Cryptography

Lecture 4

Dr/ Hanan Hamed

Table of Contents

- Symmetric Encryption
- Substitution Techniques
- Caesar Cipher
- Monoalphabetic Cipher
- Playfair Cipher
- Hill Cipher

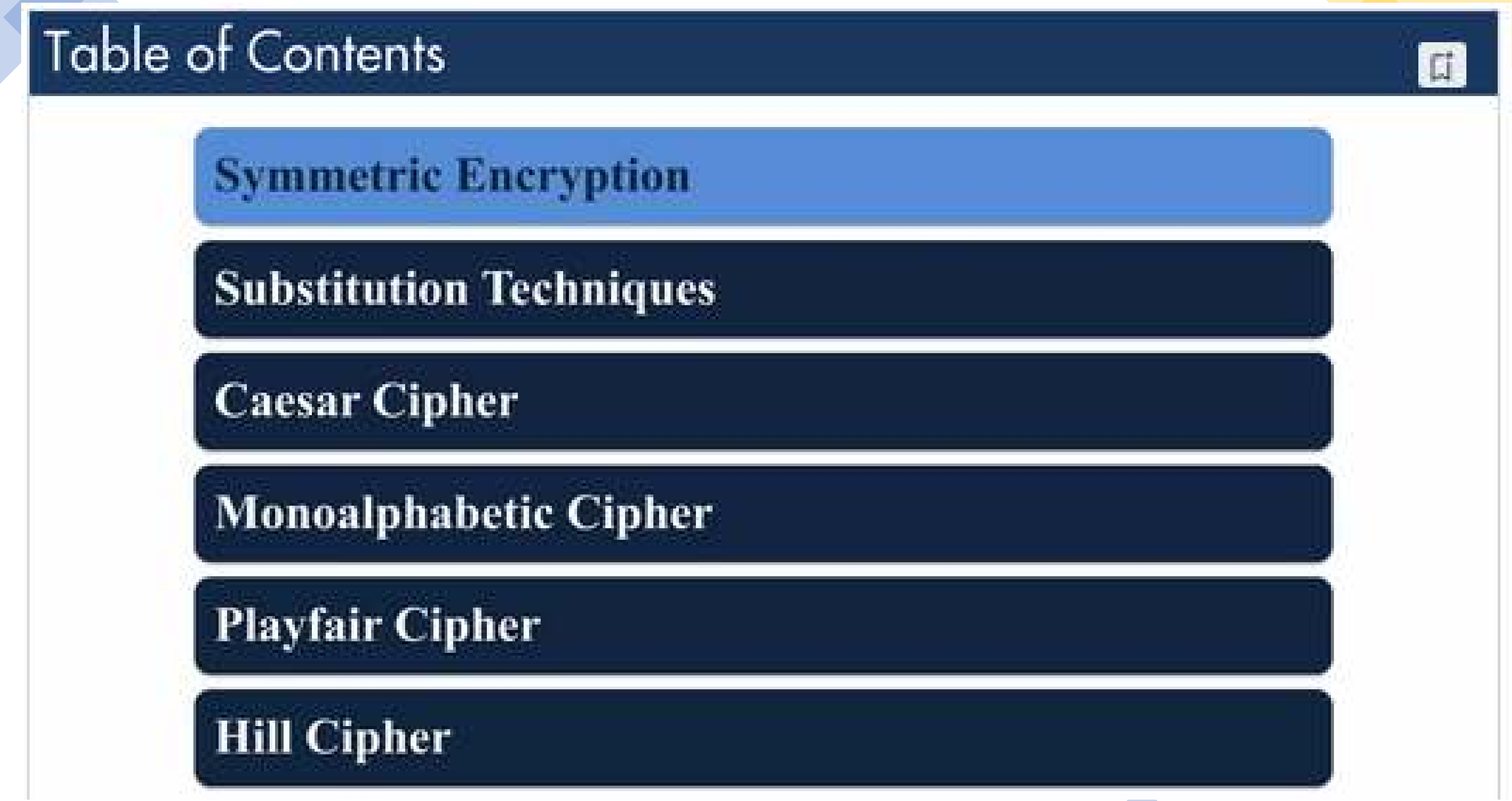
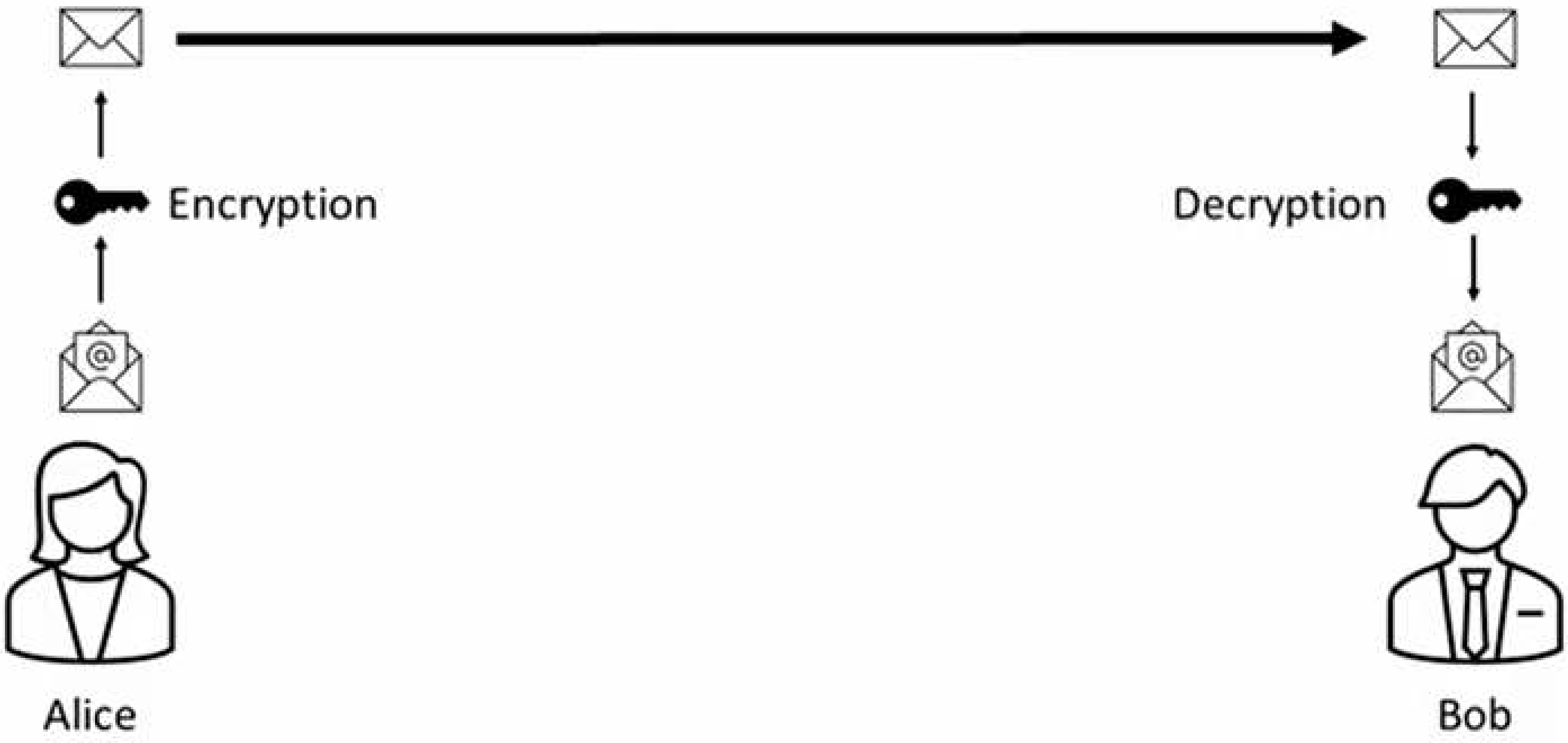


