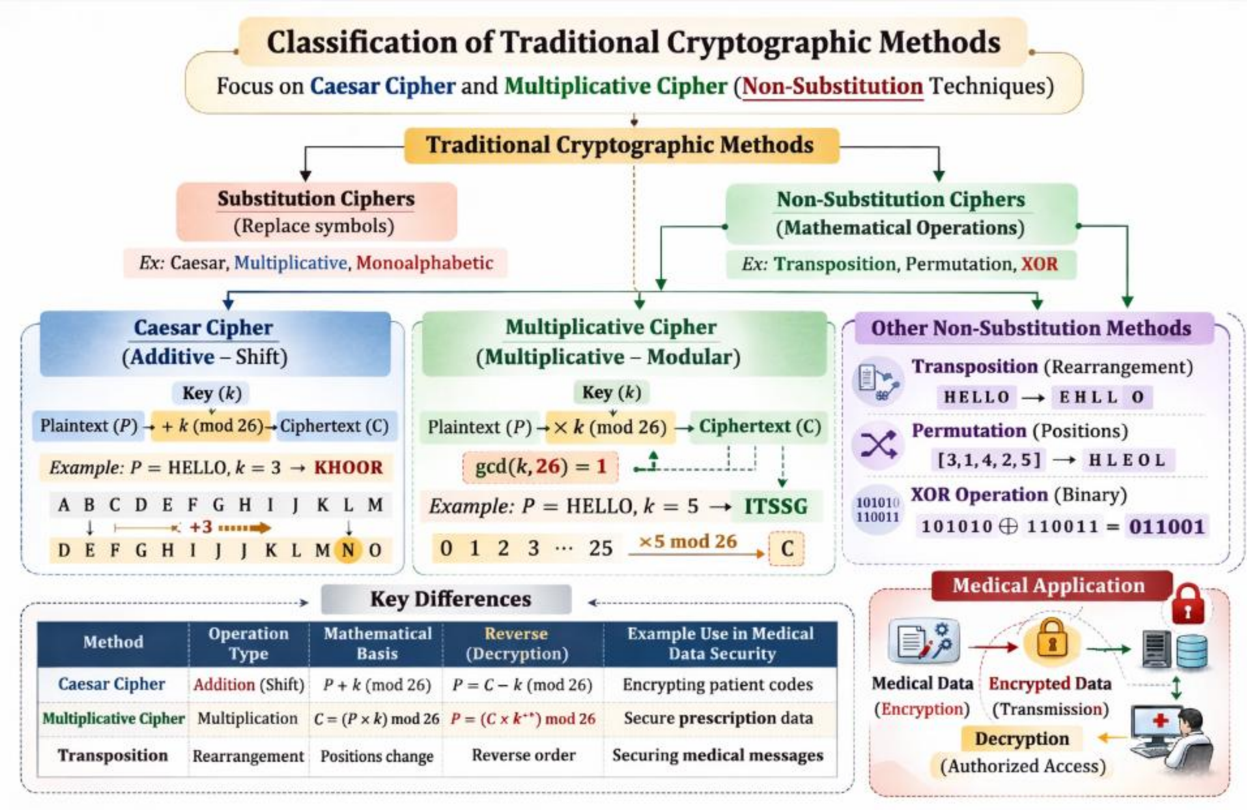
Subject: Traditional methods Ceaser cipher, Multiplicative cipher
Level: Fourth
Lecturer: Prof. Dr. Mehdi Ebady Manaa

1. Introduction: Why Healthcare Needs Strong Cyber Defense

The protection of information has been a central concern of human civilization since the earliest emergence of organized societies. In the modern era, this concern has become especially critical in the medical domain, where sensitive patient data—including *diagnostic records, laboratory results, medical histories, and treatment plans*—must be protected from unauthorized access. As healthcare systems transitioned from paper-based records to **electronic health records (EHRs)** and network-connected medical information systems, the confidentiality, integrity, and availability of medical data became fundamental requirements for ensuring patient safety, ethical compliance, and trust in healthcare institutions. Unauthorized disclosure or manipulation of medical information can lead not only to privacy violations but also to severe clinical consequences, such as incorrect treatment decisions or compromised patient outcomes.

