SAHYADRI
COLLEGE OF ENGINEERING & MANAGEMENT
An Autonomous Institution
MANGALURU

Department of Information Science & Engineering

CRYPTOGRAPHY AND NETWORK SECURITY

21CS653

By
Prof. Prajna U R
Assistant Professor
Department of Information Science & Engineering
Sahyadri College of Engineering and Management, Adyar Mangaluru
Email: prajnau.is@sahyadri.edu.in
Mob:8495971075

MODULE-2

Basics of Cryptography and Encryption

Topics to be covered

Introduction to Cryptography, Plain Text and Cipher Text, Symmetric Cipher Model, Cryptography, Cryptanalysis, Brute Force Attacks, Substitution Techniques - Caesar Cipher and Modified Caesar Cipher, Mono Alphabetic cipher, Poly-Alphabetic Cipher, Playfair Cipher, Transposition Techniques- Rail Fence technique, Simple Columnar transposition Technique.

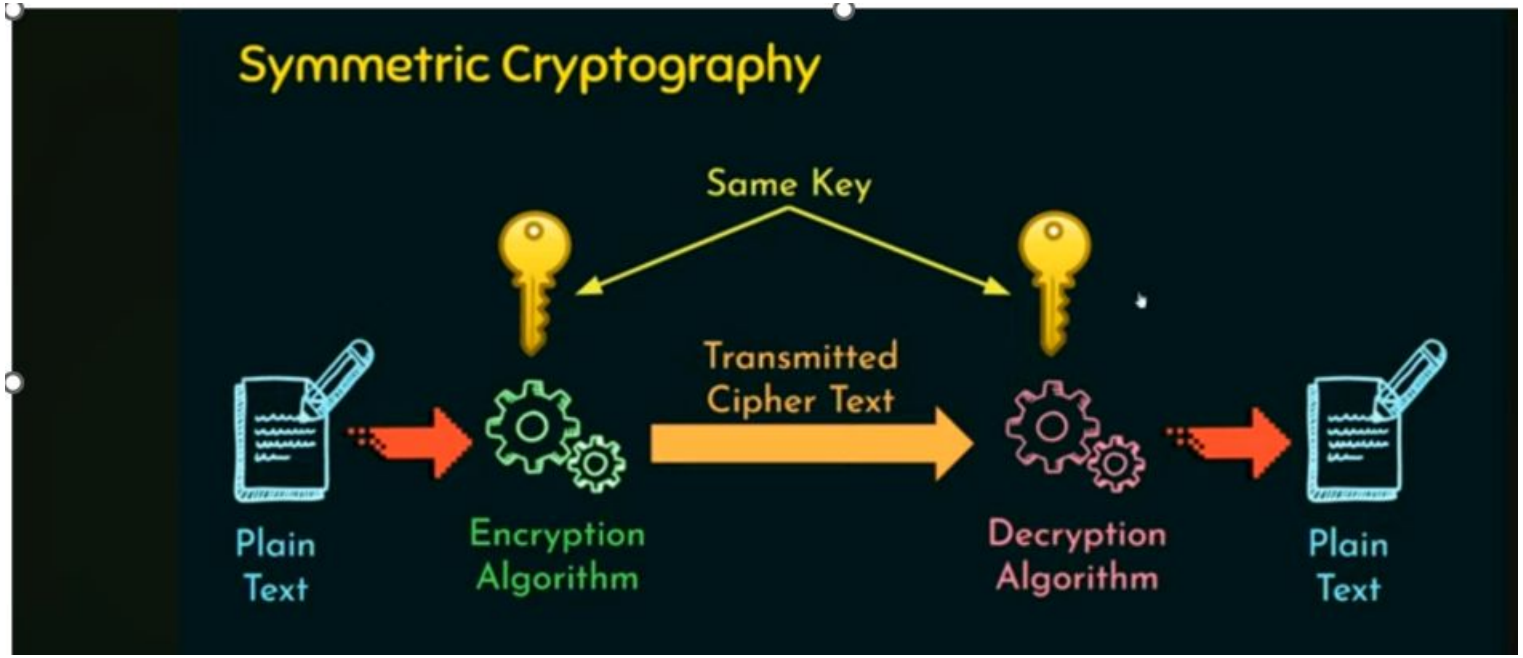
Cryptography:

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.

Types of Cryptography

Symmetric (private key)

Asymmetric (public key)



Symmetric Cryptography

Same Key

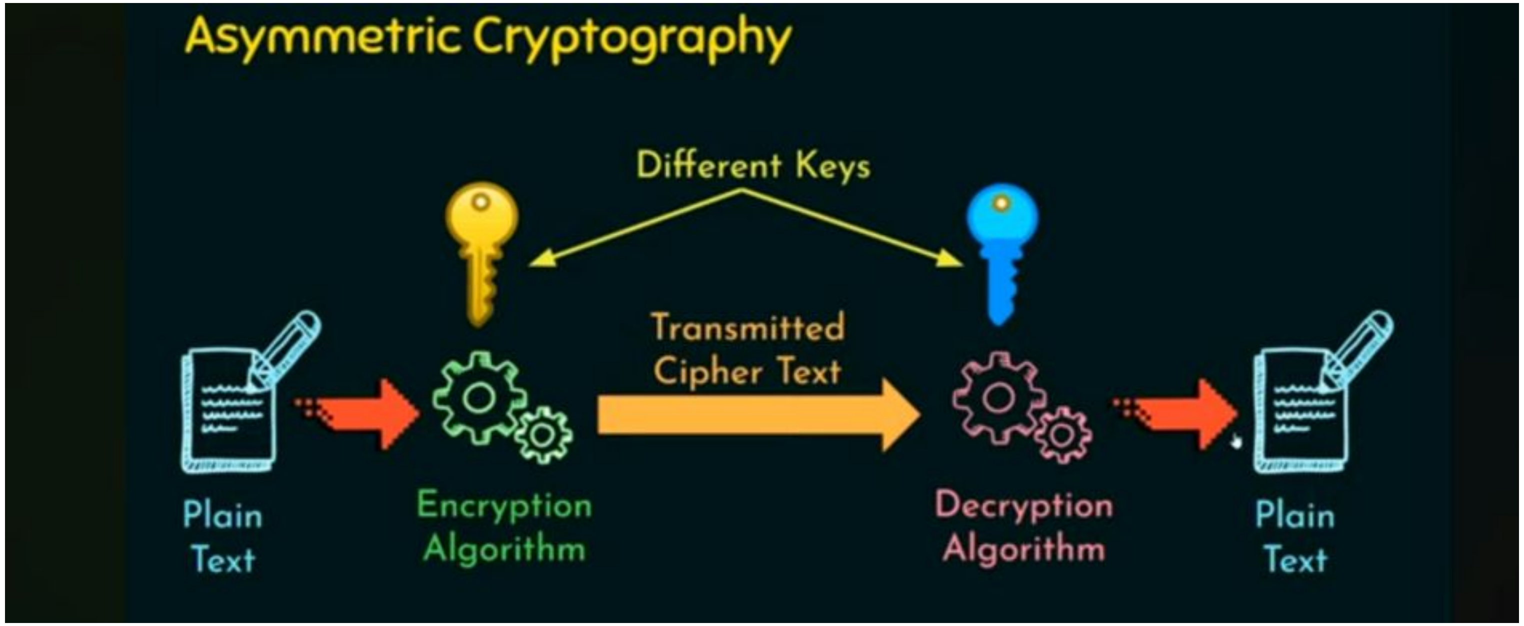
Transmitted Cipher Text

Plain Text

Encryption Algorithm

Decryption Algorithm

Plain Text



Asymmetric Cryptography

Different Keys

Transmitted Cipher Text

Plain Text

Encryption Algorithm

Decryption Algorithm

Plain Text

- Plaintext: original message

- Ciphertext: Coded message

- Enciphering or encryption: converting from plaintext to ciphertext

- Deciphering or decryption: restoring the plaintext from the ciphertext

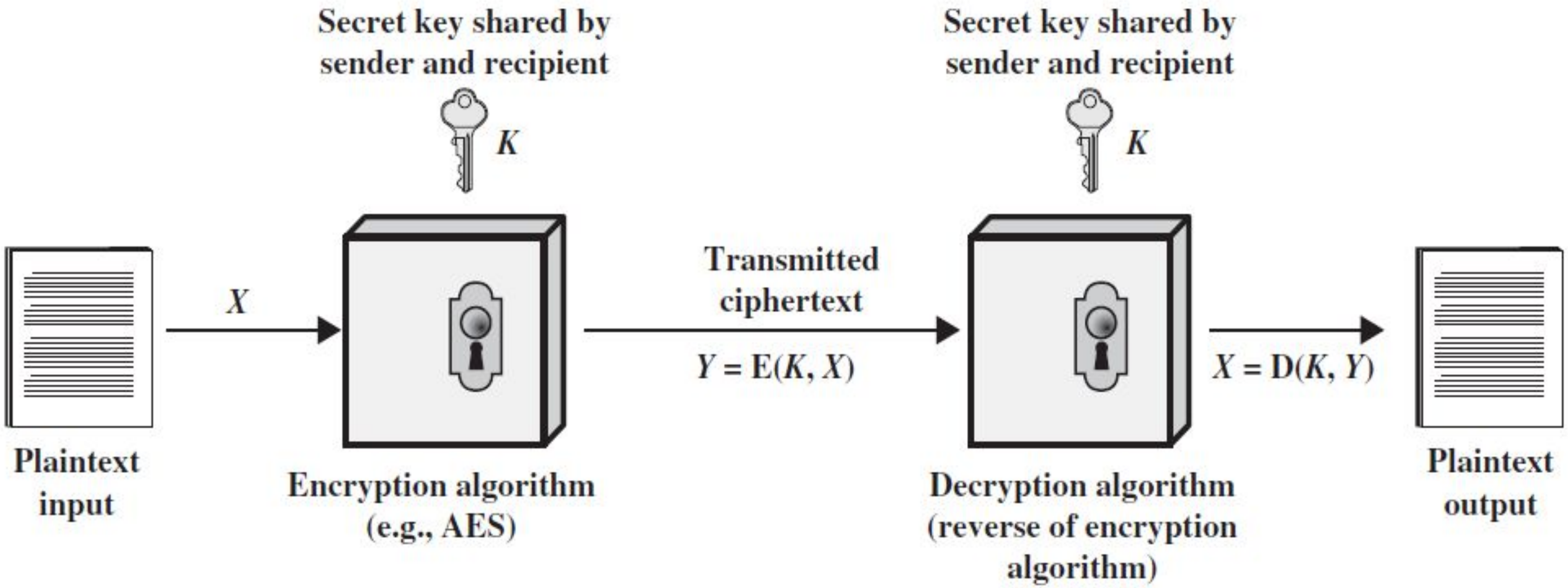
- Cryptography: The many schemes used for encryption constitute the area of study known as Cryptography.

- Such a scheme is known as a cryptographic system or a cipher.

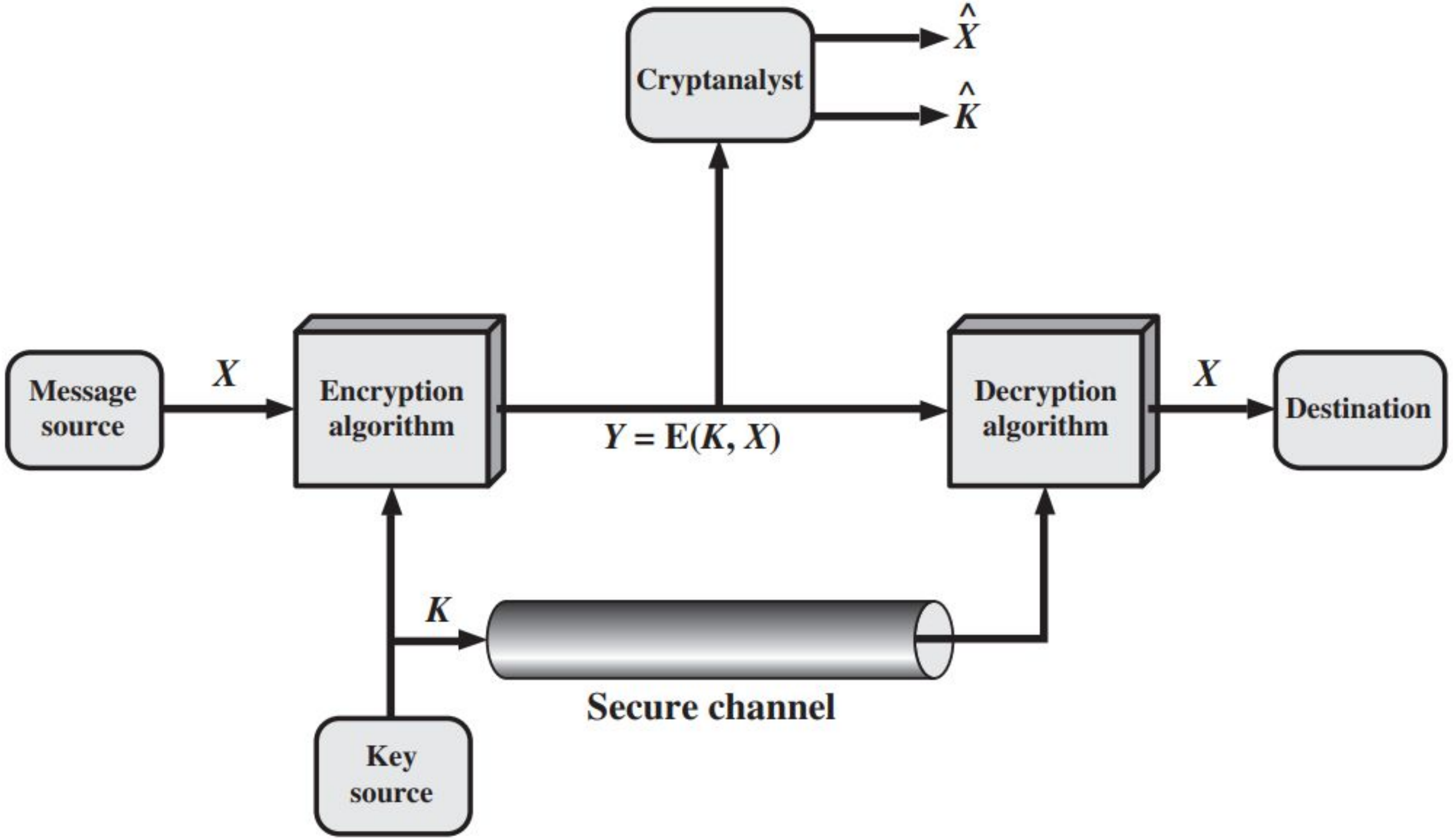
- Cryptanalysis: Techniques used for deciphering a message without any knowledge of the enciphering details. “breaking the code.”

- The areas of cryptography and cryptanalysis together are called cryptology.

Symmetric Cipher Model


Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E(K, X)
X = D(K, Y)
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Model of Symmetric Cryptosystem



Cryptograpy

- Three independent dimensions

1. The type of operations used for transforming plaintext to ciphertext.

- All encryption algorithms are based on two general principles:
  - Substitution, in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element, and
  - Transposition, in which elements in the plaintext are rearranged.

2. The number of keys used.

   - If both sender and receiver use the same key, the system is referred to as symmetric, single-key, secret-key, or conventional encryption.

   - If the sender and receiver use different keys, the system is referred to as asymmetric, two-key, or public-key encryption.

3. The way in which the plaintext is processed.

   - A block cipher processes the input one block of elements at a time, producing an output block for each input block.

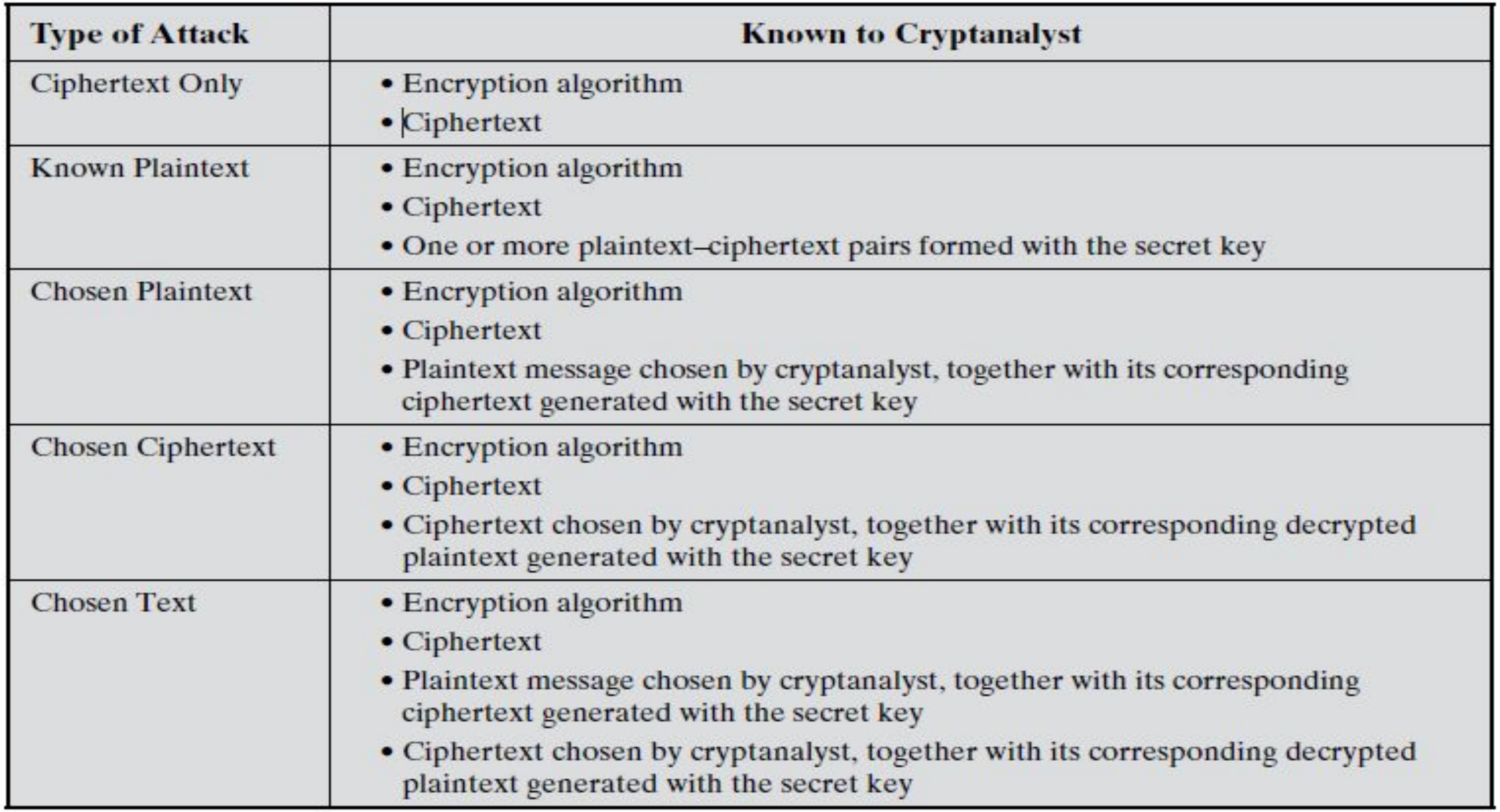
   - A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.

Cryptanalysis and Brute-Force Attack

- Cryptanalysis: Cryptanalytic attacks rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintext–ciphertext pairs. This type of attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.