Table of Contents

Symmetric Encryption – Message Decryption



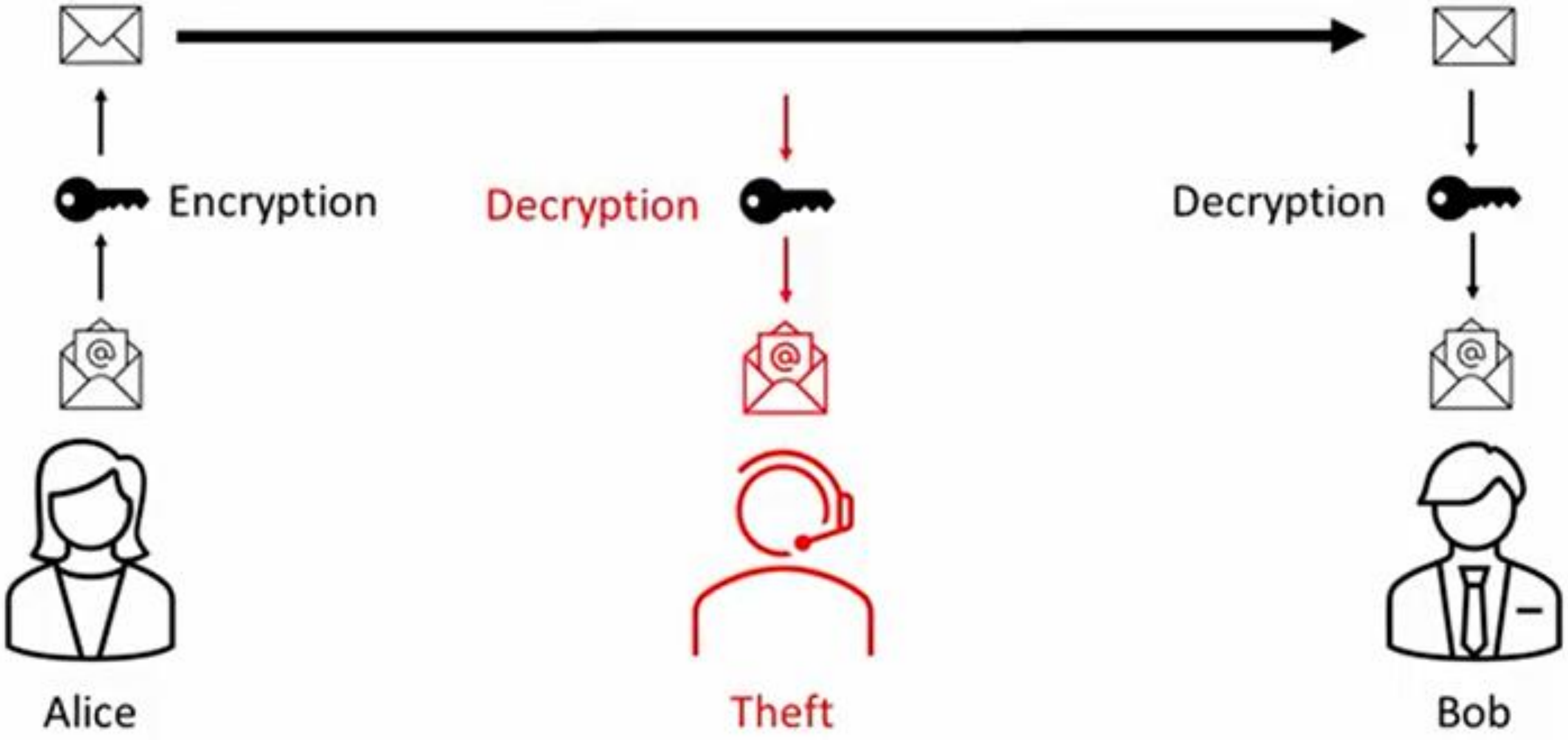
Encryption

Decryption

Alice

Bob

Symmetric Encryption - Key theft attack



Encryption

Decryption

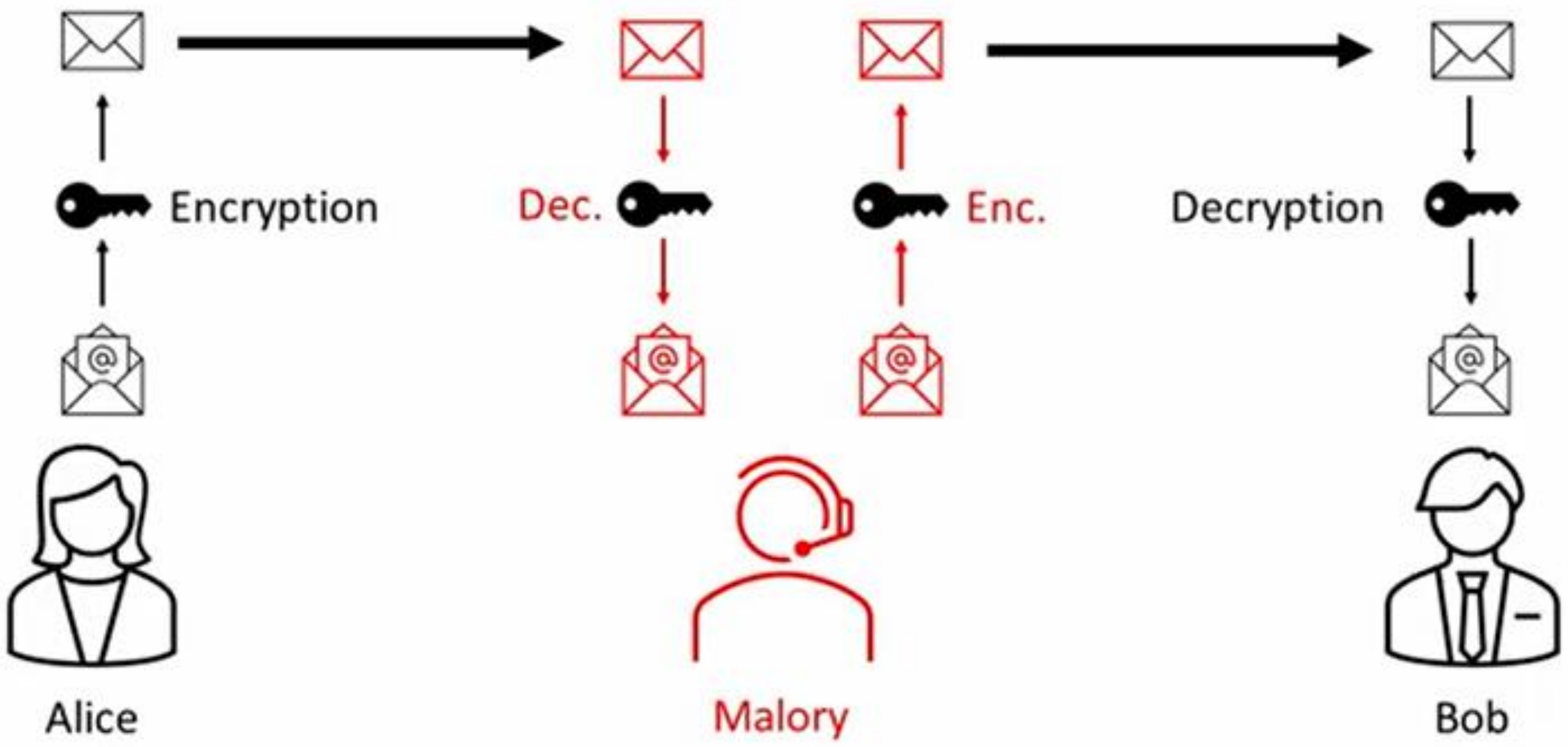
Decryption

Alice

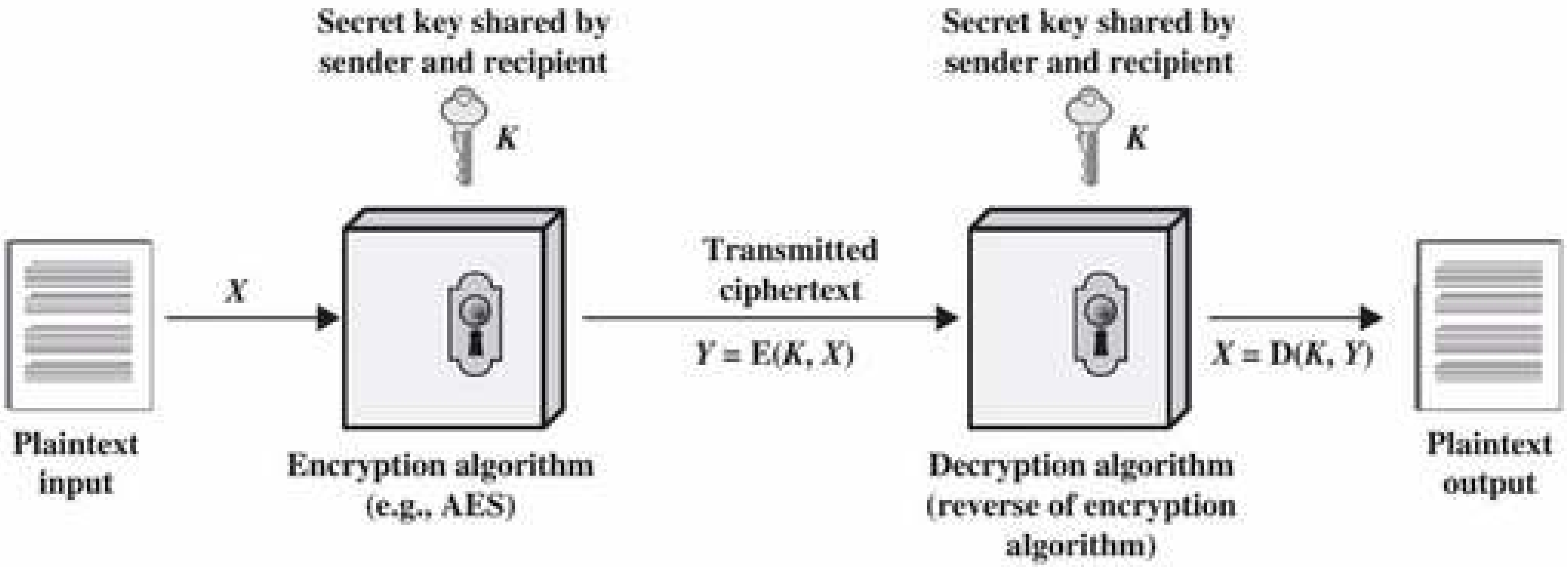
Theft

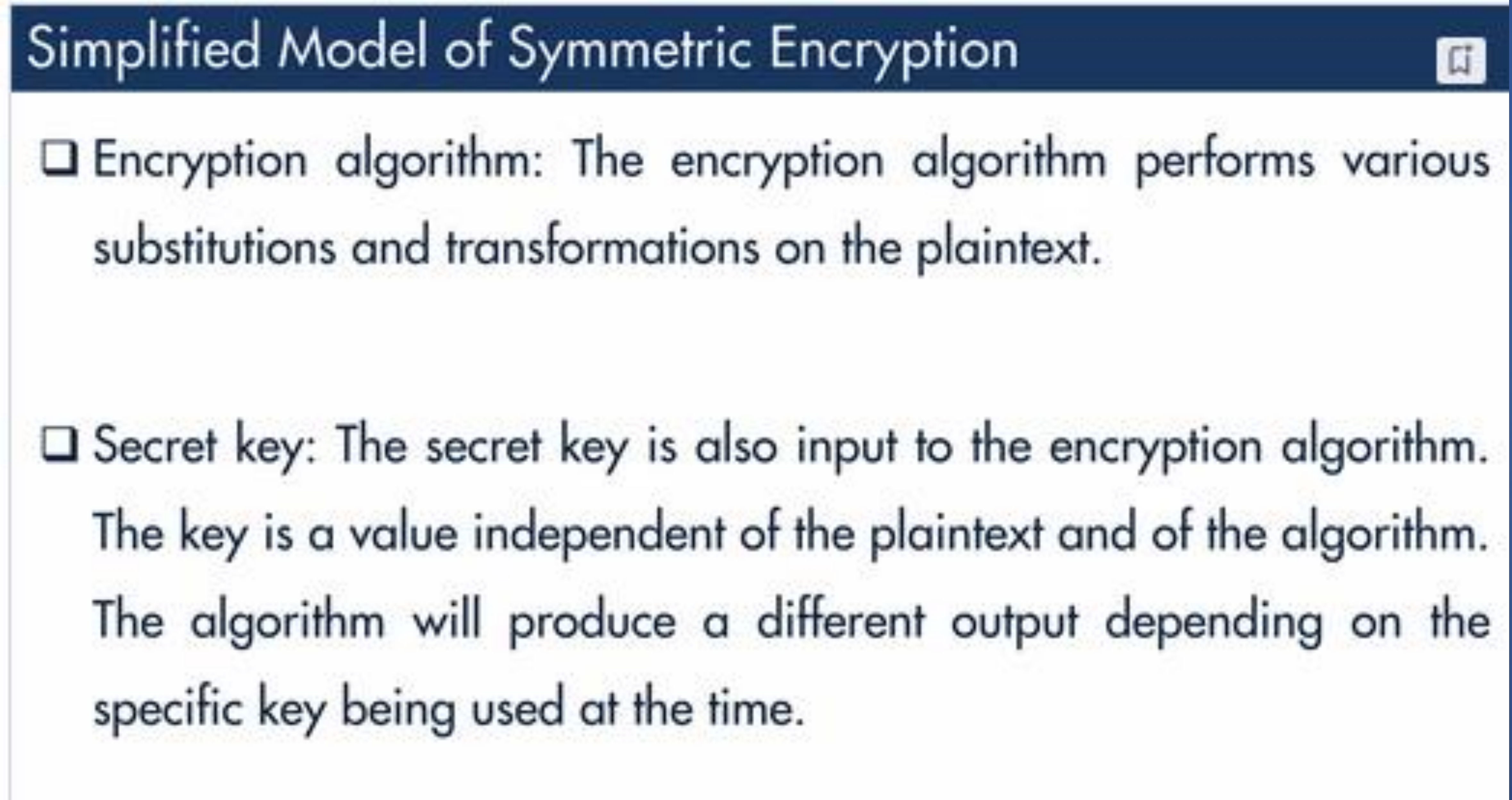
Bob

Symmetric Encryption - Man-in-the-Middle attack



Simplified Model of Symmetric Encryption

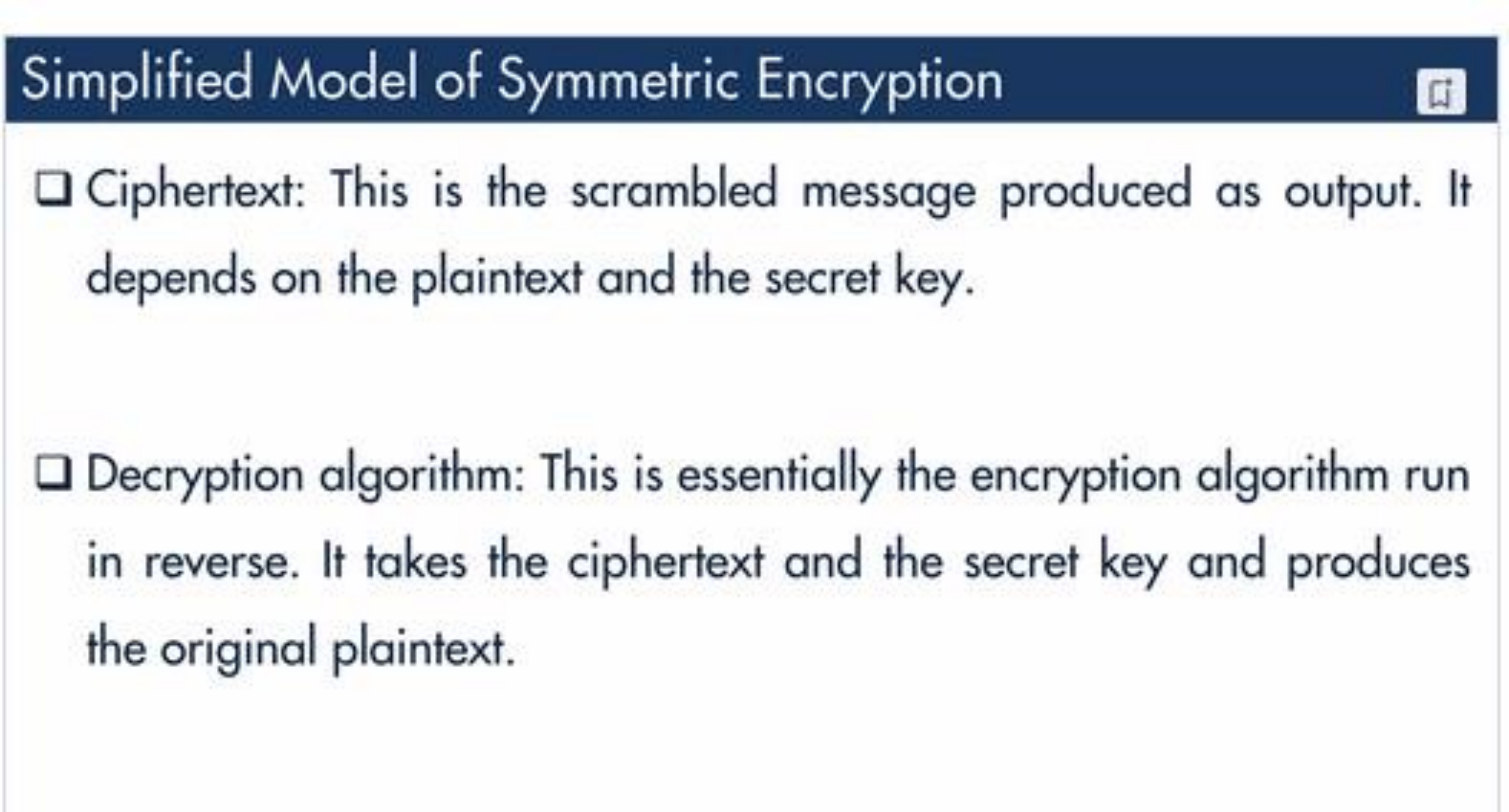

Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E(K, X)
X = D(K, Y)
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output



Simplified Model of Symmetric Encryption

❑ Encryption algorithm: The encryption algorithm performs various substitutions and transformations on the plaintext.

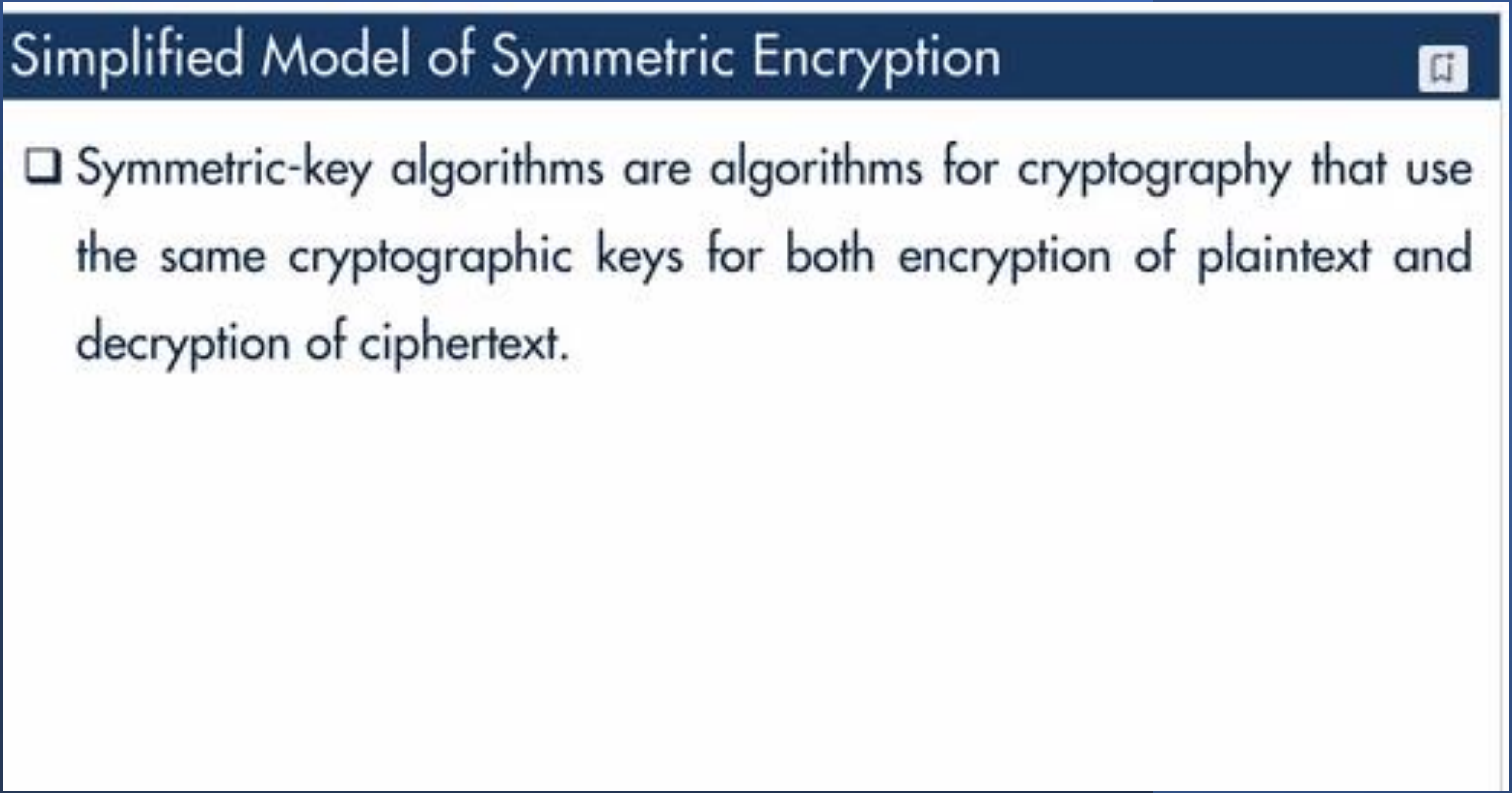
❑ Secret key: The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time.



Simplified Model of Symmetric Encryption

❑ Ciphertext: This is the scrambled message produced as output. It depends on the plaintext and the secret key.

❑ Decryption algorithm: This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.



Simplified Model of Symmetric Encryption

- Symmetric-key algorithms are algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext.