The need to protect sensitive medical communications has given rise to the integration of cryptographic techniques within healthcare information systems. Cryptography provides mathematical mechanisms to transform readable medical data into secure formats that can only be interpreted by authorized entities, such as physicians, laboratories, and healthcare administrators. Traditional cryptographic methods, often referred to as classical ciphers, represent the foundational stage of this discipline. Although these methods are considered insecure by modern standards, they played a critical role in shaping the theoretical and practical evolution of secure communication systems, including those used in early medical record protection and secure message transmission.

Among the most historically significant and conceptually influential classical encryption techniques are the *Caesar cipher and the Multiplicative cipher, both of which belong to the family of substitution ciphers*. These methods operate by transforming the original message—such as **a patient diagnosis or prescription—into an encoded form using mathematical rules and secret keys**. While simple, these ciphers illustrate essential cryptographic principles such as key-based transformation, reversibility, and confidentiality, which remain central to modern medical data security systems. Figure (1) shows the main classification techniques for cryptographic methods


Classification of Traditional Cryptographic Methods
Focus on Caesar Cipher and Multiplicative Cipher (Non-Substitution Techniques)
Traditional Cryptographic Methods
Substitution Ciphers
(Replace symbols)
Ex: Caesar, Multiplicative, Monoalphabetic
Non-Substitution Ciphers
(Mathematical Operations)
Ex: Transposition, Permutation, XOR
Caesar Cipher
(Additive – Shift)
Key (k)
Plaintext (P) → + k (mod 26) → Ciphertext (C)
Example: P = HELLO, k = 3 → KHOOR
A B C D E F G H I J K L M
+3
D E F G H I J J K L M N O
Multiplicative Cipher
(Multiplicative – Modular)
Key (k)
Plaintext (P) → × k (mod 26) → Ciphertext (C)
gcd(k, 26) = 1
Example: P = HELLO, k = 5 → ITSSG
0 1 2 3 ··· 25
×5 mod 26
C
Other Non-Substitution Methods
Transposition (Rearrangement)
HELLO → EHLL O
Permutation (Positions)
[3,1,4,2,5] → HLEOL
101010
110011
XOR Operation (Binary)
101010 ⊕ 110011 = 011001
Key Differences
Medical Application
Medical Data
(Encryption)
Encrypted Data
(Transmission)
Decryption
(Authorized Access)

Method	Operation Type	Mathematical Basis	Reverse (Decryption)	Example Use in Medical Data Security
Caesar Cipher	Addition (Shift)	$P + k \pmod{26}$	$P = C - k \pmod{26}$	Encrypting patient codes
Multiplicative Cipher	Multiplication	$C = (P \times k) \bmod 26$	$P = (C \times k^{-1}) \bmod 26$	Secure prescription data
Transposition	Rearrangement	Positions change	Reverse order	Securing medical messages

Figure 1: Classification of Cryptographic Methods

Understanding these traditional encryption techniques provides valuable insight into how secure healthcare communication evolved, forming the conceptual and mathematical foundation for advanced cryptographic algorithms now used to protect electronic health records, telemedicine communications, and medical research databases in contemporary healthcare environments. There are many techniques for encryptions:

1. Substitution

In a substitution cipher, every letter in the original message (called **plaintext, P**) is replaced by exactly one different letter (called **ciphertext, C**) according to a fixed rule or key.

Where:

$$C = f(P)$$

- P = Plaintext character
- C = Ciphertext character
- f = Encryption function (mapping rule)

Example: Substitution Cipher Mapping Table

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

A substitution cipher uses a one-to-one mapping between plaintext and ciphertext characters. This ensures that each character can be uniquely encrypted and correctly decrypted. The number of possible keys is very large (26!), but classical substitution ciphers are still vulnerable to frequency analysis and are not secure for modern medical data protection.

The Number of Available Keys

If the alphabet contains n characters:

Number of possible keys=n!