- Brute-force attack: The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

Types of Attacks on Encrypted Messages



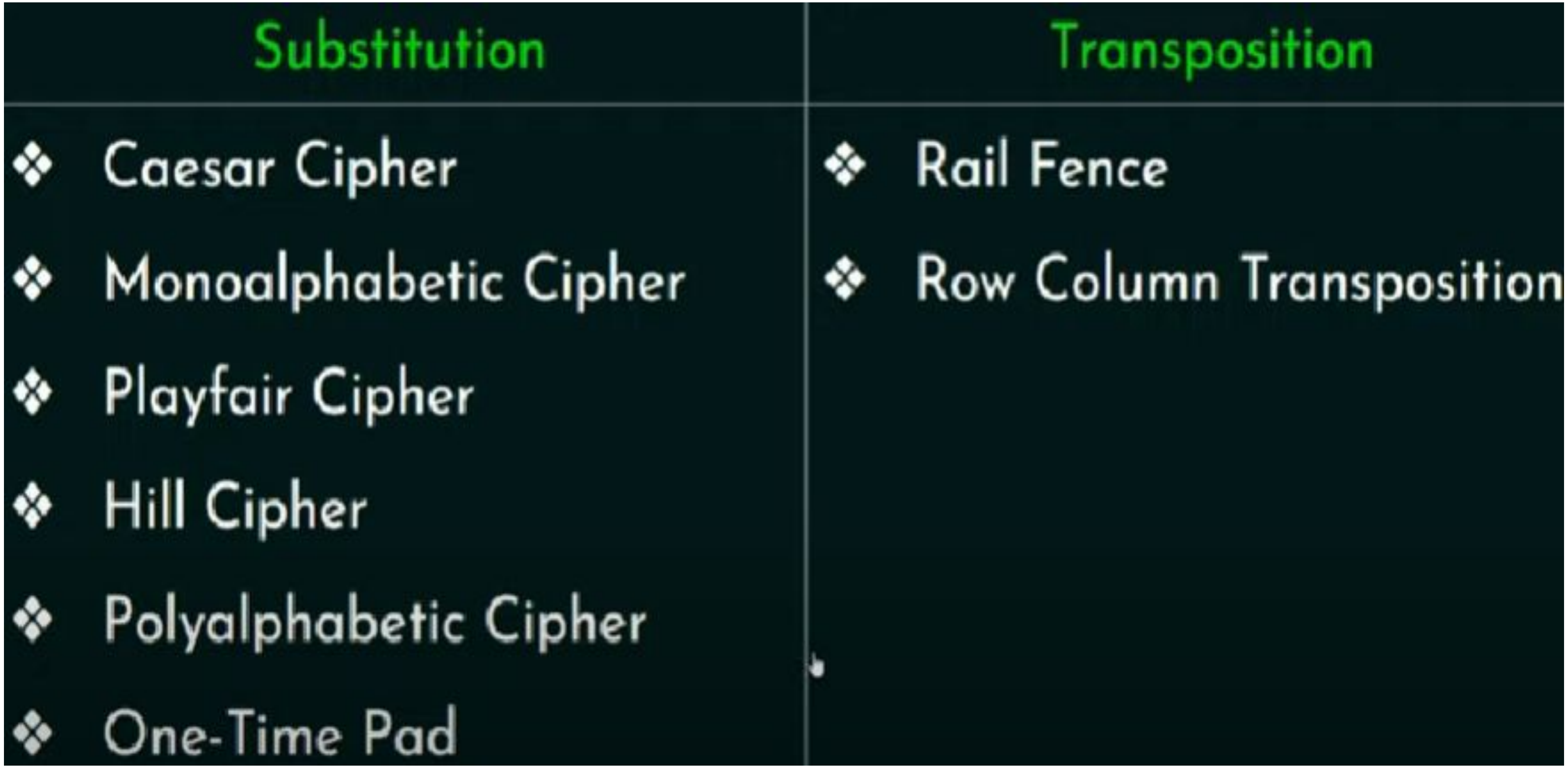
Type of Attack	Known to Cryptanalyst
Ciphertext Only	• Encryption algorithm • Ciphertext
Known Plaintext	• Encryption algorithm • Ciphertext • One or more plaintext–ciphertext pairs formed with the secret key
Chosen Plaintext	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen Ciphertext	• Encryption algorithm • Ciphertext • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen Text	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

Encryption scheme

- Unconditionally secure: if the ciphertext generated by the scheme does not contain enough information to determine uniquely the corresponding plaintext, no matter how much ciphertext is available.

- Computationally secure:
  - The cost of breaking the cipher exceeds the value of the encrypted information.
  - The time required to break the cipher exceeds the useful lifetime of the information.

Cryptograpy

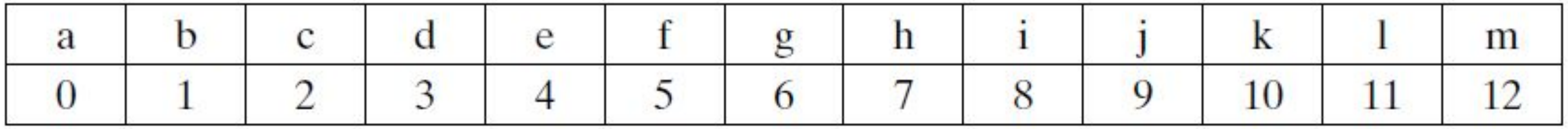


Substitution	Transposition
❖ Caesar Cipher	❖ Rail Fence
❖ Monoalphabetic Cipher	❖ Row Column Transposition
❖ Playfair Cipher	
❖ Hill Cipher	
❖ Polyalphabetic Cipher	
❖ One-Time Pad	

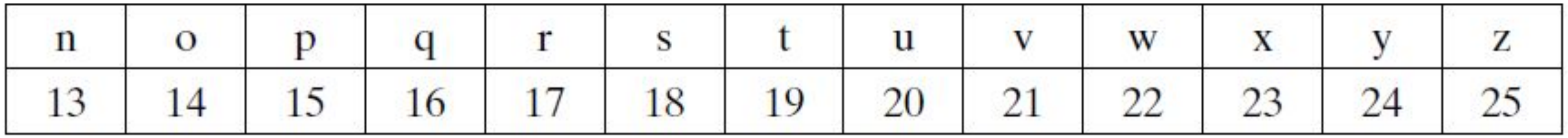
Caesar Cipher

- The earliest known, and the simplest, use of a substitution cipher was by Julius Caesar.

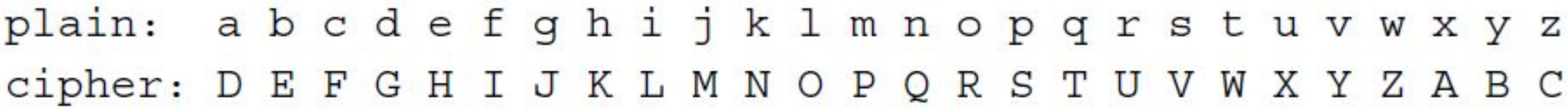
- The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet.



a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12



n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25



```
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
```

- For each plaintext letter p, substitute the ciphertext letter C

$$C = E(3, p) = (p + 3) \bmod 26$$

the general Caesar algorithm is

$$C = E(k, p) = (p + k) \bmod 26$$

where k takes on a value in the range 1 to 25.

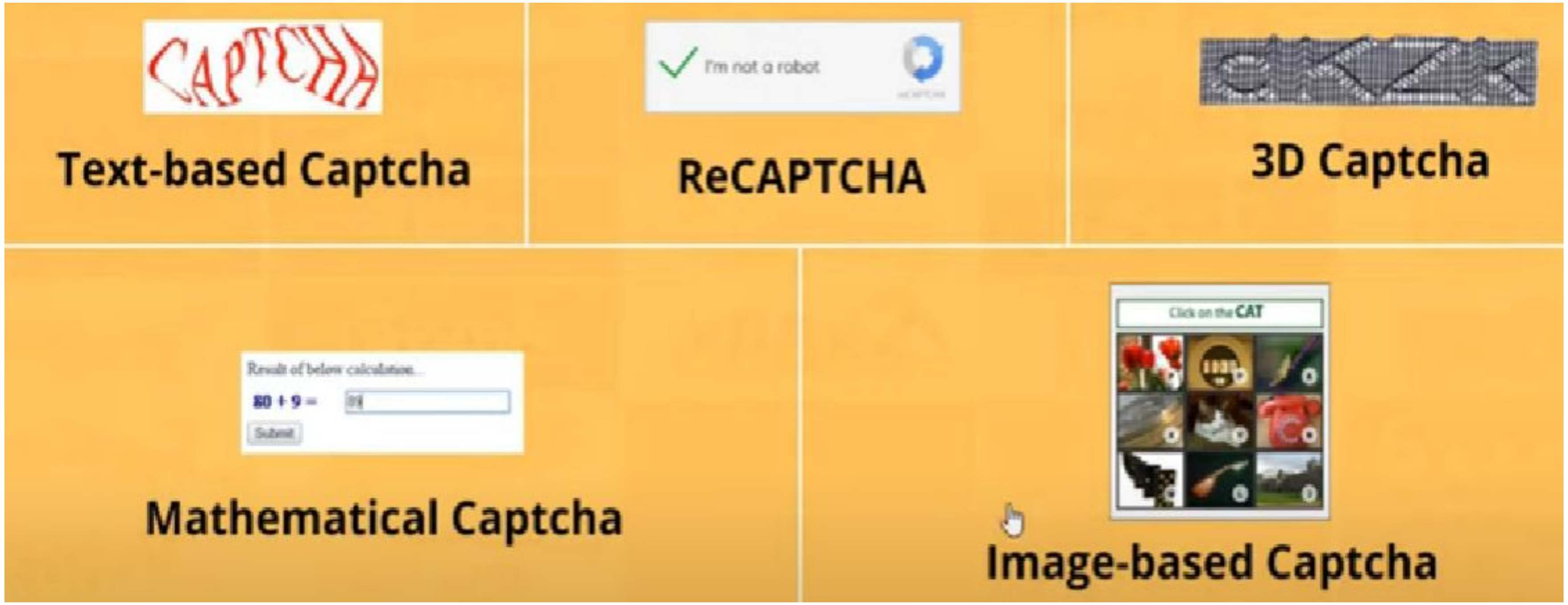
The decryption algorithm is simply

$$p = D(k, C) = (C - k) \bmod 26$$

For Caesar cipher, a brute-force cryptanalysis is easily performed: simply try all the 25 possible keys

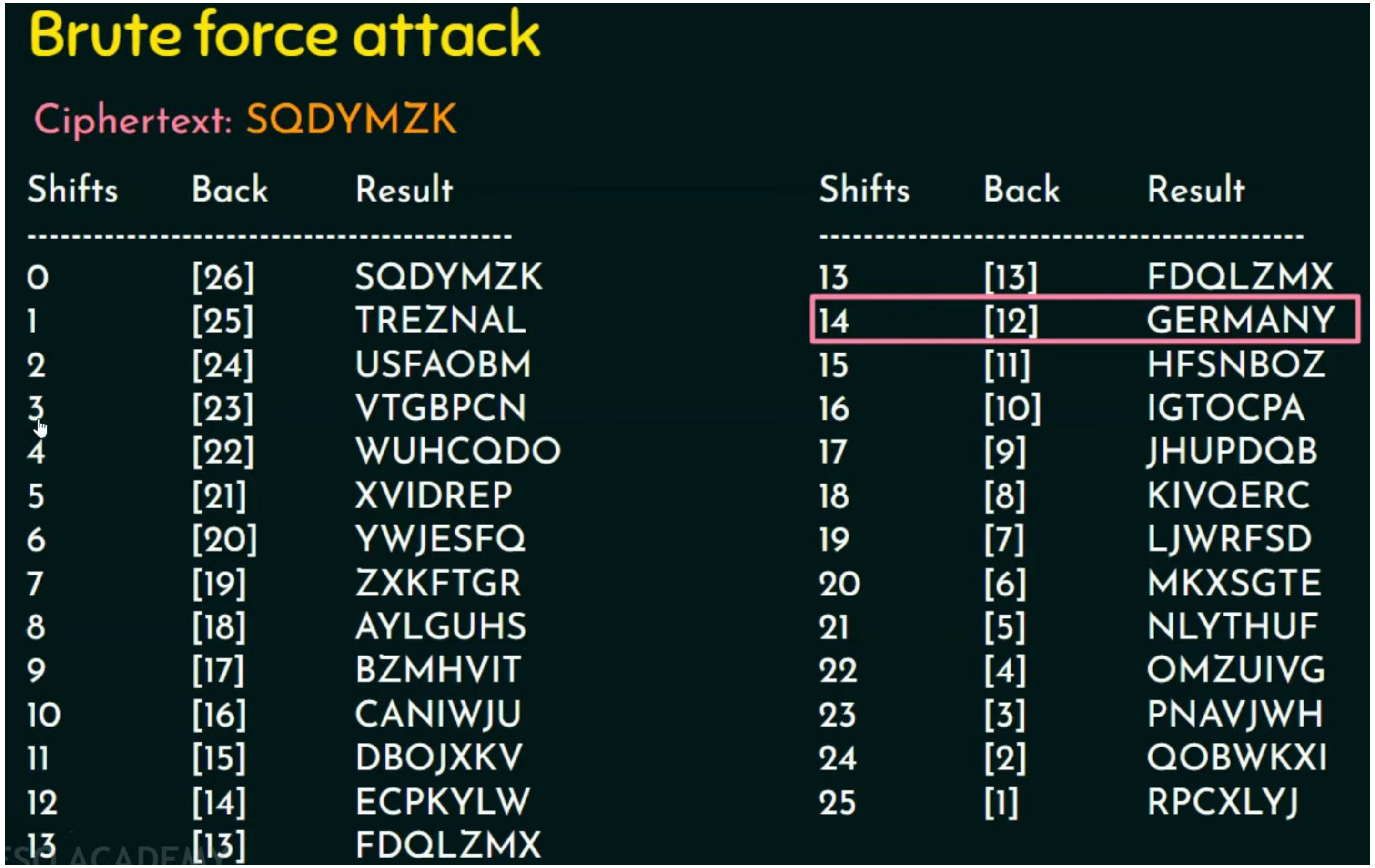
- Trying every possible key until an intelligible translation from cyphertext to plaintext is obtained.
- Guessing
- Software tools
  - Crack
  - Hydra
  - John the ripper
  - Hashcat

- CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart)
- Human being or bot



Shift cipher

- Key= 1,2,3…
- Shift cypher with key = 3 is called Caesar cypher



Brute force attack

Ciphertext: SQDYMZK

Shifts	Back	Result	Shifts	Back	Result
0	[26]	SQDYMZK	13	[13]	FDQLZMX
1	[25]	TREZNAL	14	[12]	GERMANY
2	[24]	USFAOBM	15	[11]	HFSNBOZ
3	[23]	VTGBPCN	16	[10]	IGTOCPA
4	[22]	WUHCQDO	17	[9]	JHUPDQB
5	[21]	XVIDREP	18	[8]	KIVQERC
6	[20]	YWJESFQ	19	[7]	LJWRFSD
7	[19]	ZXKFTGR	20	[6]	MKXSGTE
8	[18]	AYLGUHS	21	[5]	NLYTHUF
9	[17]	BZMHVIT	22	[4]	OMZUIVG
10	[16]	CANIWJU	23	[3]	PNAVJWH
11	[15]	DBOJXKV	24	[2]	QOBWKXI
12	[14]	ECPKYLW	25	[1]	RPCXLYJ
13	[13]	FDQLZMX			

Monoalphabetic Ciphers

- A permutation of a finite set of elements *S* is an ordered sequence of all the elements of *S*, with each element appearing exactly once.
- For example, if *S* = {a, b, c}, there are six permutations of *S*:

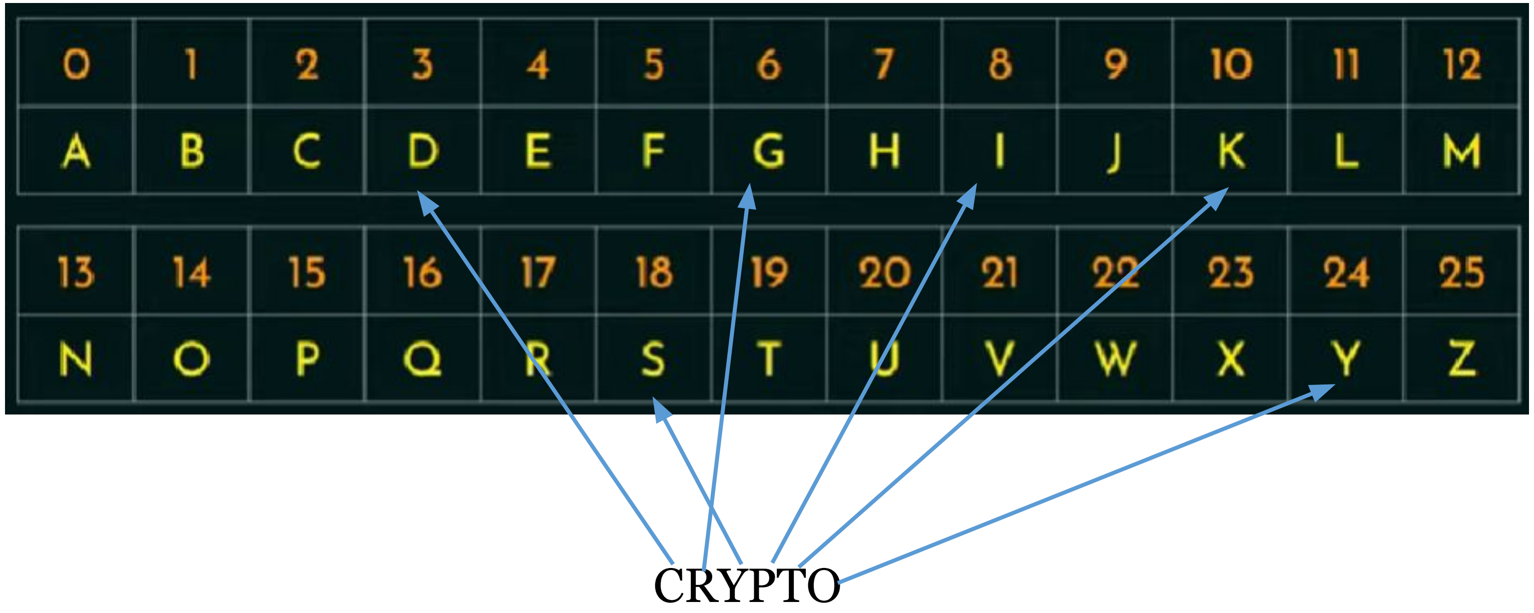
abc, acb, bac, bca, cab, cba

In general, there are n! permutations of a set of n elements

Monoalphabetic substitution cipher

26! or greater than $4 * 10^{26}$ possible keys

- The cypher line can be any permutation of 26 alphabetic characters
- A single cipher alphabet (mapping from plain alphabet to cipher alphabet) is used per message.



