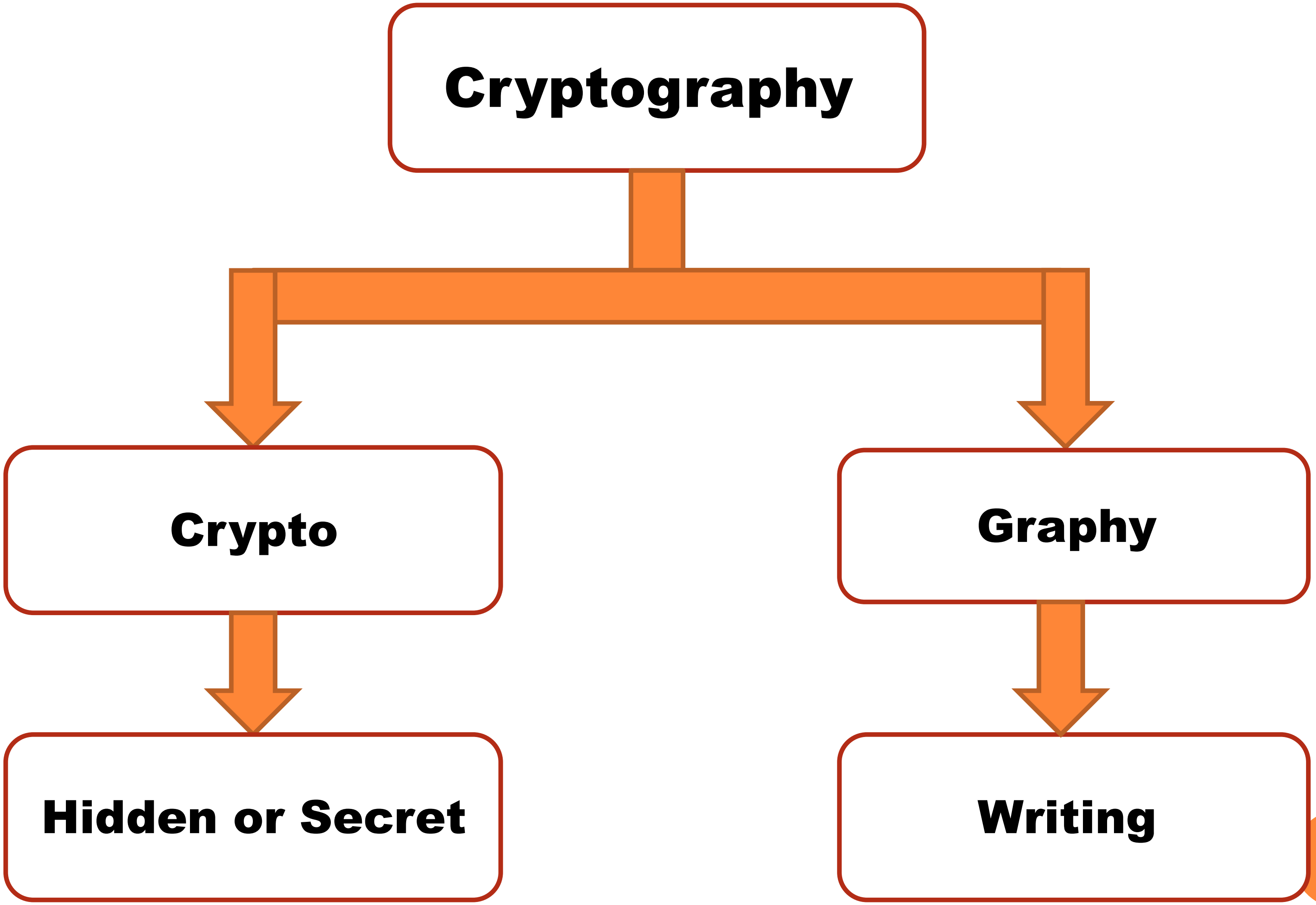
بسم الله الرحمن الرحيم

CRYPTOGRAPHY

CRYPTOGRAPHY



Cryptography

Crypto

Graphy

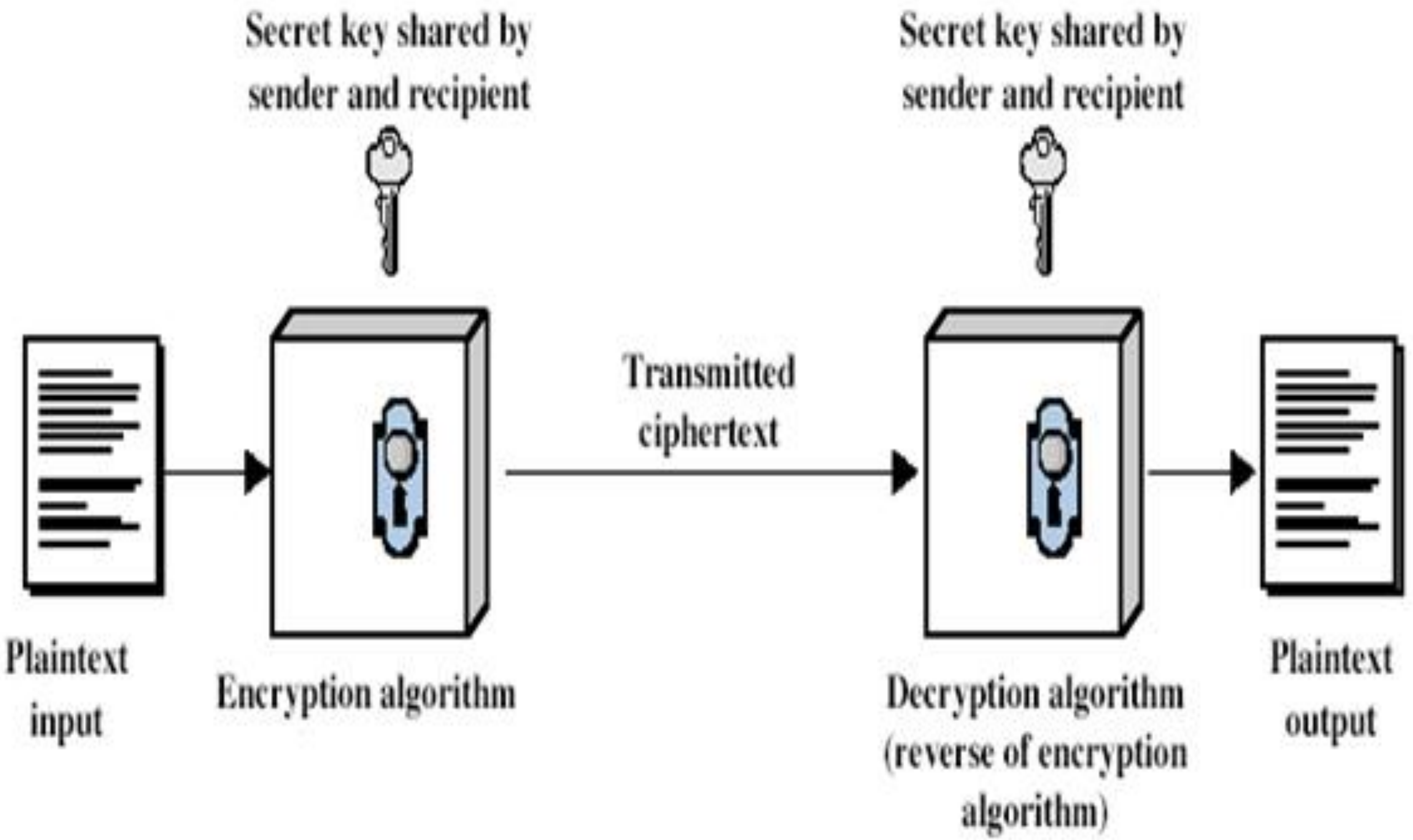
Hidden or Secret

Writing

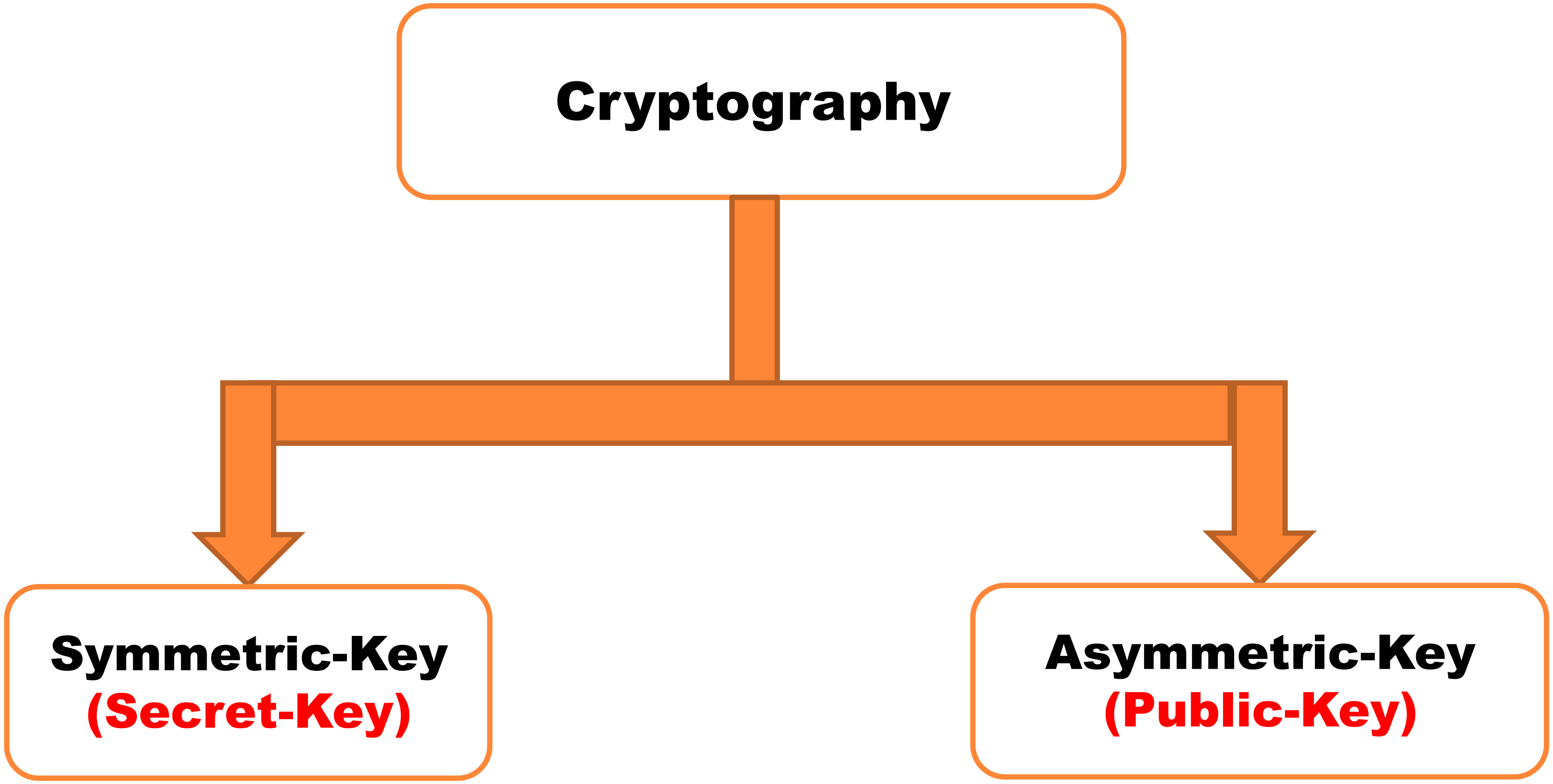
DEFINITION OF CRYPTOGRAPHY

Cryptography is the art and the science of transforming the secret data to a gibberish form that looks random and meaningless to the attacker. In other words, secret message in cryptography is scrambled such that it cannot be understood, then the