Cloud Security

M.Sc. Sem III - 2022

Dr Mukti Padhya

Assistant Professor

NFSU, Gandhinagar

Encryption

- Why Encryption
  - To achieve Confidentiality
  - Protection against unauthorized disclosure of information.

- What is Encryption?
- Types

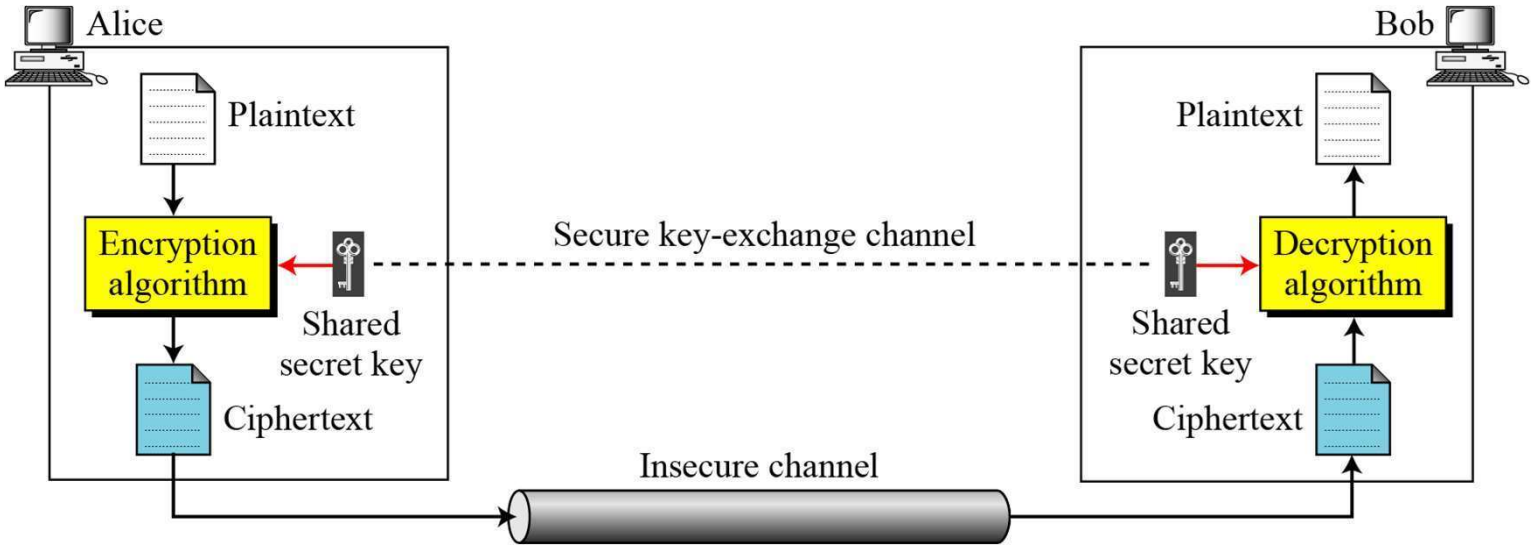
Encryption

- can characterize Encryption system by:
  - ❖ type of encryption operations used
    - ➢ Substitution (each element of PT is mapped into another element)
    - ➢ Transposition (elements in PT are rearranged)
    - ➢ Product (combination of both)
  - ❖ number of keys used
    - ➢ single-key or private or symmetric
    - ➢ two-key or public or asymmetric
  - ❖ way in which plaintext is processed
    - ➢ block
    - ➢ stream

Some Basic Terminology

- **plaintext** - original message
- **ciphertext** - coded message
- **cipher** - algorithm for transforming plaintext to ciphertext
- **key** - info used in cipher known only to sender/receiver
- **encipher (encrypt)** - converting plaintext to ciphertext
- **decipher (decrypt)** - recovering ciphertext from plaintext
- **cryptography** - study of encryption principles/methods
- **cryptanalysis (codebreaking)** - study of principles/ methods of deciphering ciphertext *without* knowing key