0	1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M

13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

CRYPTO

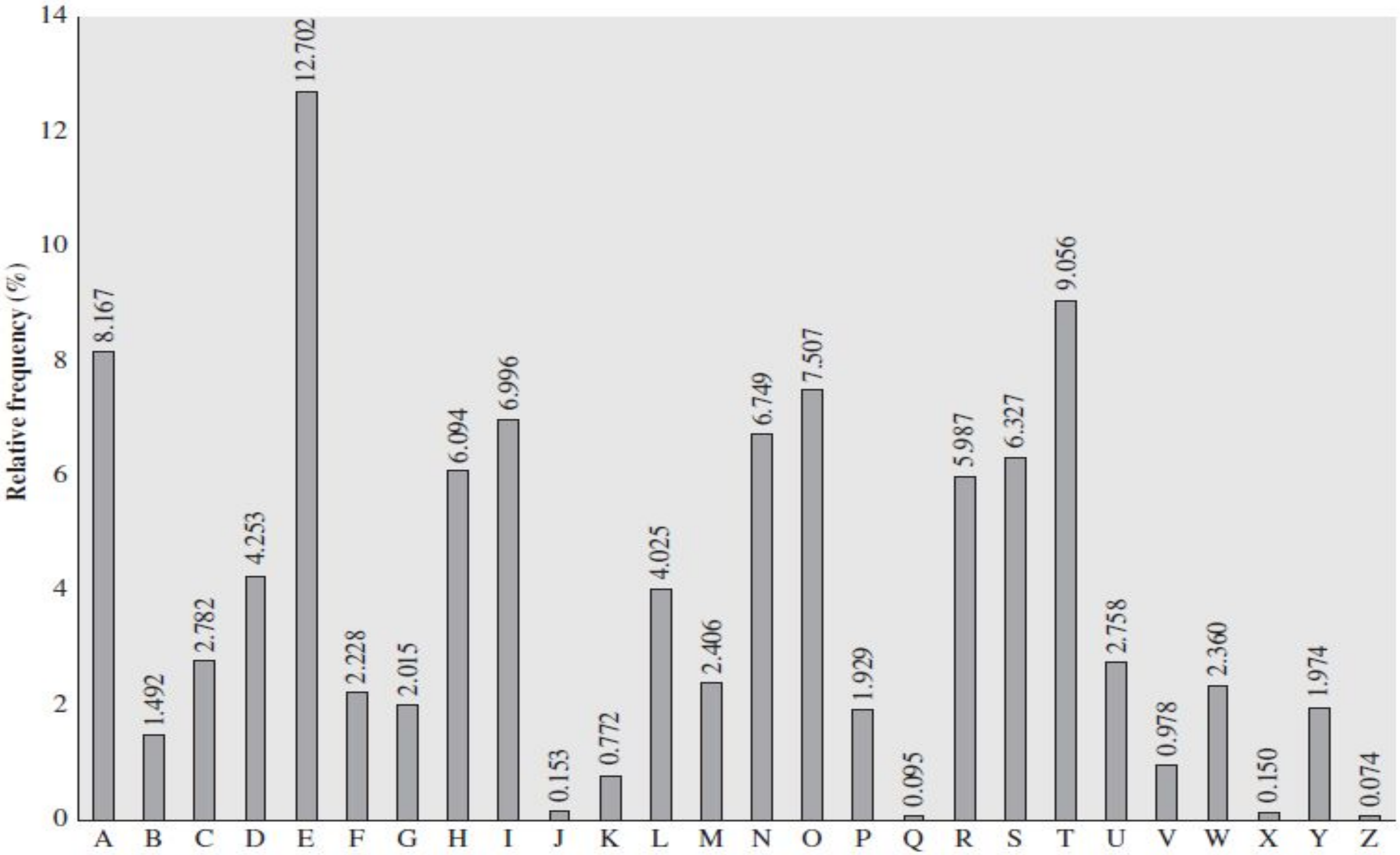
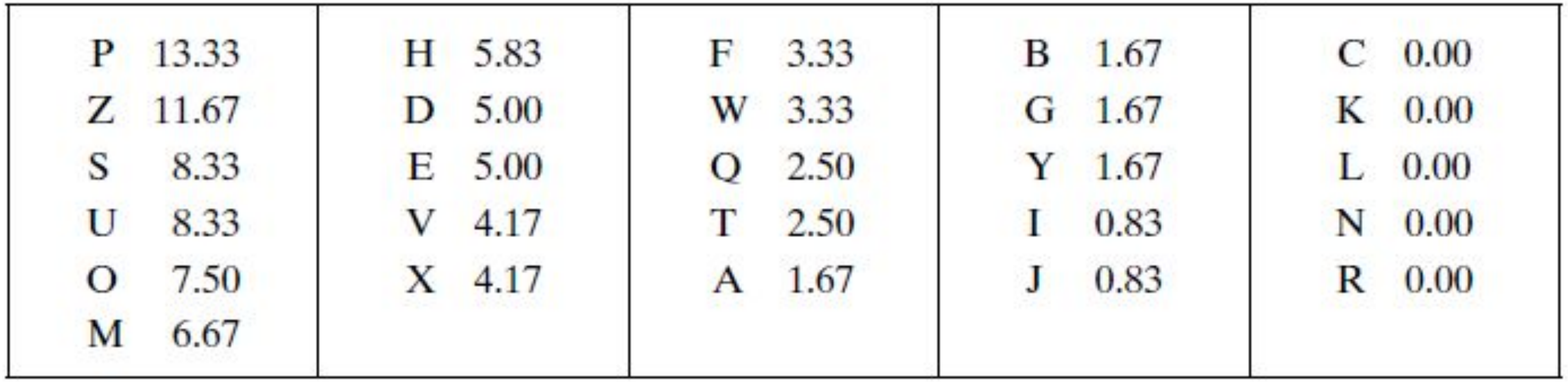


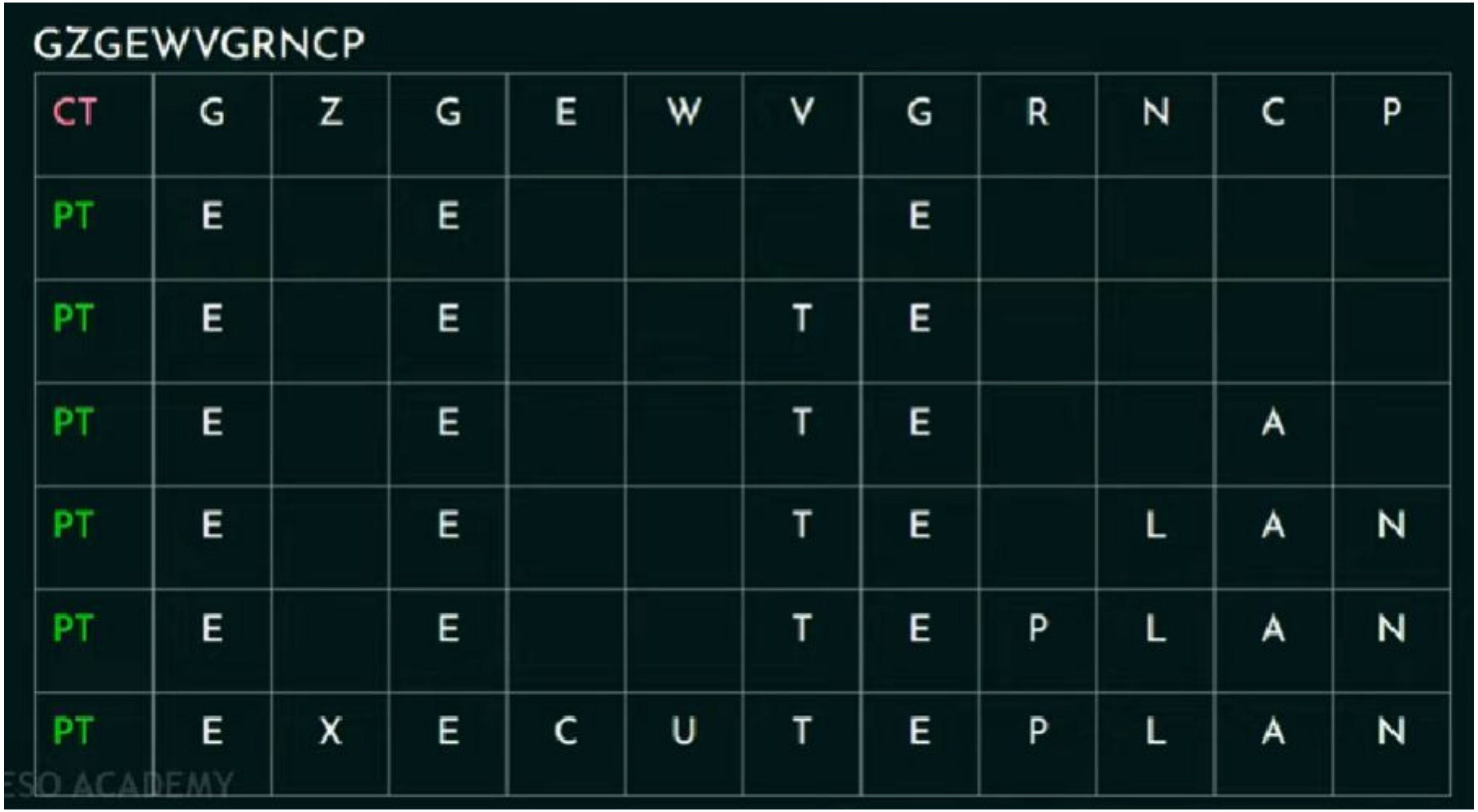
Figure 2.5 Relative Frequency of Letters in English Text

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZVUEPHZHMDZSHZOW

SFPAPPDTSVPQUZWYMXUZUHSXEPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ



P	13.33	H	5.83	F	3.33	B	1.67	C	0.00
Z	11.67	D	5.00	W	3.33	G	1.67	K	0.00
S	8.33	E	5.00	Q	2.50	Y	1.67	L	0.00
U	8.33	V	4.17	T	2.50	I	0.83	N	0.00
O	7.50	X	4.17	A	1.67	J	0.83	R	0.00
M	6.67								



GZGEWVGRNCP

CT	G	Z	G	E	W	V	G	R	N	C	P
PT	E		E				E				
PT	E		E			T	E				
PT	E		E			T	E			A	
PT	E		E			T	E		L	A	N
PT	E		E			T	E	P	L	A	N
PT	E	X	E	C	U	T	E	P	L	A	N