scrambled message is transmitted. Only the intended recipient can remove this gibberish and read the secret message.

BASIC CRYPTOGRAPHY MODEL


Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

CATEGORIES OF CRYPTOGRAPHY



Cryptography

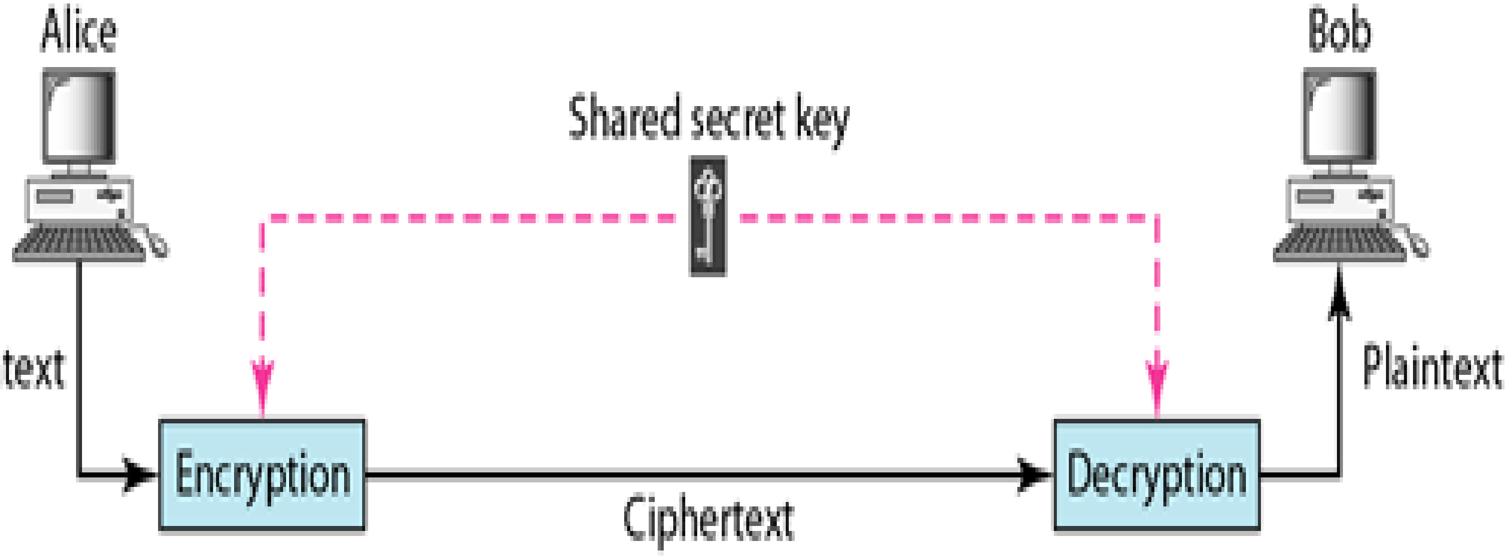
Symmetric-Key
(Secret-Key)

Asymmetric-Key
(Public-Key)

SYMMETRIC-KEY CRYPTOGRAPHY

In symmetric-key cryptography, the same key is used by the sender (for encryption) and the receiver (for decryption). The key is shared.