Asymmetric Encryption - Key Generation

Private Key

Public Key

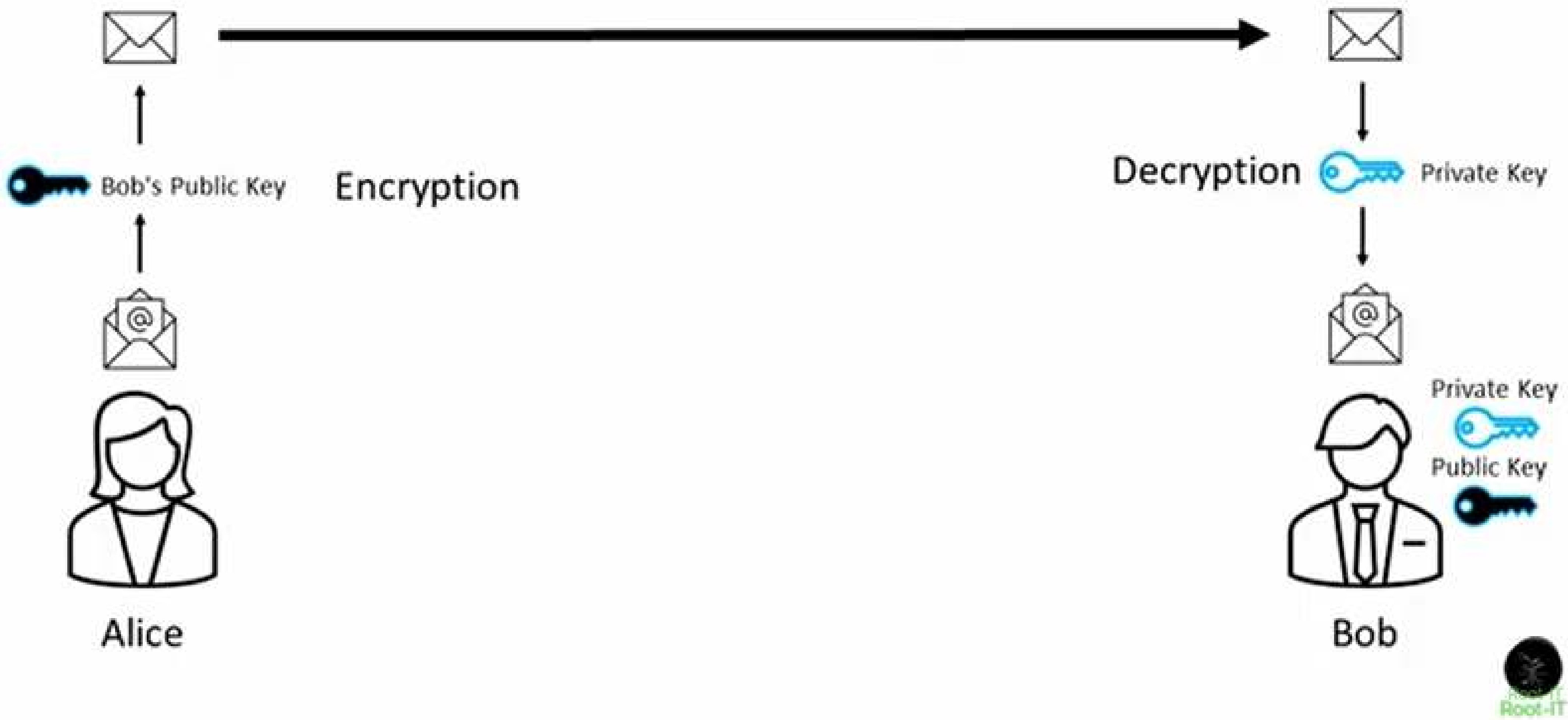
Alice

Private Key

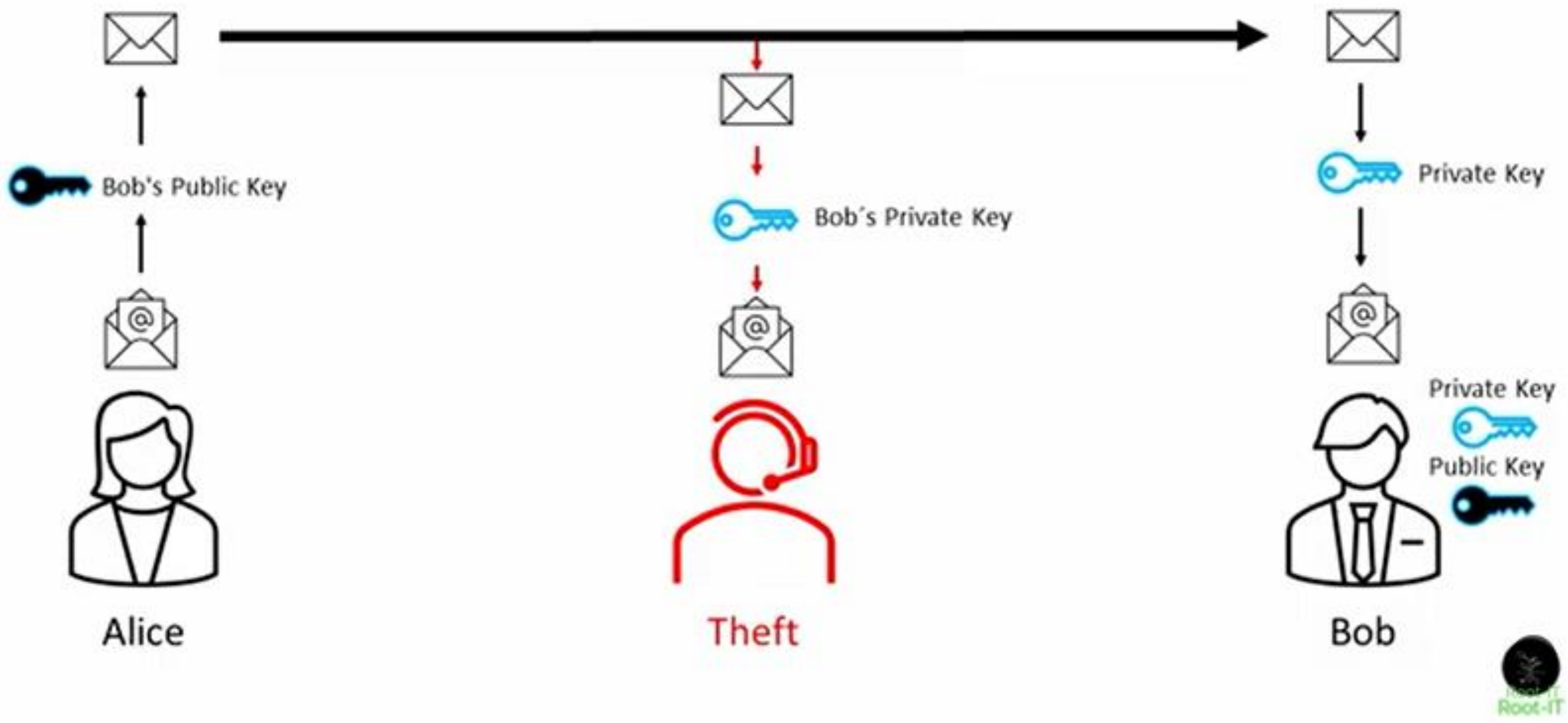
Public Key

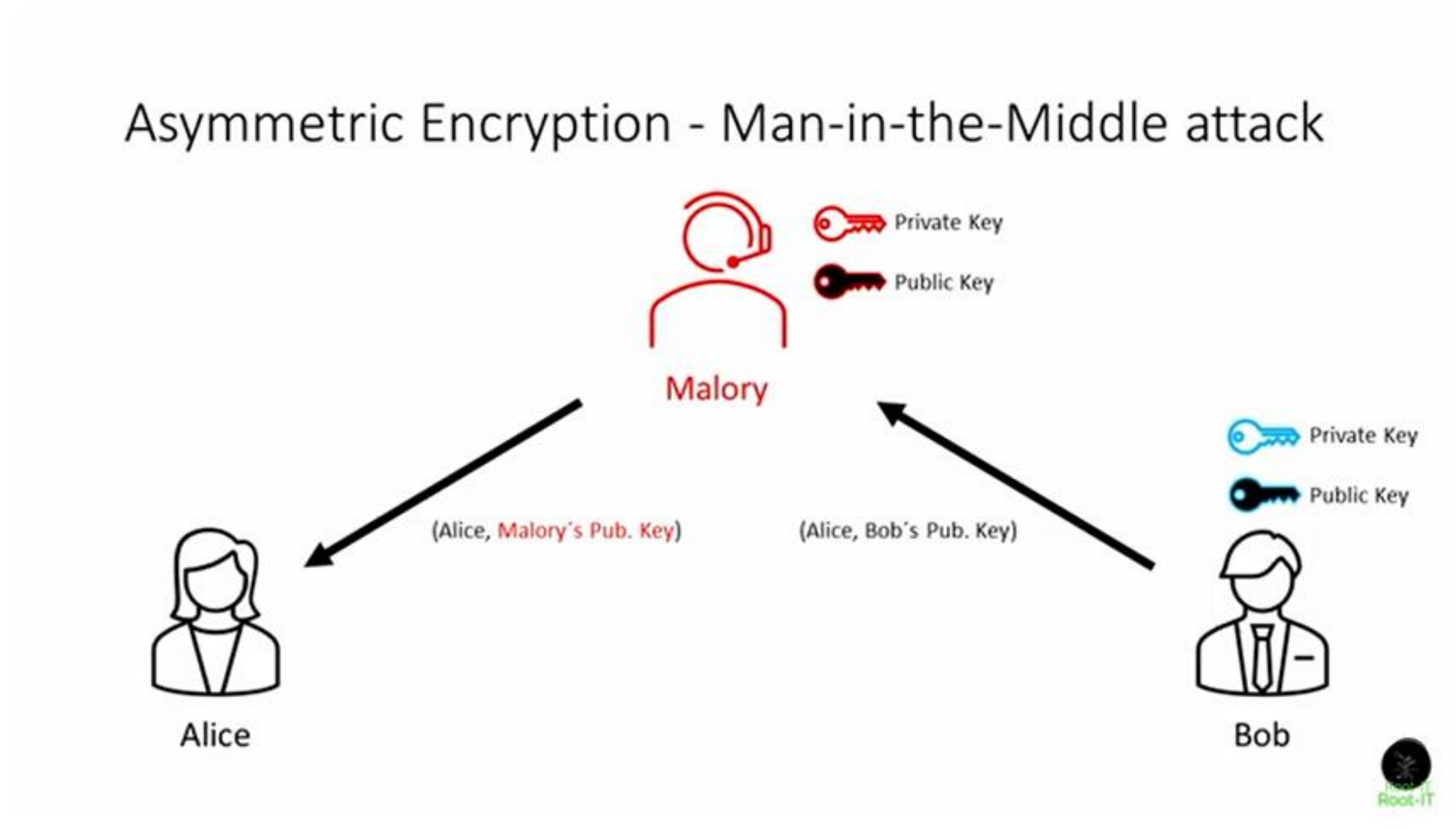
Bob

Asymmetric Encryption – Message Decryption

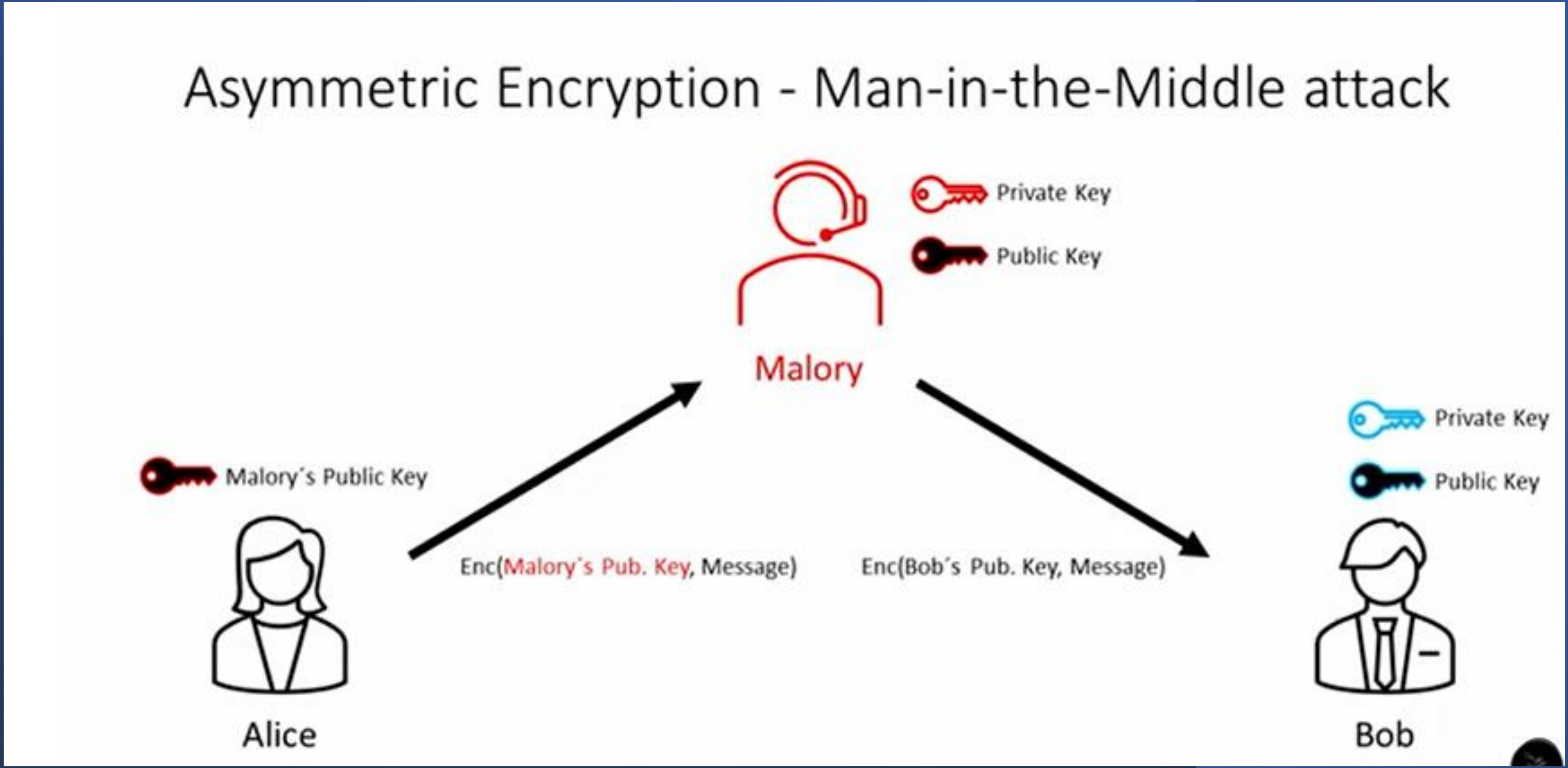


Asymmetric Encryption - Private Key theft attack





Asymmetric Encryption - Man-in-the-Middle attack



Asymmetric Encryption - Man-in-the-Middle attack

Malory

Private Key

Public Key

Malory´s Public Key

Alice

Enc(Malory´s Pub. Key, Message)

Enc(Bob´s Pub. Key, Message)