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
 t a        e  e te  a that e e a       a
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
   e t   ta t ha e ee  a e  th    t  a
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
 e  e e tat  e   the   t
```

it was disclosed yesterday that several informal but
direct contacts have been made with political
representatives of the viet cong in moscow

- Monoalphabetic ciphers are easy to break because they reflect the frequency data of the original alphabet.
- A countermeasure is to provide multiple substitutes, known as homophones, for a single letter
- The great mathematician Carl Friedrich Gauss believed that he had devised an unbreakable cipher using homophones.

Practice problem

Encrypt the plain text using Monoalphabetic Cipher

“Attack postponed to tomorrow and do not use our secret paper until further info”

Secret Key: The quick brown fox jumps over the lazy dog

Note: Ignore the second and latter occurrence of alphabets in the key

Playfair Cipher

- The best-known multiple-letter encryption cipher is the Playfair, which treats digrams in the plaintext as single units and translates these units into ciphertext digrams

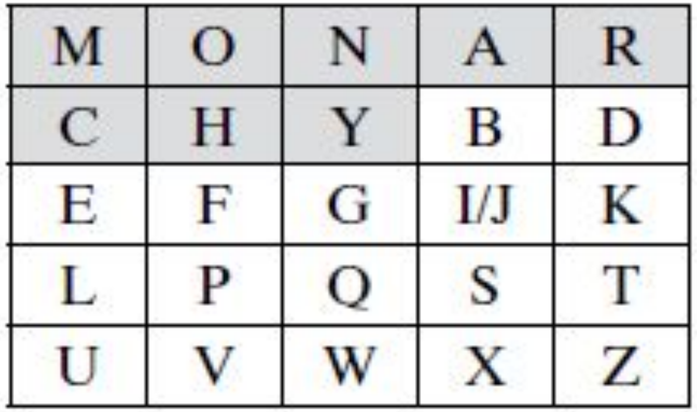
- Manual symmetric encryption technique.

- The Playfair algorithm is based on the use of a 5 * 5 matrix of letters constructed using a keyword.

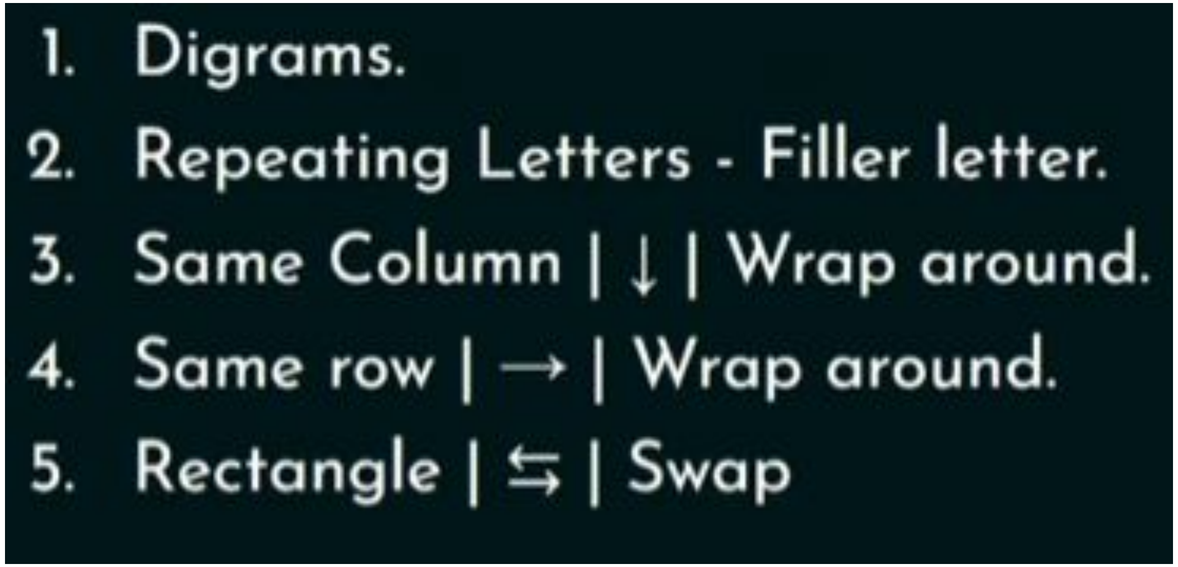
- The keyword is monarchy.

- The matrix is constructed by filling in the letters of the keyword (minus duplicates) from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabetic order.

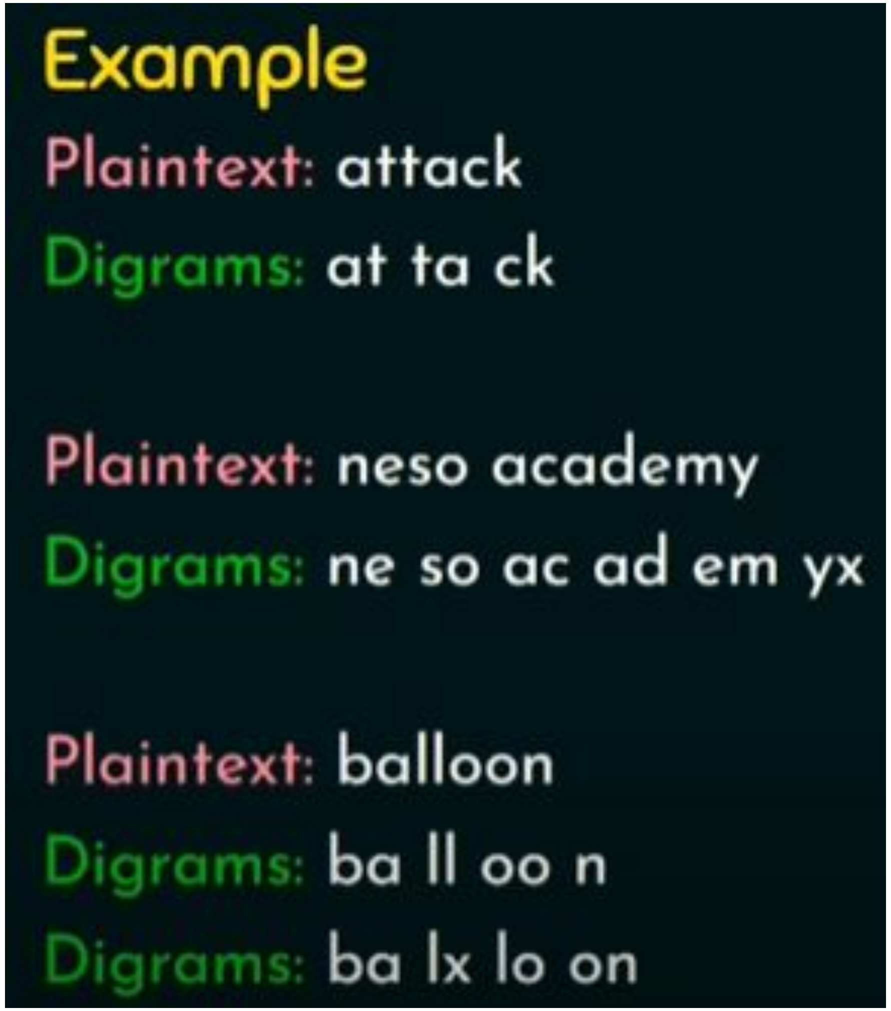
- The letters I and J count as one letter.



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



1. Digrams.
2. Repeating Letters - Filler letter.
3. Same Column | ↓ | Wrap around.
4. Same row | → | Wrap around.
5. Rectangle | ⇆ | Swap



Example

Plaintext: attack

Digrams: at ta ck

Plaintext: neso academy

Digrams: ne so ac ad em yx

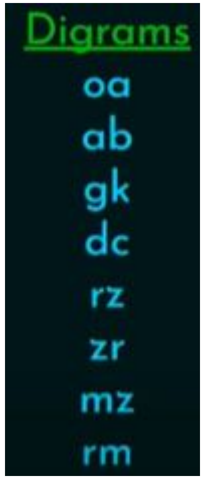
Plaintext: balloon

Digrams: ba ll oo n

Digrams: ba lx lo on

- Plaintext is encrypted two letters at a time, according to the following rules:
- Repeating plaintext letters that are in the same pair are separated with a filler letter, such as x,
- Eg: balloon would be treated as ba lx lo on.
- Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last.
- For example, ar is encrypted as RM.

- Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last.
- For example, mu is encrypted as CM.



Digrams

oa

ab

gk

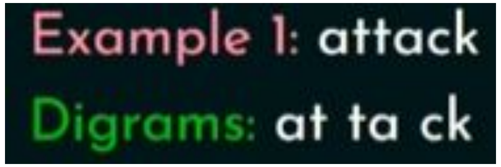
dc

rz

zr

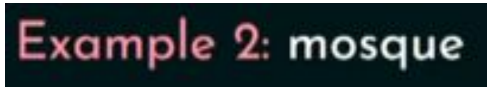
mz

rm



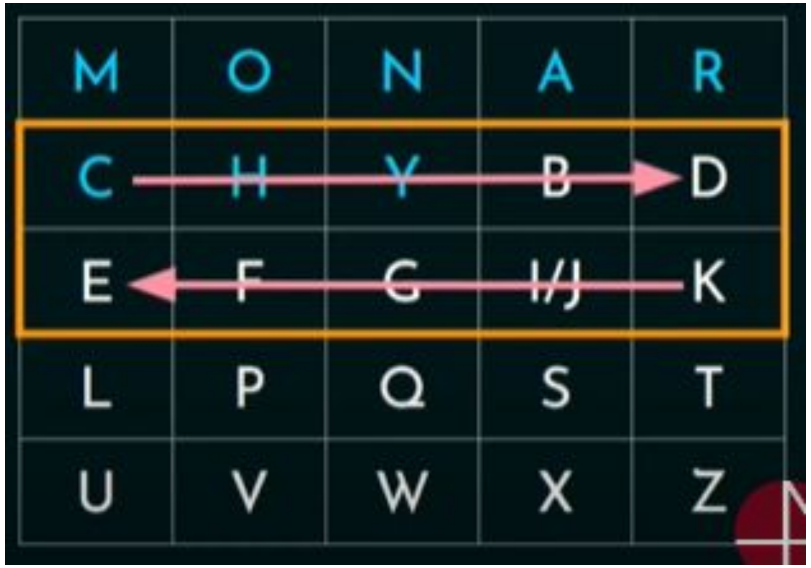
Example 1: attack

Digrams: at ta ck

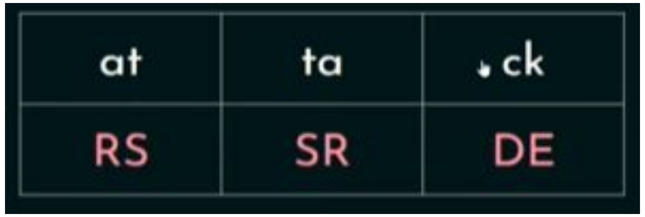


Example 2: mosque

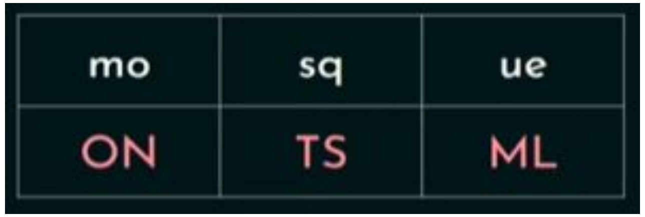
at	ta	ck



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



at	ta	ck
RS	SR	DE



mo	sq	ue
ON	TS	ML

Practice problem

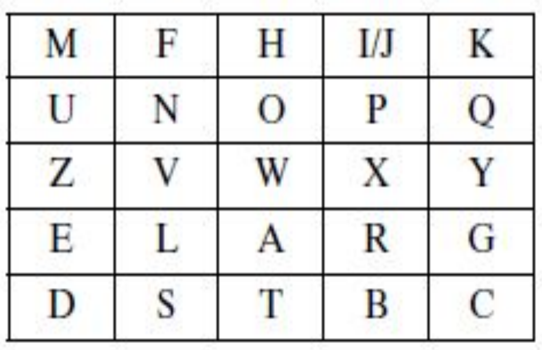
- When the PT-109 American patrol boat, under the command of Lieutenant John F. Kennedy, was sunk by a Japanese destroyer, a message was received at an Australian wireless station in Playfair code:
  - `KXJEY UREBE ZWEHE WRYTU HEYFS`
  - `KREHE GOYFI WTTTU OLKSY CAJPO`
  - `BOTEI ZONTX BYBNT GONEY CUZWR`