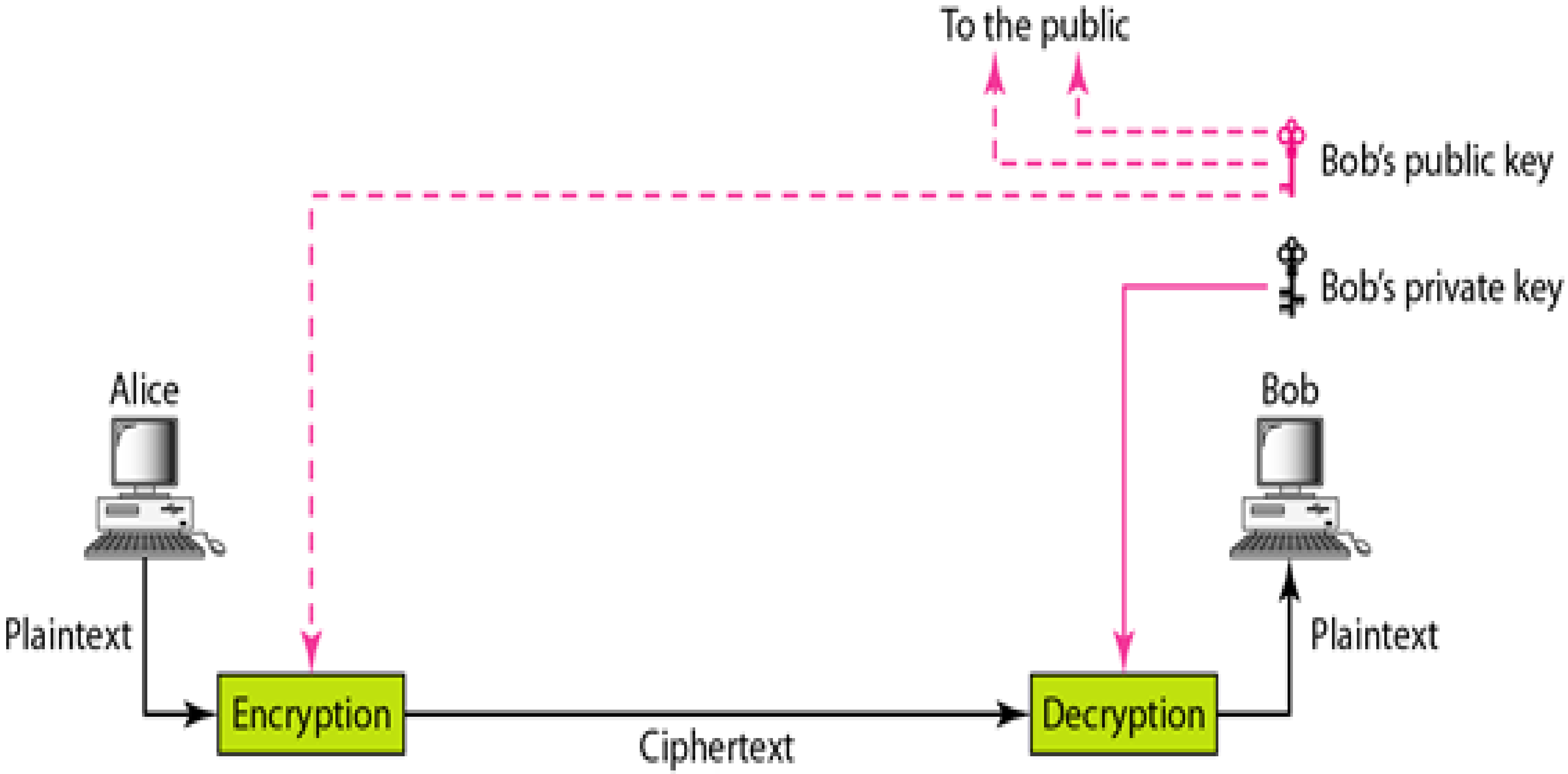
SYMMETRIC-KEY CRYPTOGRAPHY



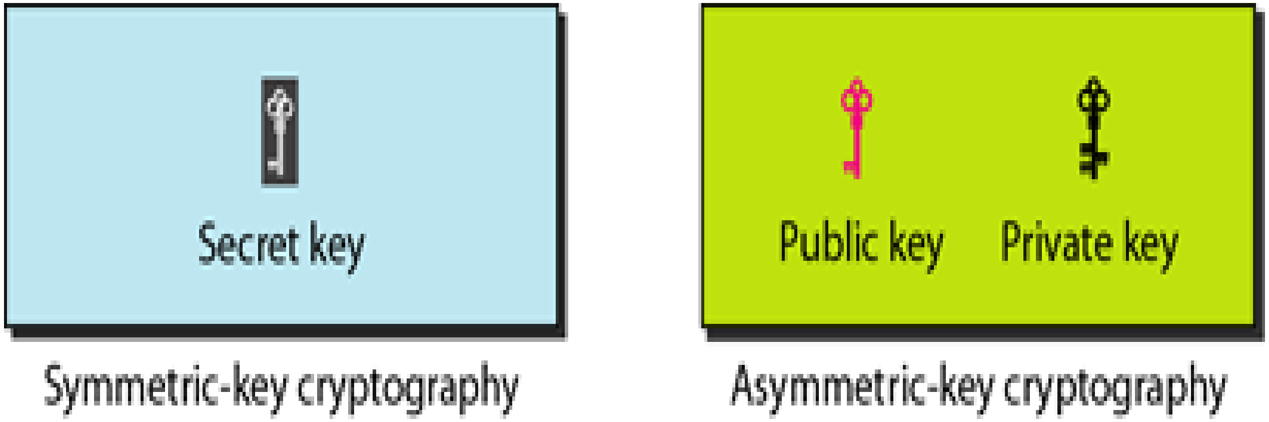
ASYMMETRIC-KEY CRYPTOGRAPHY

In asymmetric-key cryptography, two keys are used. The first one is the public key is used by the sender (for encryption), and the second one is the private key is used by the receiver (for decryption).