Private Key

Public Key

Bob

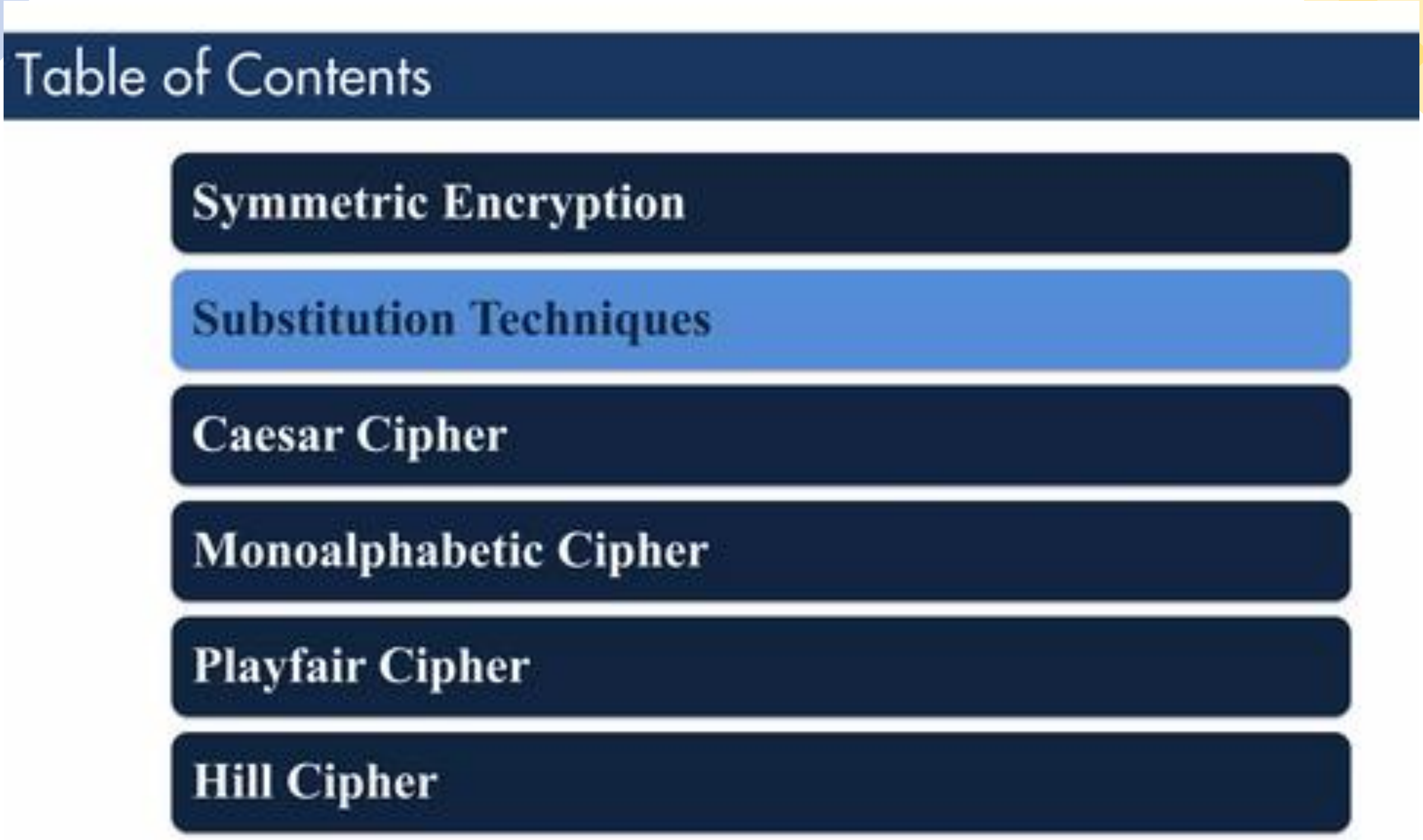


Table of Contents

Symmetric Encryption

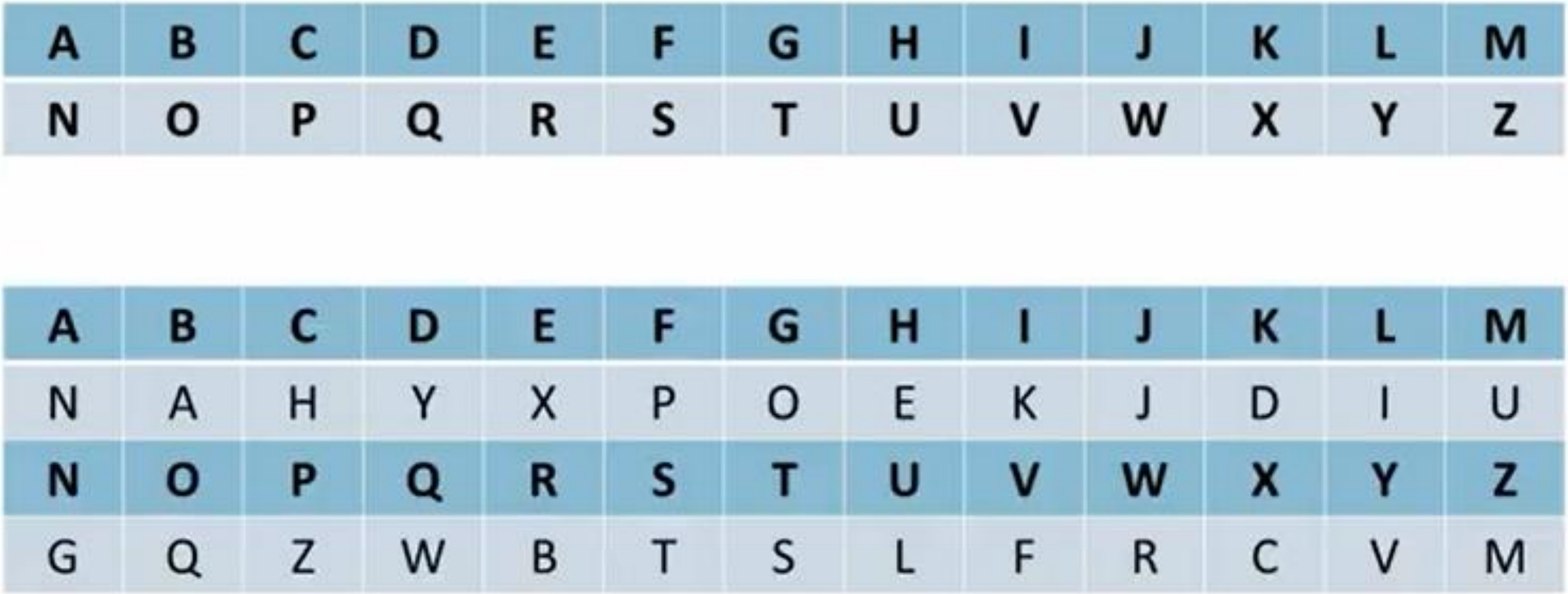
Substitution Techniques

Caesar Cipher

Monoalphabetic Cipher

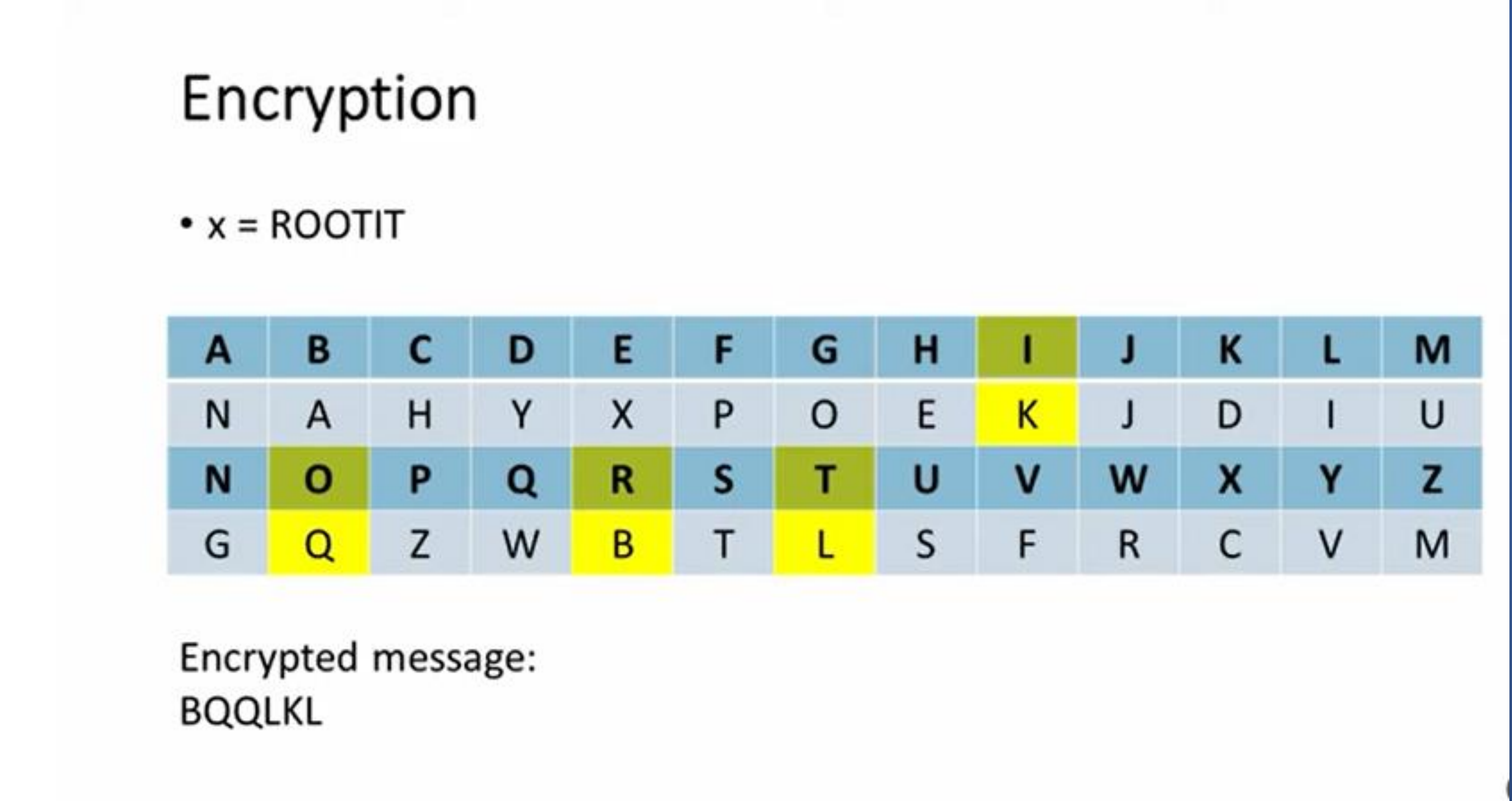
Playfair Cipher

Hill Cipher



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

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

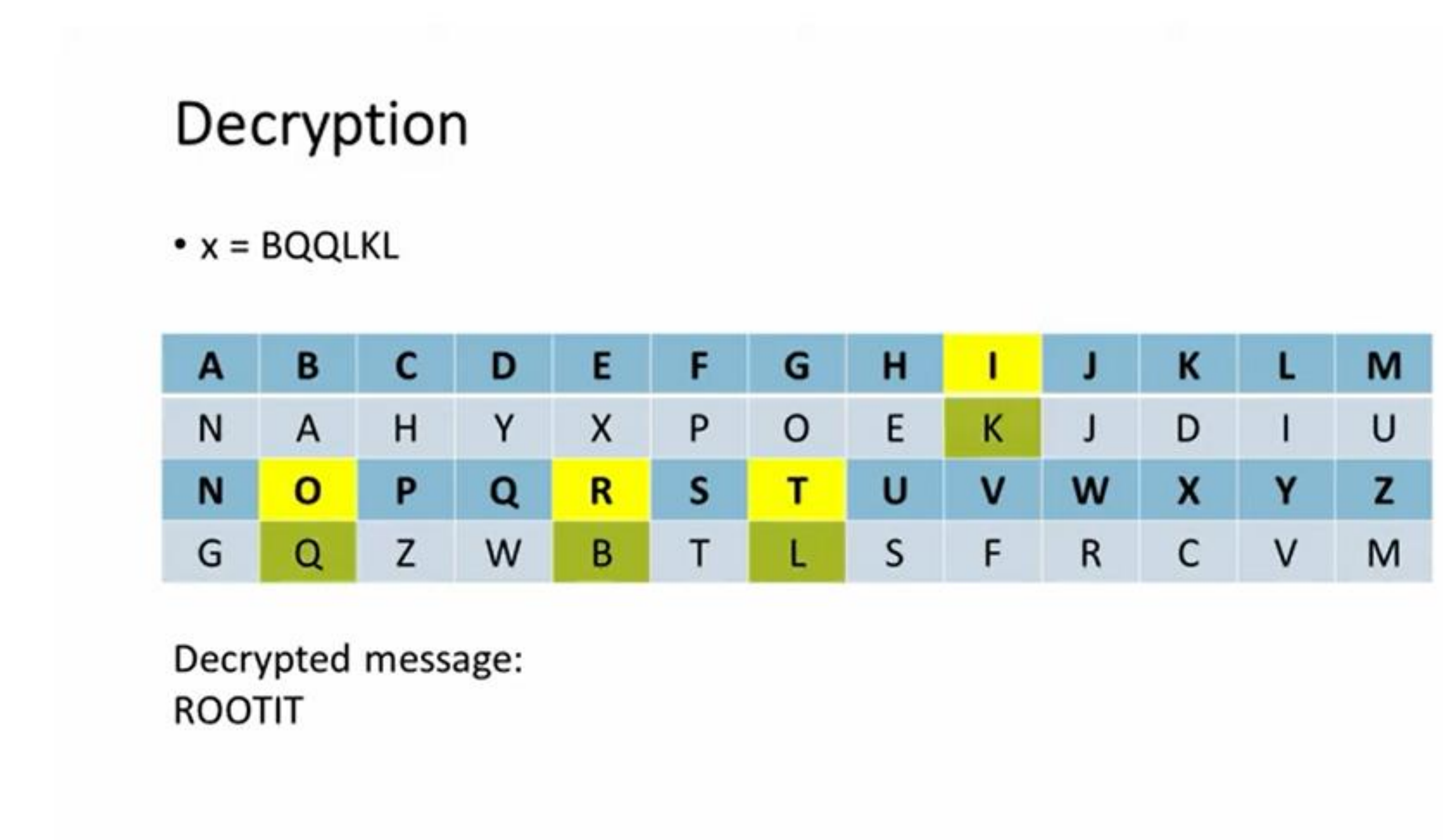


Encryption

- x = ROOTIT

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

Encrypted message:
BQQLKL

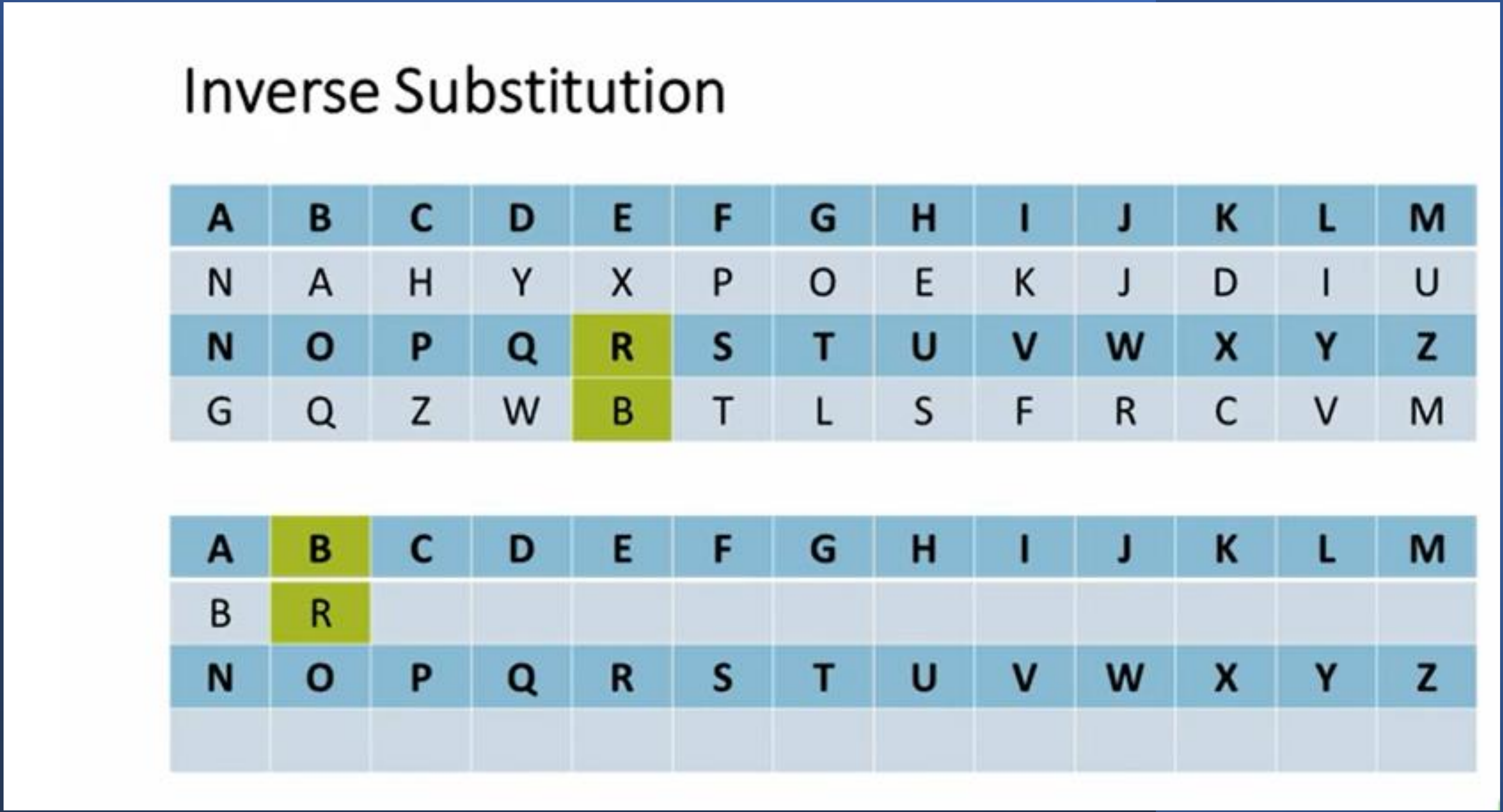


Decryption

- x = BQQLKL

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

Decrypted message:
ROOTIT



Inverse Substitution

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

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

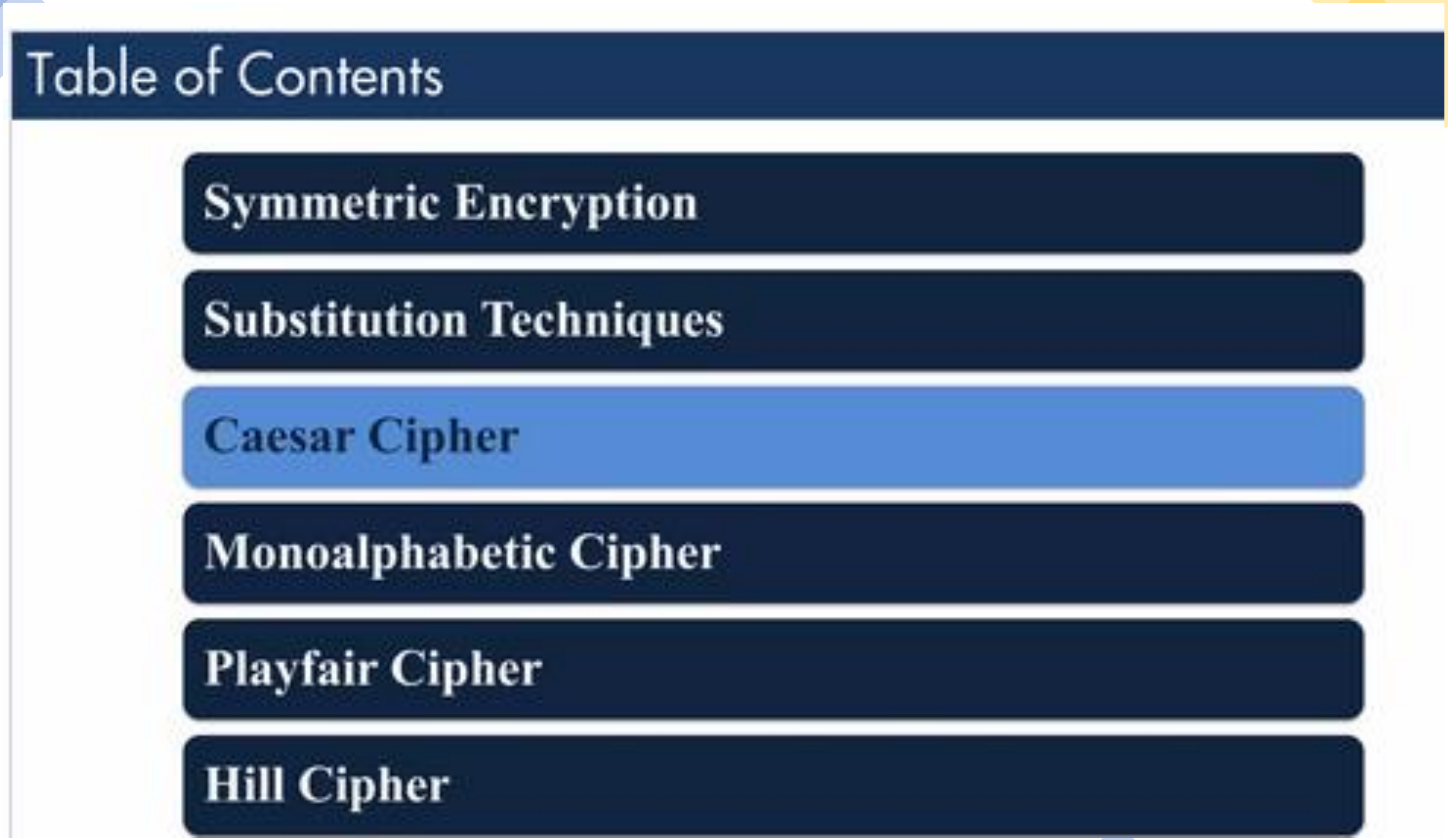
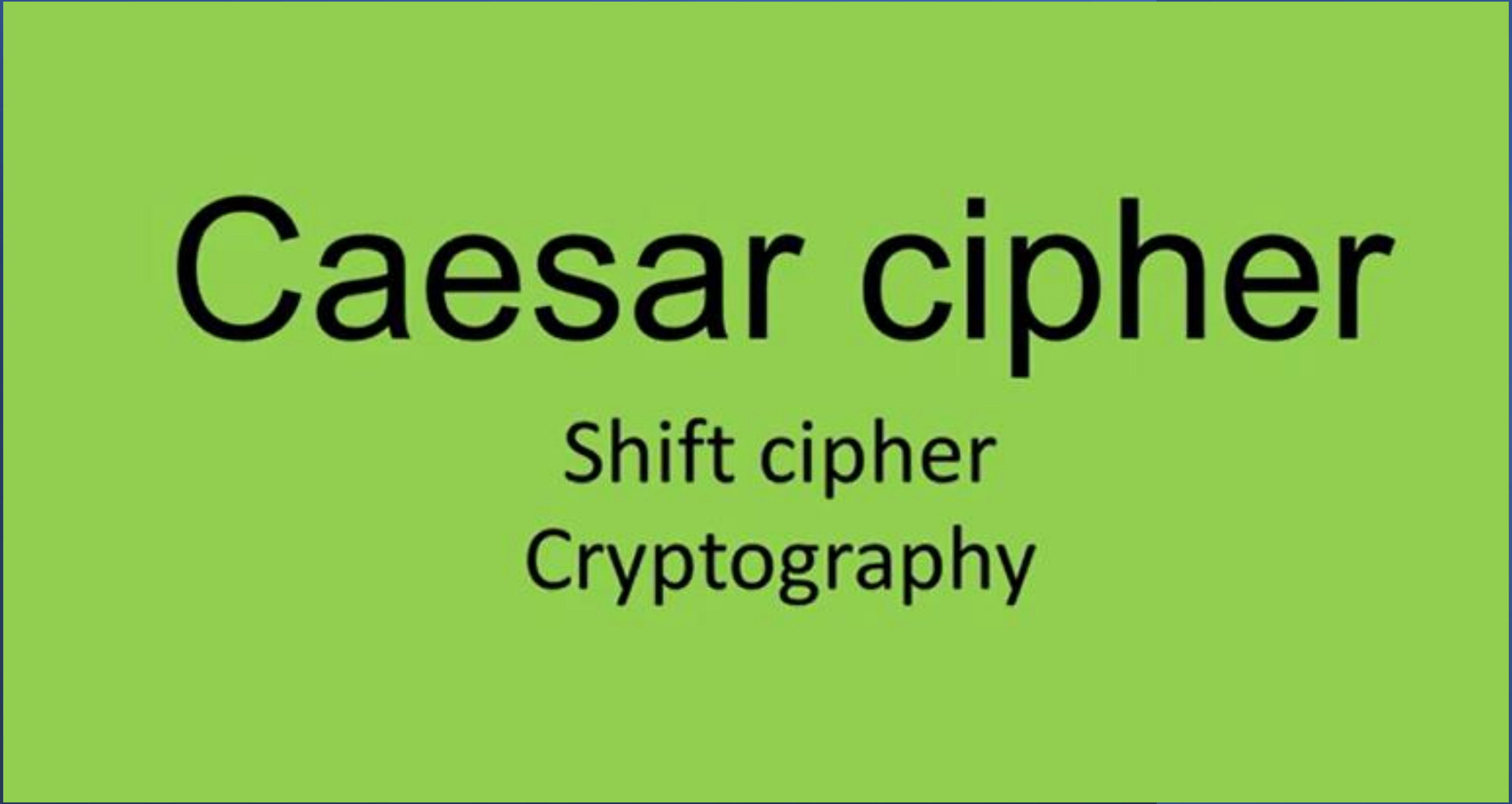


Table of Contents

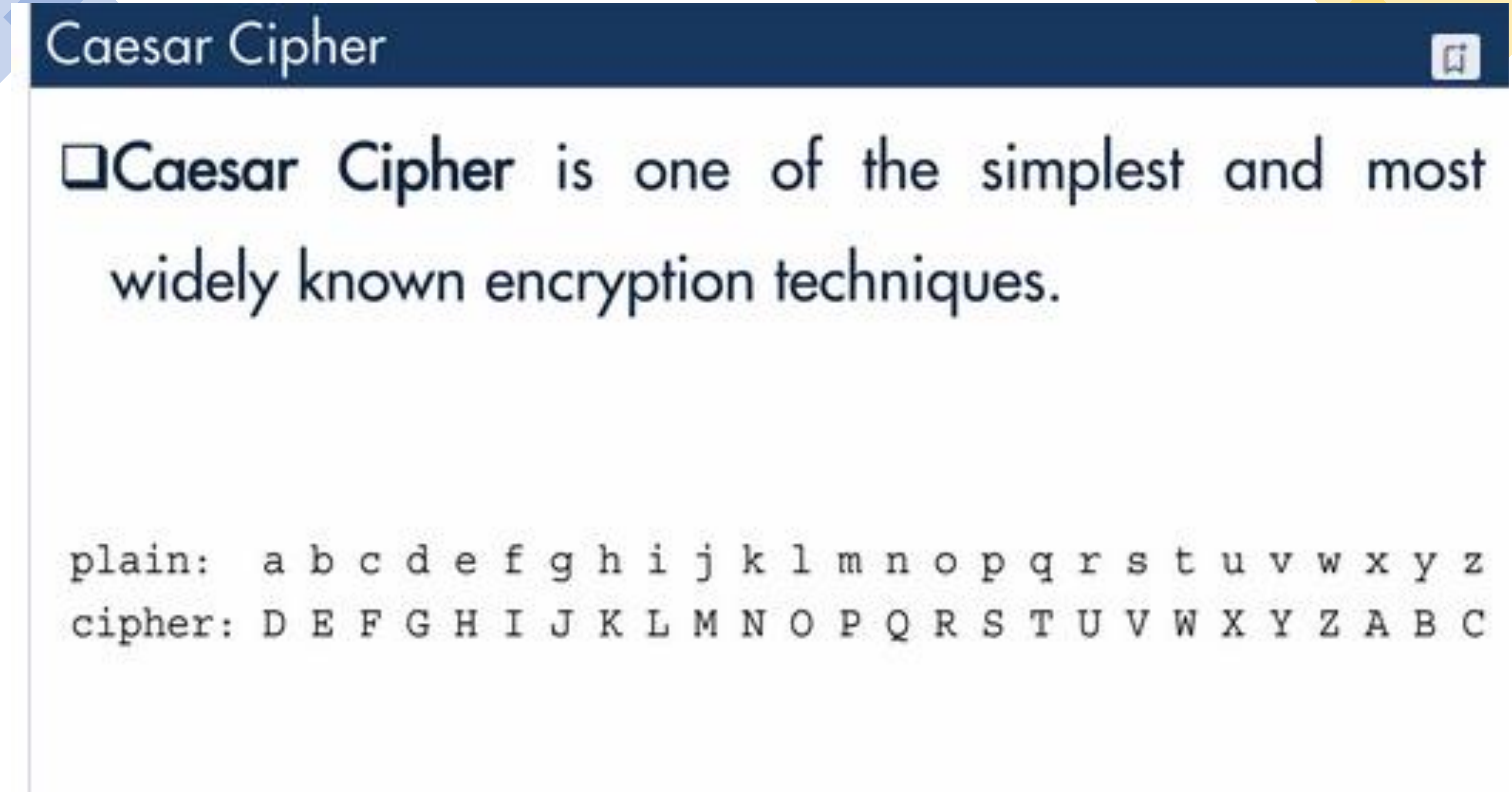
- Symmetric Encryption
- Substitution Techniques
- Caesar Cipher
- Monoalphabetic Cipher
- Playfair Cipher
- Hill Cipher