symmetric-key cipher

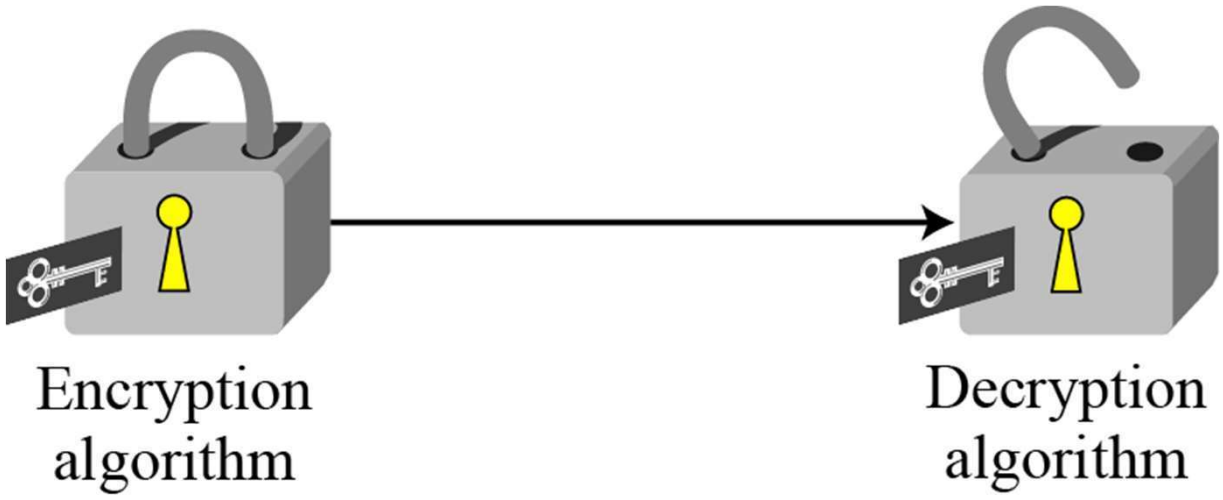


If P is the plaintext, C is the ciphertext, and K is the key,

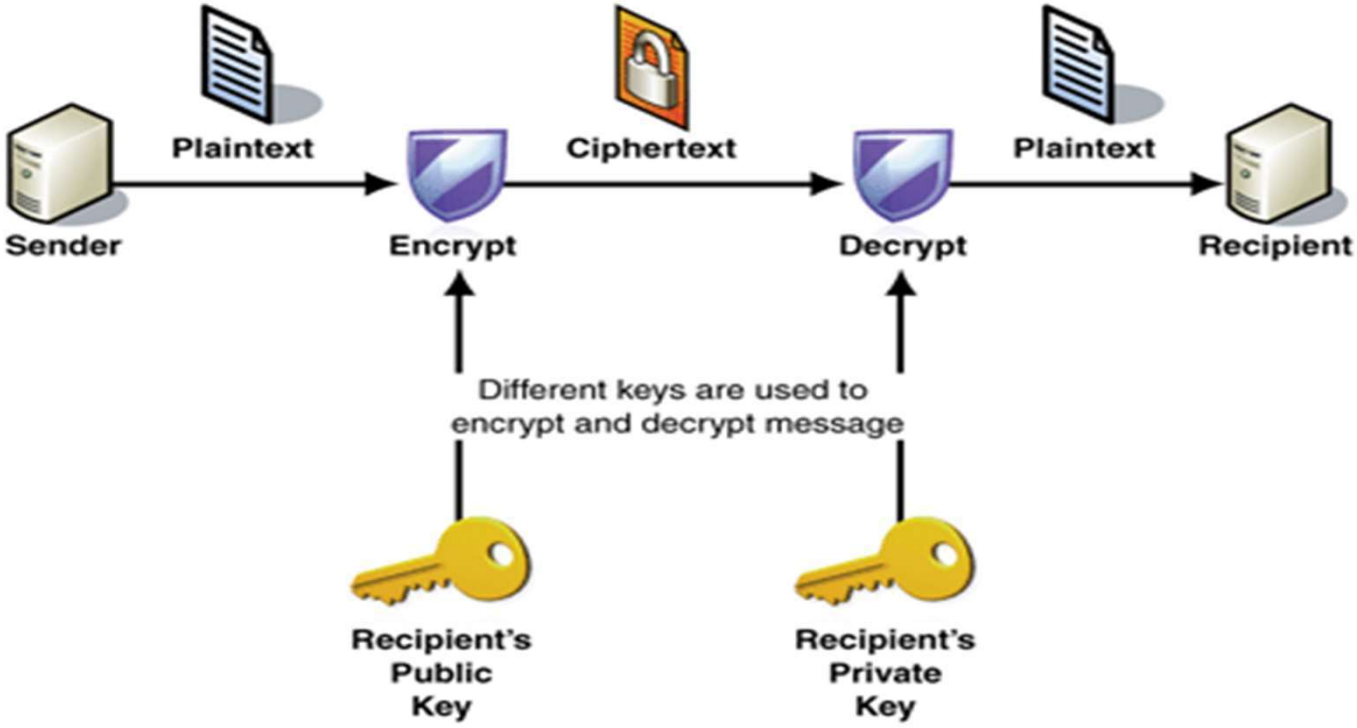
Encryption: $C = E_k(P)$ Decryption: $P = D_k(C)$