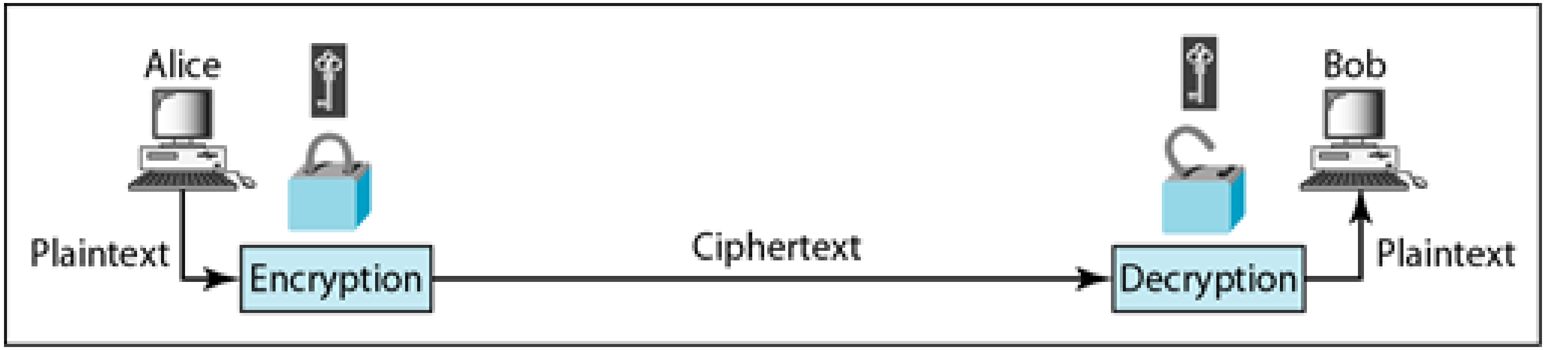
ASYMMETRIC-KEY CRYPTOGRAPHY



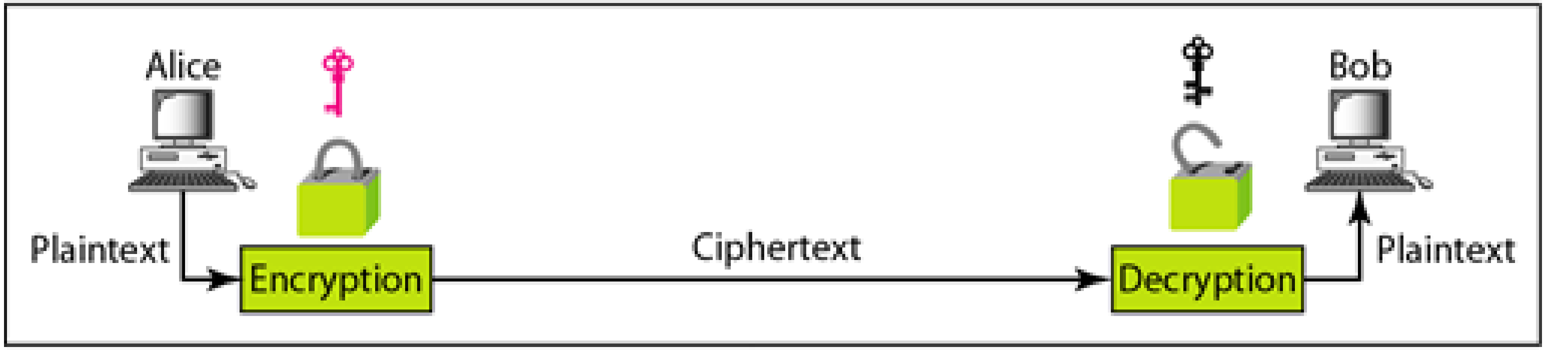
KEYS USED IN CRYPTOGRAPHY



COMPARITION BETWEEN TWO CATEGORIES OF CRYPTOGRAPHY



a. Symmetric-key cryptography

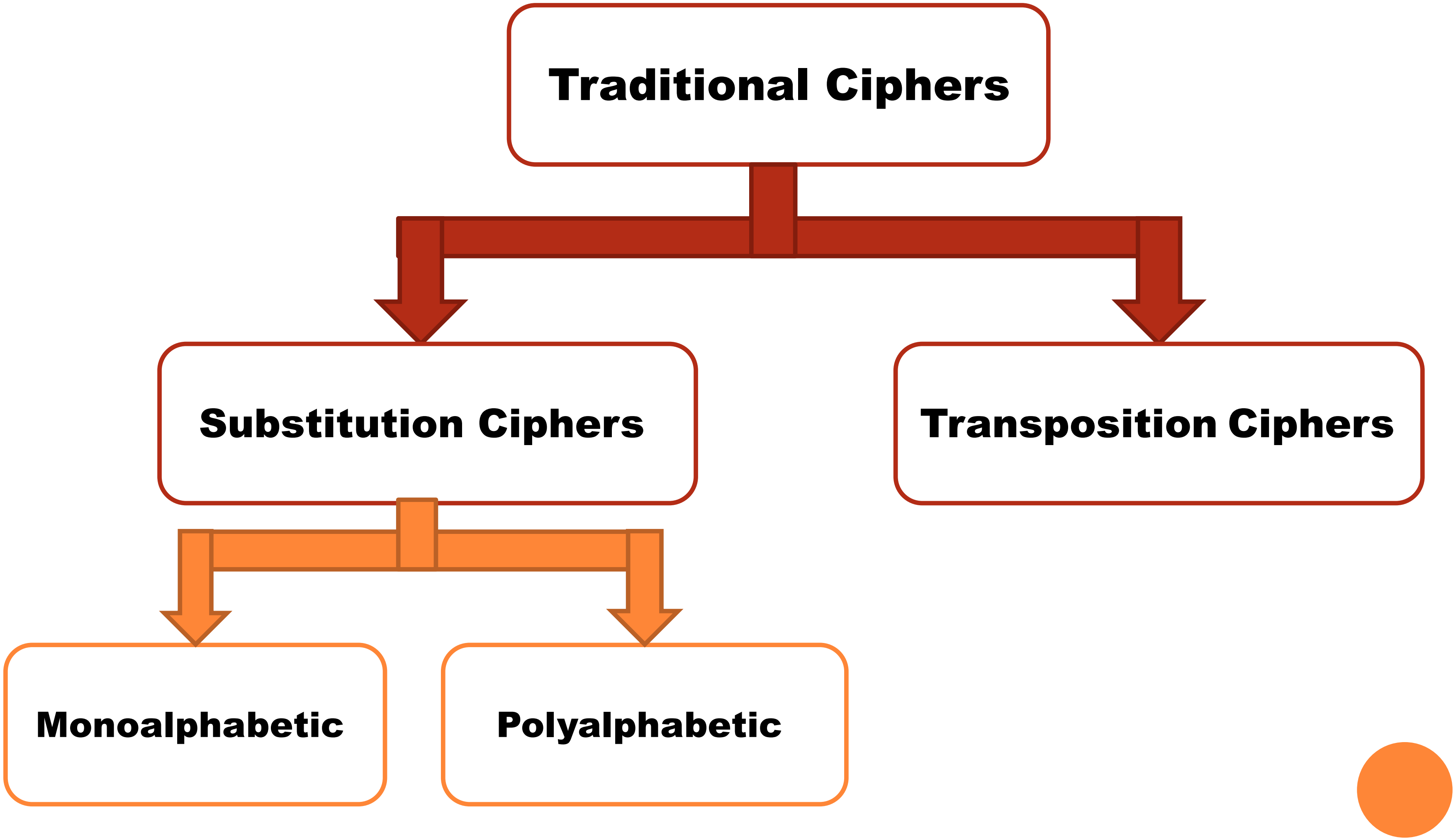


b. Asymmetric-key cryptography

SYMMETRIC-KEY CRYPTOGRAPHY

Symmetric-key cryptography started thousands of years ago when people needed to exchange secrets (for example, in a war). We still mainly use symmetric-key cryptography in our network security.