For English alphabet:

n=26➔ 26!=403,291,499,200,000,000,000,00026! =

Number of Bits Required to Represent the Key

Number of bits=$\log_2(n)$ ➔ For English alphabet: $\log_2(26!) \approx 88.4$ bits

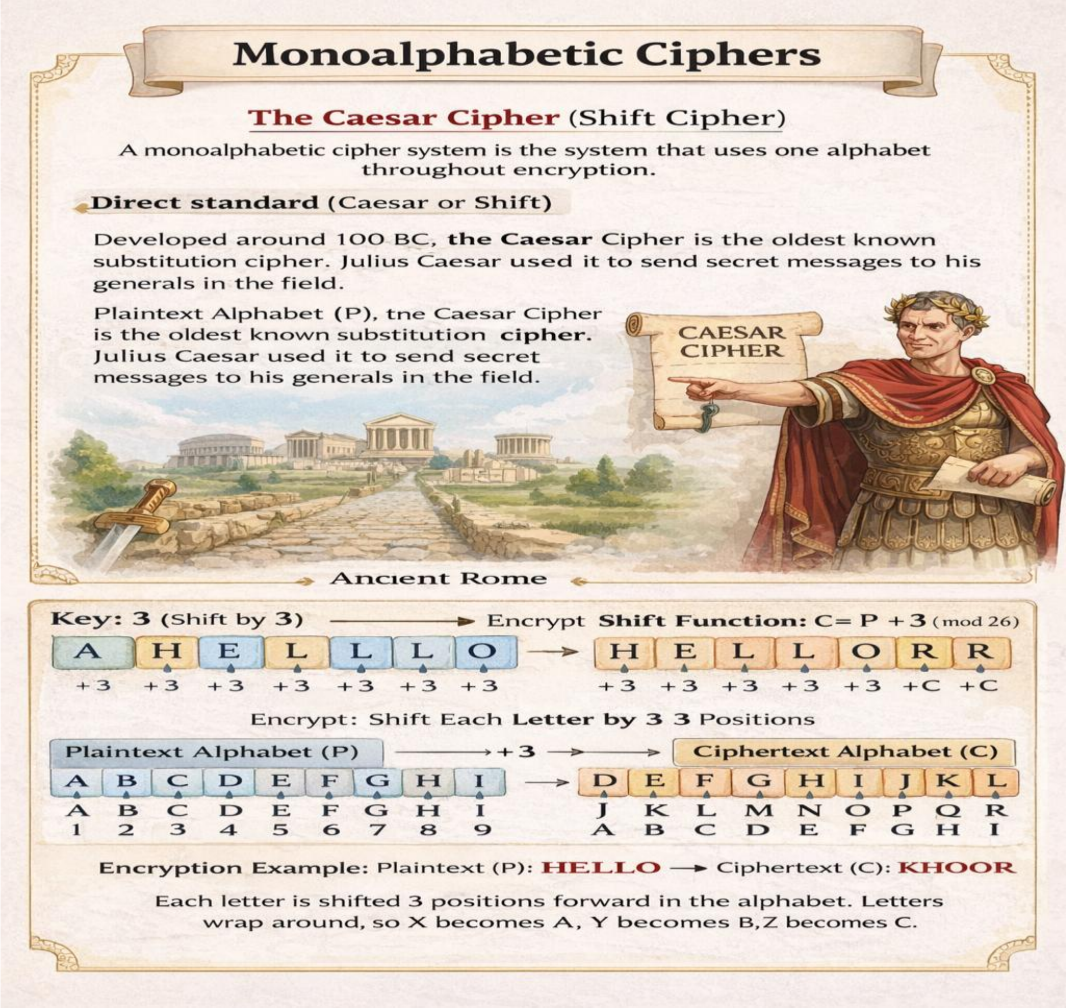
Cipher for words “Patient”, “Medical”, “Electronic Health Recod”

2. Monoalphabetic

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

- Direct standard (Caesar or Shift)

The Caesar cipher is the most famous (the earliest) and simplest of all ciphers. The "Caesar Box" or "Caesar Cipher" is one of the earliest known ciphers. Developed around 100 BC, it was used by Julius Caesar to send secret messages to his generals in the field. It is classified as a substitution cipher because the sender replaces the letters in the actual message with a new set of letters. In the Caesar cipher, each letter is replaced ***with the third letter following it in the alphabet***.