In which, $D_k(E_k(x)) = E_k(D_k(x)) = x$

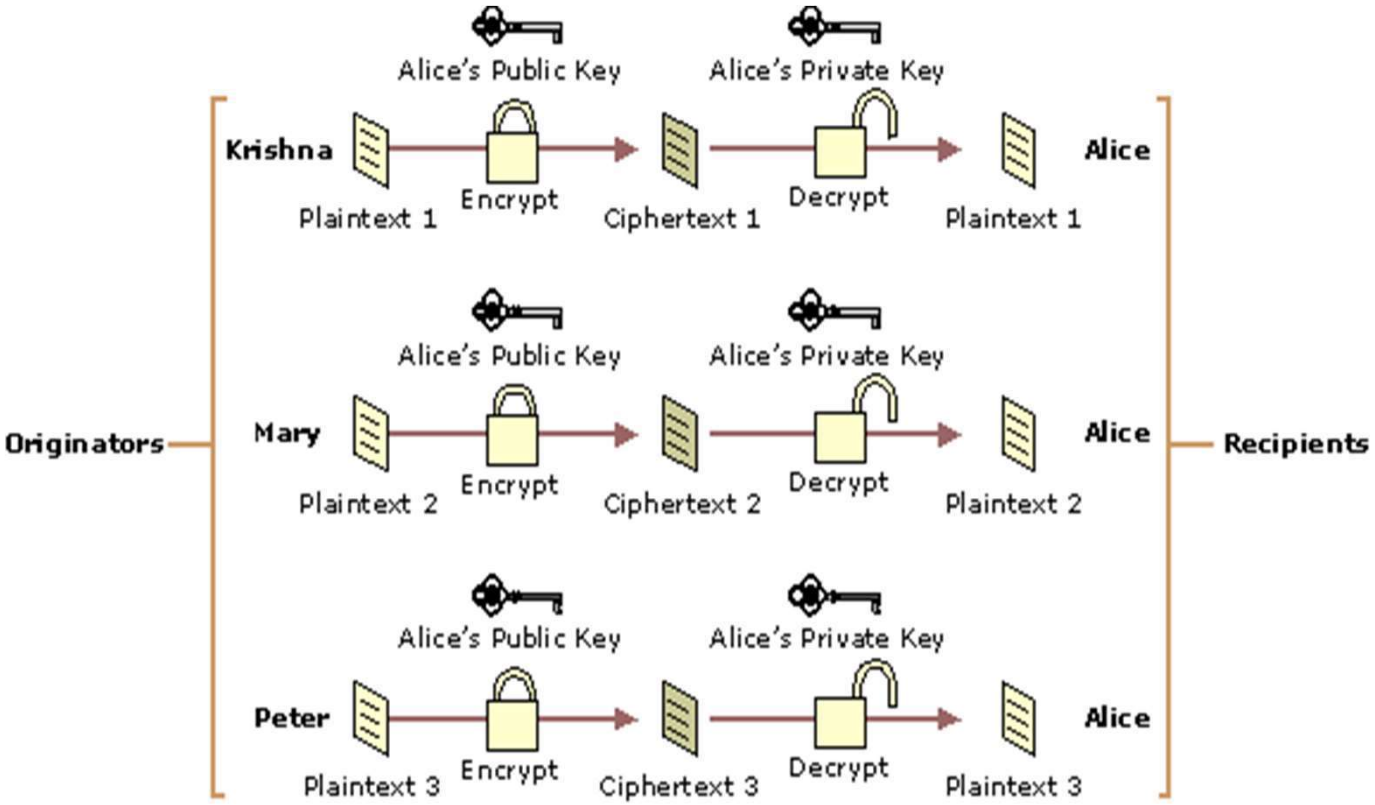
Locking and unlocking
with the same key



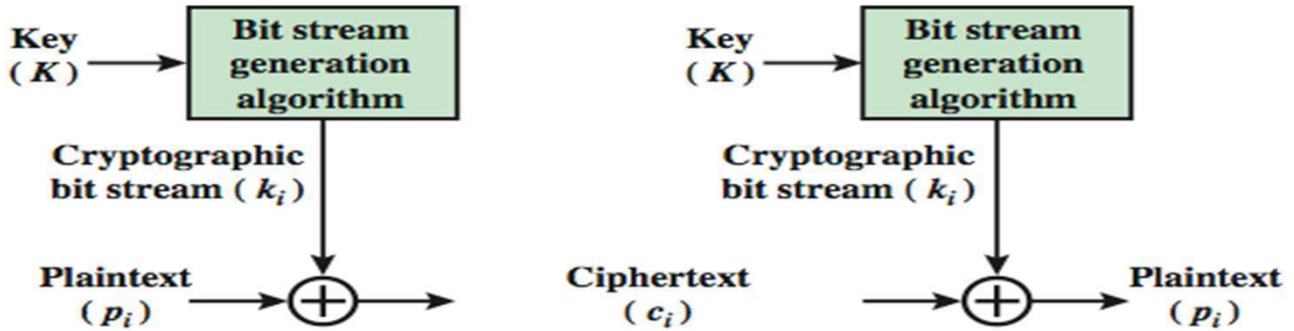
Asymmetric-key Cipher



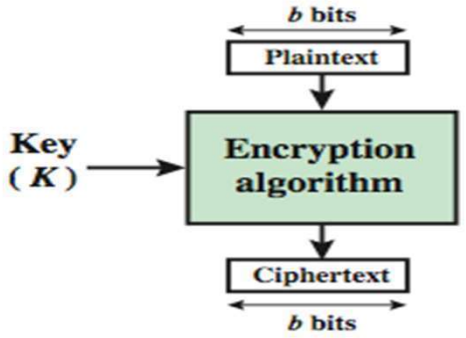
Asymmetric-key Cipher



Block Vs Stream Ciphers



(a) Stream Cipher Using Algorithmic Bit Stream Generator



(b) Block Cipher

Block vs Stream Ciphers

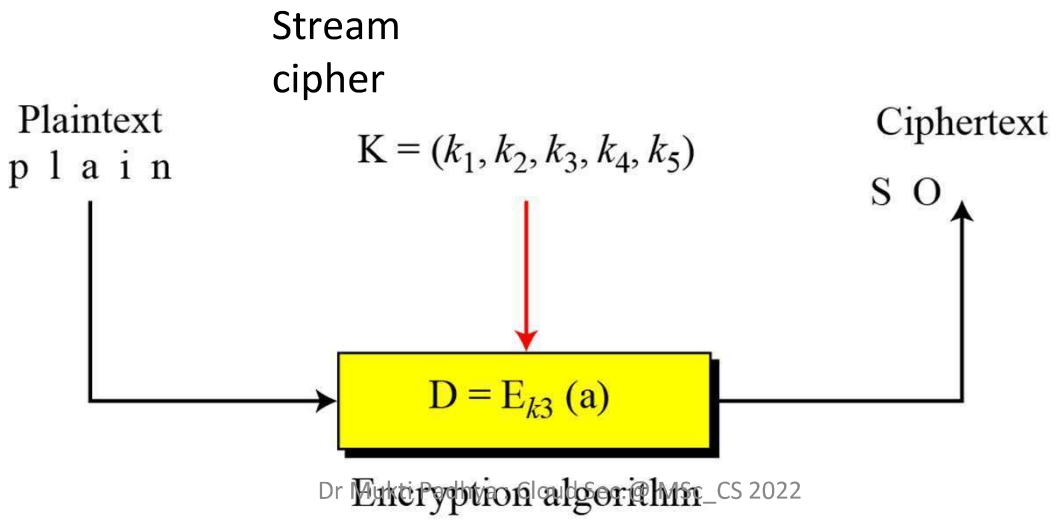
- block ciphers process messages in blocks, each of which is then en/decrypted
  - like a substitution on very big characters
  - 64-bits or more
- stream ciphers process messages a bit or byte at a time when en/decrypting
- many current ciphers are block ciphers
  - broader range of applications