  - `GDSON SXBOU YWRHE BAAHY USEDQ`
- The key used was *royal new zealand navy*. Decrypt the message. Translate TT into tt.

Practice problem

- **a.** Construct a Playfair matrix with the key *largest*.
- **b.** Construct a Playfair matrix with the key *occurrence*. Make a reasonable assumption about how to treat redundant letters in the key.

Practice problem

- a. Using this Playfair matrix:



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

- Encrypt this message:
  - Must see you over Cadogan West. Coming at once.
- *Note:* The message is from the Sherlock Holmes story, *The Adventure of the Bruce-Partington Plans*.
- b. Repeat part (a) using the Playfair matrix from Problem in the last slide.
- c. How do you account for the results of this problem? Can you generalize your conclusion?

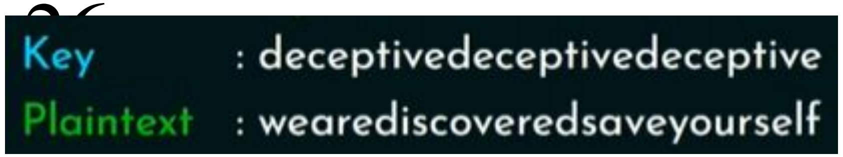
Polyalphabetic Ciphers

1. A set of related monoalphabetic substitution rules is used.
2. A key determines which particular rule is chosen for a given transformation.

Vigenère Cipher

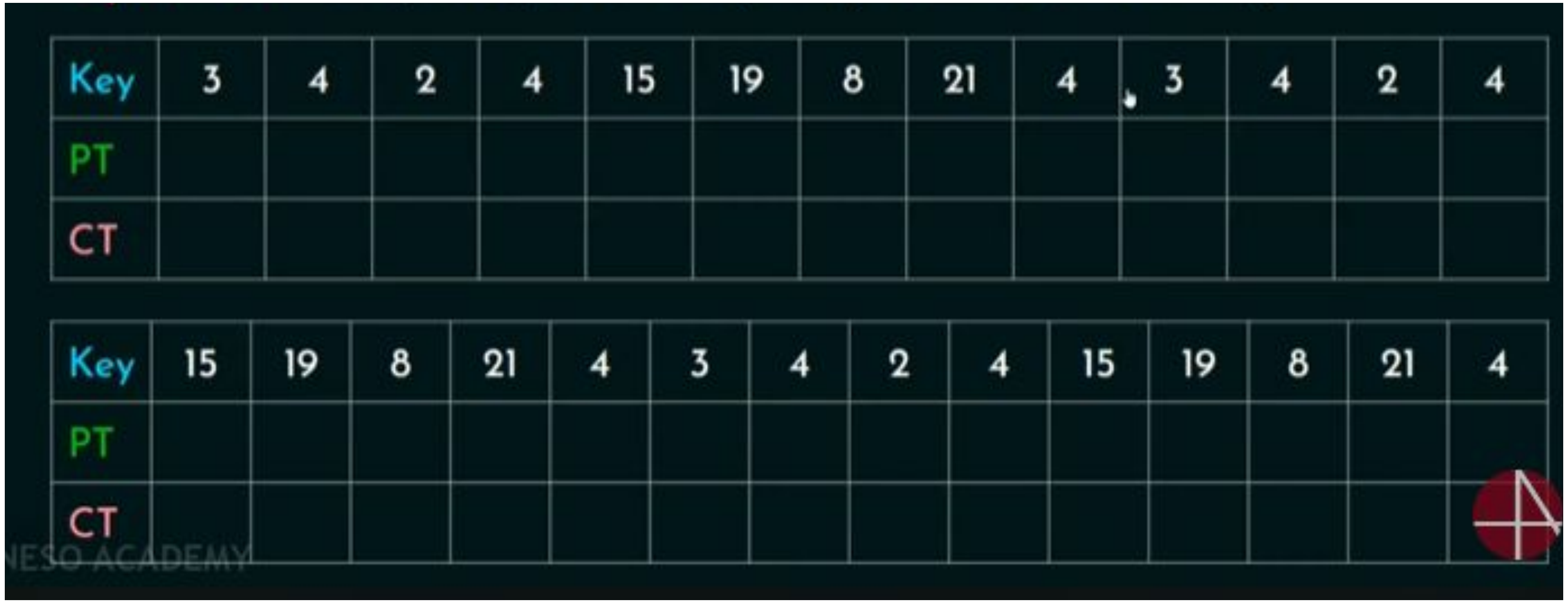
- The set of related monoalphabetic substitution rules consists of the 26 Caesar ciphers with shifts of 0 through 25

$$C_i = (p_i + k_{i \bmod m}) \bmod 26$$



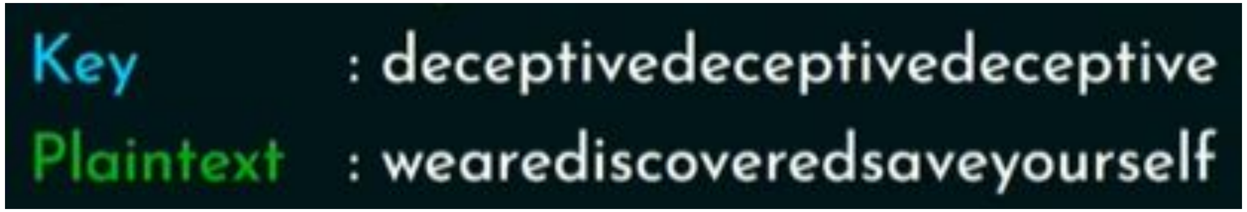
Key : deceptivedeceptivedeceptive

Plaintext : wearediscoveredsaveyourself



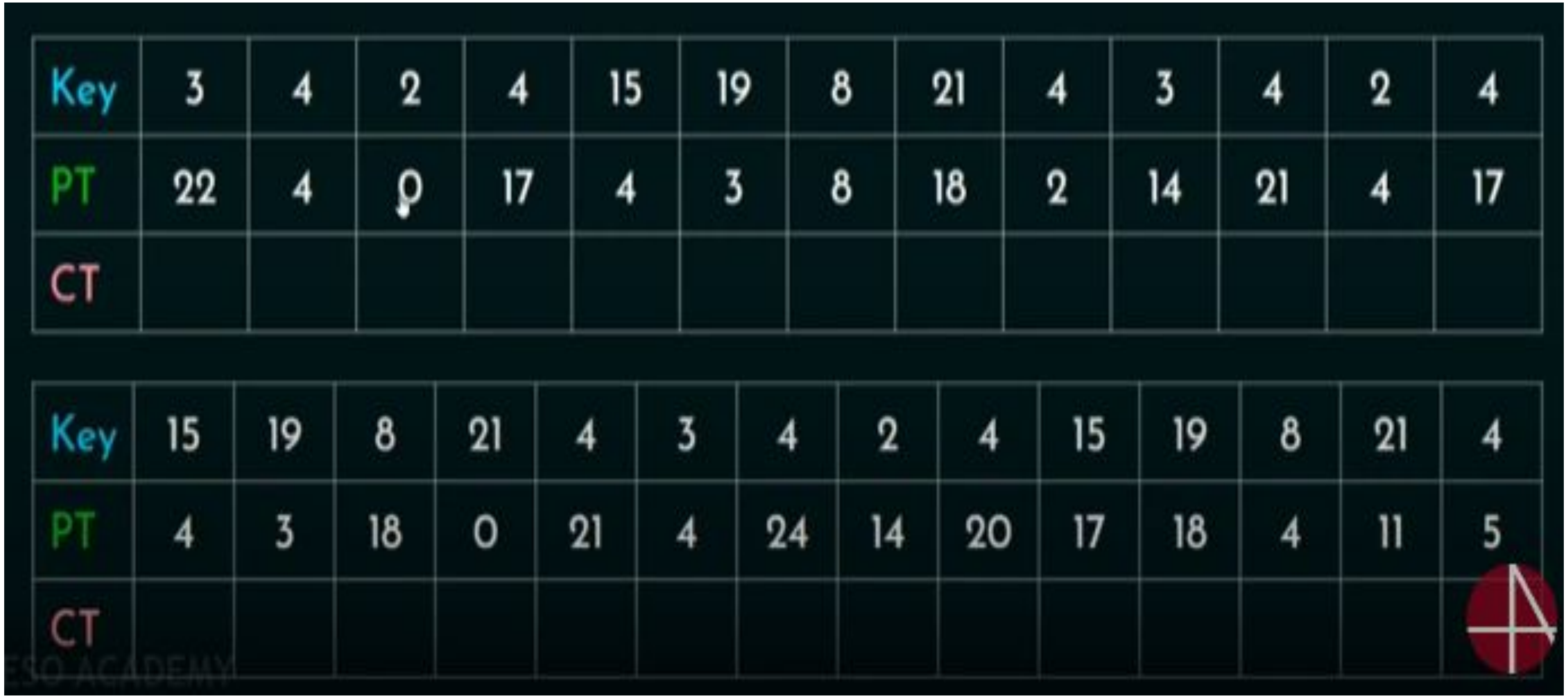
Key	3	4	2	4	15	19	8	21	4	3	4	2	4
PT													
CT													

Key	15	19	8	21	4	3	4	2	4	15	19	8	21	4
PT														
CT														



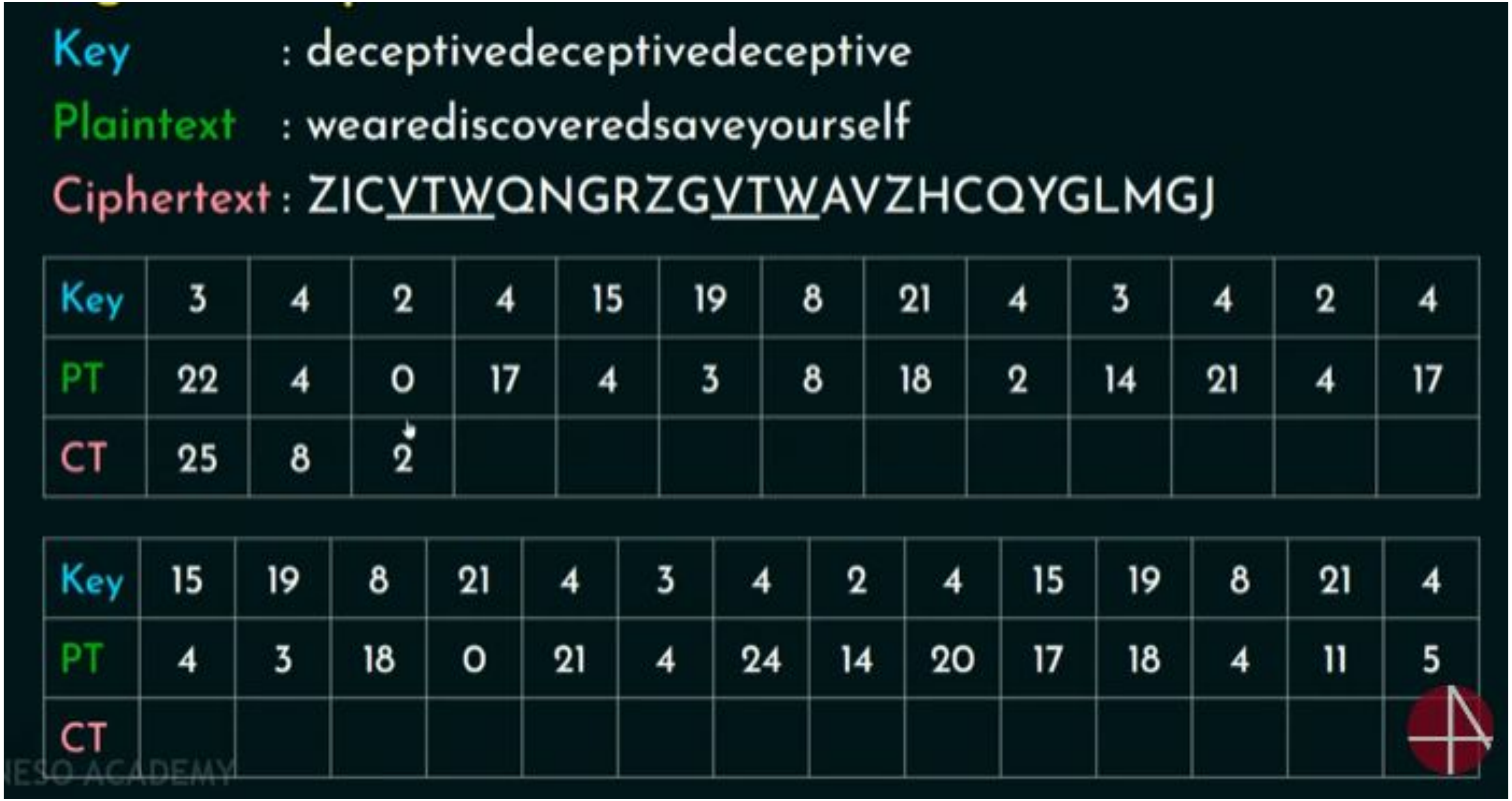
Key : deceptivedeceptivedeceptive

Plaintext : wearediscoveredsaveyourself



Key	3	4	2	4	15	19	8	21	4	3	4	2	4
PT	22	4	0	17	4	3	8	18	2	14	21	4	17
CT													

Key	15	19	8	21	4	3	4	2	4	15	19	8	21	4
PT	4	3	18	0	21	4	24	14	20	17	18	4	11	5
CT														



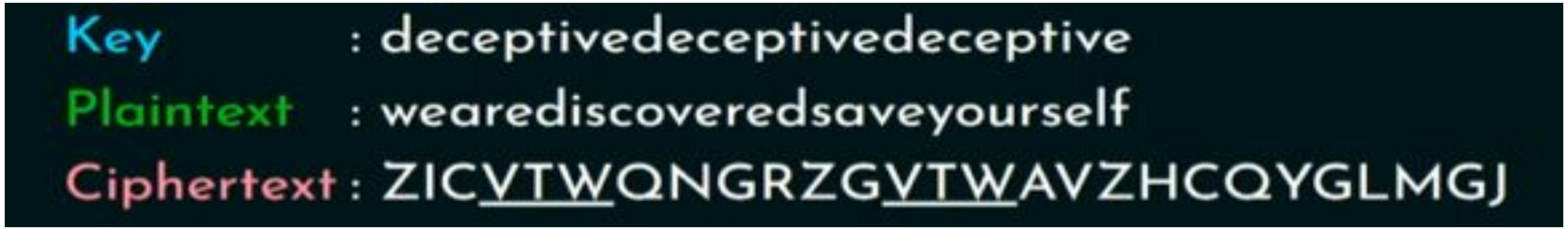
Key : deceptivedeceptivedeceptive

Plaintext : wearediscoveredsaveyourself

Ciphertext : ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Key	3	4	2	4	15	19	8	21	4	3	4	2	4
PT	22	4	0	17	4	3	8	18	2	14	21	4	17
CT	25	8	2										

Key	15	19	8	21	4	3	4	2	4	15	19	8	21	4
PT	4	3	18	0	21	4	24	14	20	17	18	4	11	5
CT														

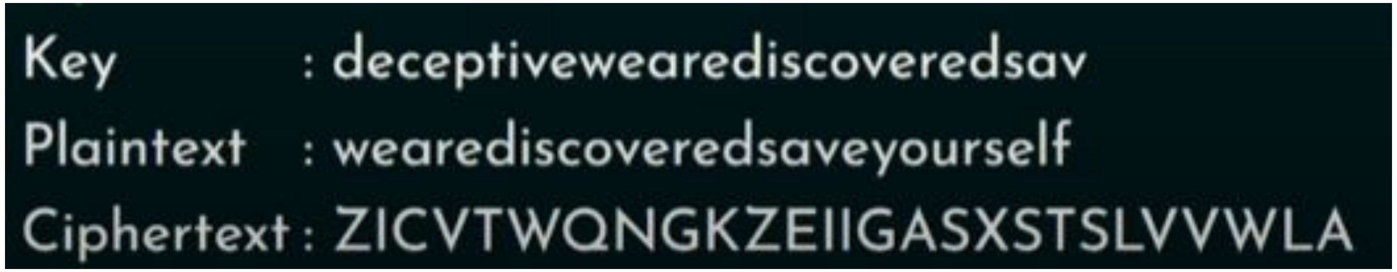


Key : deceptivedeceptivedeceptive

Plaintext : wearediscoveredsaveyourself

Ciphertext : ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Autokey system



Key : deceptivewearediscoveredsav

Plaintext : wearediscoveredsaveyourself

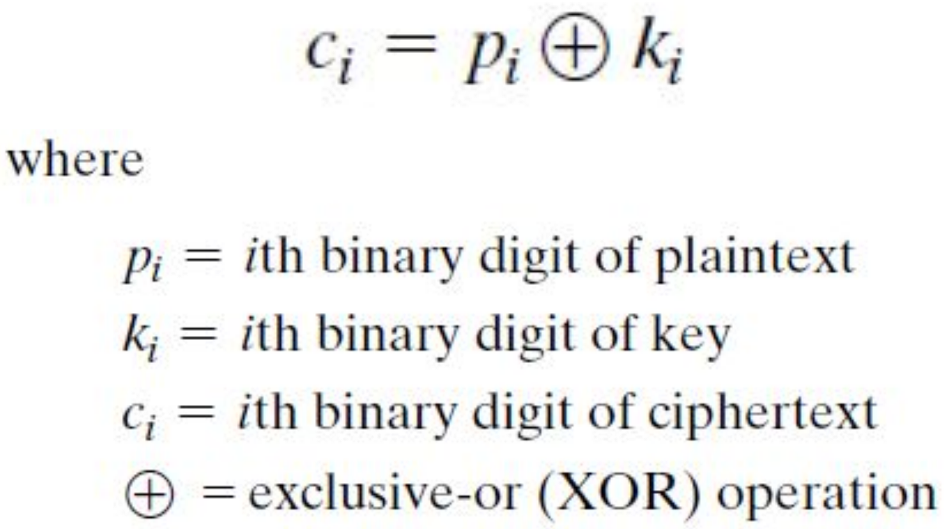
Ciphertext : ZICVTWQNGKZEIIGASXSTSLVVWLA

Vernam Cipher

- Ultimate defense: to choose a keyword that is as long as the plaintext and has no statistical relationship to it.

- Such a system was introduced by an AT&T engineer named Gilbert Vernam in 1918.

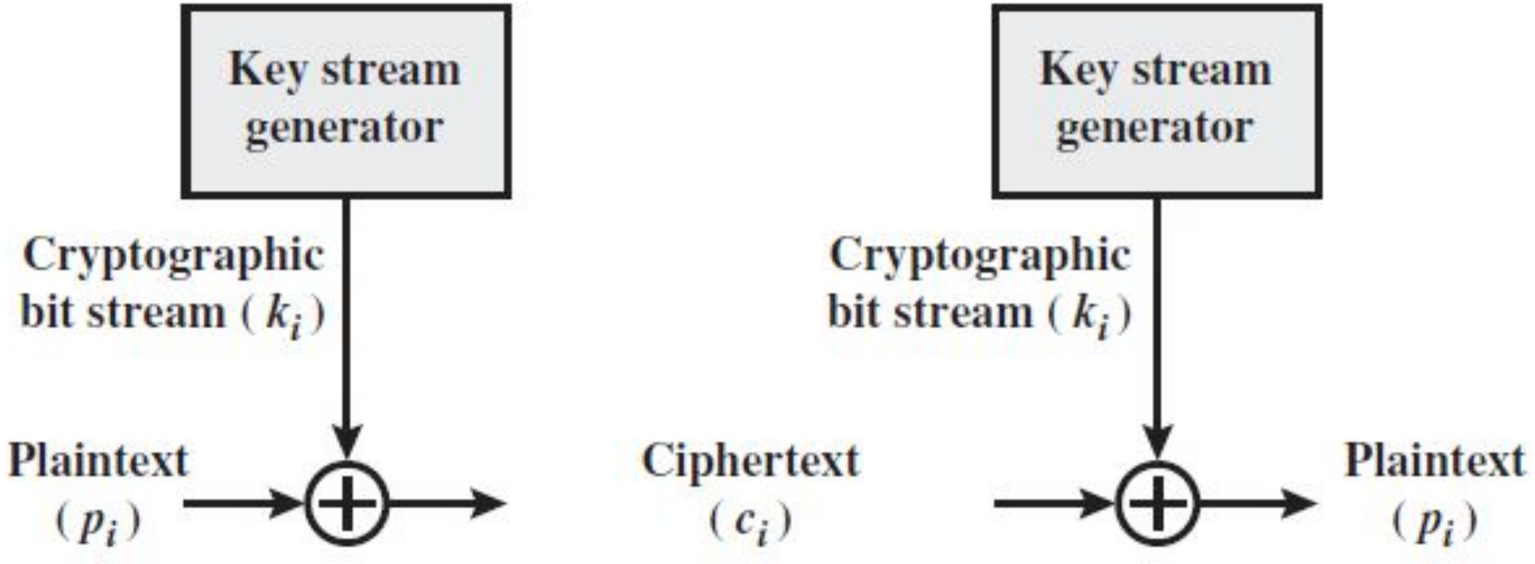
- Works on binary data (bits) rather than letters



$$c_i = p_i \oplus k_i$$

where

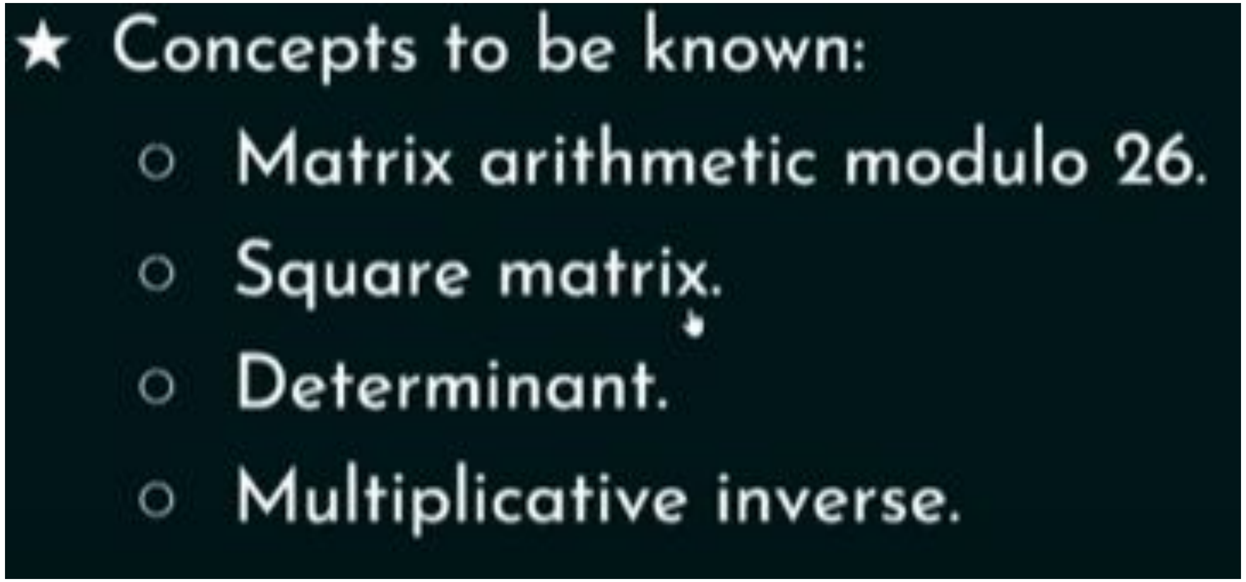
p_i = ith binary digit of plaintext
k_i = ith binary digit of key
c_i = ith binary digit of ciphertext
$\oplus$ = exclusive-or (XOR) operation



- Vernam proposed the use of a running loop of tape that eventually repeated the key
- The system worked with a very long but repeating keyword.
- It can be broken with sufficient ciphertext, the use of known or probable plaintext sequences, or both.