Monoalphabetic Ciphers

The Caesar Cipher (Shift Cipher)

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

Direct standard (Caesar or Shift)

Developed around 100 BC, **the Caesar** Cipher is the oldest known substitution cipher. Julius Caesar used it to send secret messages to his generals in the field.

Plaintext Alphabet (P), tne Caesar Cipher is the oldest known substitution **cipher.** Julius Caesar used it to send secret messages to his generals in the field.

Key: 3 (Shift by **3**) → Encrypt **Shift Function:** C= P +3 (mod 26)

A H E L L L O → H E L L O R R

+3 +3 +3 +3 +3 +3 +3   +3 +3 +3 +3 +3 +C +C

Encrypt: Shift Each **Letter by 3 3** Positions

Plaintext Alphabet (P) → +3 → → Ciphertext Alphabet (C)

A B C D E F G H I → D E F G H I J K L

A B C D E F G H I   J K L M N O P Q R
1 2 3 4 5 6 7 8 9   A B C D E F G H I

Encryption Example: Plaintext (P): **HELLO** → Ciphertext (C): **KHOOR**

Each letter is shifted 3 positions forward in the alphabet. Letters wrap around, so X becomes A, Y becomes B,Z becomes C.

Figure 2: Caesar Cipher Ancient Method

The alphabet wraps around, so if the letter in the actual message were X, Y, or Z, it would be

replaced with A, B, or C, respectively. The modern English alphabet actually contains several letters not in the Roman alphabet, but we will demonstrate the cipher using the modern English alphabet.

Here is the format in **four rows**, optimized for **A4 portrait layout**:

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

Plaintext and Ciphertext (Caesar Shift k = 3)

Plaintext	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**
Ciphertext	D	E	F	G	H	I	J	K	L	M	N	O	P
Plaintext	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Then the algorithm can be expressed as follows. For each plaintext letter (p), substitute the ciphertext letter (C). **C = E(k, p) = (p + 3) mod 26 .** A shift may be of any amount, so that the general Caesar algorithm is:

Encryption:

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

Decryption:

p = D(k, C) = (C - k) mod 26 ....(2)