Caesar cipher

Shift cipher

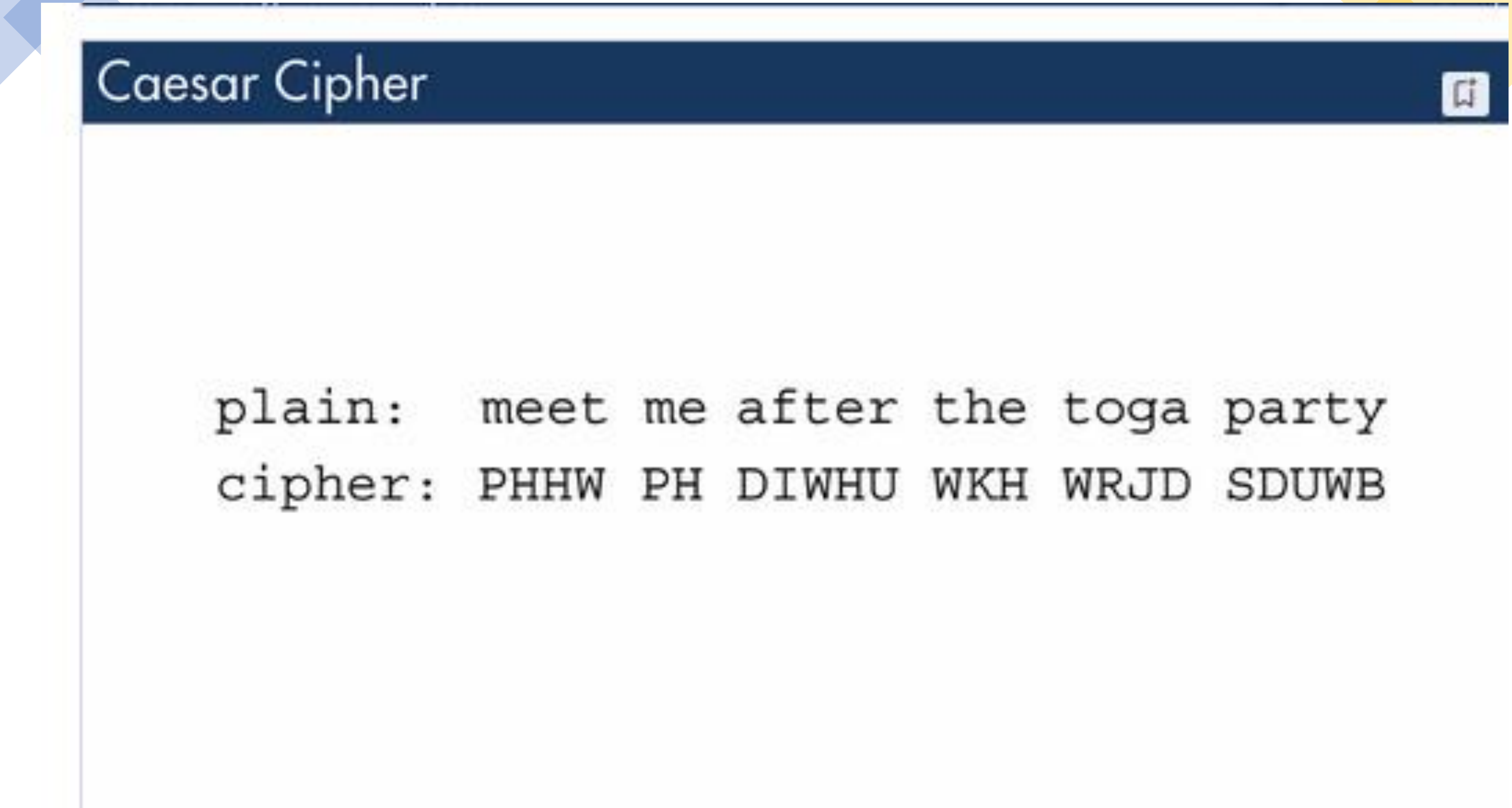
Cryptography



Caesar Cipher

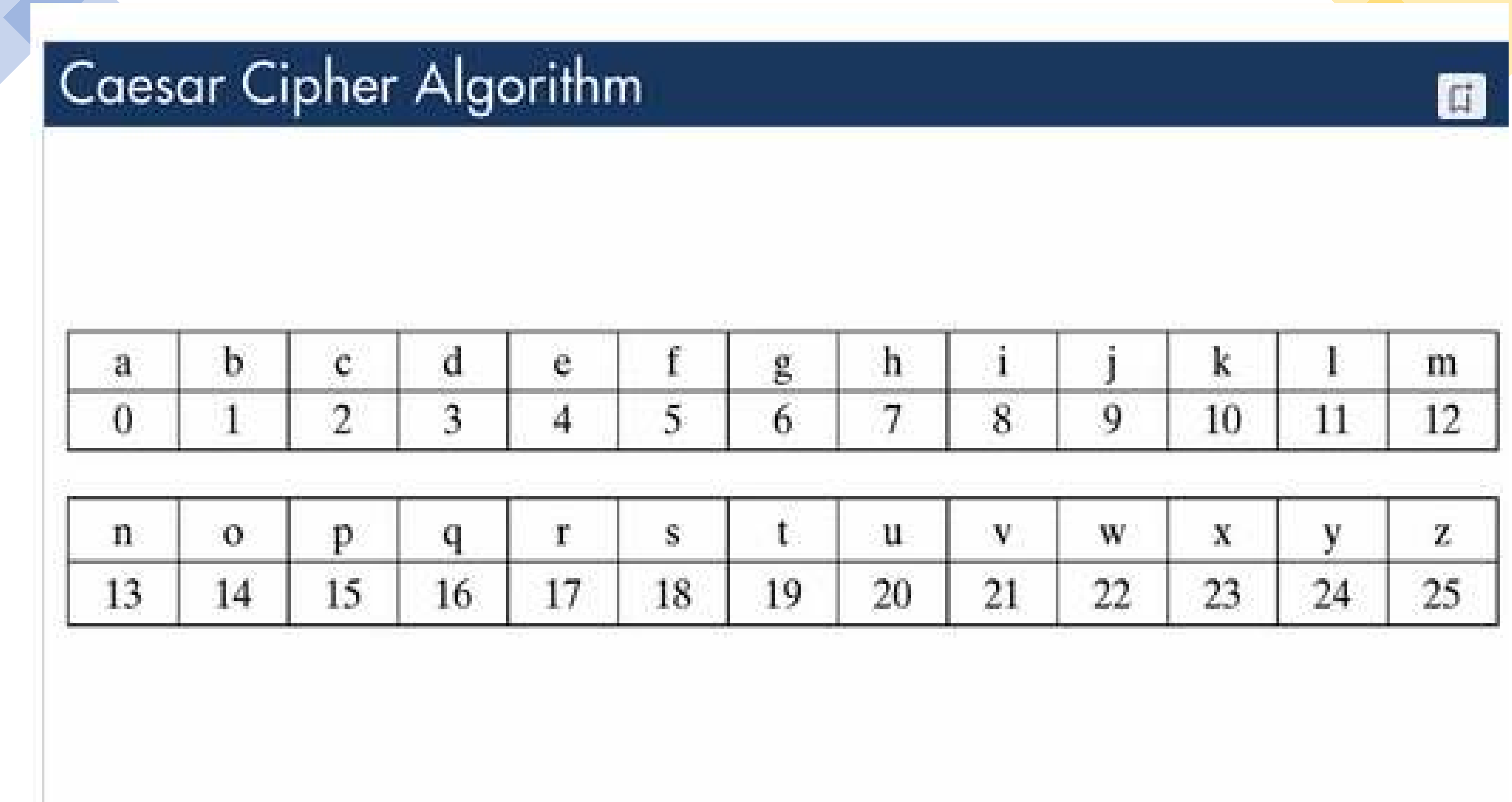
❑Caesar Cipher is one of the simplest and most widely known encryption techniques.

```
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
```



Caesar Cipher

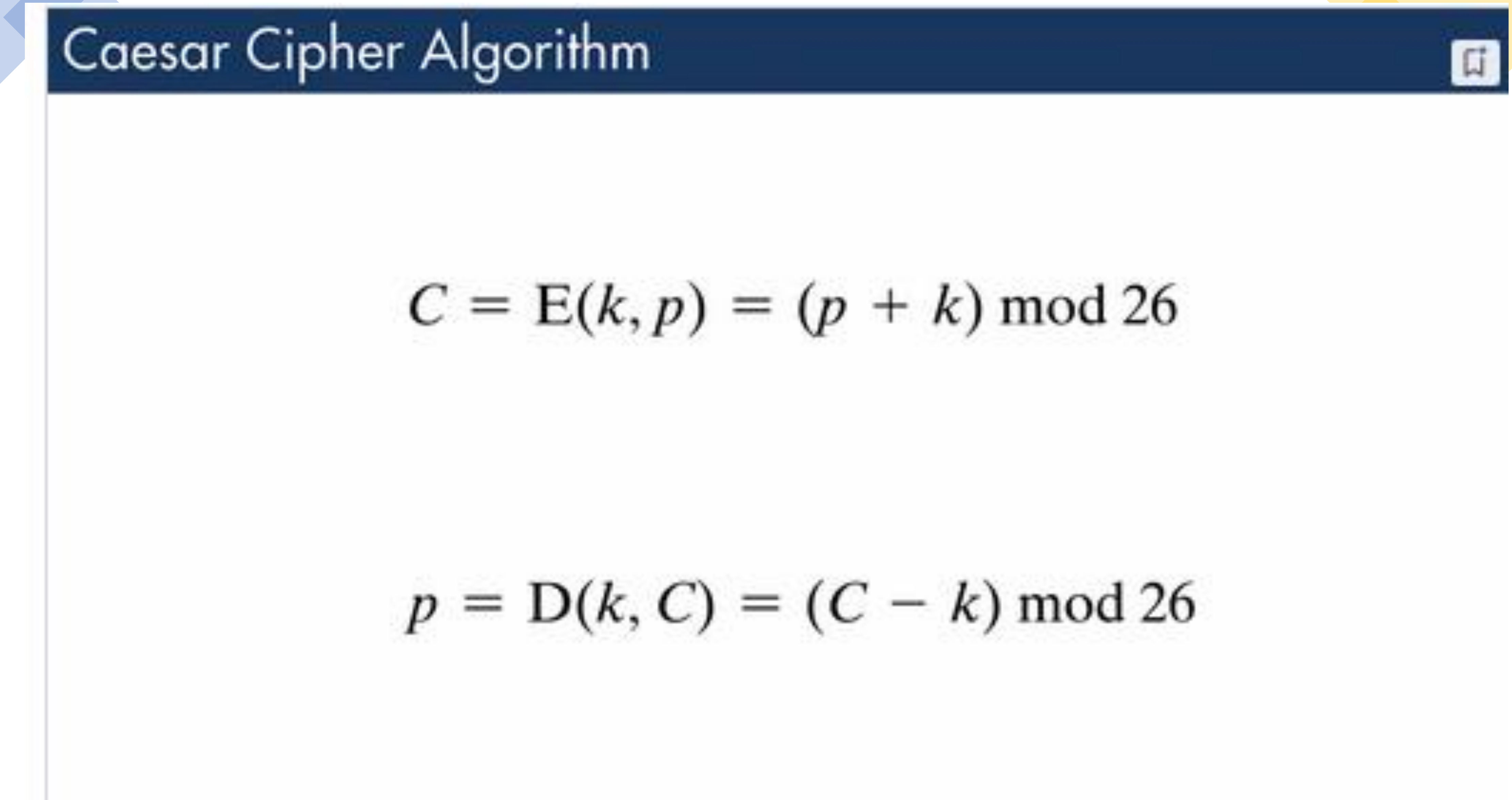
```
plain:  meet me after the toga party
cipher: PHHW PH DIWHU WKH WRJD SDUWB
```



Caesar Cipher Algorithm

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

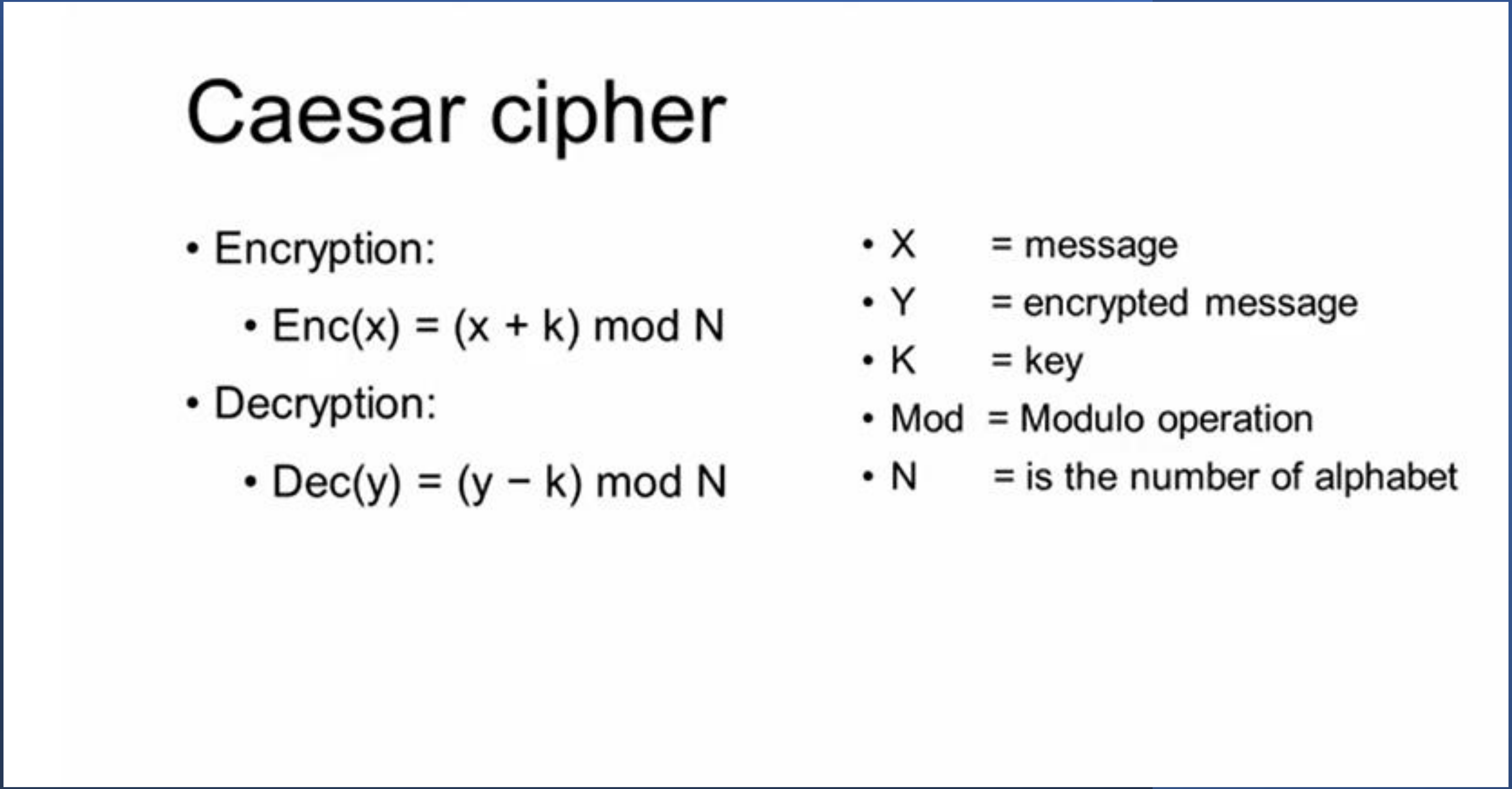
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25



Caesar Cipher Algorithm

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

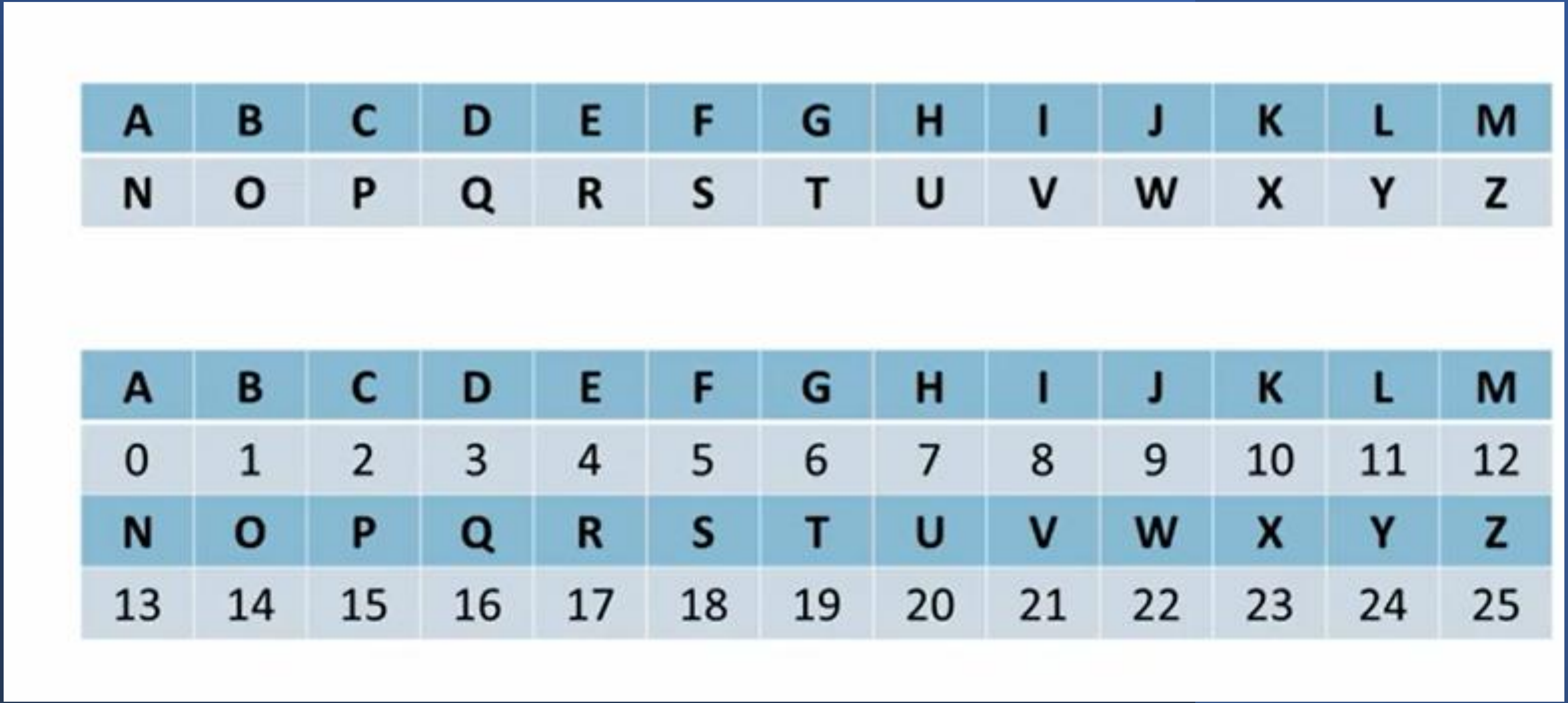
$$p = \mathrm{D}(k, C) = (C - k) \bmod 26$$