TRADITIONAL CIPHERS



Traditional Ciphers

Substitution Ciphers

Transposition Ciphers

Monoalphabetic

Polyalphabetic

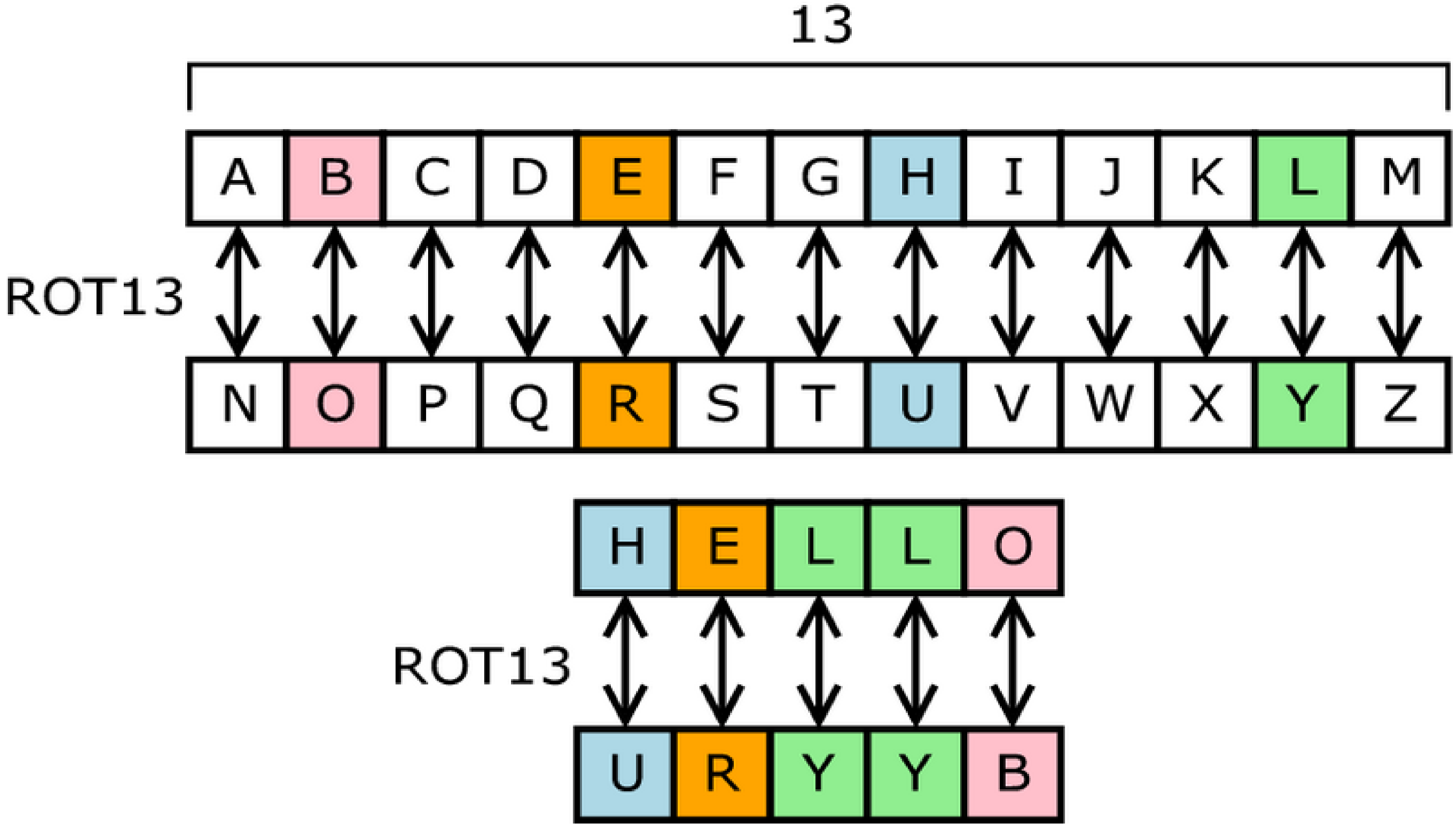
SUBSTITUTION CIPHER

A substitution cipher replaces each letter of alphabet in the plaintext by another letter or symbol or number, or several symbols to produce the ciphertext.

MONOALPHABETIC CIPHERS (SIMPLE SUBSTITUATION CIPHER)

A monoalphabetic substitution cipher, also known as a simple substitution cipher, relies on a fixed replacement structure. That is, the substitution is fixed for each letter of the alphabet. Thus, if "a" is encrypted to "R", then every time we see the letter "a" in the plaintext, we replace it with the letter "R" in the ciphertext.

ROT13



13

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

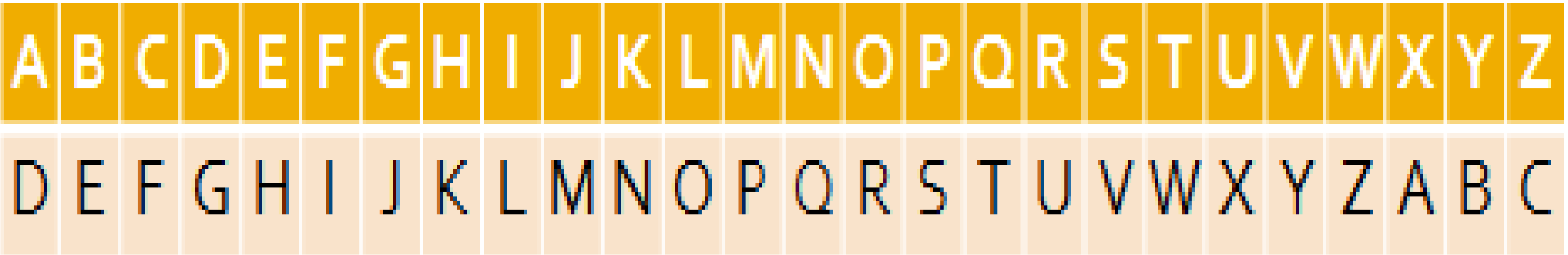
ROT13

H	E	L	L	O
U	R	Y	Y	B

ROT13

CAESAR CIPHER (SHIFT CIPHER)

Replaces each letter by 3rd letter on.

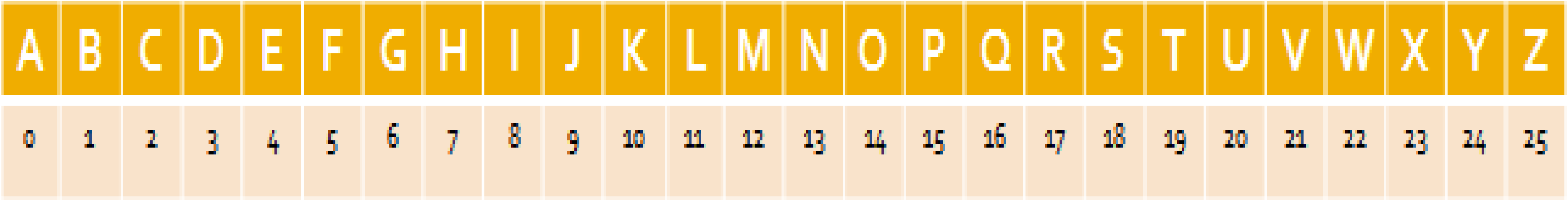


A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

H	E	L	L	O
K	H	O	O	R

CAESAR CIPHER

mathematically give each letter a number starting from 0 as shown:



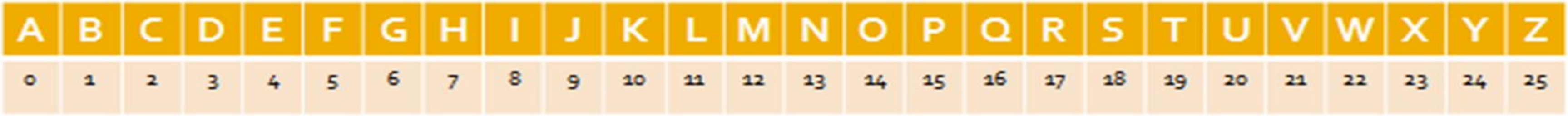
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Then we have Caesar cipher as:

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

This will give us the index of the encrypted letter. As you can see, the modulus is the total number of letters in the alphabet. For English, this modulus is 26.

CAESAR CIPHER



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

E(HELLO)=KHOOR **(K=3)**

C=E(H)=(P+K) mod 26=(7+3) mod 26=10 mod 26=10=K

C=E(E)=(P+K) mod 26=(4+3) mod 26= 7 mod 26=7=H

C=E(L)=(P+K) mod 26=(11+3) mod 26=14 mod 26=14=O

C=E(L)=(P+K) mod 26=(11+3) mod 26=14 mod 26=14=O

C=E(O)=(P+K) mod 26=(14+3) mod 26=17 mod 26=17=R

D(KHOOR)=HELLO

P=D(K)=(C-K) mod 26=(10-3) mod 26=7 mod 26=7=H

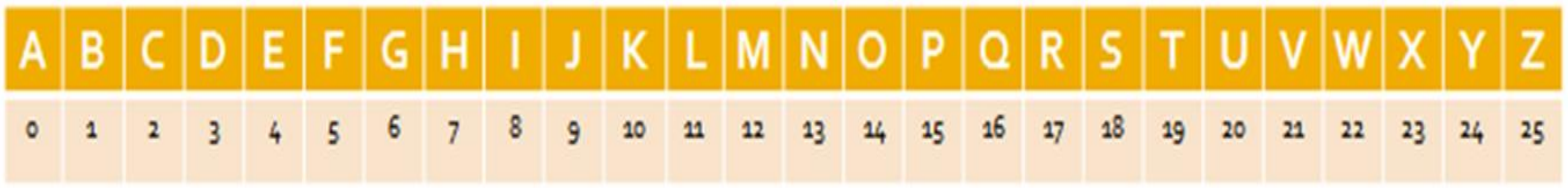
P=D(H)=(C-K) mod 26=(7-3) mod 26= 4 mod 26=4=E