Stream Ciphers

Call the plaintext stream P, the ciphertext stream C, and the key stream K.

$$P = P_1P_2P_3, \ldots \qquad C = C_1C_2C_3, \ldots \qquad K = (k_1, k_2, k_3, \ldots)$$

$$C_1 = E_{k1}(P_1) \qquad C_2 = E_{k2}(P_2) \qquad C_3 = E_{k3}(P_3) \ldots$$



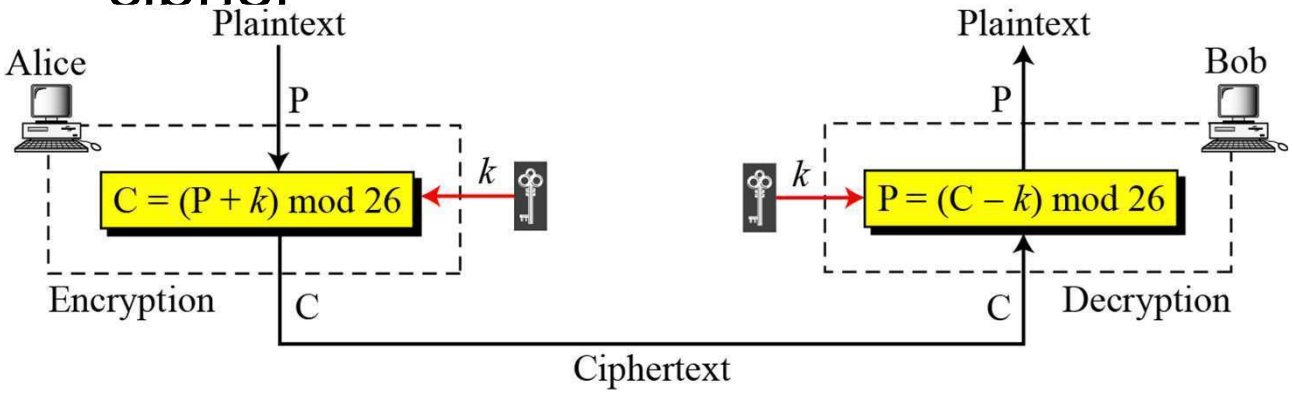
- Additive ciphers can be categorized as stream ciphers in which the key stream is the repeated value of the key. In other words, the key stream is considered as a predetermined stream of keys or K = (k, k, …, k).

- The monoalphabetic substitution ciphers are also stream ciphers.

- However, each value of the key stream in this case is the mapping of the current plaintext character to the corresponding ciphertext character in the mapping table.

Continued

Additive cipher



The simplest monoalphabetic cipher is the additive cipher. This cipher is sometimes called a shift cipher and sometimes a Caesar cipher, but the term additive cipher better reveals its mathematical nature.

When the cipher is additive, the plaintext, ciphertext, and key are integers in Z_{26}.

Continued

Example

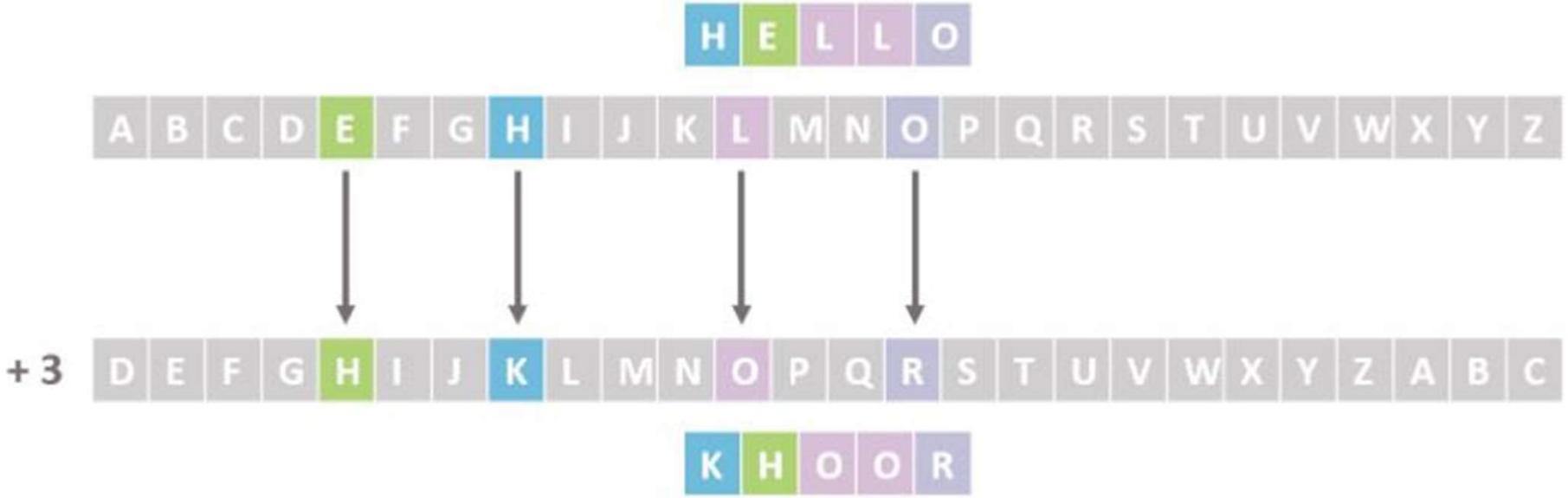
Use the additive cipher with key = 15 to encrypt the message “hello”.