Hill Cipher

- Hill cipher, developed by the mathematician Lester Hill in 1929.
- Multi-letter cypher
- Group of letter: Digraph, trigraph, polygraph



★ Concepts to be known:

- ○ Matrix arithmetic modulo 26.
- ○ Square matrix.
- ○ Determinant.
- ○ Multiplicative inverse.

$\mathbf{C} = \mathrm{E}(\mathbf{K}, \mathbf{P}) = \mathbf{PK} \bmod 26$

$\mathbf{P} = \mathrm{D}(\mathbf{K}, \mathbf{C}) = \mathbf{CK}^{-1} \bmod 26 = \mathbf{PKK}^{-1} = \mathbf{P}$

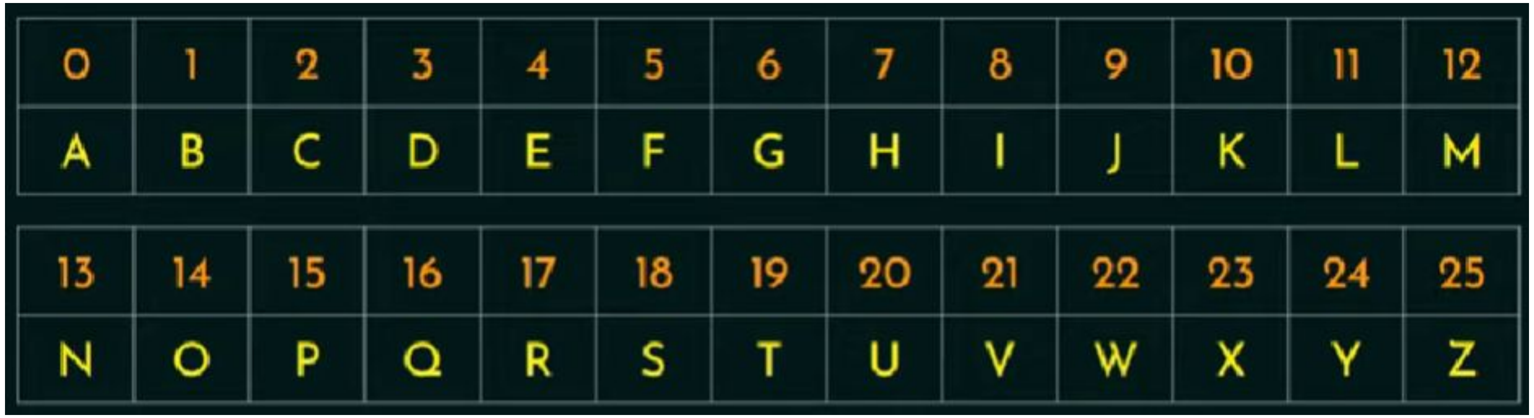
$$(c_1\ c_2\ c_3) = (p_1\ \ p_2\ \ p_3)\begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \bmod 26$$

$$\mathbf{C} = \mathbf{PK} \bmod 26$$

$$c_1 = (k_{11}p_1 + k_{21}p_2 + k_{31}p_3) \bmod 26$$
$$c_2 = (k_{12}p_1 + k_{22}p_2 + k_{32}p_3) \bmod 26$$
$$c_3 = (k_{13}p_1 + k_{23}p_2 + k_{33}p_3) \bmod 26$$

- Consider the plaintext “paymoremoney” and use the encryption key

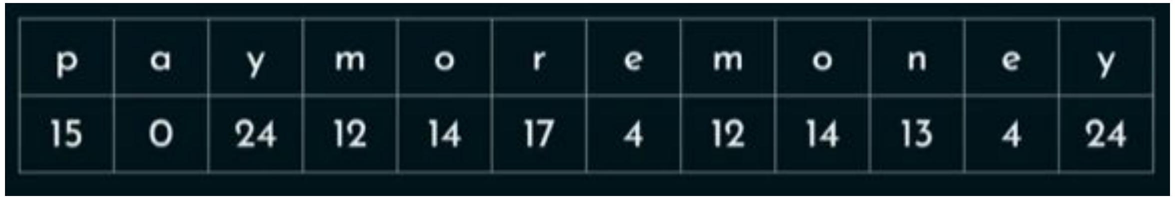
$$\mathbf{K} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$



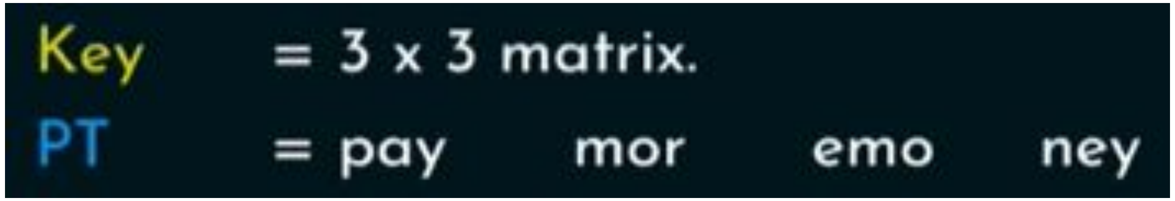
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

- The first three letters of the plaintext are represented by the vector (15 0 24).

- Then(15 0 24)K = (303 303 531) mod 26 = (17 17 11) = RRL.

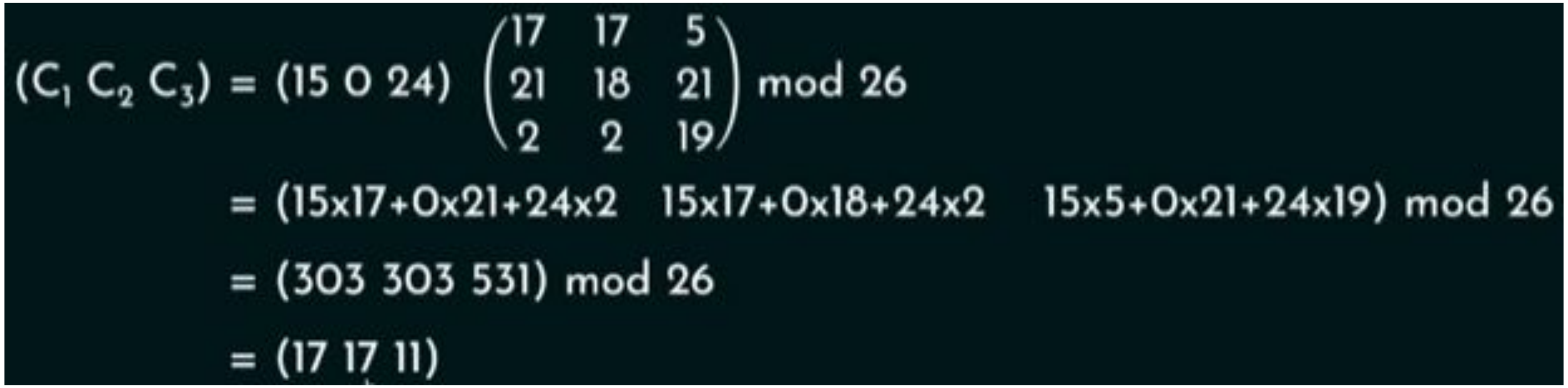


p	a	y	m	o	r	e	m	o	n	e	y
15	0	24	12	14	17	4	12	14	13	4	24



Key = 3 x 3 matrix.

PT = pay mor emo ney

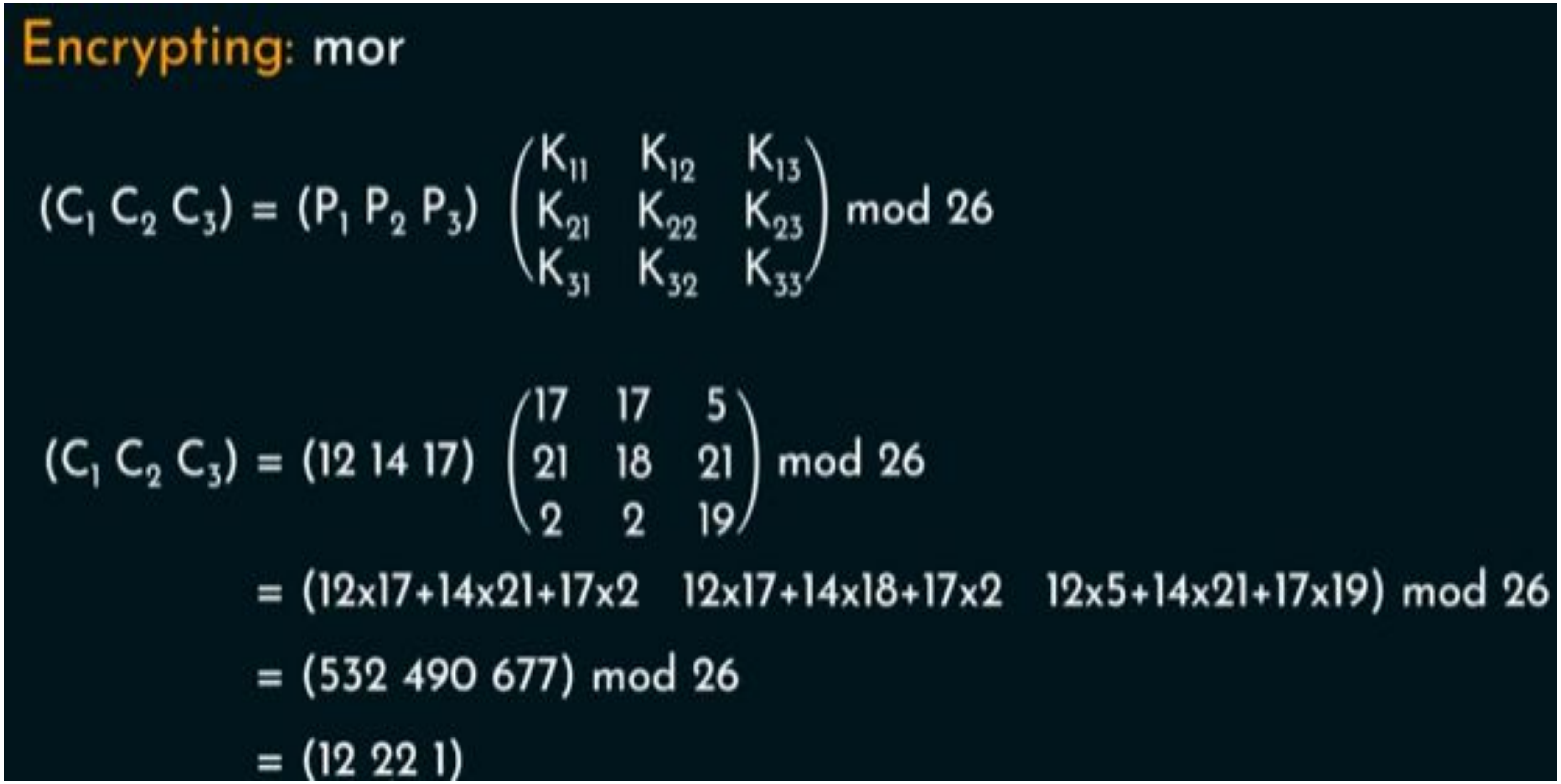


$$(C_1\ C_2\ C_3) = (15\ 0\ 24)\begin{pmatrix}17 & 17 & 5\\ 21 & 18 & 21\\ 2 & 2 & 19\end{pmatrix} \text{ mod } 26$$

$$= (15\text{x}17+0\text{x}21+24\text{x}2 \quad 15\text{x}17+0\text{x}18+24\text{x}2 \quad 15\text{x}5+0\text{x}21+24\text{x}19) \text{ mod } 26$$

$$= (303\ 303\ 531) \text{ mod } 26$$

$$= (17\ 17\ 11)$$



Encrypting: mor

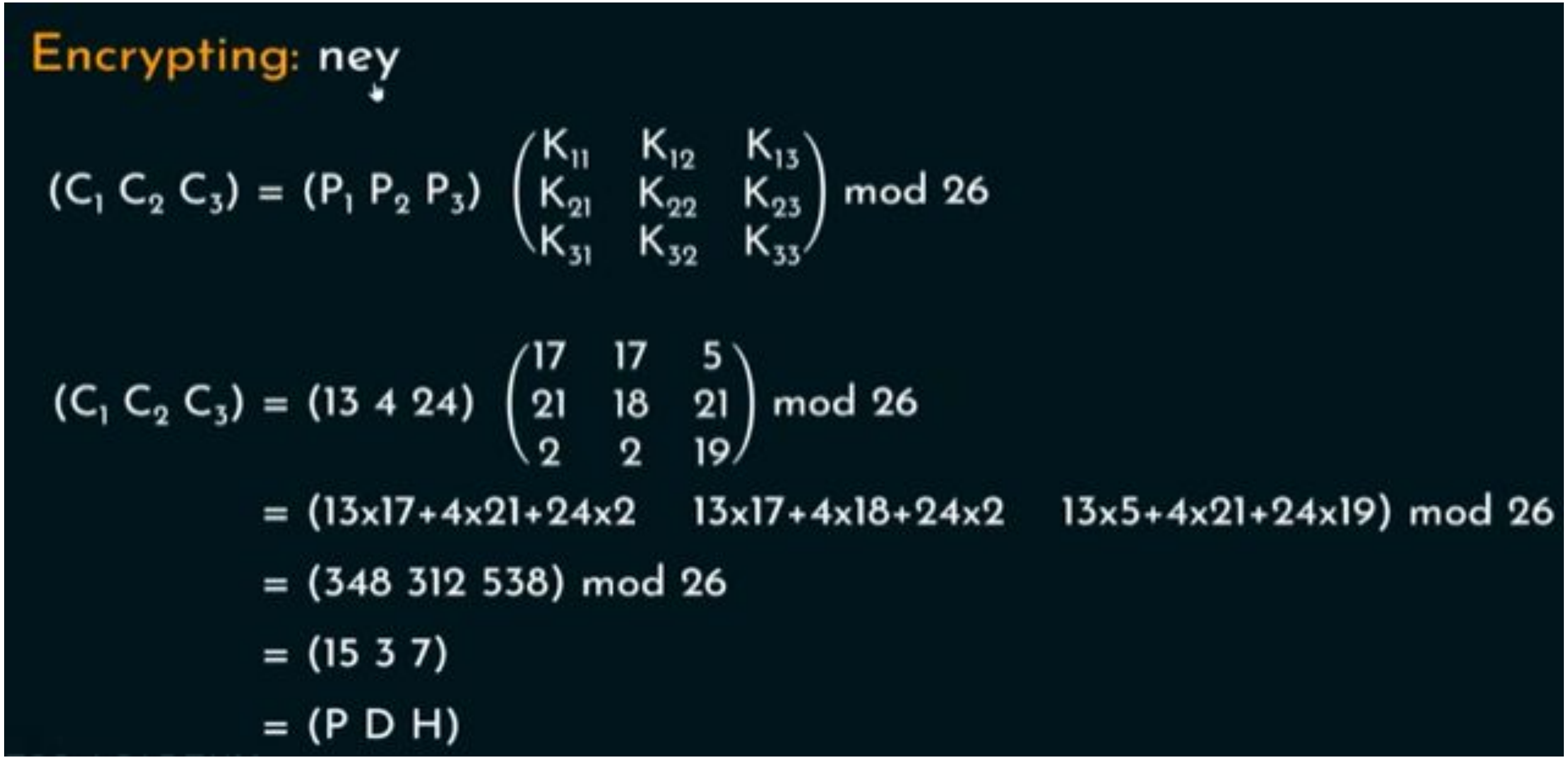
$$(C_1\ C_2\ C_3) = (P_1\ P_2\ P_3) \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \bmod 26$$

$$(C_1\ C_2\ C_3) = (12\ 14\ 17) \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \bmod 26$$

$$= (12\text{x}17+14\text{x}21+17\text{x}2 \quad 12\text{x}17+14\text{x}18+17\text{x}2 \quad 12\text{x}5+14\text{x}21+17\text{x}19) \bmod 26$$

$$= (532\ 490\ 677) \bmod 26$$

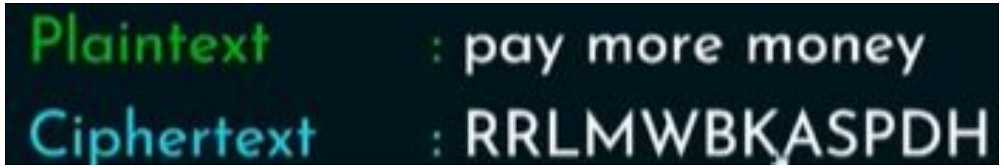
$$= (12\ 22\ 1)$$



Encrypting: ney

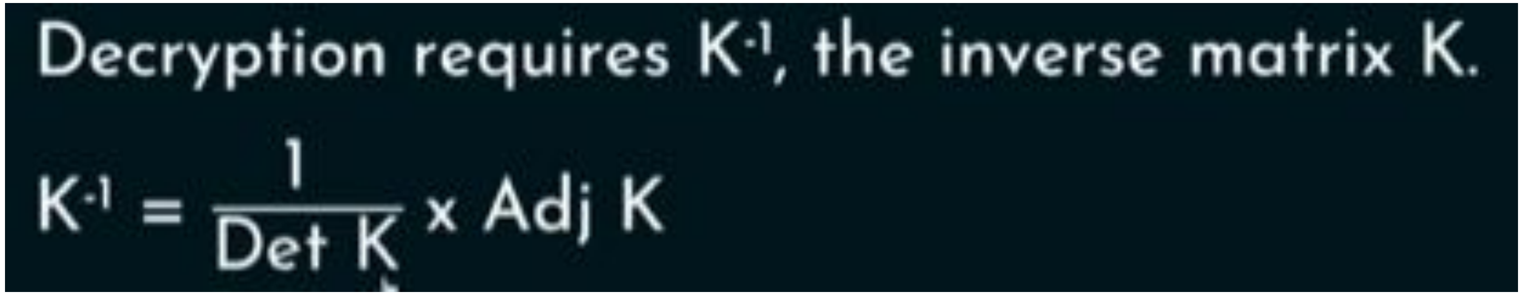
$$(C_1\ C_2\ C_3) = (P_1\ P_2\ P_3) \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \bmod 26$$

$$\begin{aligned} (C_1\ C_2\ C_3) &= (13\ 4\ 24) \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \bmod 26 \\ &= (13\text{x}17+4\text{x}21+24\text{x}2 \quad 13\text{x}17+4\text{x}18+24\text{x}2 \quad 13\text{x}5+4\text{x}21+24\text{x}19) \bmod 26 \\ &= (348\ 312\ 538) \bmod 26 \\ &= (15\ 3\ 7) \\ &= (\text{P D H}) \end{aligned}$$



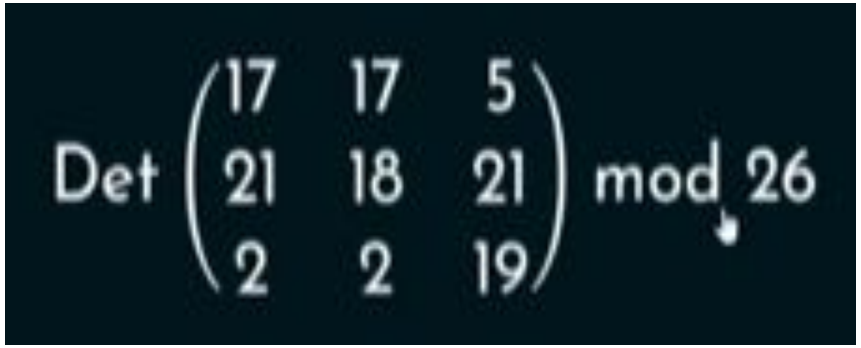
Plaintext : pay more money

Ciphertext : RRLMWBKASPDH

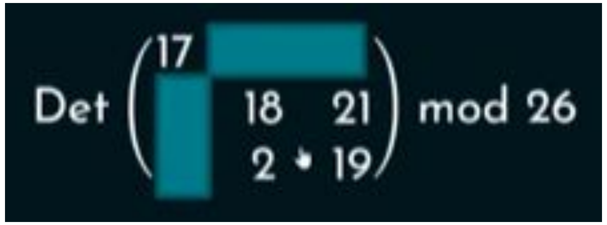


Decryption requires K^{-1}, the inverse matrix K.

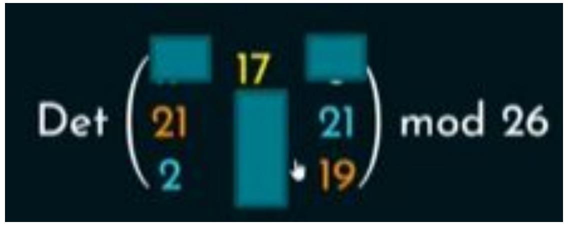
$$K^{-1} = \frac{1}{\text{Det } K} \times \text{Adj } K$$



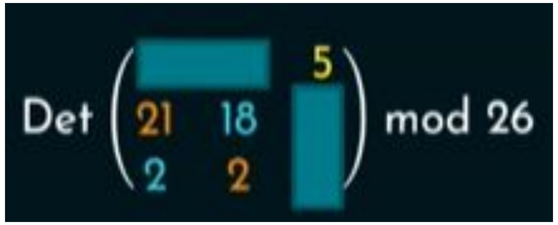
$$\text{Det} \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \text{mod } 26$$



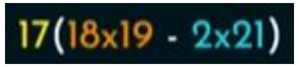
$$\text{Det} \begin{pmatrix} 17 & & \\ & 18 & 21 \\ & 2 & 19 \end{pmatrix} \text{mod } 26$$