P=D(O)=(C-K) mod 26=(14-3) mod 26=11 mod 26=11=L

P=D(O)=(C-K) mod 26=(14-3) mod 26=11 mod 26=11=L

P=D(R)=(C-K) mod 26=(17-3) mod 26=14 mod 26=14=O

CAESAR CIPHER



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

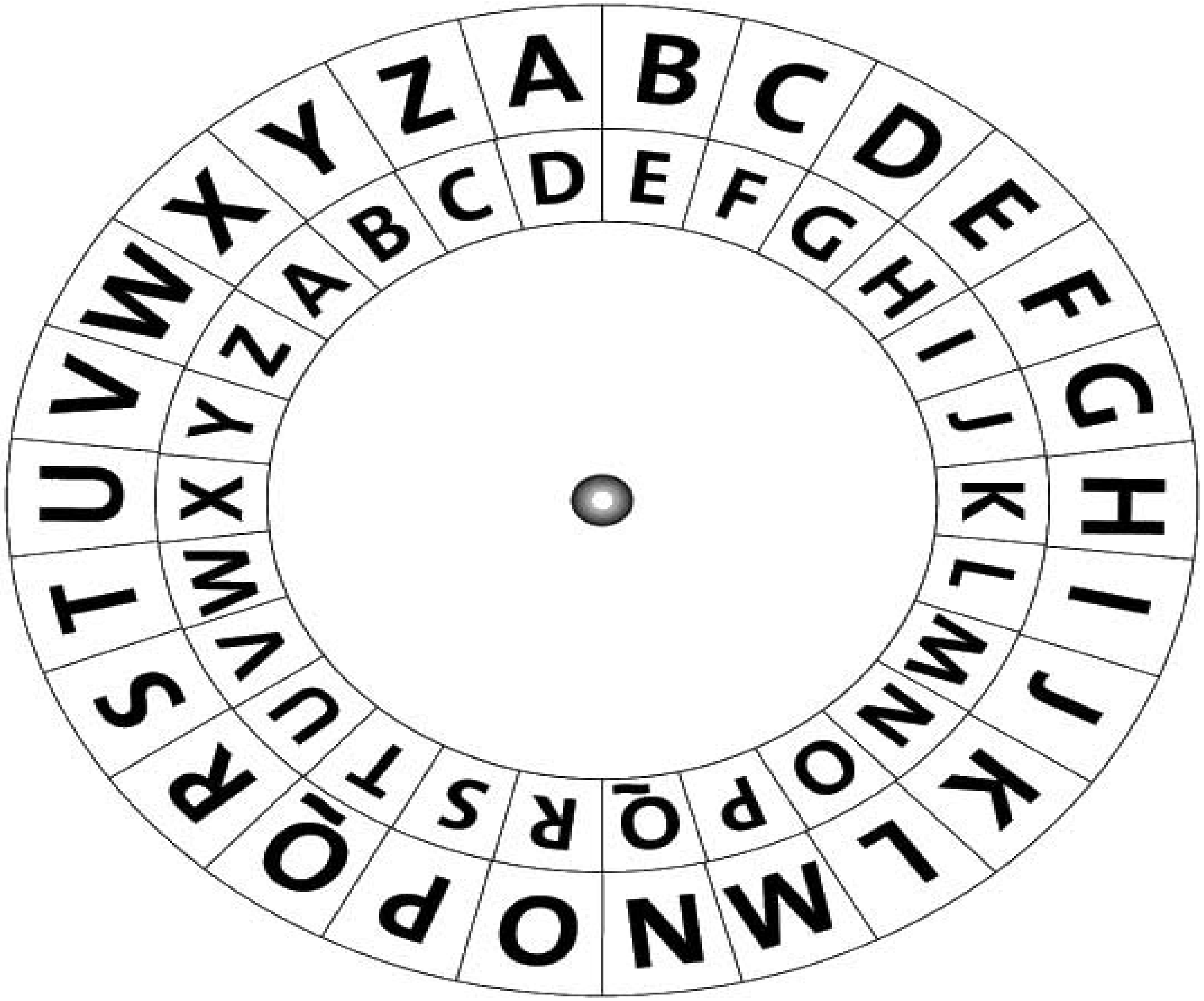
Plaintext: meet me after the toga party.

Ciphertext: PHHW PH DIWHU WKH WRJD SDUWB.

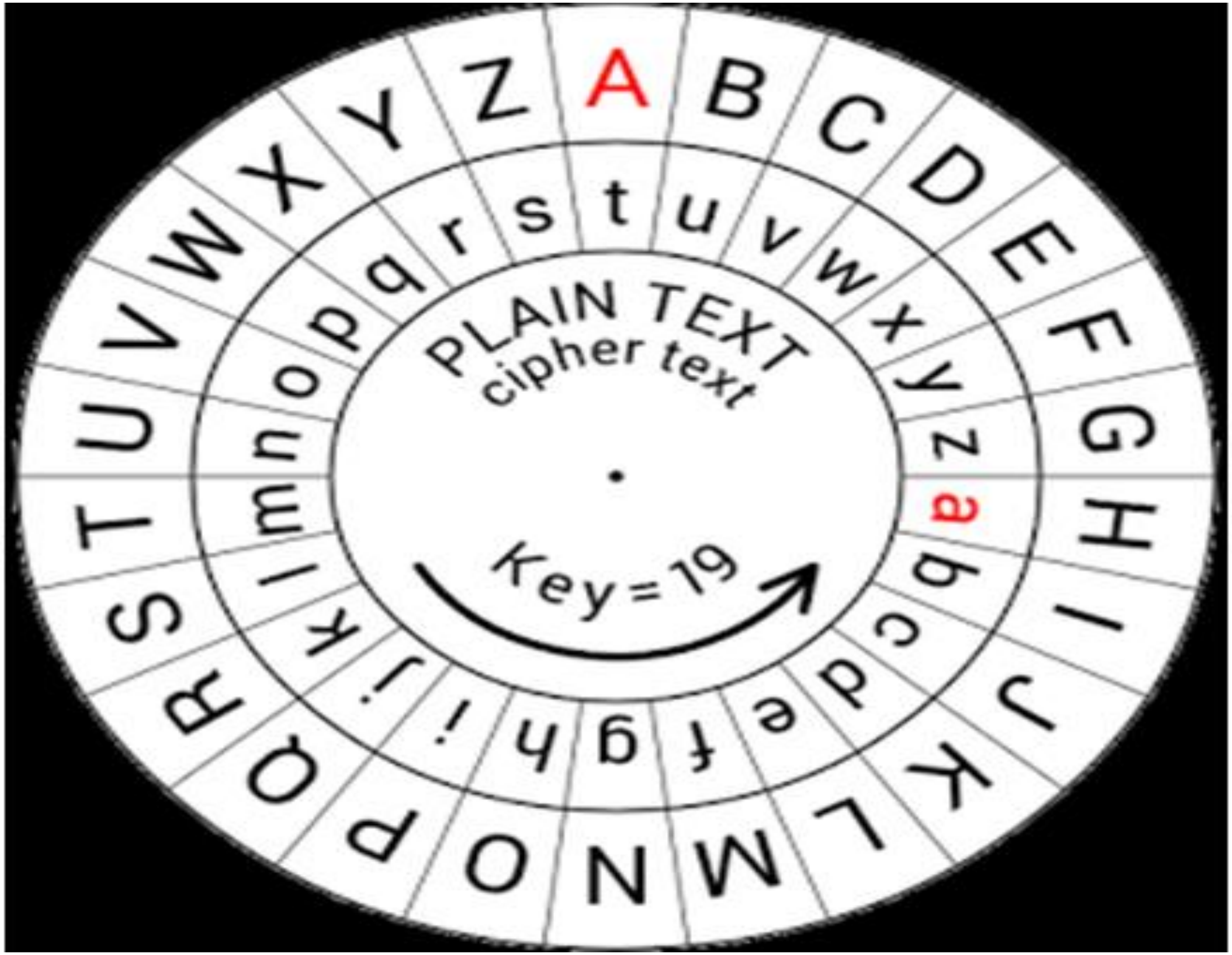
Plaintext: math is the best.