a-0, b-1,c-2……,z-25

Solution

We apply the encryption algorithm to the plaintext, character by character:

Plaintext: h → 07	Encryption: (07 + 15) mod 26	Ciphertext: 22 → W
Plaintext: e → 04	Encryption: (04 + 15) mod 26	Ciphertext: 19 → T
Plaintext: l → 11	Encryption: (11 + 15) mod 26	Ciphertext: 00 → A
Plaintext: l → 11	Encryption: (11 + 15) mod 26	Ciphertext: 00 → A
Plaintext: o → 14	Encryption: (14 + 15) mod 26	Ciphertext: 03 → D


H E L L O
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
+3
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
K H O O R

- mathematically give each letter a number

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 have Caesar cipher as:

$c = E(p) = (p + k) \bmod (26)$

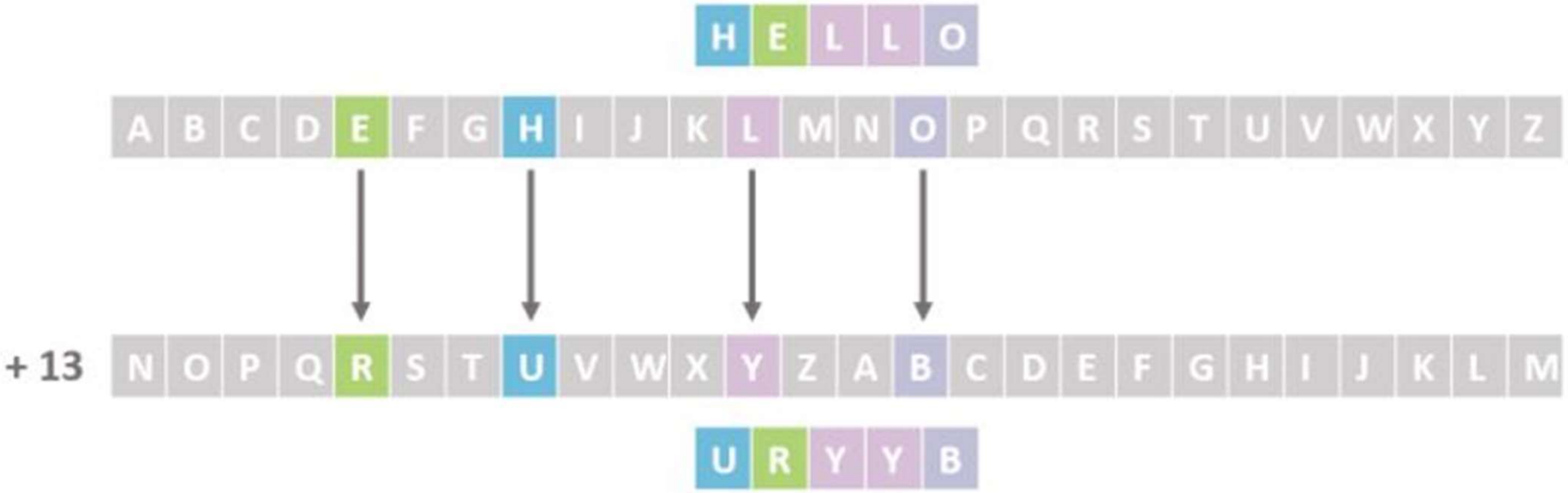
$p = D(c) = (c - k) \bmod (26)$

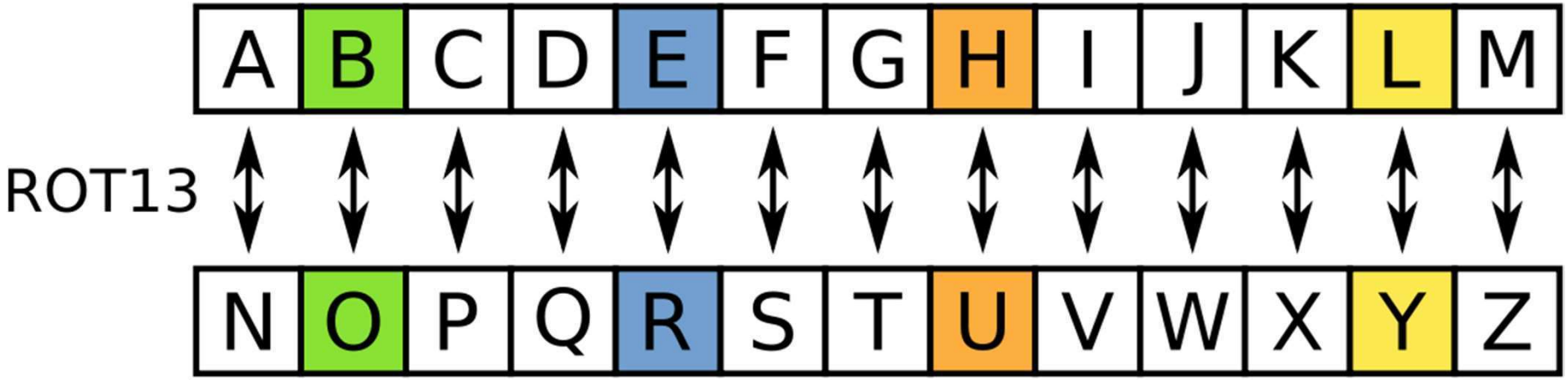
Plaintext : HELLO Key =13 Ciphertext : ?