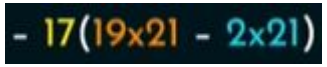
$$\text{Det} \begin{pmatrix} & 17 & \\ 21 & & 21 \\ 2 & & 19 \end{pmatrix} \text{mod } 26$$



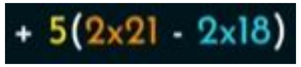
$$\text{Det} \begin{pmatrix} & & 5 \\ 21 & 18 & \\ 2 & 2 & \end{pmatrix} \text{mod } 26$$



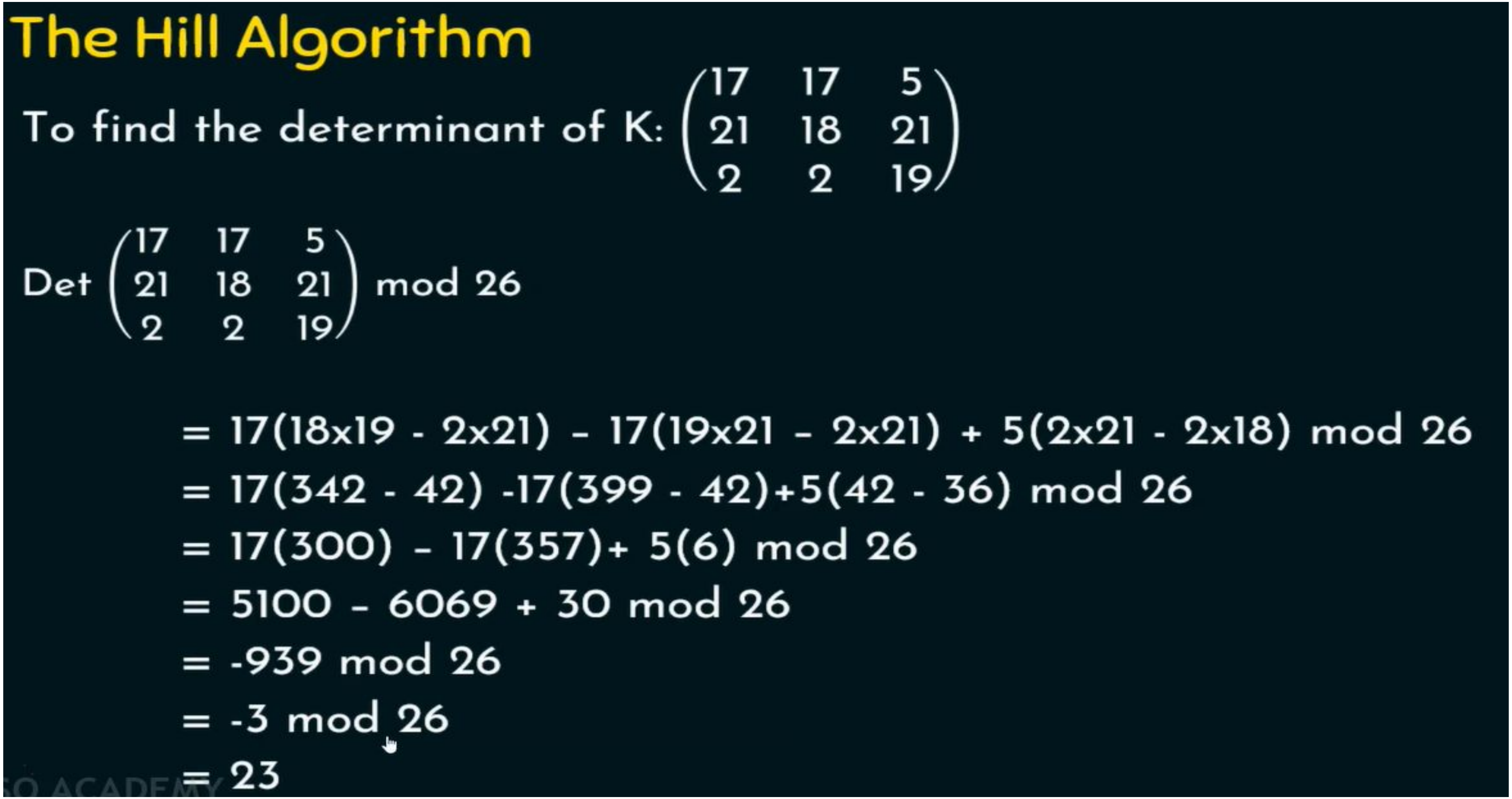
17(18x19 - 2x21)



- 17(19x21 - 2x21)



+ 5(2x21 - 2x18)



The Hill Algorithm

To find the determinant of K: $\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$

$$\text{Det}\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \text{ mod } 26$$

$$= 17(18\text{x}19 - 2\text{x}21) - 17(19\text{x}21 - 2\text{x}21) + 5(2\text{x}21 - 2\text{x}18) \text{ mod } 26$$

$$= 17(342 - 42) -17(399 - 42)+5(42 - 36) \text{ mod } 26$$

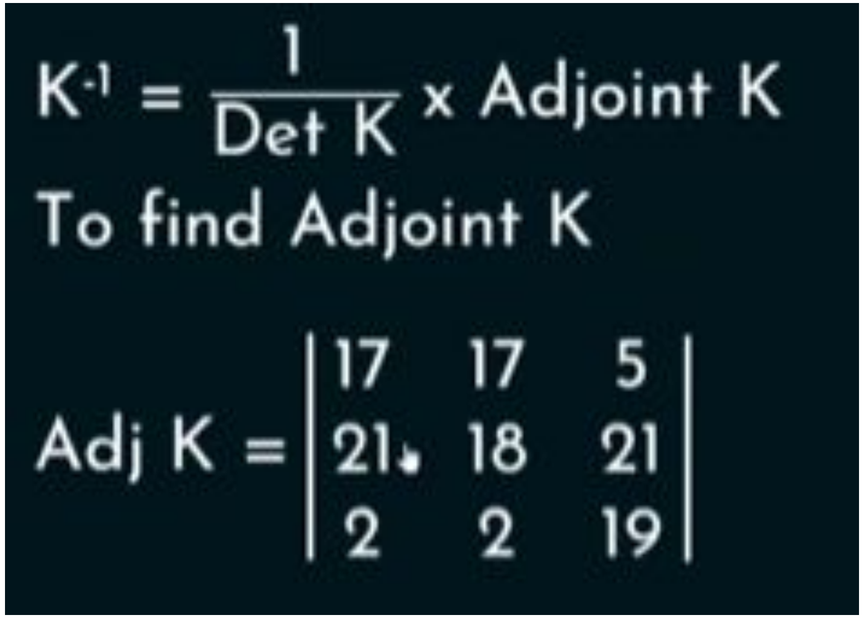
$$= 17(300) - 17(357)+ 5(6) \text{ mod } 26$$

$$= 5100 - 6069 + 30 \text{ mod } 26$$

$$= -939 \text{ mod } 26$$

$$= -3 \text{ mod } 26$$

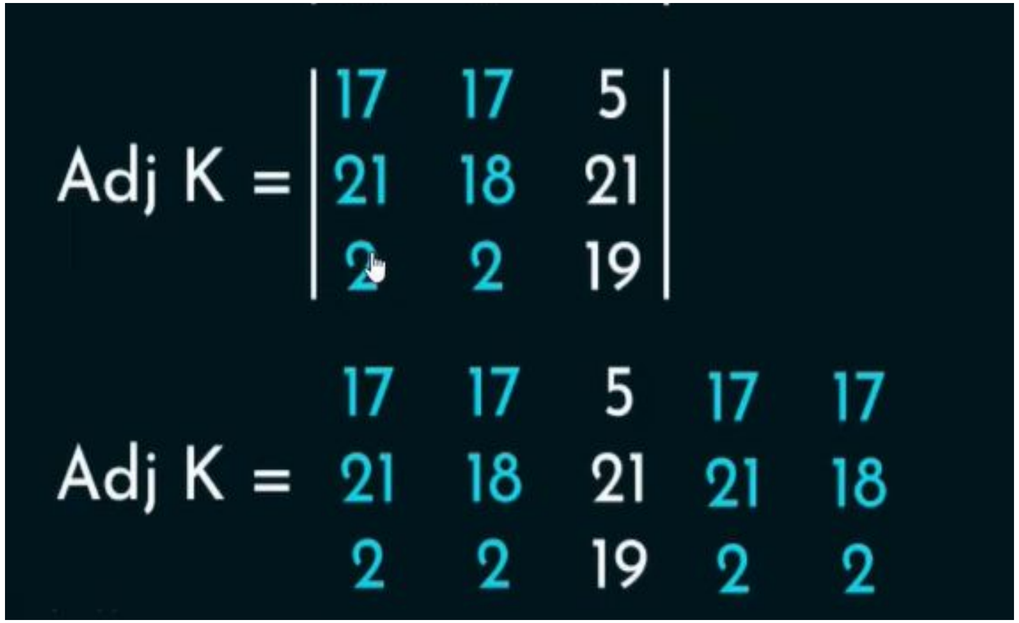
$$= 23$$



$$K^{-1} = \frac{1}{\text{Det } K} \times \text{Adjoint } K$$

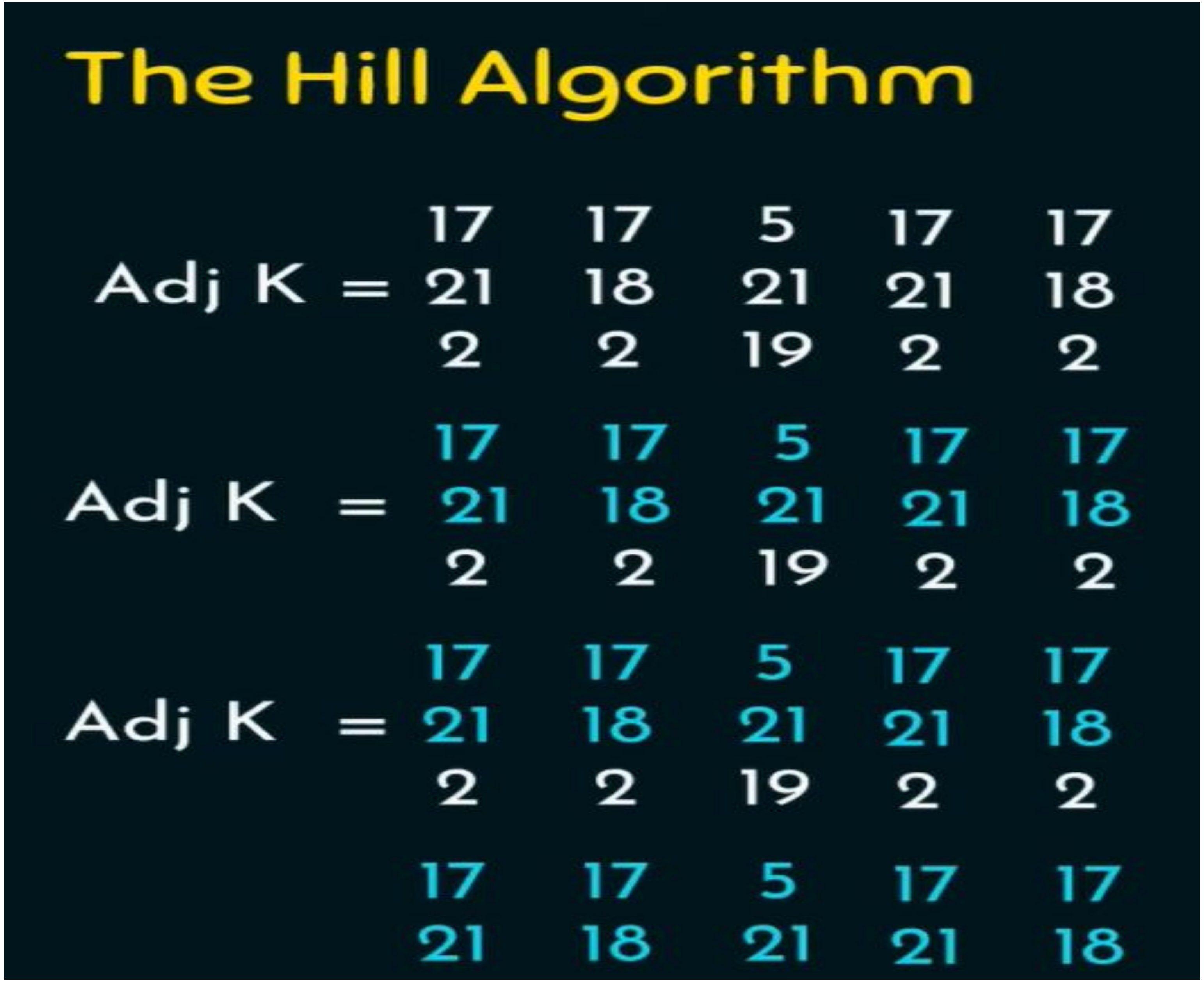
To find Adjoint K

$$\text{Adj } K = \begin{vmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{vmatrix}$$



$$\text{Adj } K = \begin{vmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{vmatrix}$$

$$\text{Adj } K = \begin{matrix} 17 & 17 & 5 & 17 & 17 \\ 21 & 18 & 21 & 21 & 18 \\ 2 & 2 & 19 & 2 & 2 \end{matrix}$$



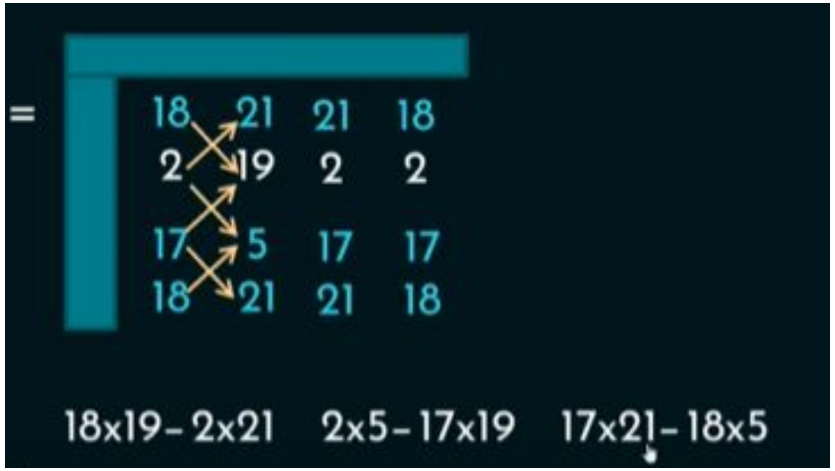
The Hill Algorithm

$$\text{Adj } K = \begin{matrix} 17 & 17 & 5 & 17 & 17 \\ 21 & 18 & 21 & 21 & 18 \\ 2 & 2 & 19 & 2 & 2 \end{matrix}$$

$$\text{Adj } K = \begin{matrix} 17 & 17 & 5 & 17 & 17 \\ 21 & 18 & 21 & 21 & 18 \\ 2 & 2 & 19 & 2 & 2 \end{matrix}$$

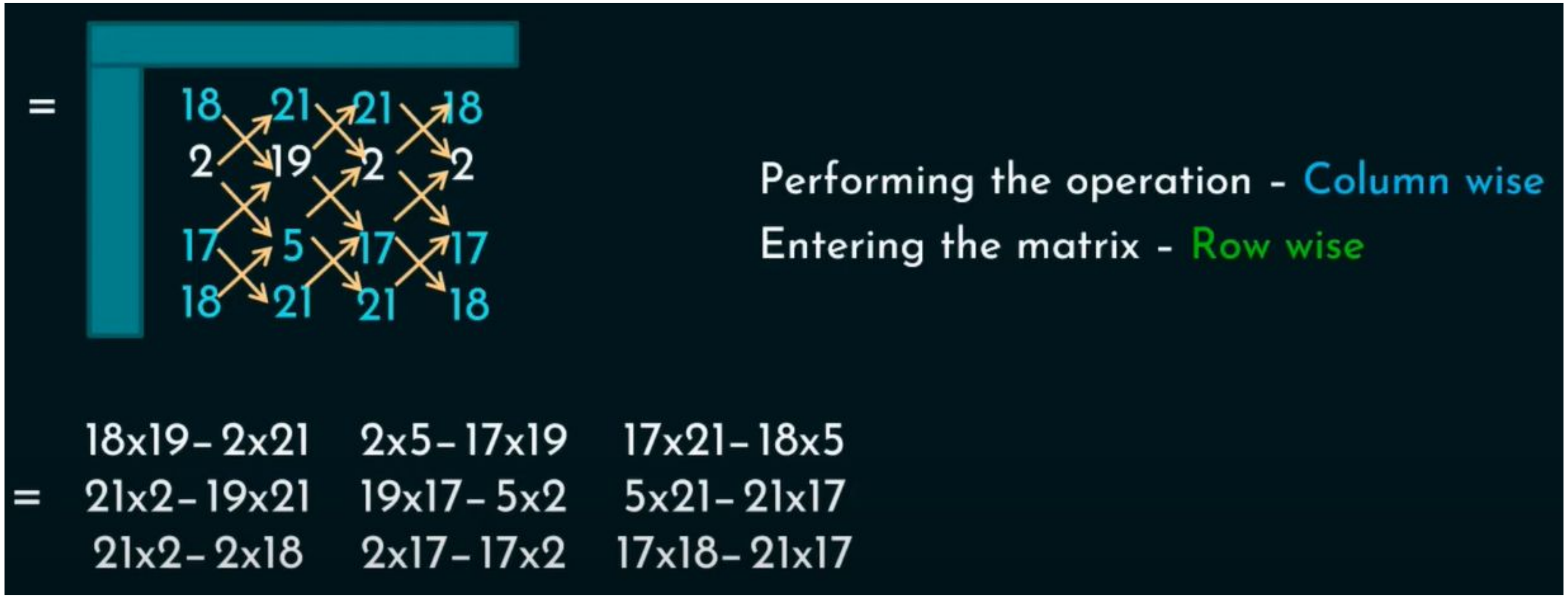
$$\text{Adj } K = \begin{matrix} 17 & 17 & 5 & 17 & 17 \\ 21 & 18 & 21 & 21 & 18 \\ 2 & 2 & 19 & 2 & 2 \end{matrix}$$

$$\begin{matrix} 17 & 17 & 5 & 17 & 17 \\ 21 & 18 & 21 & 21 & 18 \end{matrix}$$



$$= \begin{matrix} 18 & 21 & 21 & 18 \\ 2 & 19 & 2 & 2 \\ 17 & 5 & 17 & 17 \\ 18 & 21 & 21 & 18 \end{matrix}$$

$18 \times 19 - 2 \times 21 \quad 2 \times 5 - 17 \times 19 \quad 17 \times 21 - 18 \times 5$

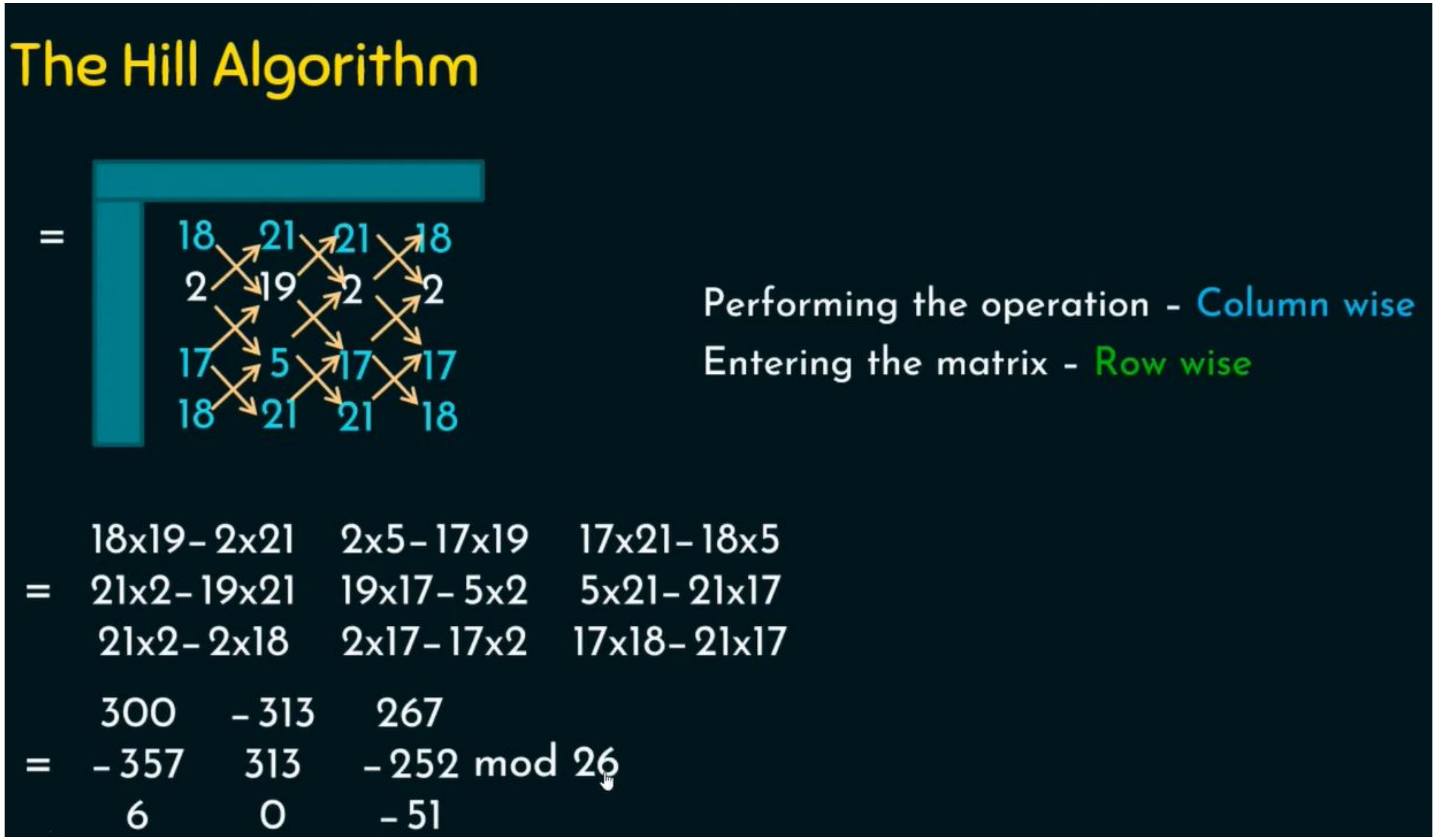


$$= \begin{matrix} 18 & 21 & 21 & 18 \\ 2 & 19 & 2 & 2 \\ 17 & 5 & 17 & 17 \\ 18 & 21 & 21 & 18 \end{matrix}$$

Performing the operation - Column wise

Entering the matrix - Row wise

$$= \begin{matrix} 18 \times 19 - 2 \times 21 & 2 \times 5 - 17 \times 19 & 17 \times 21 - 18 \times 5 \\ 21 \times 2 - 19 \times 21 & 19 \times 17 - 5 \times 2 & 5 \times 21 - 21 \times 17 \\ 21 \times 2 - 2 \times 18 & 2 \times 17 - 17 \times 2 & 17 \times 18 - 21 \times 17 \end{matrix}$$



The Hill Algorithm

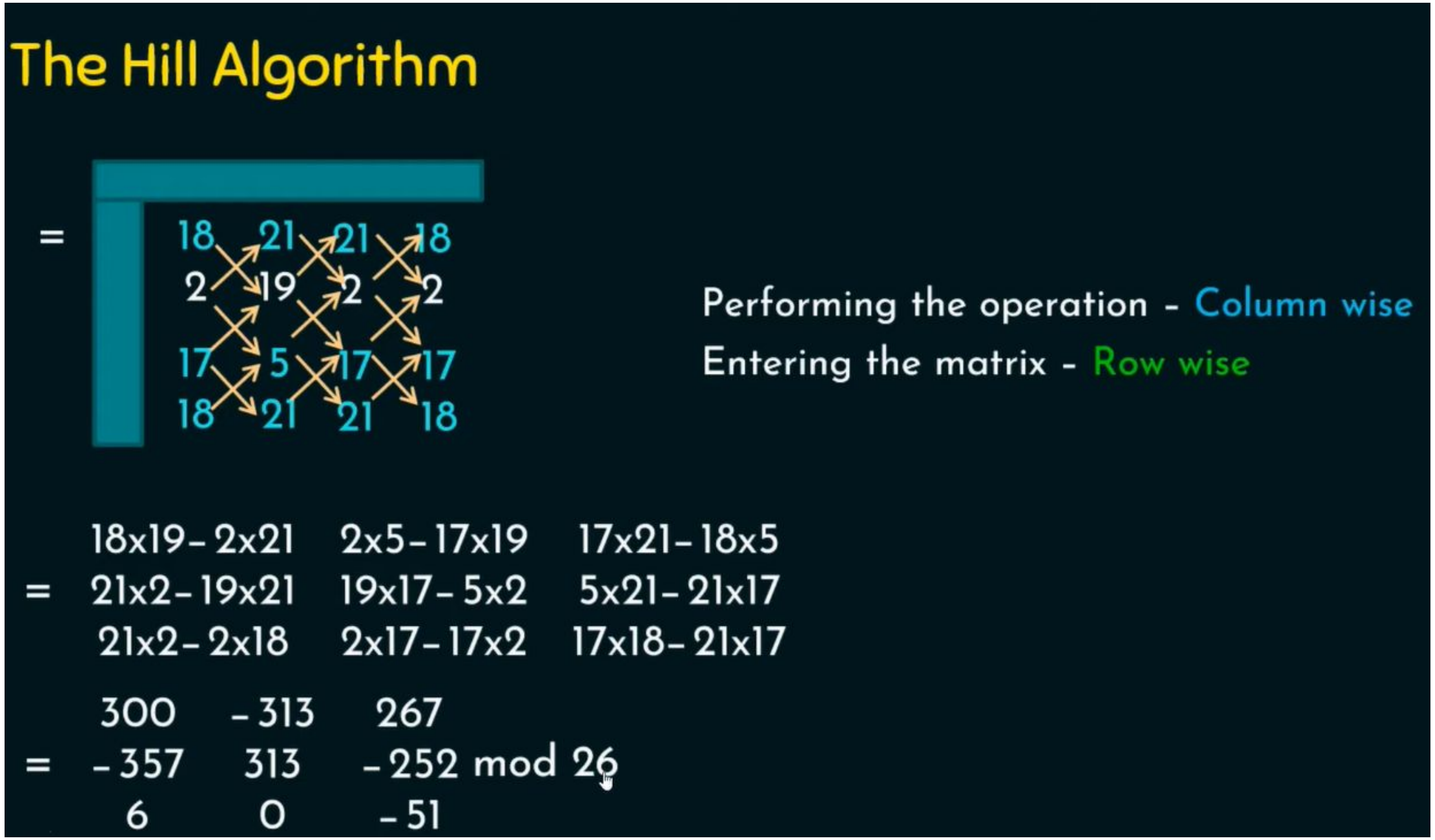
$$= \begin{array}{cccc} 18 & 21 & 21 & 18 \\ 2 & 19 & 2 & 2 \\ 17 & 5 & 17 & 17 \\ 18 & 21 & 21 & 18 \end{array}$$

Performing the operation - Column wise

Entering the matrix - Row wise

$$= \begin{array}{ccc} 18x19-2x21 & 2x5-17x19 & 17x21-18x5 \\ 21x2-19x21 & 19x17-5x2 & 5x21-21x17 \\ 21x2-2x18 & 2x17-17x2 & 17x18-21x17 \end{array}$$

$$= \begin{array}{ccc} 300 & -313 & 267 \\ -357 & 313 & -252 \\ 6 & 0 & -51 \end{array} \text{ mod } 26$$



The Hill Algorithm

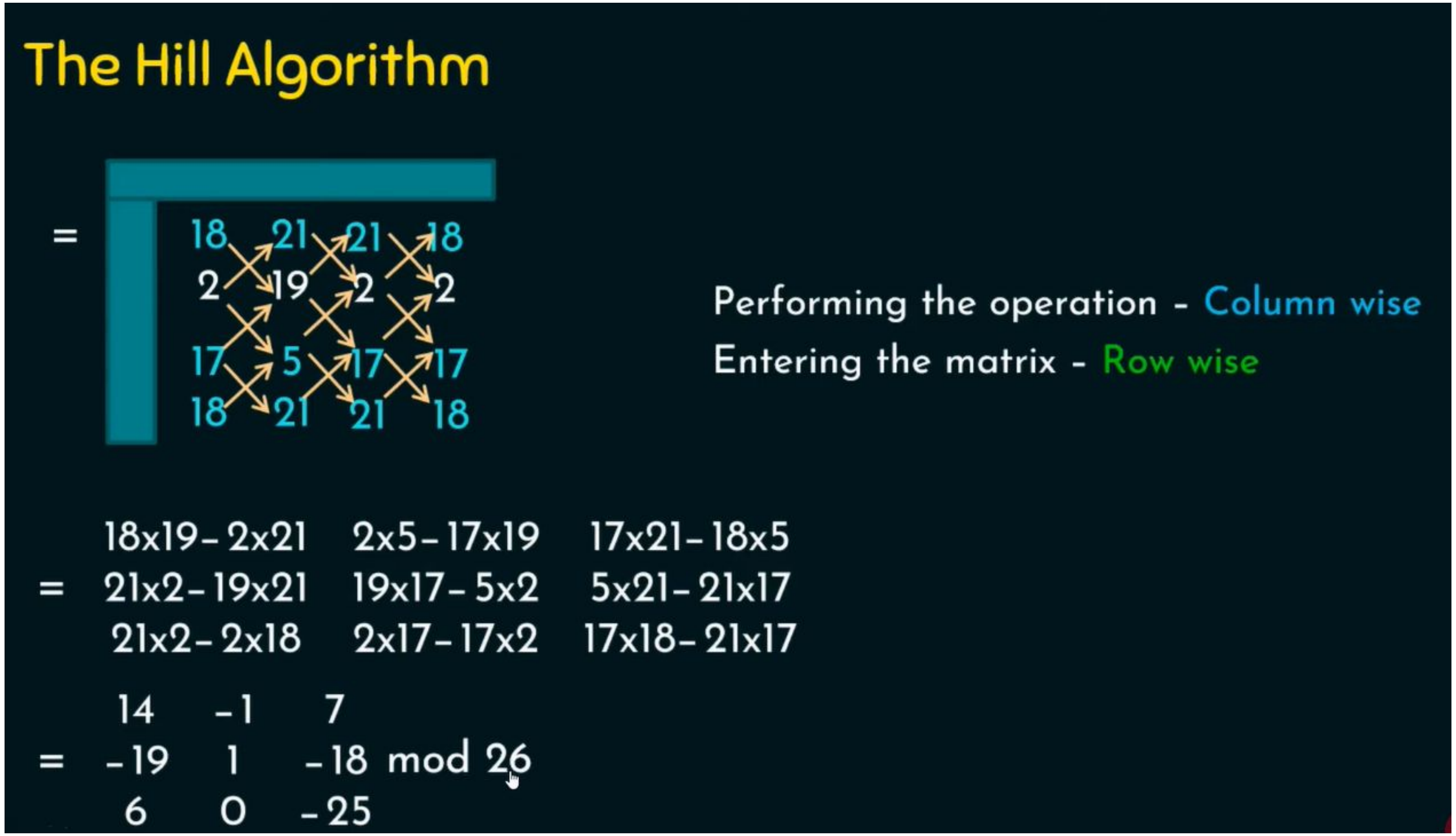