Ciphertext: 120197 818 1974 141819.

CAESAR CIPHER (K=3)


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
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

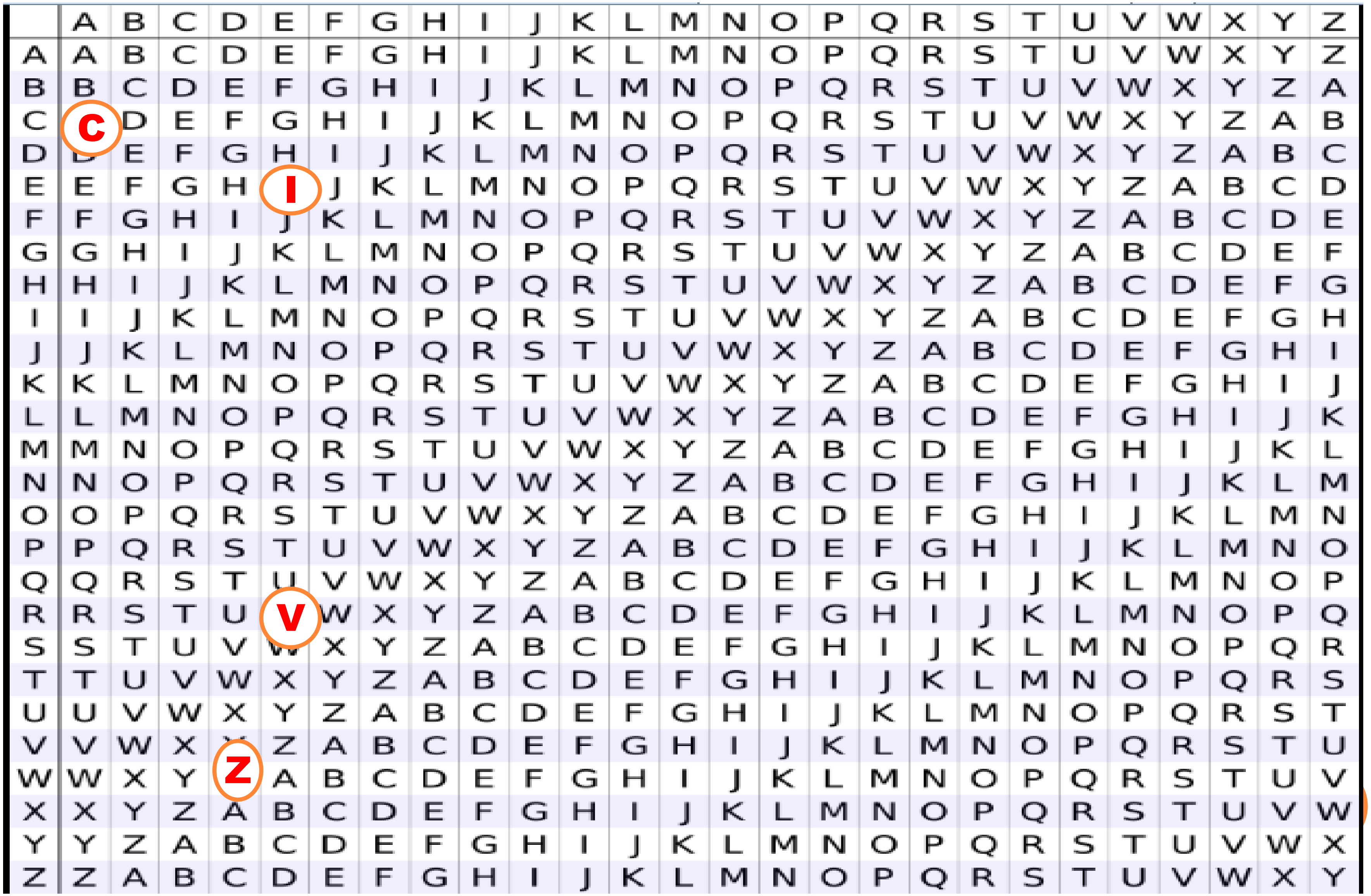
CAESAR CIPHER (K=19)


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
t u v w x y z a b c d e f g h i j k l m n o p q r s
PLAIN TEXT
cipher text
Key=19

POLYALPHABETIC CIPHERS

In a polyalphabetic cipher, multiple cipher alphabets are used. To facilitate encryption, all the alphabets are usually written out in a large table, traditionally called a tableau. Usually the tableau is 26 × 26, so that 26 full ciphertext alphabets are available. The method of filling the tableau, and of choosing which alphabet to use next, defines the particular polyalphabetic cipher.

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

VIGENERE CIPHER

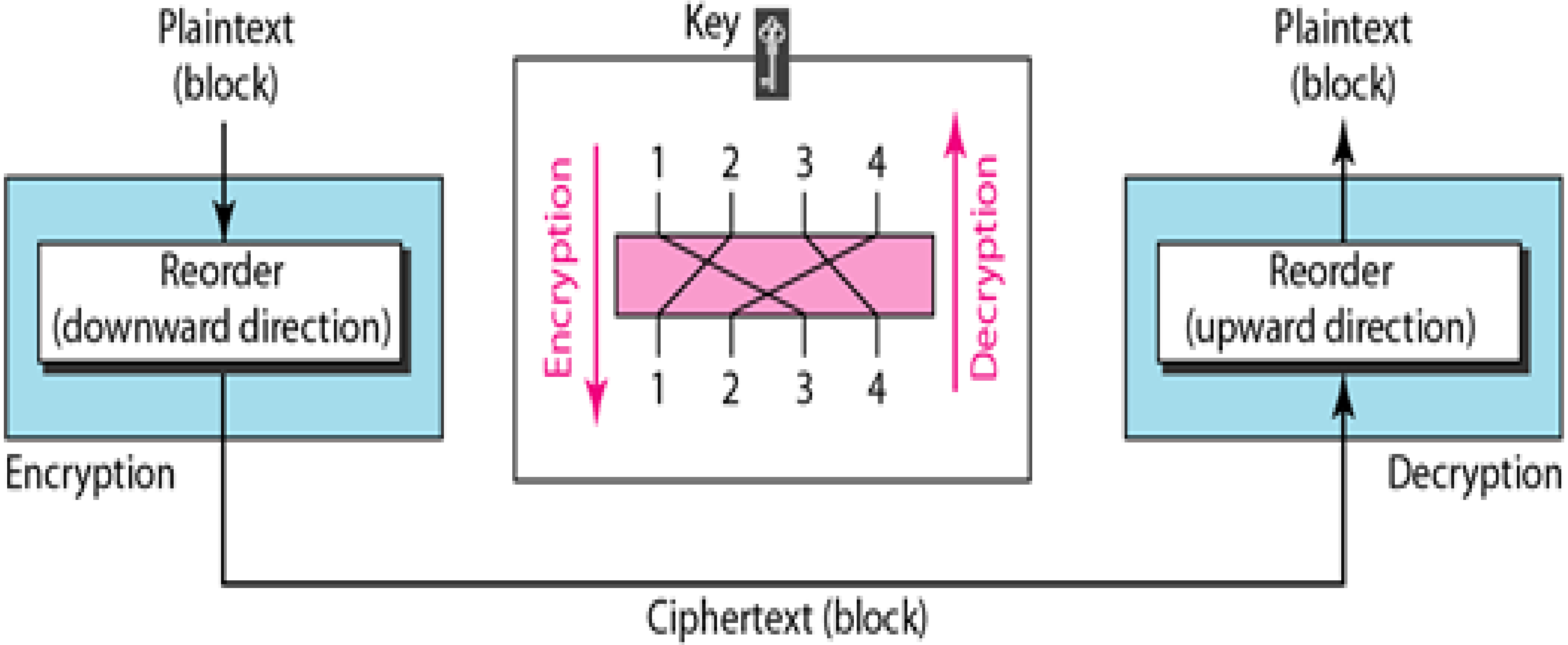
Key=deceptive

P=we are discovered save yourself

K	d	e	c	e	p	t	i	v	e	d	e	c	e	p	t	i	v	e	d	e	c	e	p	t	i	v	e
P	w	e	a	r	e	d	i	s	c	o	v	e	r	e	d	s	a	v	e	y	o	u	r	s	e	l	f
C	Z	I	C	V	T	W	Q	N	G	R	Z	G	V	T	W	A	V	Z	H	C	Q	Y	G	L	M	G	J

TRANPOSITION CIPHERS

A transposition cipher reorders (permutes) or rearranging the letter order without altering the actual letters used.