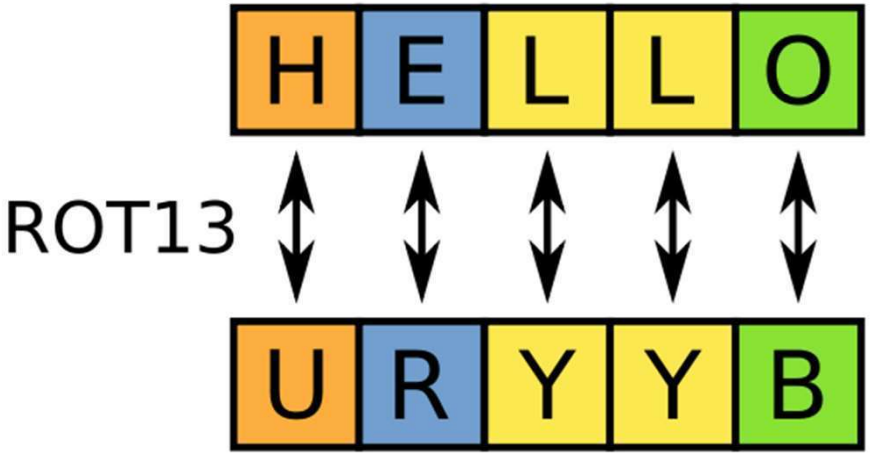
Note: mod operation x mod n then if x > n and n can divide x so output of mod is ZERO

If x < n then output will be x itself

If x is negative then output will be x+n


H E L L O
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
+ 13
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
U R Y Y B


A B C D E F G H I J K L M
ROT13
N O P Q R S T U V W X Y Z


H E L L O
ROT13
U R Y Y B

Continued

Monoalphabetic Substitution Cipher

- Because additive, multiplicative, and affine ciphers have small key domains, they are very vulnerable to brute-force attack.
- A better solution is to create a mapping between each plaintext character and the corresponding ciphertext character. Alice and Bob can agree on a table showing the mapping for each character.

An example key for monoalphabetic substitution cipher

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

Continued

Example
encrypt the message

this message is easy to encrypt but hard to find the key

The ciphertext is

ICFVQRVVNEFVRNVSIYRGAHSLIOJICNHTIYBFGTICRXRS

Vigenere ciphers are also stream ciphers according to the definition.

In this case, the key stream is a repetition of m values, where m is the size of the keyword.

In other words,

$$K = (k_1, k_2, \ldots k_m, k_1, k_2, \ldots k_m, \ldots)$$

Polyalphabetic Ciphers

In polyalphabetic substitution, each occurrence of a character may have a different substitute. The relationship between a character in the plaintext to a character in the ciphertext is one-to-many.

Autokey Cipher

$P = P_1P_2P_3 \ldots$ $C = C_1C_2C_3 \ldots$ $k = (k_1, P_1, P_2, \ldots)$

Encryption: $C_i = (P_i + k_i) \bmod 26$ Decryption: $P_i = (C_i - k_i) \bmod 26$

Continued

Vigenere Cipher

$P = P_1P_2P_3 \ldots \qquad C = C_1C_2C_3 \ldots \qquad K = [(k_1, k_2, \ldots, k_m), (k_1, k_2, \ldots, k_m), \ldots]$

Encryption: $C_i = P_i + k_i$ Decryption: $P_i = C_i - k_i$

Example

We can encrypt the message “She is listening” using the 6-character keyword “PASCAL”.

Continued

Example

Let us see how we can encrypt the message “She is listening” using the 6-character keyword “PASCAL”. The initial key stream is (15, 0, 18, 2, 0, 11). The key stream is the repetition of this initial key stream (as many times as needed).

Plaintext:	s	h	e	i	s	l	i	s	t	e	n	i	n	g
P’s values:	18	07	04	08	18	11	08	18	19	04	13	08	13	06
Key stream:	***15***	***00***	***18***	***02***	***00***	***11***	***15***	***00***	***18***	***02***	***00***	***11***	***15***	***00***
C’s values:	**07**	**07**	**22**	**10**	**18**	**22**	**23**	**18**	**11**	**6**	**13**	**19**	**02**	**06**
Ciphertext:	**H**	**H**	**W**	**K**	**S**	**W**	**X**	**S**	**L**	**G**	**N**	**T**	**C**	**G**

Ciphertext : DATG

Key : 19

DECRYPTION

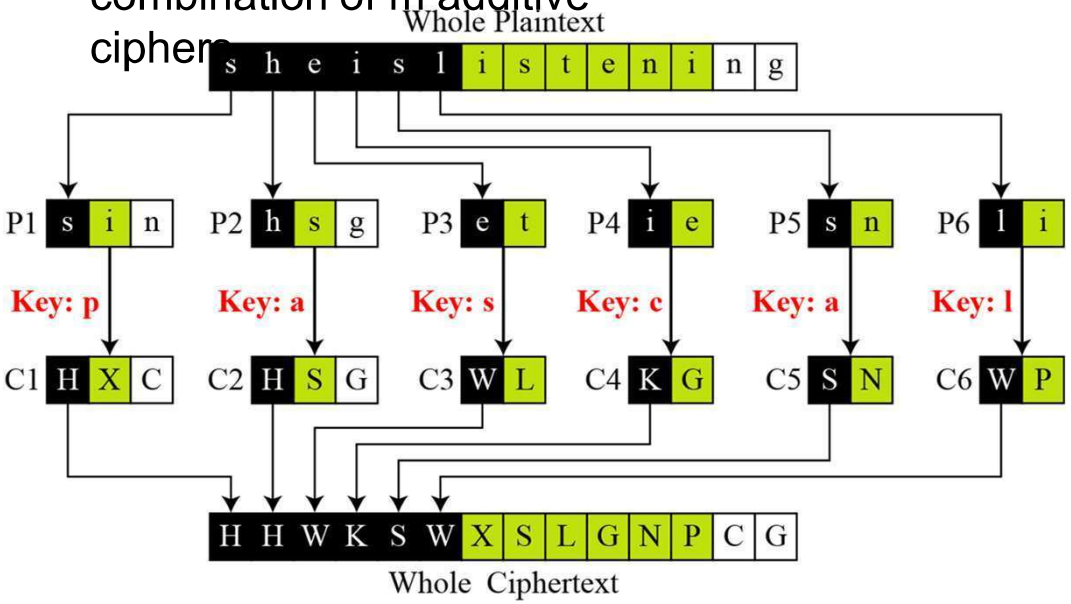
	D	A	T	G	
	3	0	19	6	
-	19	19	19	19	
(	-16	-19	0	-13	) mod 26
	10	7	0	13	
	K	H	A	N	

Continued

Example

Vigenere cipher can be seen as combinations of m additive ciphers.