$$= \begin{array}{cccc} 18 & 21 & 21 & 18 \\ 2 & 19 & 2 & 2 \\ 17 & 5 & 17 & 17 \\ 18 & 21 & 21 & 18 \end{array}$$

Performing the operation - Column wise

Entering the matrix - Row wise

$$= \begin{array}{ccc} 18x19 - 2x21 & 2x5 - 17x19 & 17x21 - 18x5 \\ 21x2 - 19x21 & 19x17 - 5x2 & 5x21 - 21x17 \\ 21x2 - 2x18 & 2x17 - 17x2 & 17x18 - 21x17 \end{array}$$

$$= \begin{array}{ccc} 300 & -313 & 267 \\ -357 & 313 & -252 \\ 6 & 0 & -51 \end{array} \bmod 26$$



The Hill Algorithm

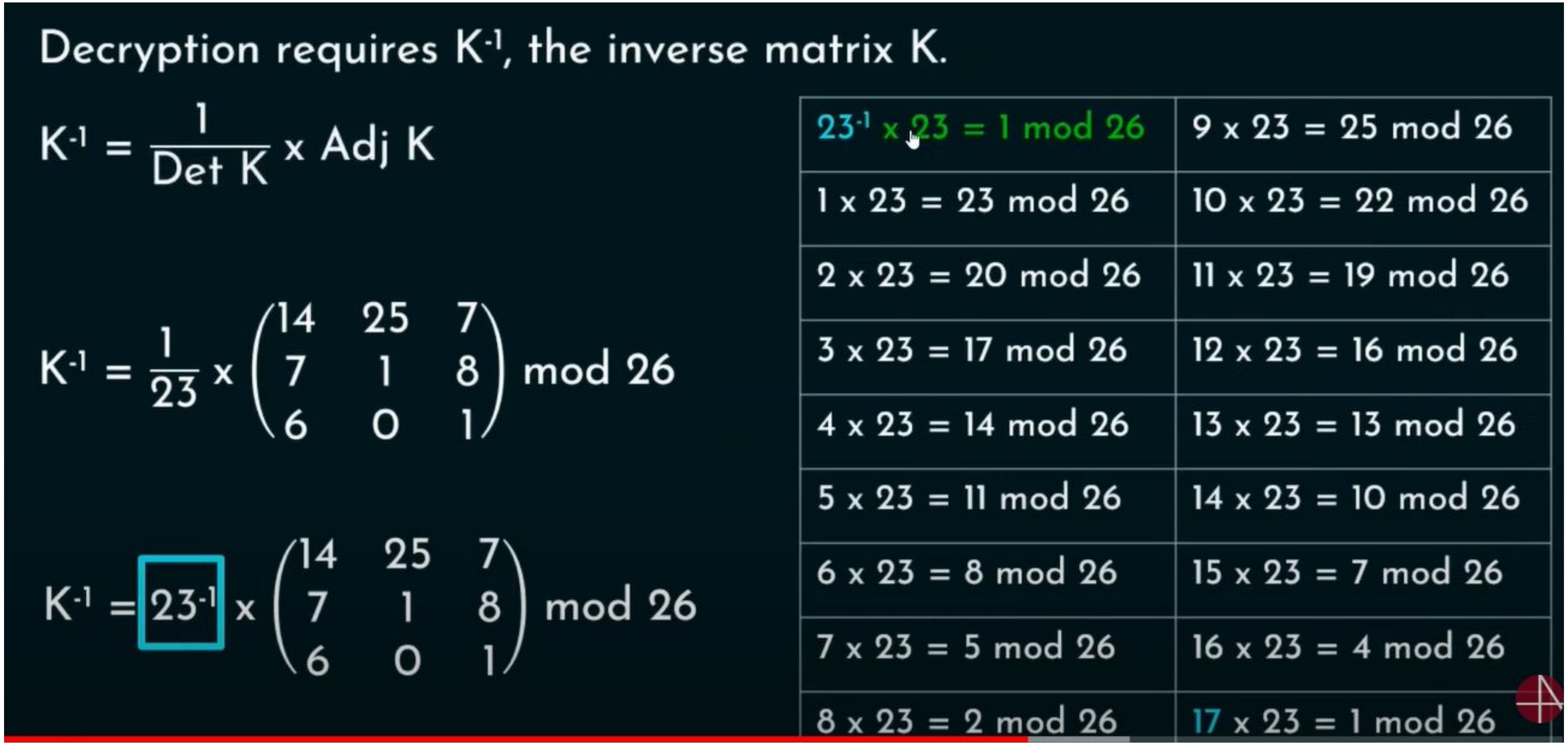
$$= \begin{array}{cccc} 18 & 21 & 21 & 18 \\ 2 & 19 & 2 & 2 \\ 17 & 5 & 17 & 17 \\ 18 & 21 & 21 & 18 \end{array}$$

Performing the operation - Column wise

Entering the matrix - Row wise

$$= \begin{array}{ccc} 18x19-2x21 & 2x5-17x19 & 17x21-18x5 \\ 21x2-19x21 & 19x17-5x2 & 5x21-21x17 \\ 21x2-2x18 & 2x17-17x2 & 17x18-21x17 \end{array}$$

$$= \begin{array}{ccc} 14 & -1 & 7 \\ -19 & 1 & -18 \\ 6 & 0 & -25 \end{array} \text{ mod } 26$$



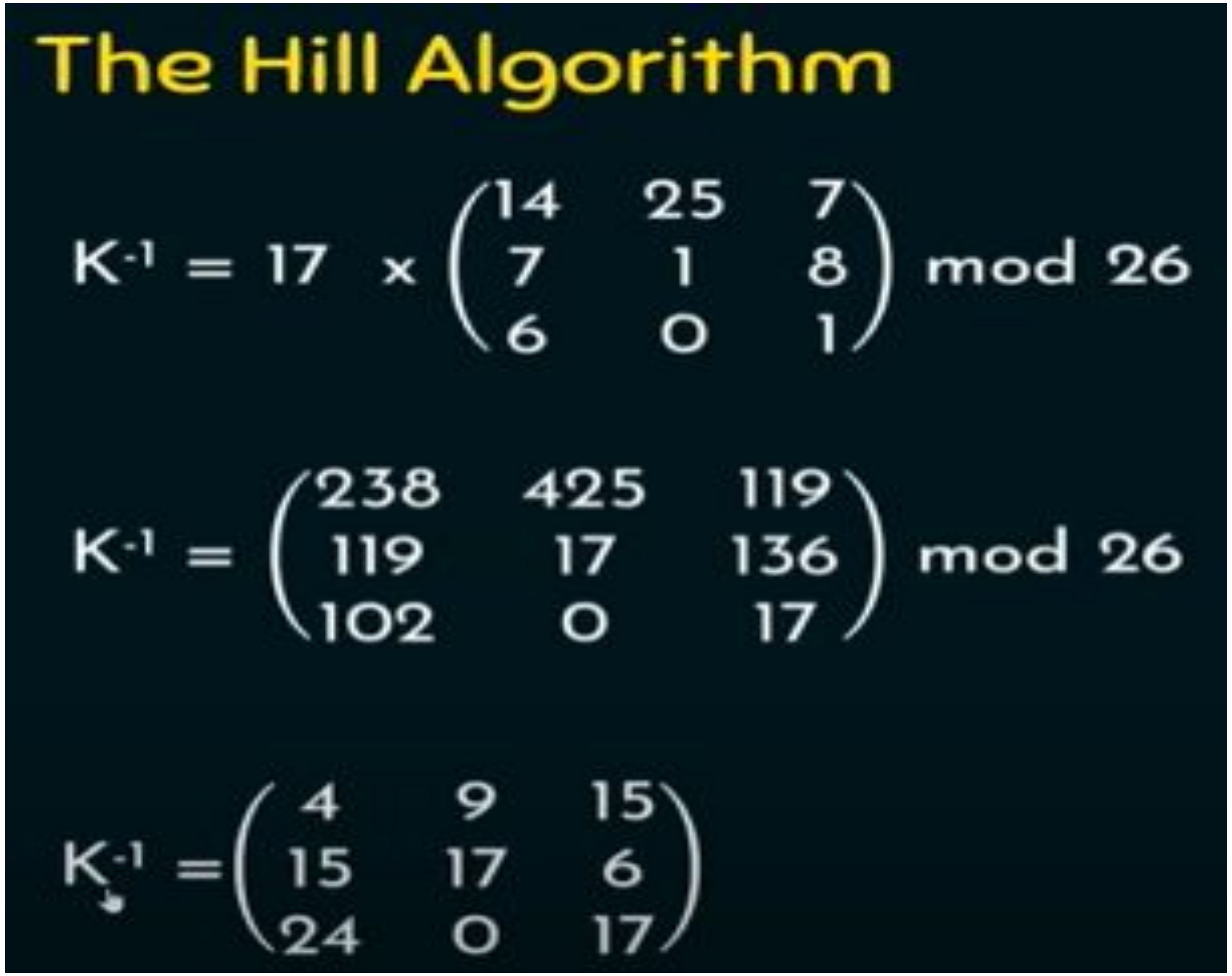
Decryption requires K⁻¹, the inverse matrix K.

$$K^{-1} = \frac{1}{\text{Det K}} \text{ x Adj K}$$

$$K^{-1} = \frac{1}{23} \text{ x } \begin{pmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{pmatrix} \text{ mod } 26$$

$$K^{-1} = \boxed{23^{-1}} \text{ x } \begin{pmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{pmatrix} \text{ mod } 26$$

23^{-1} x 23 = 1 mod 26	9 x 23 = 25 mod 26
1 x 23 = 23 mod 26	10 x 23 = 22 mod 26
2 x 23 = 20 mod 26	11 x 23 = 19 mod 26
3 x 23 = 17 mod 26	12 x 23 = 16 mod 26
4 x 23 = 14 mod 26	13 x 23 = 13 mod 26
5 x 23 = 11 mod 26	14 x 23 = 10 mod 26
6 x 23 = 8 mod 26	15 x 23 = 7 mod 26
7 x 23 = 5 mod 26	16 x 23 = 4 mod 26
8 x 23 = 2 mod 26	17 x 23 = 1 mod 26

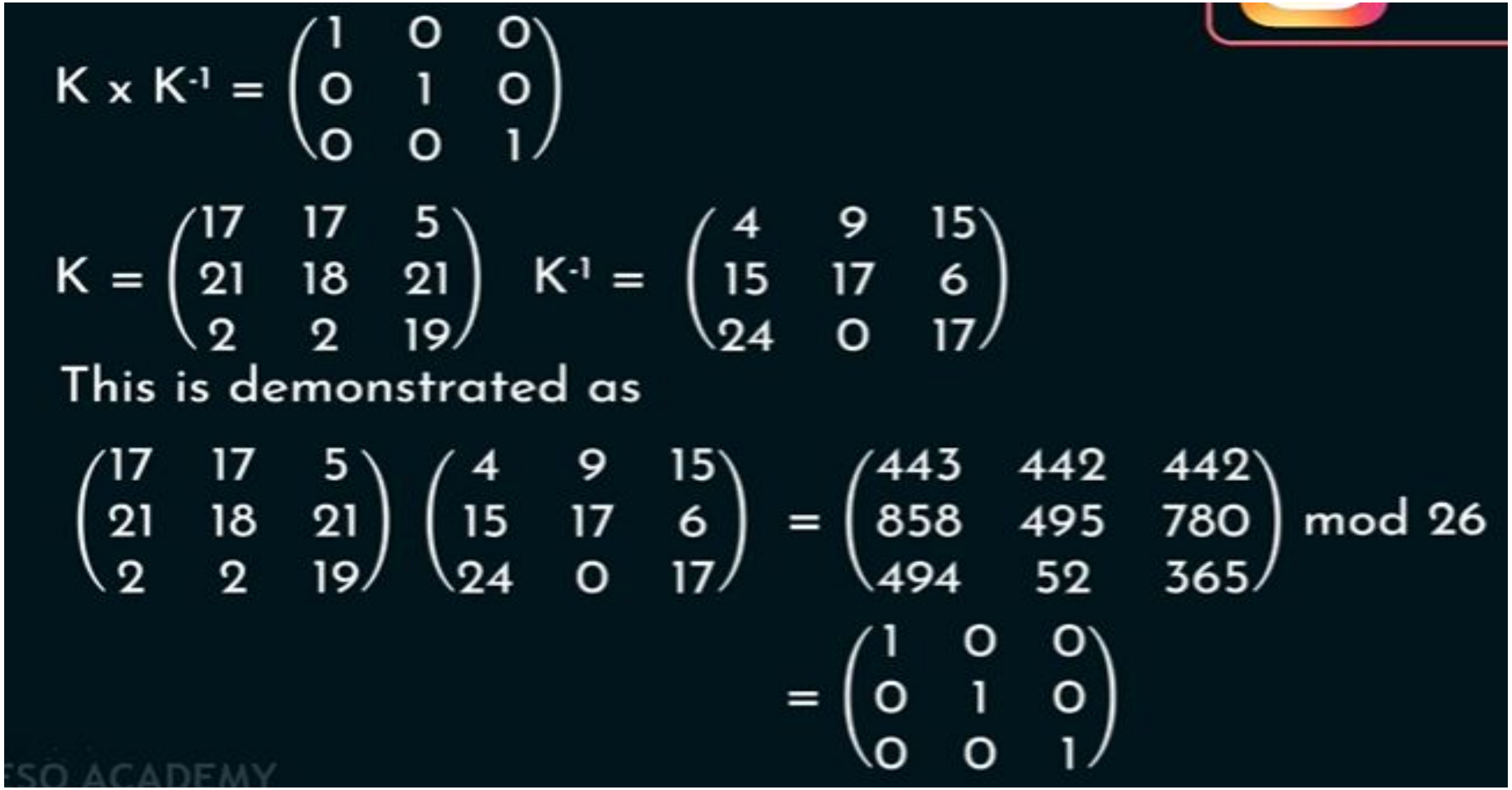


The Hill Algorithm

$$K^{-1} = 17 \times \begin{pmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{pmatrix} \bmod 26$$

$$K^{-1} = \begin{pmatrix} 238 & 425 & 119 \\ 119 & 17 & 136 \\ 102 & 0 & 17 \end{pmatrix} \bmod 26$$

$$K^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$



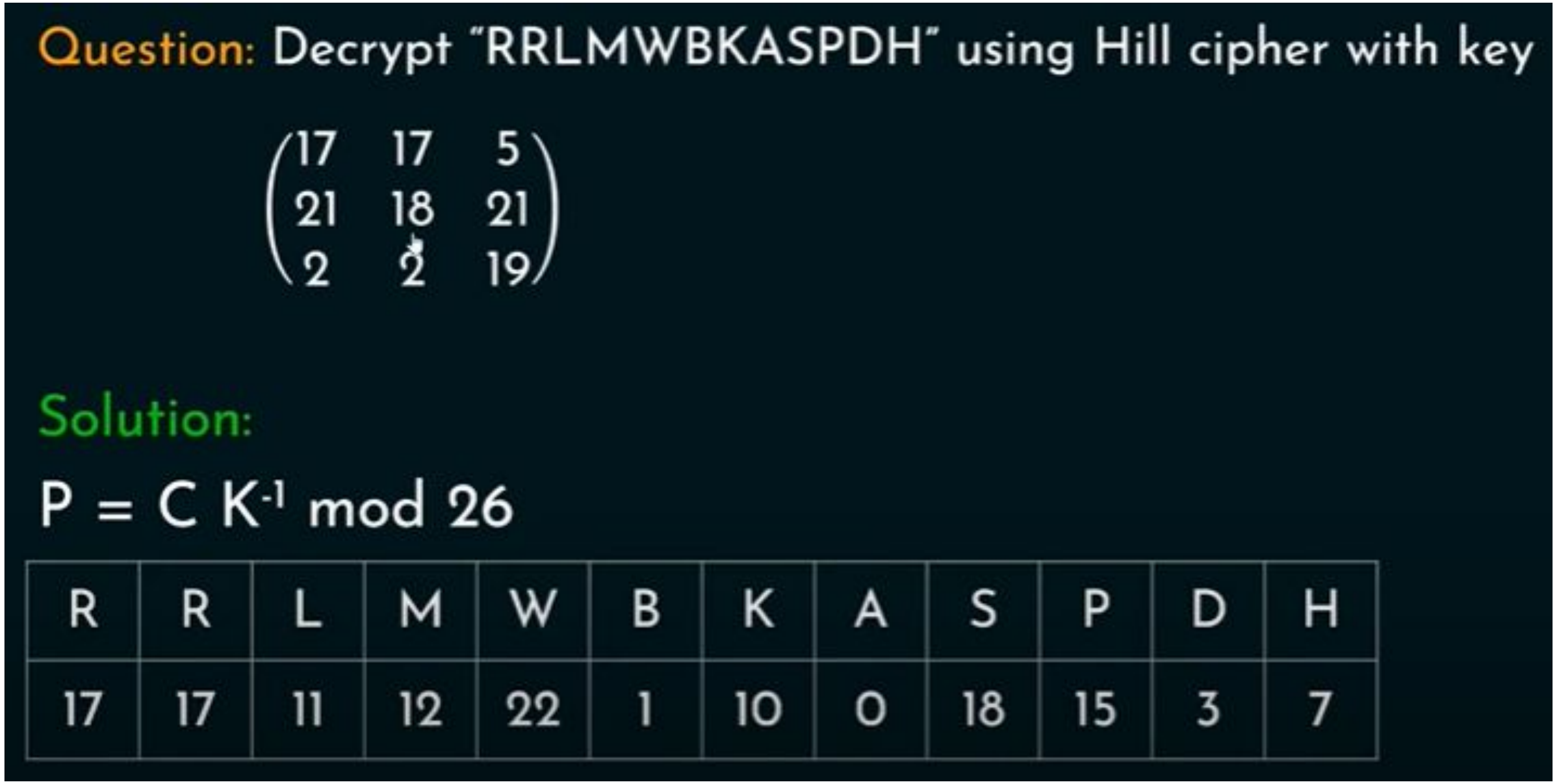
$$K \times K^{-1} = \begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}$$

$$K = \begin{pmatrix}17 & 17 & 5\\ 21 & 18 & 21\\ 2 & 2 & 19\end{pmatrix} \quad K^{-1} = \begin{pmatrix}4 & 9 & 15\\ 15 & 17 & 6\\ 24 & 0 & 17\end{pmatrix}$$

This is demonstrated as

$$\begin{pmatrix}17 & 17 & 5\\ 21 & 18 & 21\\ 2 & 2 & 19\end{pmatrix}\begin{pmatrix}4 & 9 & 15\\ 15 & 17 & 6\\ 24 & 0 & 17\end{pmatrix} = \begin{pmatrix}443 & 442 & 442\\ 858 & 495 & 780\\ 494 & 52 & 365\end{pmatrix} \bmod 26$$

$$= \begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}$$



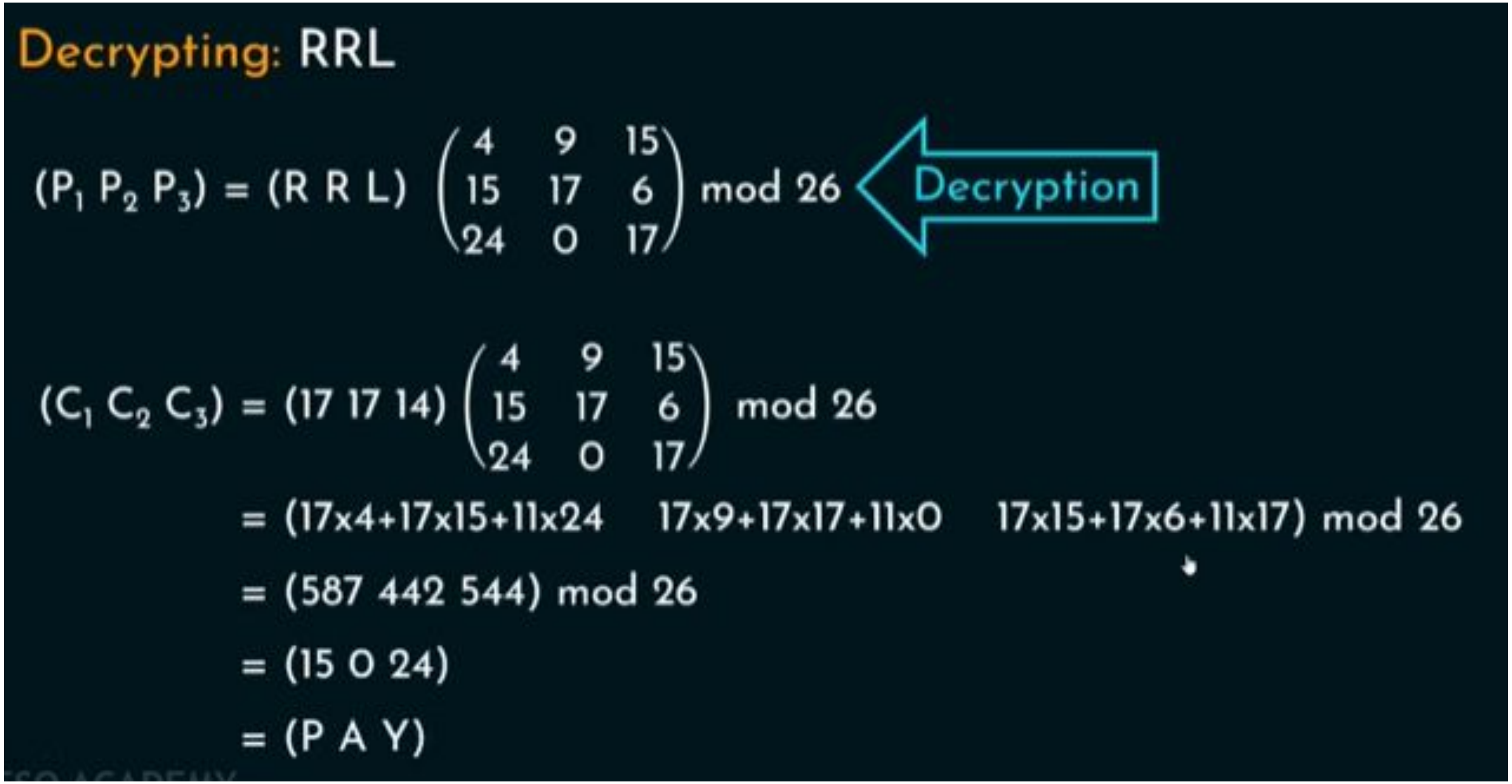
Question: Decrypt "RRLMWBKASPDH" using Hill cipher with key

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

Solution:

$P = C\,K^{-1} \bmod 26$

R	R	L	M	W	B	K	A	S	P	D	H
17	17	11	12	22	1	10	0	18	15	3	7



Decrypting: RRL

$$(P_1\ P_2\ P_3) = (R\ R\ L)\begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \bmod 26$$

Decryption

$$(C_1\ C_2\ C_3) = (17\ 17\ 14)\begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \bmod 26$$

$$= (17\text{x}4+17\text{x}15+11\text{x}24 \quad 17\text{x}9+17\text{x}17+11\text{x}0 \quad 17\text{x}15+17\text{x}6+11\text{x}17) \bmod 26$$

$$= (587\ 442\ 544) \bmod 26$$

$$= (15\ 0\ 24)$$

$$= (P\ A\ Y)$$