TRANPOSITION CIPHERS

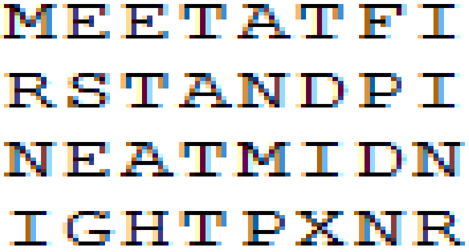
Encrypt the message “HELLO MY DEAR,” using transposition cipher.

We first remove the spaces in the message. We then divide the text into blocks of four characters. We add a bogus character Z at the end of the third block. The result is HELL OMYD EARZ. We create a three-block ciphertext ELHLMDOYAZER.

TRANPOSITION CIPHERS

Encrypt the message "Meet at First and Pine at midnight" using rows 8 characters long.

We write the message in rows of 8 characters each. Nonsense characters are added to the end to complete the last row.



```
MEETATFI
RSTANDPI
NEATMIDN
IGHTPXNR
```

We could then encode the message by recording down the columns. The first column, reading down, would be MRNI. All together, the encoded message would be MRNIESEGETAHTATT ANMPTDIXFPDNIINR.

TRANPOSITION CIPHERS

Decrypt the message "CEE IAI MNL NOG LTR VMH NW" using the method above with a table with rows of 5 characters.

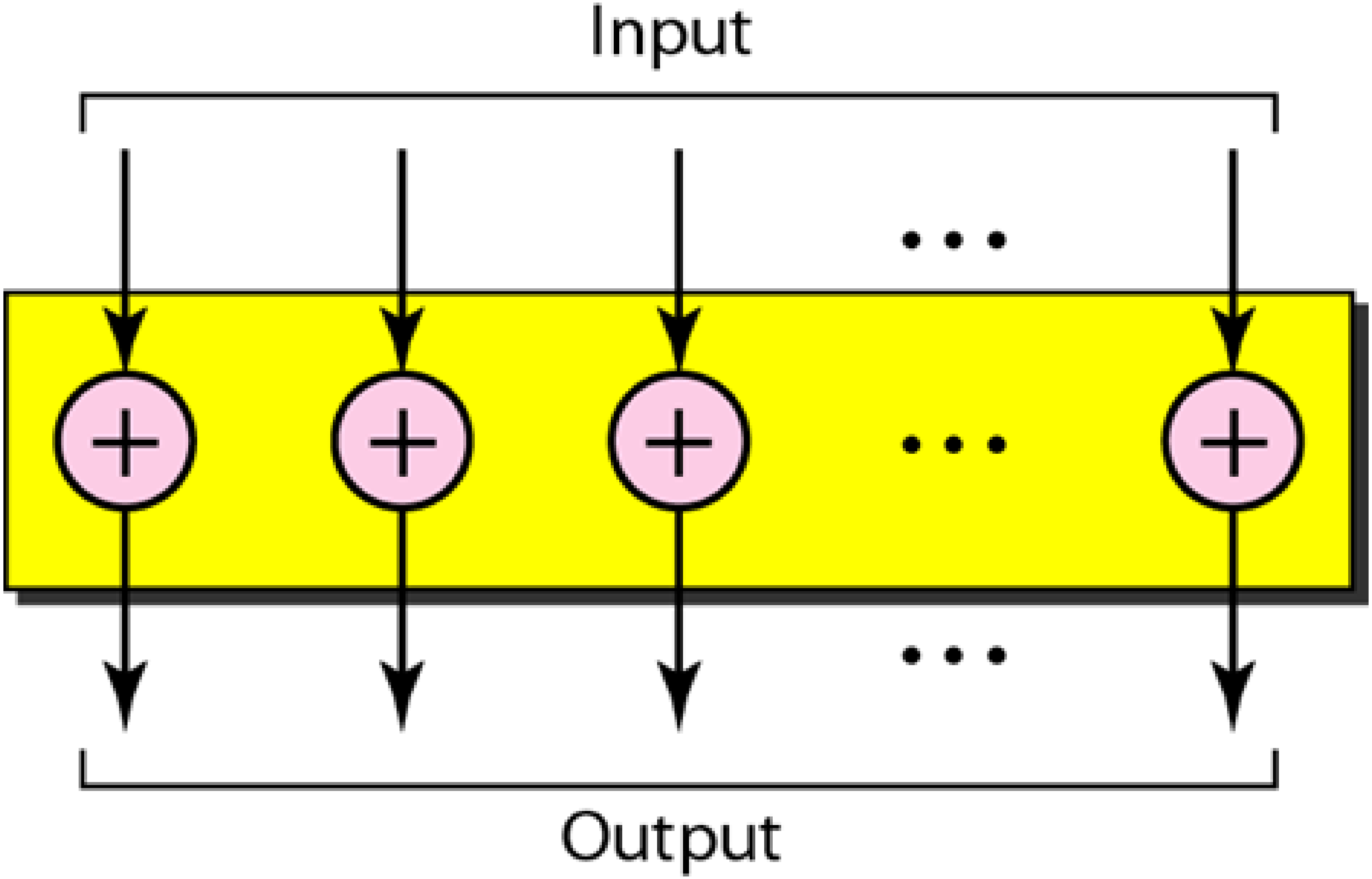
Since there are total of 20 characters and each row should have 5 characters, then there will be 20/5 = 4 rows.

We start writing, putting the first 4 letters, CEEI, down the first column.

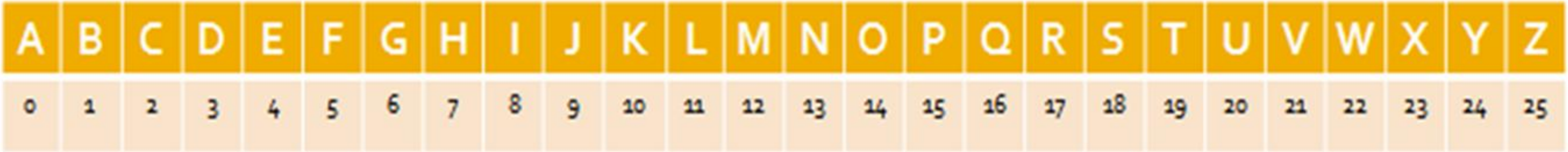
CALLM
EINTH
EMORN
INGVW

We can now read the message: CALL ME IN THE MORNING VW. The VW is likely nonsense characters used to fill out the message.

XOR CIPHER



XOR CIPHER



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

Plaintext	H	E	L	L	O
P(Decimal)	7	4	11	11	14
P(Binary)	0111	0100	1011	1011	1110
Key (C)	0010	0010	0010	0010	0010
XOR	0101	0110	1001	1001	1100
C(Decimal)	5	6	9	9	12
Ciphertext	F	G	J	J	M

thank you