Caesar cipher

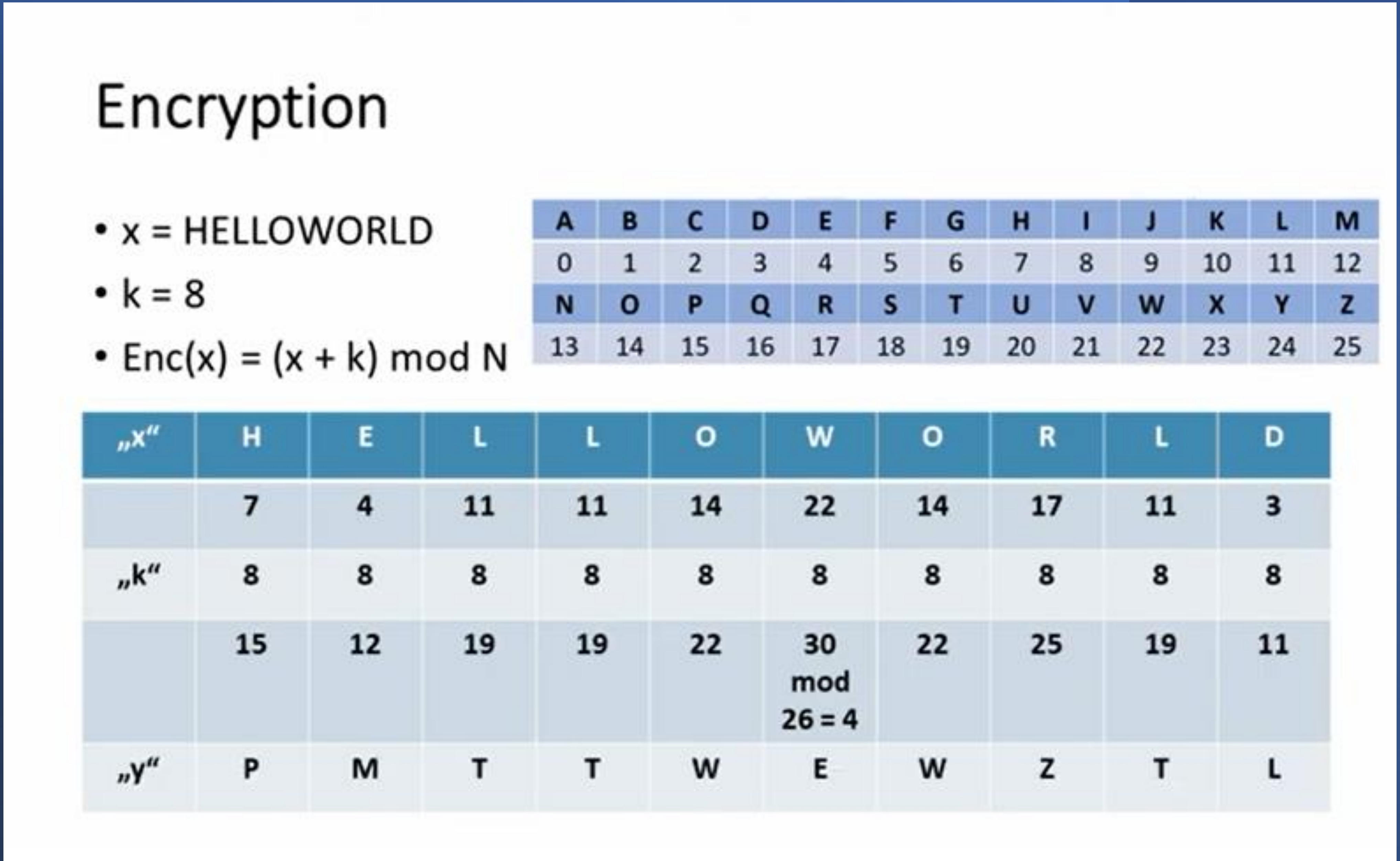
- Encryption:
  - Enc(x) = (x + k) mod N
- Decryption:
  - Dec(y) = (y − k) mod N

- X = message
- Y = encrypted message
- K = key
- Mod = Modulo operation
- N = is the number of alphabet



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

A	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

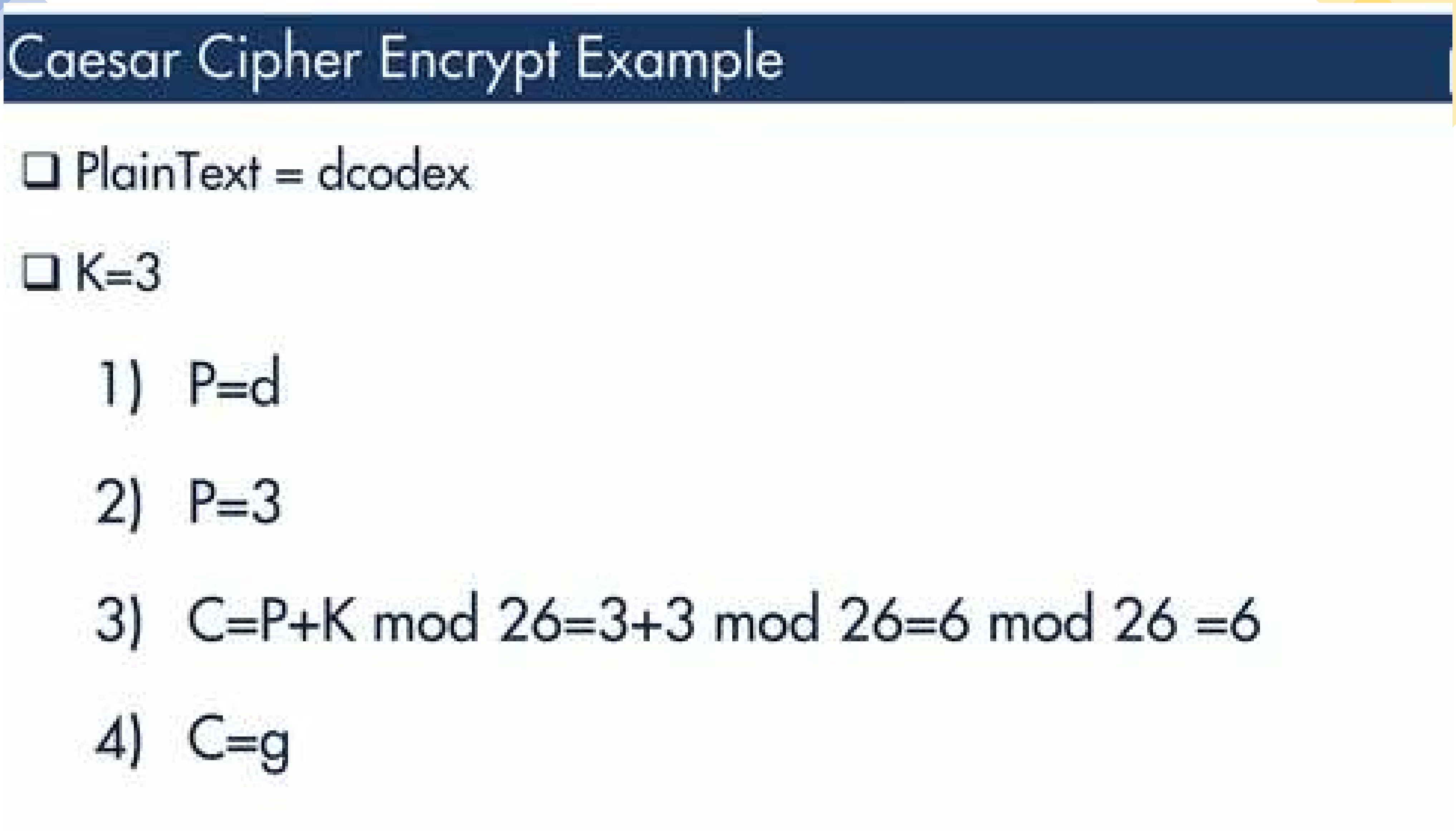


Encryption

- x = HELLOWORLD
- k = 8
- Enc(x) = (x + k) mod N

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

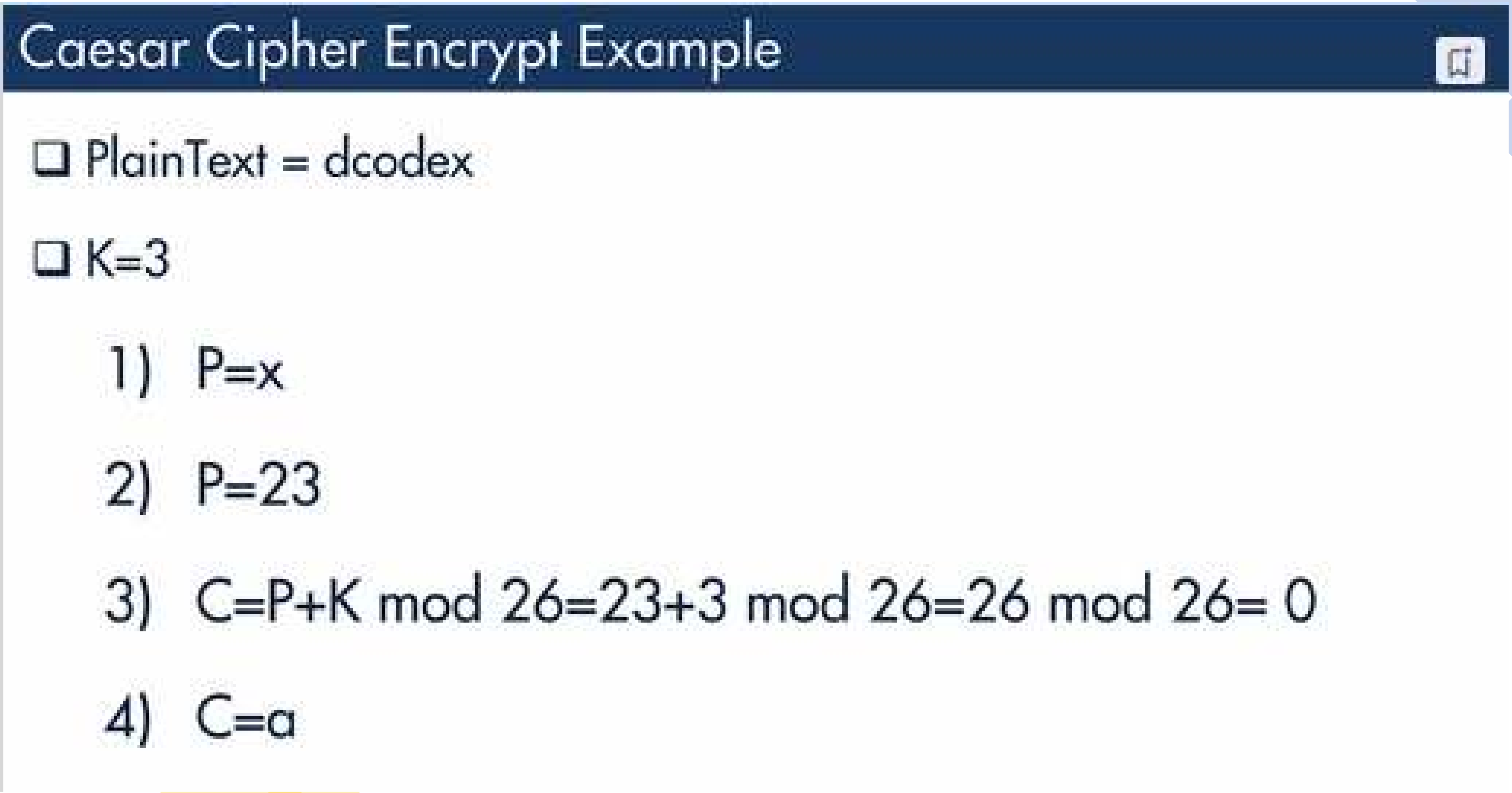
„x“	H	E	L	L	O	W	O	R	L	D
	7	**4**	**11**	**11**	**14**	**22**	**14**	**17**	**11**	**3**
„k“	**8**	**8**	**8**	**8**	**8**	**8**	**8**	**8**	**8**	**8**
	15	**12**	**19**	**19**	**22**	**30 mod 26 = 4**	**22**	**25**	**19**	**11**
„y“	**P**	**M**	**T**	**T**	**W**	**E**	**W**	**Z**	**T**	**L**



Caesar Cipher Encrypt Example

- ❑ PlainText = dcodex
- ❑ K=3

1) P=d
2) P=3
3) C=P+K mod 26=3+3 mod 26=6 mod 26 =6
4) C=g



Caesar Cipher Encrypt Example

□ PlainText = dcodex

□ K=3

1) P=x
2) P=23
3) C=P+K mod 26=23+3 mod 26=26 mod 26= 0
4) C=a

Caesar Cipher Encrypt Example

- ❑ P= dcodex
- ❑ C= gfrgha
- ❑ K=3

Caesar Cipher Decrypt Example

- ❑ CipherText = gfrgha
- ❑ K=3

1) C=g
2) C=6
3) P=C-K mod 26=6-3 mod 26=3
4) P=d

Caesar Cipher Decrypt Example

❑ CipherText = gfrgha

❑ $K=3$

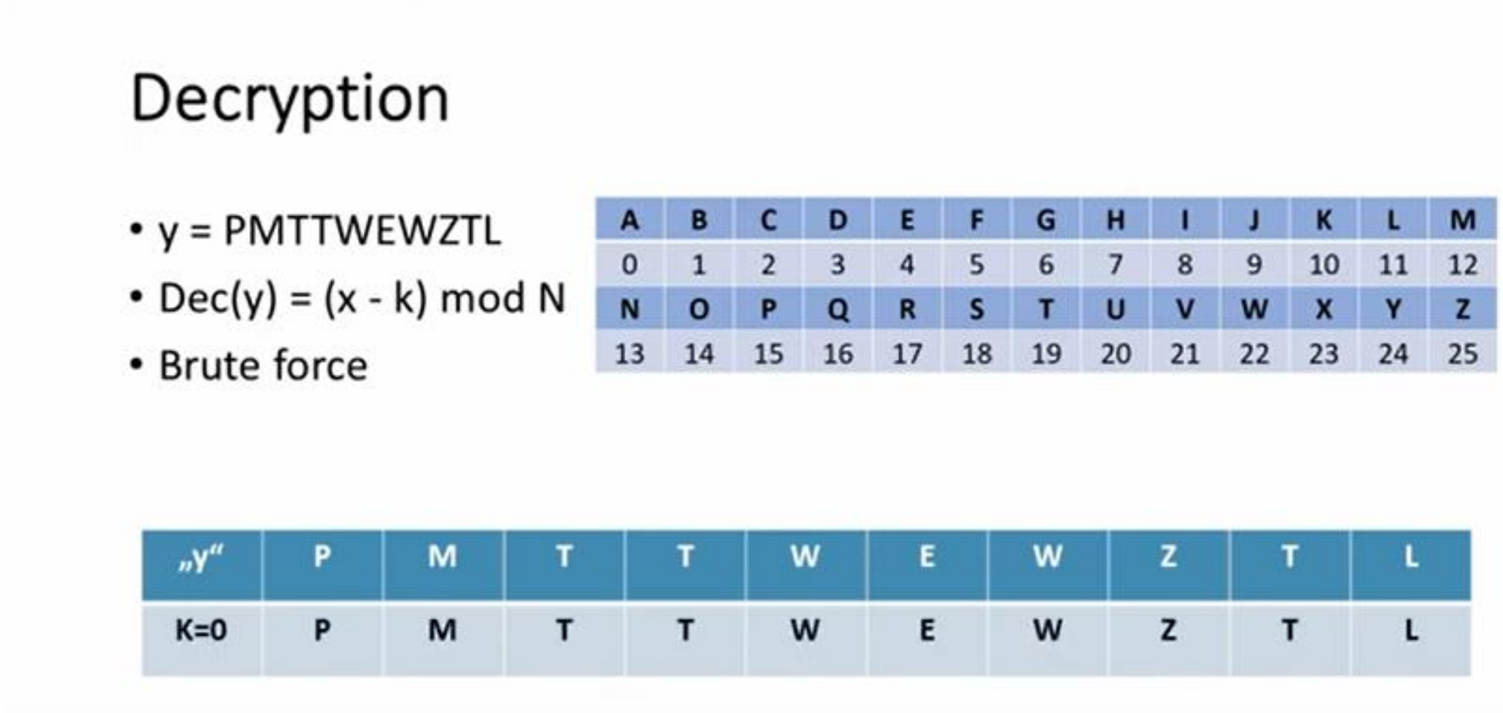
1) $C=a$
2) $C=0$
3) $P=C-K \bmod 26=0-3 \bmod 26=-3 \bmod 26 =23$
4) $P=x$

Caesar Cipher Decrypt Example

- C= gfrgha
- P= dcodex
- K=3

Bruteforce Cryptanalysis

- Three important characteristics of this problem enabled us to use a bruteforce cryptanalysis:
  - The encryption and decryption algorithms are known.
  - There are only 25 keys to try.
  - The language of the plaintext is known and easily recognizable.



Decryption

- y = PMTTWEWZTL
- Dec(y) = (x - k) mod N
- Brute force

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

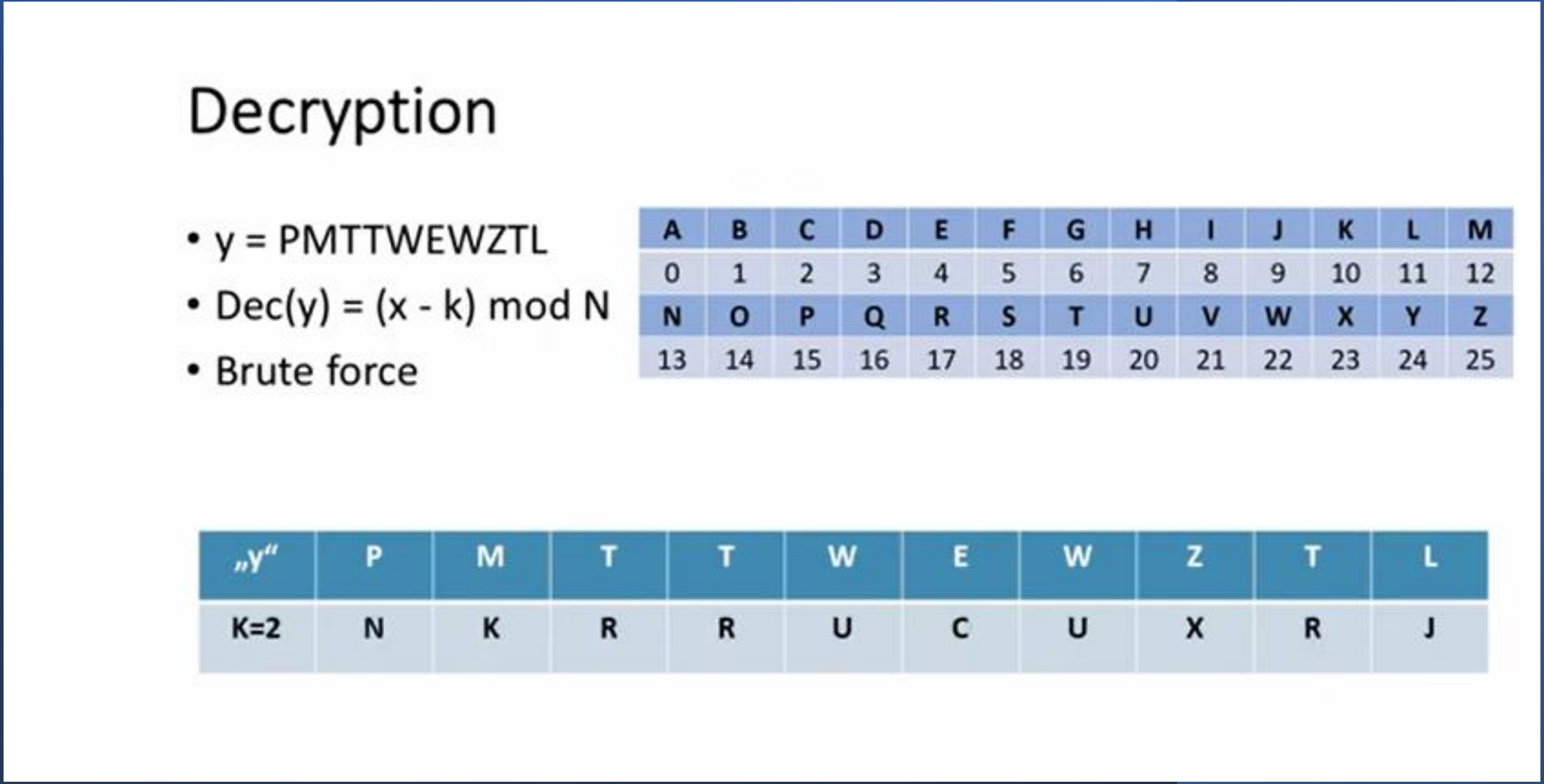
„y“	P	M	T	T	W	E	W	Z	T	L
K=0	P	M	T	T	W	E	W	Z	T	L