A Vigenere cipher as a combination of m additive ciphers



Continued

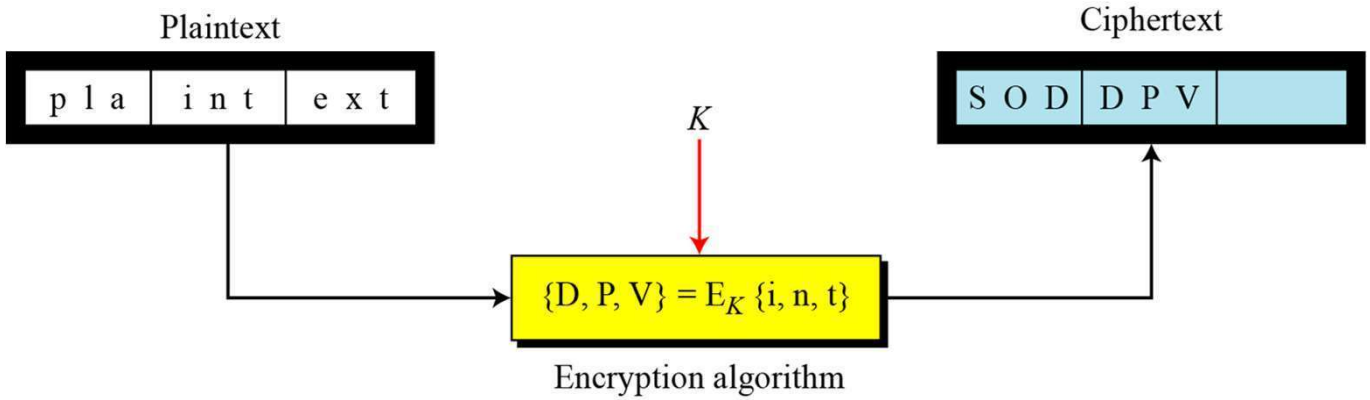
A Vigenere Table

	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	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

Block Ciphers

- In a block cipher, a group of plaintext symbols of size m (m > 1) are encrypted together creating a group of ciphertext of the same size.

- A single key is used to encrypt the whole block even if the key is made of multiple values.



- Playfair ciphers are block ciphers. The size of the block is m = 2. Two characters are encrypted together.

- Hill ciphers are block ciphers. A block of plaintext, of size 2 or more is encrypted together using a single key (a matrix).

- Although the key is made of m × m values, it is considered as a single key.

Playfair Cipher

- not even the large number of keys in a monoalphabetic cipher provides security
- one approach to improving security was to encrypt multiple letters
- the **Playfair Cipher** is an example
- invented by Charles Wheatstone in 1854, but named after his friend Baron Playfair

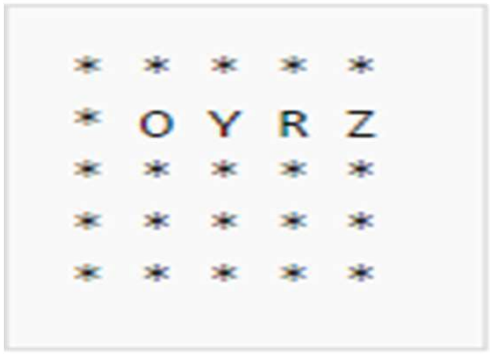
Playfair Key Matrix

- a 5X5 matrix of letters based on a keyword
- fill in letters of keyword (without duplicates)
- fill rest of matrix with other letters
- eg. using the keyword MONARCHY

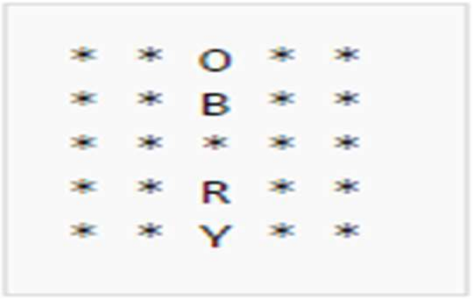
M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

Encrypting and Decrypting

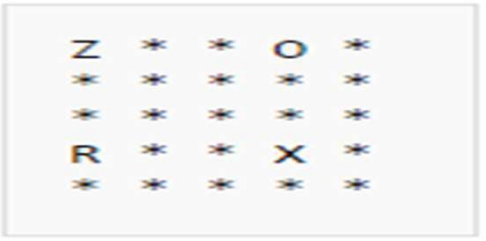
- plaintext is encrypted two letters at a time
  - if a pair is a repeated letter, insert filler like 'X
  - ABC AB CX