Example

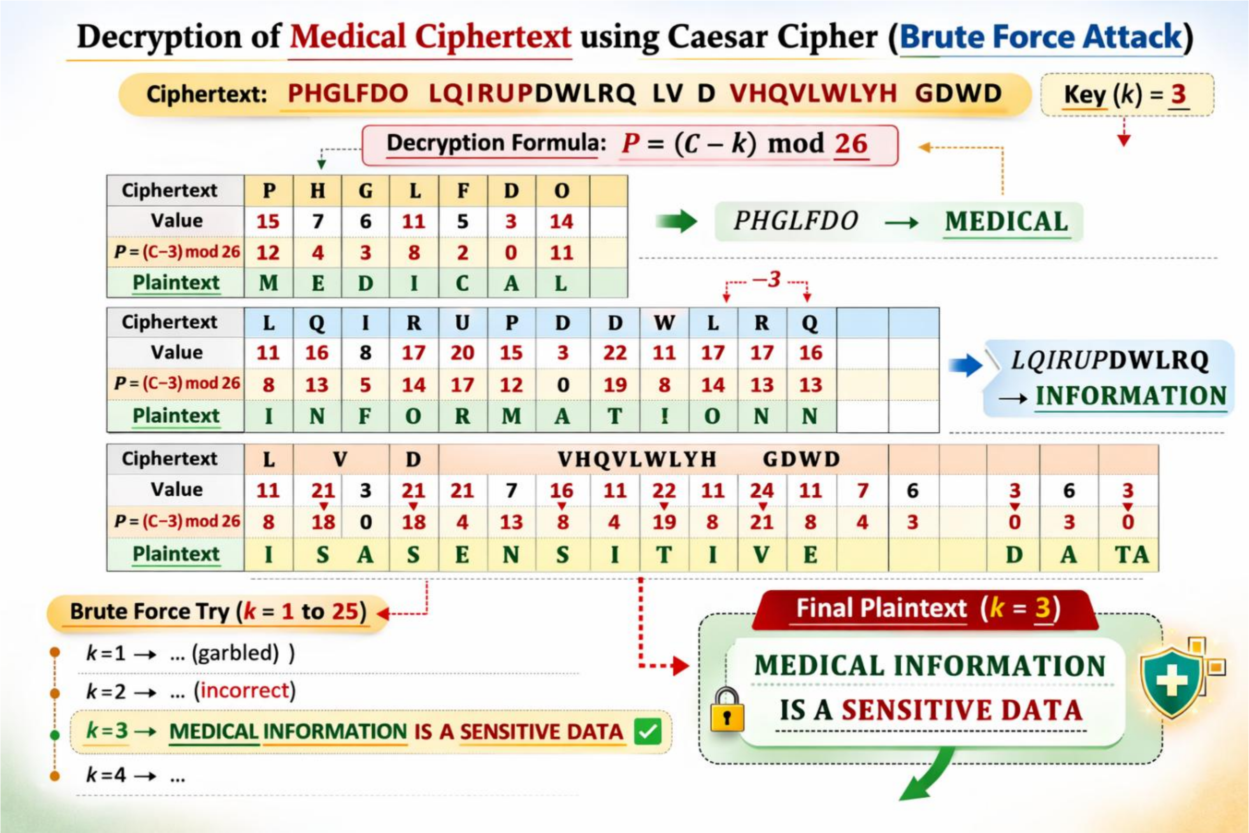
Cipher the following sentences “**MEDICAL INFORMATION IS A SENSITIVE DATA” , k=3**

Plaintext	**M**	**E**	**D**	**I**	**C**	**A**	**L**				
Ciphertext	P	H	G	L	F	D	O				
Plaintext	**I**	**N**	**F**	**O**	**R**	**M**	**A**	**T**	**I**	**O**	**N**
Ciphertext	L	Q	I	R	U	P	D	W	L	R	Q
Plaintext	**I**	**S**									
Ciphertext	L	V									
Plaintext	**S**	**E**	**N**	**S**	**I**	**T**	**I**	**V**	**E**		
Ciphertext	V	H	Q	V	L	W	L	Y	H		

Final Cipher Text “PHGLFDO LQIRUPDWLRQ LV D VHQVLWLYH GDWD”

H.W.

Find decipher for the following
“PHGLFDO LQIRUPDWLRQ LV D VHQVLWLYH GDWD”



Decryption of Medical Ciphertext using Caesar Cipher (Brute Force Attack)

Ciphertext: PHGLFDO LQIRUPDWLRQ LV D VHQVLWLYH GDWD

Key (k) = 3

Decryption Formula: $P = (C - k) \bmod 26$

Ciphertext	P	H	G	L	F	D	O	
Value	15	7	6	11	5	3	14	
$P = (C-3) \bmod 26$	12	4	3	8	2	0	11	
Plaintext	M	E	D	I	C	A	L	

PHGLFDO → MEDICAL

Ciphertext	L	Q	I	R	U	P	D	D	W	L	R	Q		
Value	11	16	8	17	20	15	3	22	11	17	17	16		
$P = (C-3) \bmod 26$	8	13	5	14	17	12	0	19	8	14	13	13		
Plaintext	I	N	F	O	R	M	A	T	I	O	N	N		

LQIRUPDWLRQ → INFORMATION

Ciphertext	L	V		D	VHQVLWLYH GDWD													
Value	11	21	3	21	21	7	16	11	22	11	24	11	7	6		3	6	3
$P = (C-3) \bmod 26$	8	18	0	18	4	13	8	4	19	8	21	8	4	3		0	3	0
Plaintext	I	S	A	S	E	N	S	I	T	I	V	E				D	A	TA

Brute Force Try (k = 1 to 25)

- k=1 → ... (garbled))
- k=2 → ... (incorrect)
- k=3 → MEDICAL INFORMATION IS A SENSITIVE DATA ✓
- k=4 → ...