Decryption

- y = PMTTWEWZTL
- Dec(y) = (x - k) mod N
- Brute force

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

„y“	P	M	T	T	W	E	W	Z	T	L
K=1	O	L	S	S	V	D	V	Y	S	K

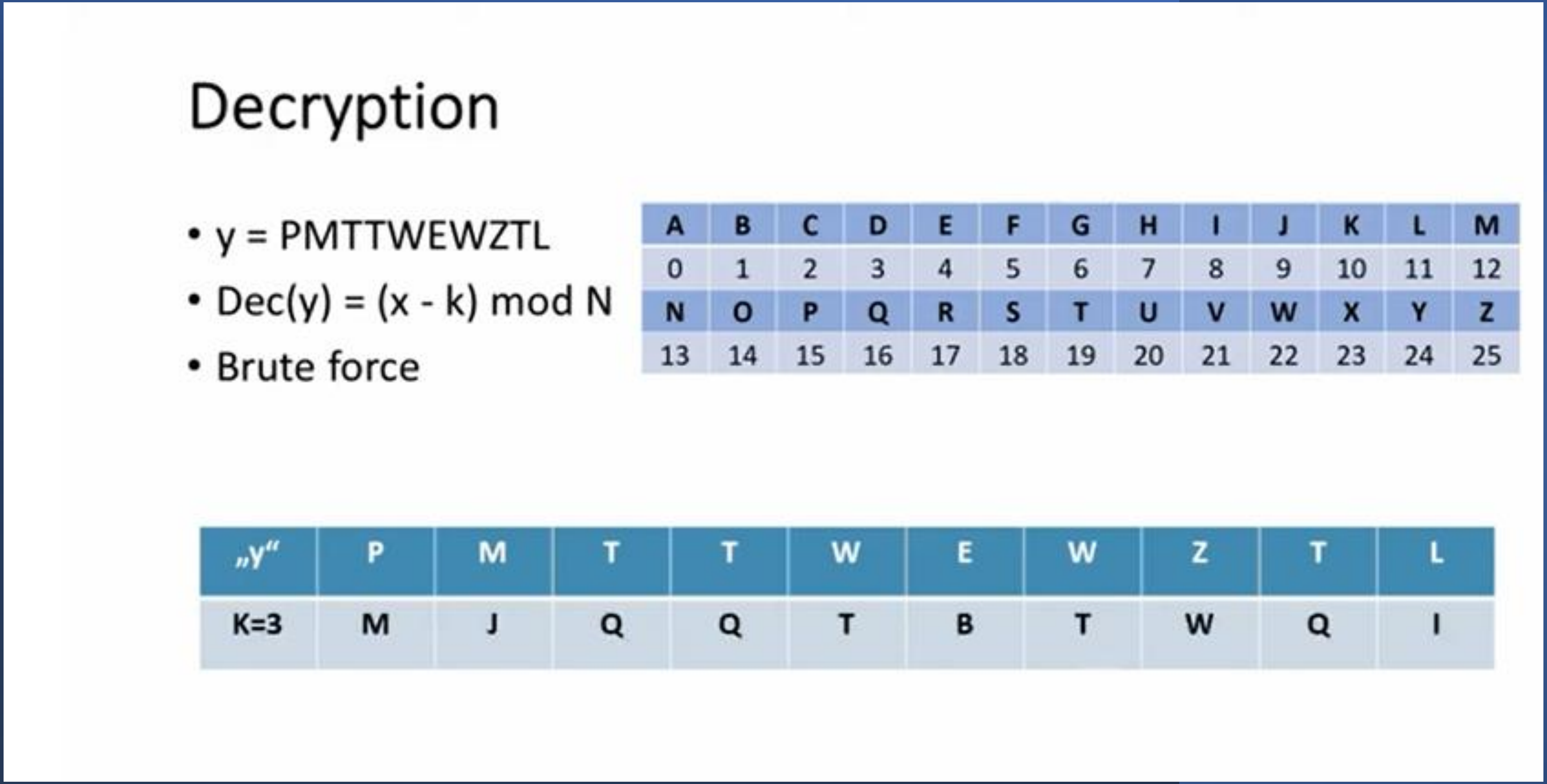


Decryption

- y = PMTTWEWZTL
- Dec(y) = (x - k) mod N
- Brute force

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

„y“	P	M	T	T	W	E	W	Z	T	L
K=2	N	K	R	R	U	C	U	X	R	J

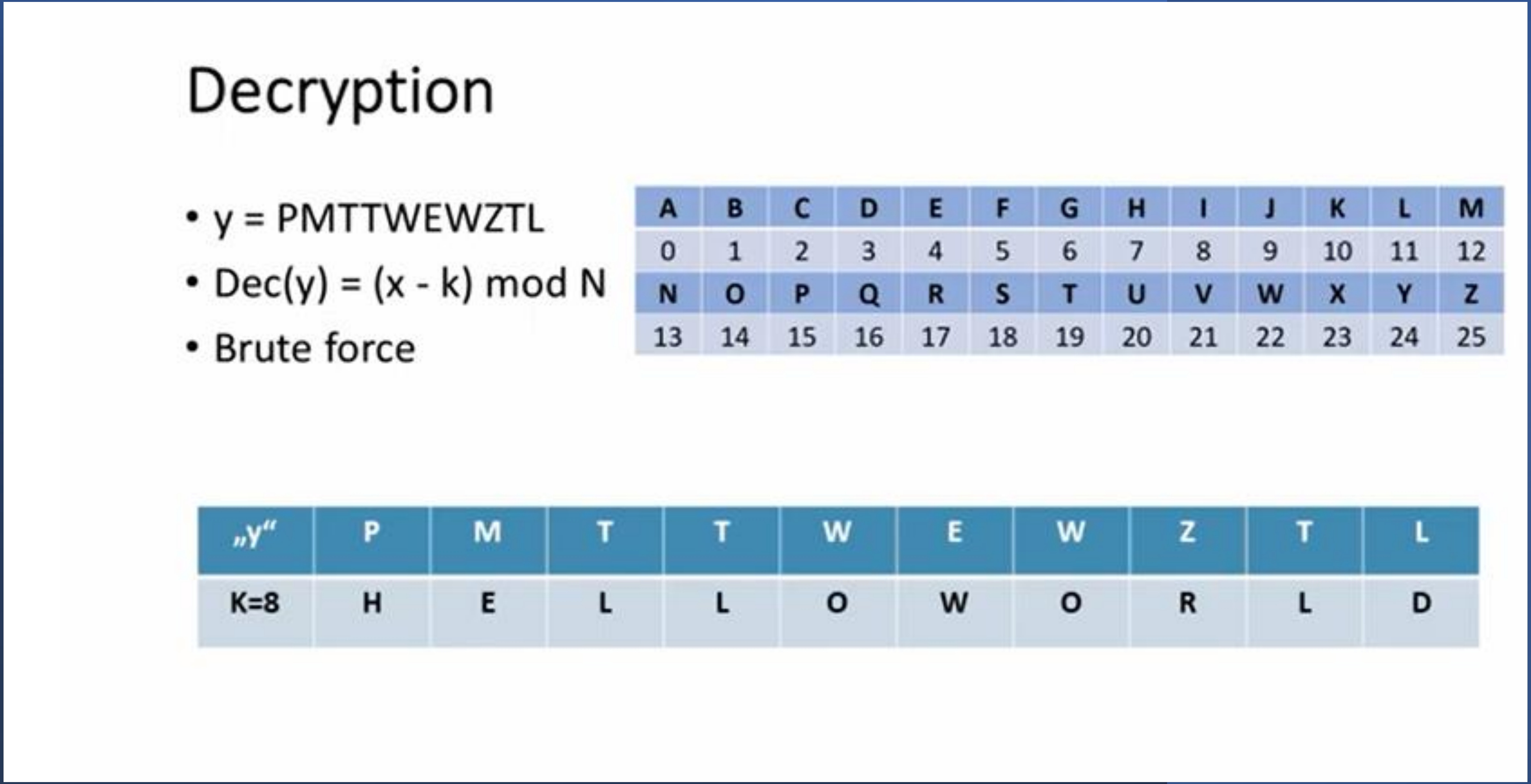


Decryption

- y = PMTTWEWZTL
- Dec(y) = (x - k) mod N
- Brute force

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

„y“	P	M	T	T	W	E	W	Z	T	L
K=3	M	J	Q	Q	T	B	T	W	Q	I

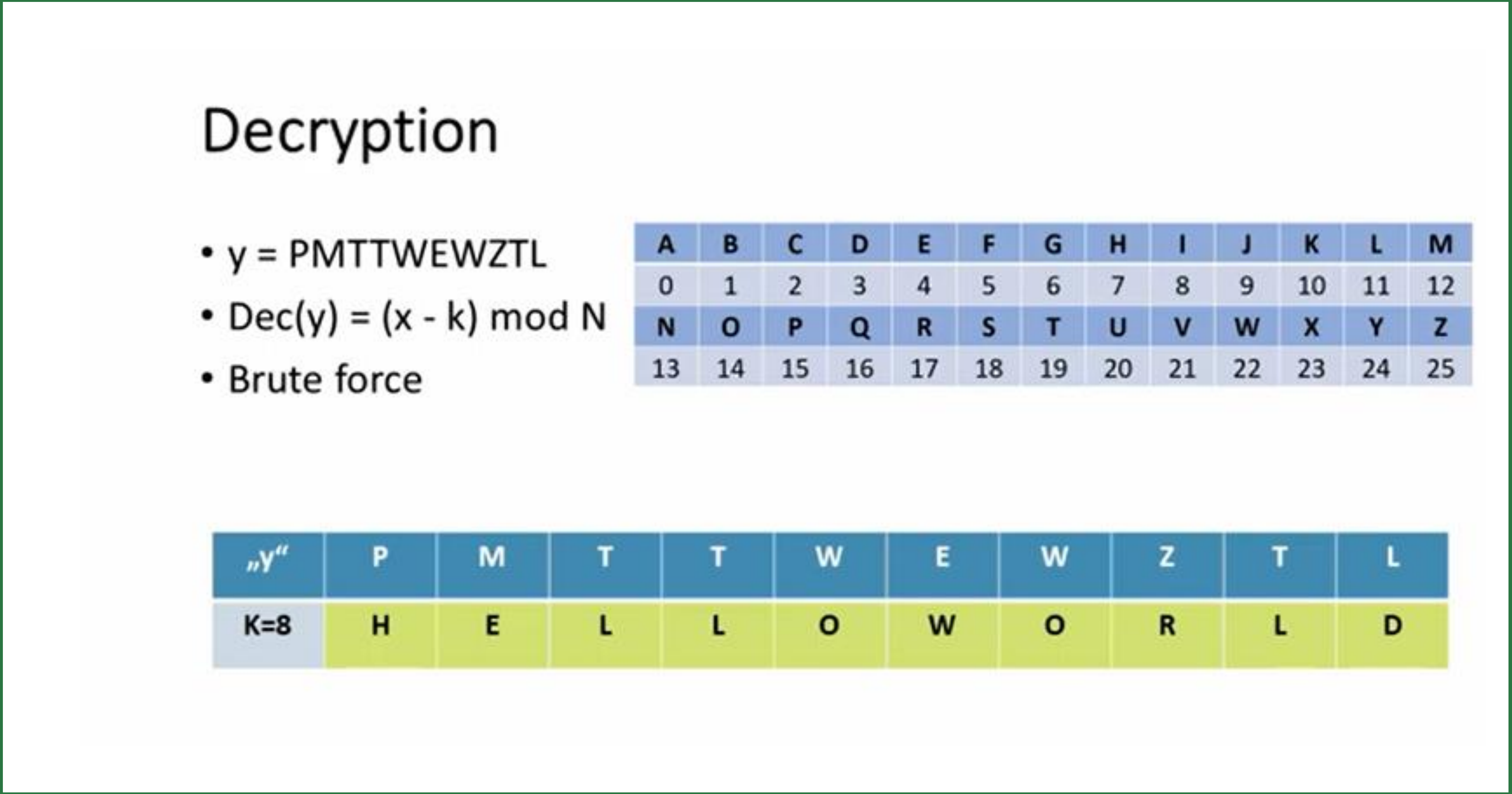


Decryption

- y = PMTTWEWZTL
- Dec(y) = (x - k) mod N
- Brute force

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

„y“	P	M	T	T	W	E	W	Z	T	L
K=8	H	E	L	L	O	W	O	R	L	D



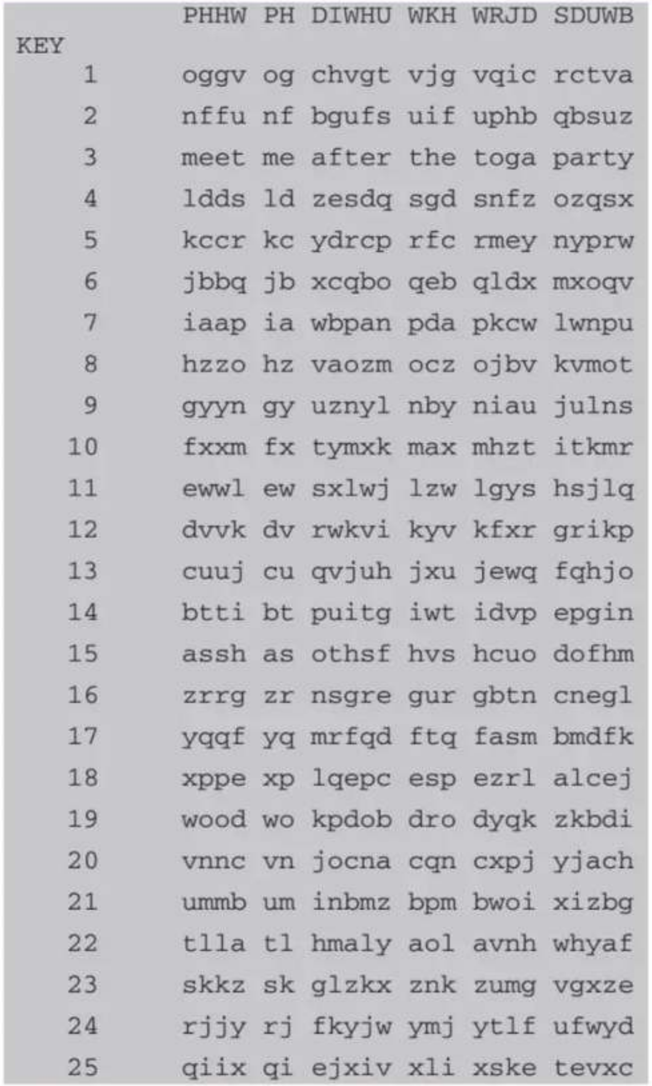
Decryption

- y = PMTTWEWZTL
- Dec(y) = (x - k) mod N
- Brute force

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

„y“	P	M	T	T	W	E	W	Z	T	L
K=8	H	E	L	L	O	W	O	R	L	D

Bruteforce Cryptanalysis



KEY	PHHW	PH	DIWHU	WKH	WRJD	SDUWB
1	oggv	og	chvgt	vjg	vqic	rctva
2	nffu	nf	bgufs	uif	uphb	qbsuz
3	meet	me	after	the	toga	party
4	ldds	ld	zesdq	sgd	snfz	ozqsx
5	kccr	kc	ydrcp	rfc	rmey	nyprw
6	jbbq	jb	xcqbo	qeb	qldx	mxoqv
7	iaap	ia	wbpan	pda	pkcw	lwnpu
8	hzzo	hz	vaozm	ocz	ojbv	kvmot
9	gyyn	gy	uznyl	nby	niau	julns
10	fxxm	fx	tymxk	max	mhzt	itkmr
11	ewwl	ew	sxlwj	lzw	lgys	hsjlq
12	dvvk	dv	rwkvi	kyv	kfxr	grikp
13	cuuj	cu	qvjuh	jxu	jewq	fqhjo
14	btti	bt	puitg	iwt	idvp	epgin
15	assh	as	othsf	hvs	hcuo	dofhm
16	zrrg	zr	nsgre	gur	gbtn	cnegl
17	yqqf	yq	mrfqd	ftq	fasm	bmdfk
18	xppe	xp	lqepc	esp	ezrl	alcej
19	wood	wo	kpdob	dro	dyqk	zkbdi
20	vnnc	vn	jocna	cqn	cxpj	yjach
21	ummb	um	inbmz	bpm	bwoi	xizbg
22	tlla	tl	hmaly	aol	avnh	whyaf
23	skkz	sk	glzkx	znk	zumg	vgxze
24	rjjy	rj	fkyjw	ymj	ytlf	ufwyd
25	qiix	qi	ejxiv	xli	xske	tevxc

Task1

- **How to implement Caesar Cipher technique on Arabic letters?**

Table of Contents

- Symmetric Encryption
- Substitution Techniques
- Caesar Cipher
- Monoalphabetic Cipher
- Playfair Cipher
- Hill Cipher