Hence, OR -> YZ



Hence, OR -> BY



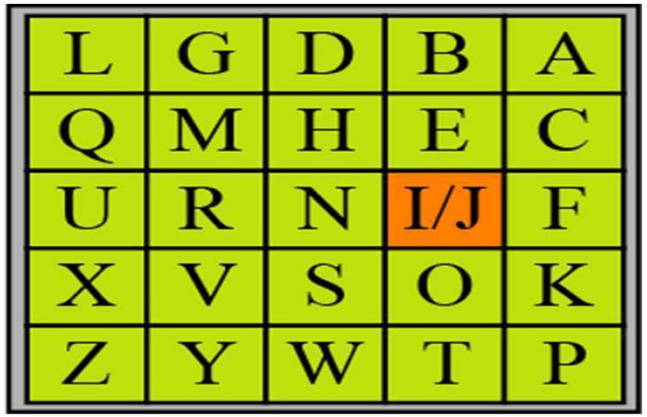
Hence, OR -> ZX

Playfair Cipher

Example

An example of a secret key in the Playfair cipher

Secret Key =



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

encrypt the plaintext “hello”

he → EC lx → QZ lo → BX

Plaintext: hello Ciphertext: ECQZBX

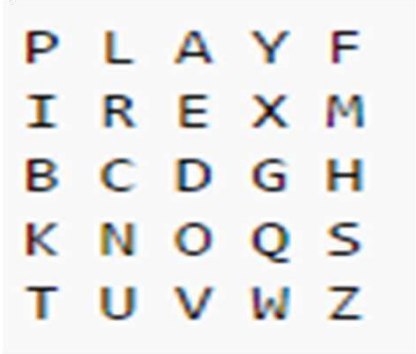
Example

- Key: playfair example

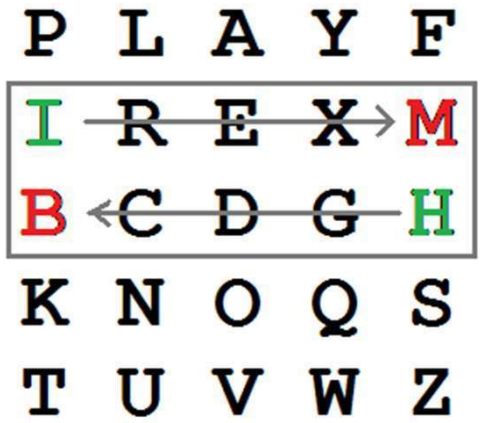
- Message "Hide the gold in the tree stump“
- (note the null "X" used to separate the repeated "E"s)

Example

- Key: playfair example 007



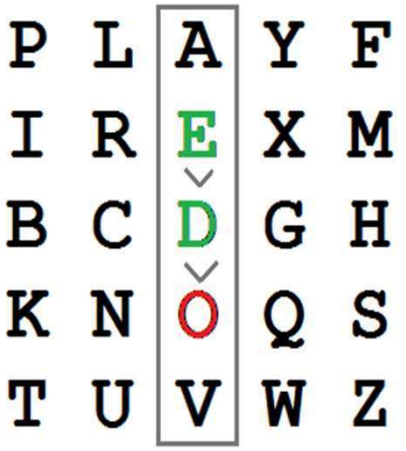
- Message "Hide the gold in the tree stump“
- (note the null "X" used to separate the repeated "E"s)



HI

Shape: Rectangle
Rule: Pick Same Rows, Opposite Corners

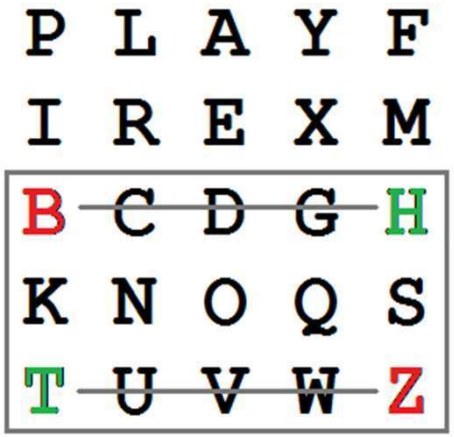
BM



DE

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

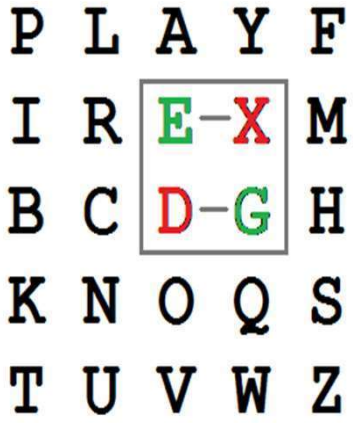
OD



TH

Shape: Rectangle
Rule: Pick Same Rows, Opposite Corners

ZB

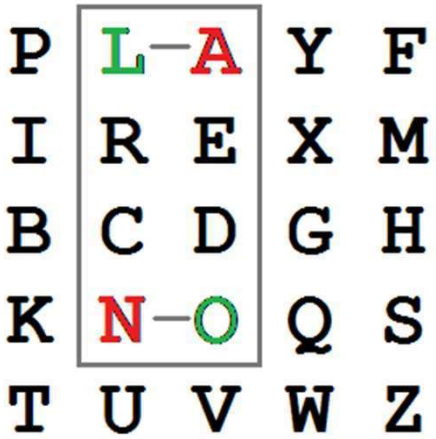


EG

Shape: Rectangle
Rule: Pick Same Rows, Opposite Corners

XD

- 6. The pair DI forms a rectangle, replace it with BE
- 7. The pair NT forms a rectangle, replace it with KU
- 8. The pair HE forms a rectangle, replace it with DM
- 9. The pair TR forms a rectangle, replace it with UI



OL

Shape: Rectangle
Rule: Pick Same Rows,
Opposite Corners

NA

- 11. The pair ES forms a rectangle, replace it with MO
- 12. The pair TU is in a row, replace it with UV
- 13. The pair MP forms a rectangle, replace it with IF

- Ciphertext: BM OD ZB XD NA BE KU DM UI XM MO UV IF