Final Plaintext (k = 3)

MEDICAL INFORMATION IS A SENSITIVE DATA

Figure 3: Caesar with Brute Force Attack

3. Multiplicative cipher

Multiplicative cipher is encrypted by multiplying each character in plaintext by a key (k) modulo 26.

Encryption:

C=E(k, p)=(p x k) mod n = (p x k) mod 26

Decryption:

p=D(k, C)=(C x k−**1**) mod n = (C x k−**1**) mod 26

The key and 26 are relatively prime (GCD (key, 26) =1). Where GCD is the Greatest Common Divisor.

To decrypt the ciphertext, the modular inverse of the key (k^{-1}) is used and multiplied by each Ciphertext ’s
character. The modular inverse of key is a number k^{-1}such that
(k x k^{-1}) mod 26= 1. So that in this case the key must be an odd number and not equal to 13. By trying all 26 possible multipliers modulo 26, we would discover that only 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, and 25 have inverses.

k	1	3	5	7	9	11	15	17	19	21	23	25
k^{-1}	**1**	**9**	**21**	**15**	**3**	**19**	**7**	**23**	**11**	**5**	**17**	**25**

Note

$1 \times 1 = 1 \bmod 26$, $3 \times 9 = 27 = 1 \bmod 26$, $5 \times 21 = 105 = 1 \bmod 26$, $7 \times 15 = 105 = 1 \bmod 26$, $11 \times 19 = 209 = 1 \bmod 26$, $17 \times 23 = 391 = 1 \bmod 26$, and $25 \times 25 = 625 = 1 \bmod 26$. But, 2, for example, does not have an inverse; there is no number mod 26 that 2 can be multiplied by that will result in 1.

Example: Decrypt the given Ciphertext: “SWEFYPKX” , with key=9, using Multiplicative cipher.
Ans. : k −**1** = 3
p=D(k, C)=(C x k −**1**) mod 26
p=D(S)=(18 x 3) mod 26 = 54 mod 26 = 2 = c
p=D(W)=(22 x 3) mod 26 = 66 mod 26 = 14 = o
p=D(E)=(4 x 3) mod 26 = 12 mod 26 = 12 = m
p=D(F)=(5 x 3) mod 26 = 15 mod 26 = 2 = p
p=D(Y)=(24 x 3) mod 26 = 72 mod 26 = 20 = u
p=D(P)=(15 x 3) mod 26 = 45 mod 26 = 19 = t
p=D(K)=(10 x 3) mod 26 = 30 mod 26 = 4 = e
p=D(X)=(23 x 3) mod 26 = 69 mod 26 = 17 = r
Plaintext: “computer”.

<u>Example</u>: Encrypt the message: “hello”, with key=7, using Multiplicative cipher.

Plaintext (p)	**h=7**	**e=4**	**l=11**	**l=11**	**o=14**
Ciphertext (C)	**X=23**	**C=2**	**Z=25**	**Z=25**	**U=20**

$C=E(k, p)=(p \times k) \bmod 26$
$C=E(h)=(7 \times 7) \bmod 26 = 49 \bmod 26 = 23 = X$

$C=E(e)=(4 \times 7) \bmod 26 = 28 \bmod 26 = 2 = C$
$C=E(l)=(11 \times 7) \bmod 26 = 77 \bmod 26 = 25 = Z$
$C=E(o)=(14 \times 7) \bmod 26 = 98 \bmod 26 = 20= U$

Ciphertext: “XCZZU”.

Plaintext (p)	**h=7**	**e=4**	**l=11**	**l=11**	**o=14**
Ciphertext (C)	**X=23**	**C=2**	**Z=25**	**Z=25**	**U=20**