Monoalphabetic Cipher

- ❑A **monoalphabetic cipher** uses fixed substitution over the entire message

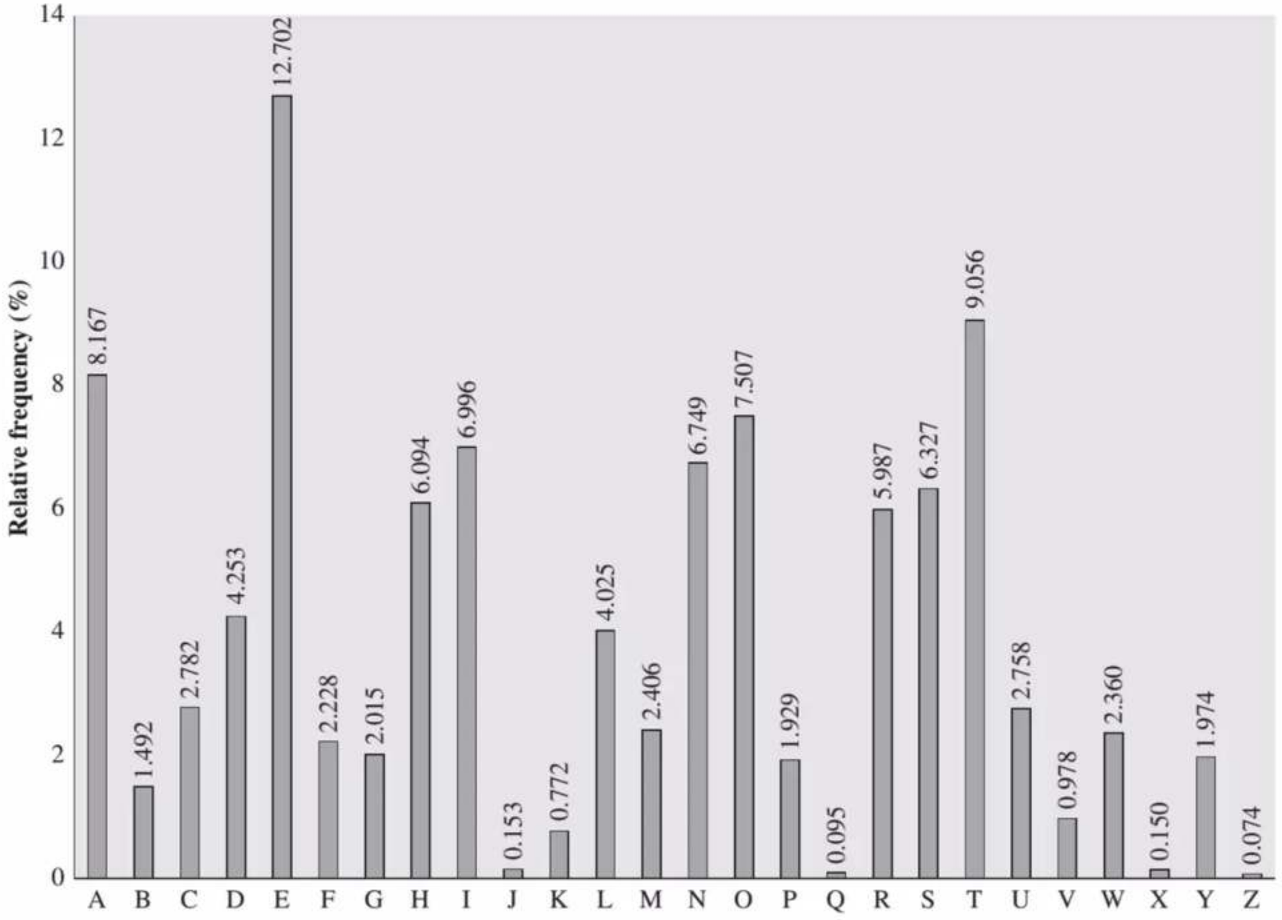
- ❑Random Key

Monoalphabetic Cipher

- Example:
  - Plaintext alphabets: ABCDEFGHIJKLMNOPQRSTUVWXYZ
  - Ciphertext alphabet: ZEBRASCDFGHIJKLMNOPQTUVWXY
- P= ITEMS
- Encoding
- C= FQAIP
- Decoding
- P= ITEMS

Monoalphabetic Cipher Cryptanalysis

- ❑ Relative Frequency of Letters in English Text



Monoalphabetic Cipher Cryptanalysis

- cipher letters P and Z are the equivalents of plain letters e and t

```
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
```

Monoalphabetic Cipher Cryptanalysis

❑ cipher letters P and Z are the equivalents of plain letters e and t

```
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
```

Task2

- ❑How to implement Monoalphabetic Cipher technique on Arabic letters?

Table of Contents

- Symmetric Encryption
- Substitution Techniques
- Caesar Cipher
- Monoalphabetic Cipher
- Playfair Cipher
- Hill Cipher

Playfair Cipher

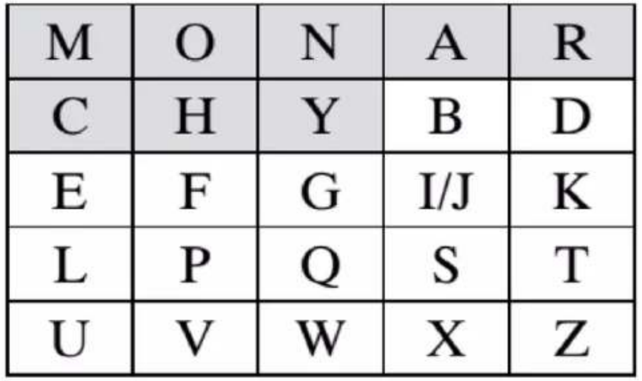
❑ The Playfair system was invented by Charles Wheatstone, who first described it in 1854.

❑ Used by many countries during wartime

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

Playfair Cipher

- ❑ In this case, the keyword is **monarchy**.



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

Playfair Cipher

❑ 4 Rules:

1) If both letters are the same (or only one letter is left), add an "X" after the first letter.

2) If the letters appear on the same row of your table, replace them with the letters to their immediate right respectively

Playfair Cipher

- ❑ 4 Rules:

  3) If the letters appear on the same column of your table, replace them with the letters immediately below respectively

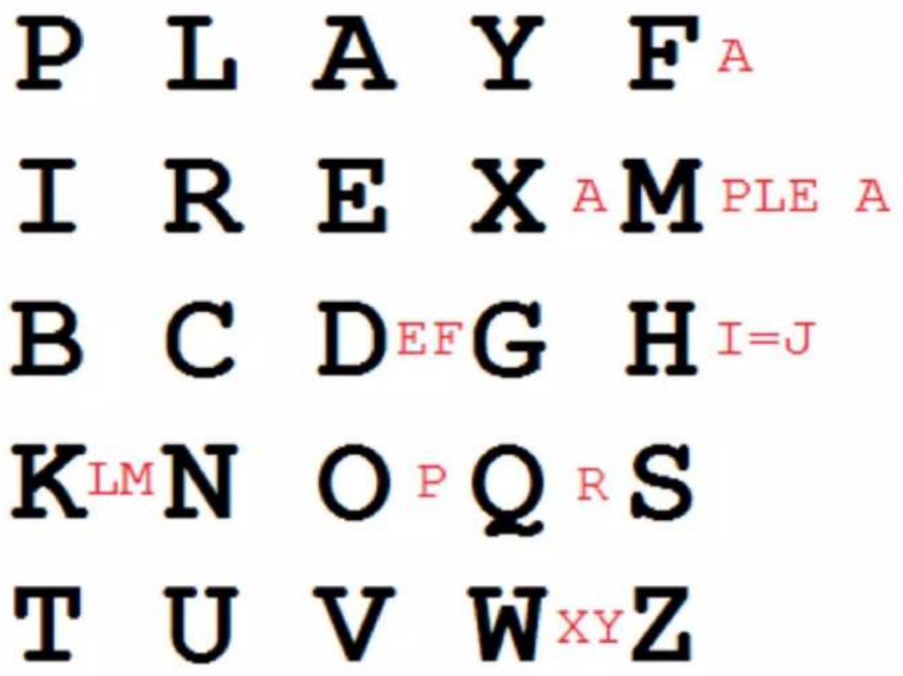
  4) If the letters are not on the same row or column, replace them with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair.

Playfair Cipher

- P=Hide the gold in the tree stump (note the null "X" used to separate the repeated "E"s)
- P= HI DE TH EG OL DI NT HE TR EX ES TU MP

Playfair Cipher

❑ How to build 5x5 Matrix (assuming that I and J are interchangeable), the table becomes (omitted letters in red):

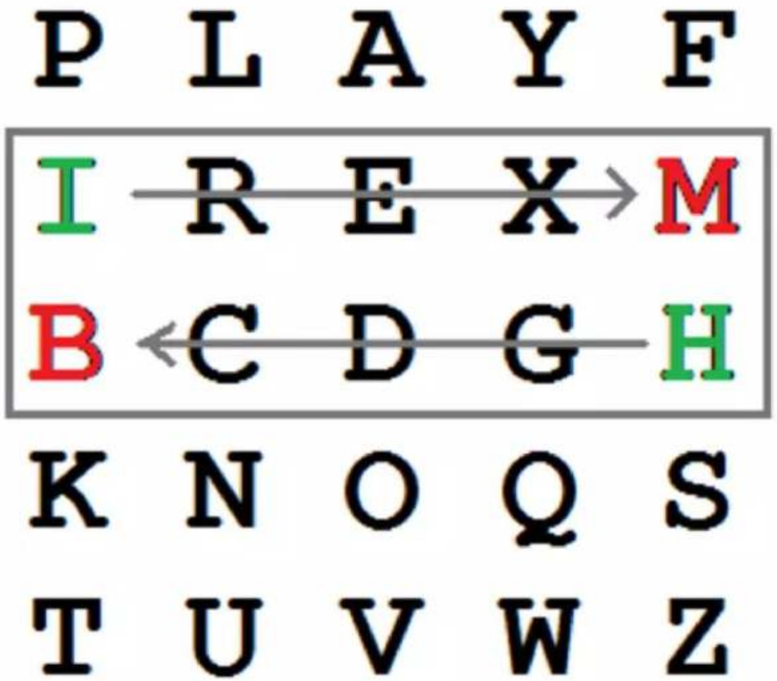


P	L	A	Y	F A
I	R	E	X A	M PLE A
B	C	D EF	G	H I=J
K LM	N	O P	Q R	S
T	U	V	W XY	Z

Playfair Cipher

- ❑ P= HI DE TH EG OL DI NT HE TR EX ES TU MP

1. The pair HI forms a rectangle, replace it with BM



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

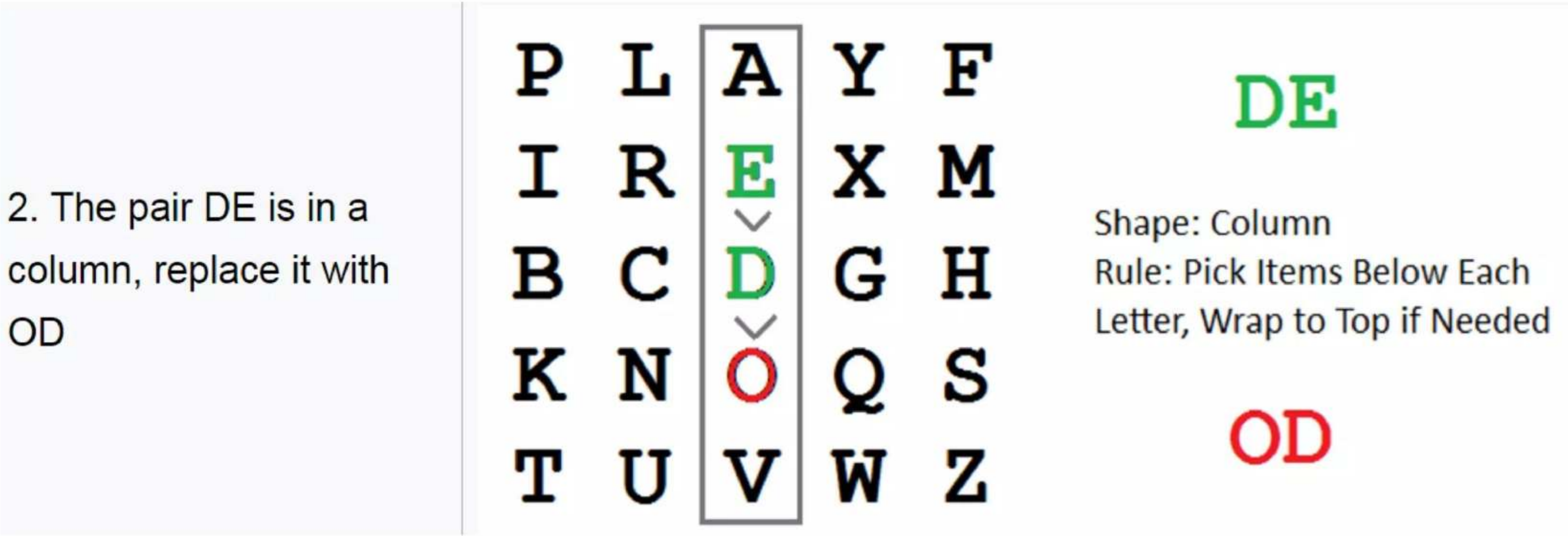
HI

Shape: Rectangle
Rule: Pick Same Rows,
Opposite Corners

BM

Playfair Cipher

- ❑ P= HI DE TH EG OL DI NT HE TR EX ES TU MP



2. The pair DE is in a column, replace it with OD

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

DE

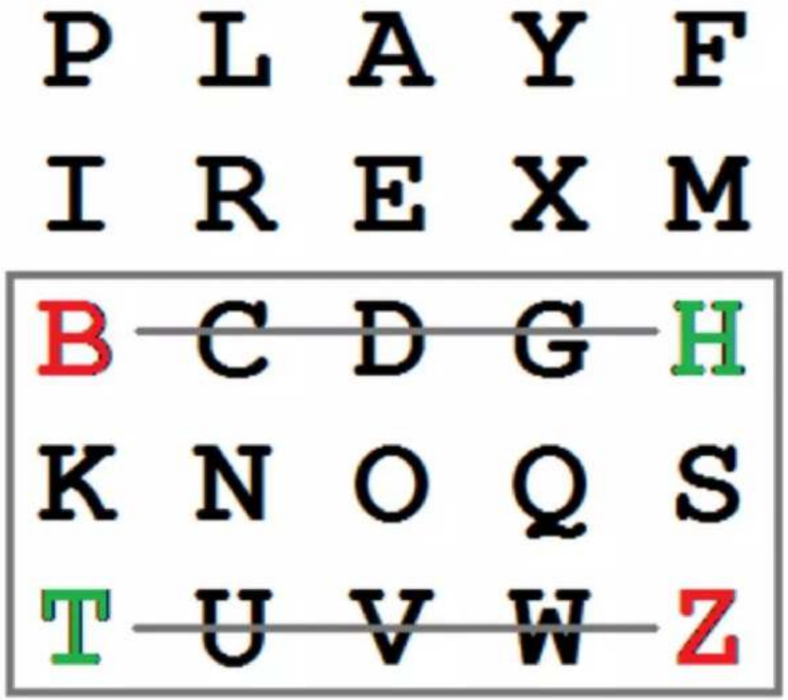
Shape: Column
Rule: Pick Items Below Each Letter, Wrap to Top if Needed

OD

Playfair Cipher

- P= HI DE TH EG OL DI NT HE TR EX ES TU MP

3. The pair TH forms a rectangle, replace it with ZB



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

TH

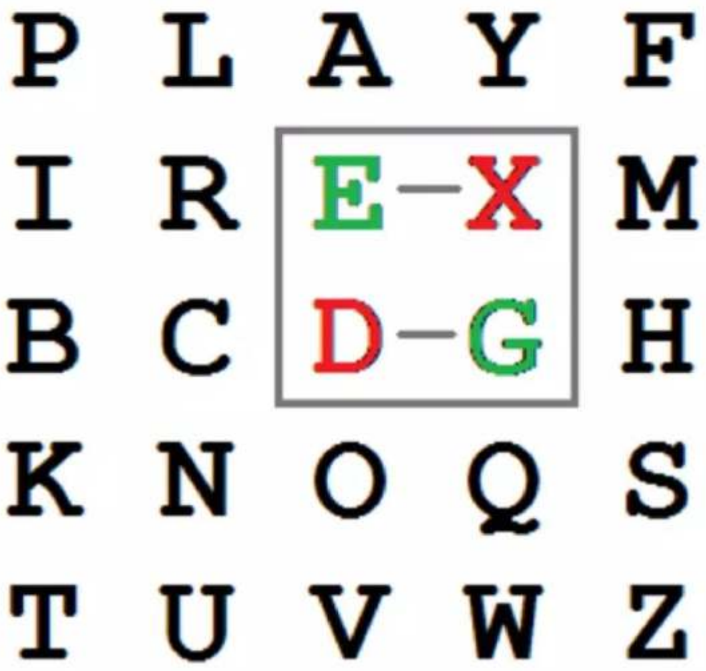
Shape: Rectangle
Rule: Pick Same Rows, Opposite Corners

ZB

Playfair Cipher

❑ P= HI DE TH EG OL DI NT HE TR EX ES TU MP

4. The pair EG forms a rectangle, replace it with XD



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

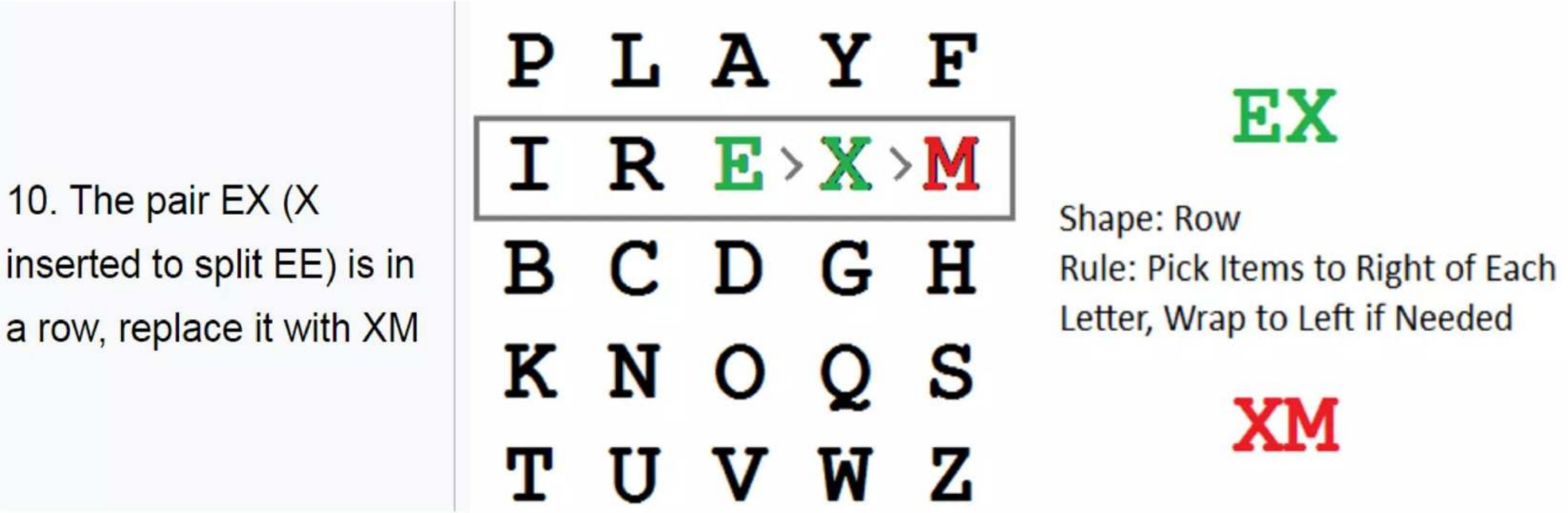
EG

Shape: Rectangle
Rule: Pick Same Rows, Opposite Corners

XD

Playfair Cipher

- ❑ P= HI DE TH EG OL DI NT HE TR EX ES TU MP



10. The pair EX (X inserted to split EE) is in a row, replace it with XM

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

EX

Shape: Row
Rule: Pick Items to Right of Each Letter, Wrap to Left if Needed

XM

Playfair Cipher

- C= BM OD ZB XD NA BE KU DM UI XM MO UV IF

- the message "Hide the gold in the tree stump" becomes "BMODZ BXDNA BEKUD MUIXM MOUVI F"

Task3

❑Using Playfair Cipher how to decrepit the following cipher text:

C= “BMODZ BXDNA BEKUD MUIXM MOUVI F”

K= playfair example