The Islamic University
College of Technical Engineering
Department of Computer Technical Engineering

Fourth Stage

Security

Lecture 3

Asst. Lec. Yousif Samer Mudhafar

Email: yousif.samir19@gmail.com

Lecture objectives

The student will recognize the following objectives :

1. **Encryption and Decryption using Vigenere Cipher.**
2. **Encryption and Decryption using Autokey Cipher.**

Vigenere Cipher

The best known and one of the simplest, polyalphabetic ciphers is the Vigenere cipher. In this scheme, the set of related monoalphabetic substitution rules consists of the 26 Caesar ciphers with shifts of 0 through 25. Each cipher is denoted by a Key letter, which is the Ciphertext letter that substitutes for the plaintext latter.

Encryption equation will be : $C_i = (P_i + K_i) \; mod \; 26$

Decryption equation will be : $P_i = (C_i - K_i) \; mod \; 26$

Where $P_i = P_1, P_2, P_3, \ldots\ldots\ldots\ldots\ldots P_p$

$C_i = C_1, C_2, C_3, \ldots\ldots\ldots\ldots\ldots C_c$

$K_i = K_1, K_2, K_3, \ldots\ldots\ldots\ldots\ldots K_k$

Vigenere Cipher

Alice

Sender

Bob

Receiver

$C_i=(P_i + K_i) \bmod 26$ ← K

Encryption

K → $P_i=(C_i - K_i) \bmod 26$

Decryption

Cipher text

Example 1

Encrypt and decrypt for the Plaintext "**She is Listening**" by using **Vigenere Cipher** by using the Key = **pascal**

Ans:-

1. Encryption Algorithm

$$C_i = (P_i + K_i)\ mod\ 26$$

Plaintext	s	h	e	i	s	l	i	s	t	e	n	i	n	g
Plaintext Value	18	7	4	8	18	11	8	18	19	4	13	8	13	6
Key Stream	p	a	s	c	a	l	p	a	s	c	a	l	p	a
Key Value	15	0	18	2	0	11	15	0	18	2	0	11	15	0
$C_i = (P_i + K_i)\ mod\ 26$	7	7	22	10	18	22	23	18	11	6	13	19	2	6
Cipher text	H	H	W	K	S	W	X	S	L	G	N	T	C	G

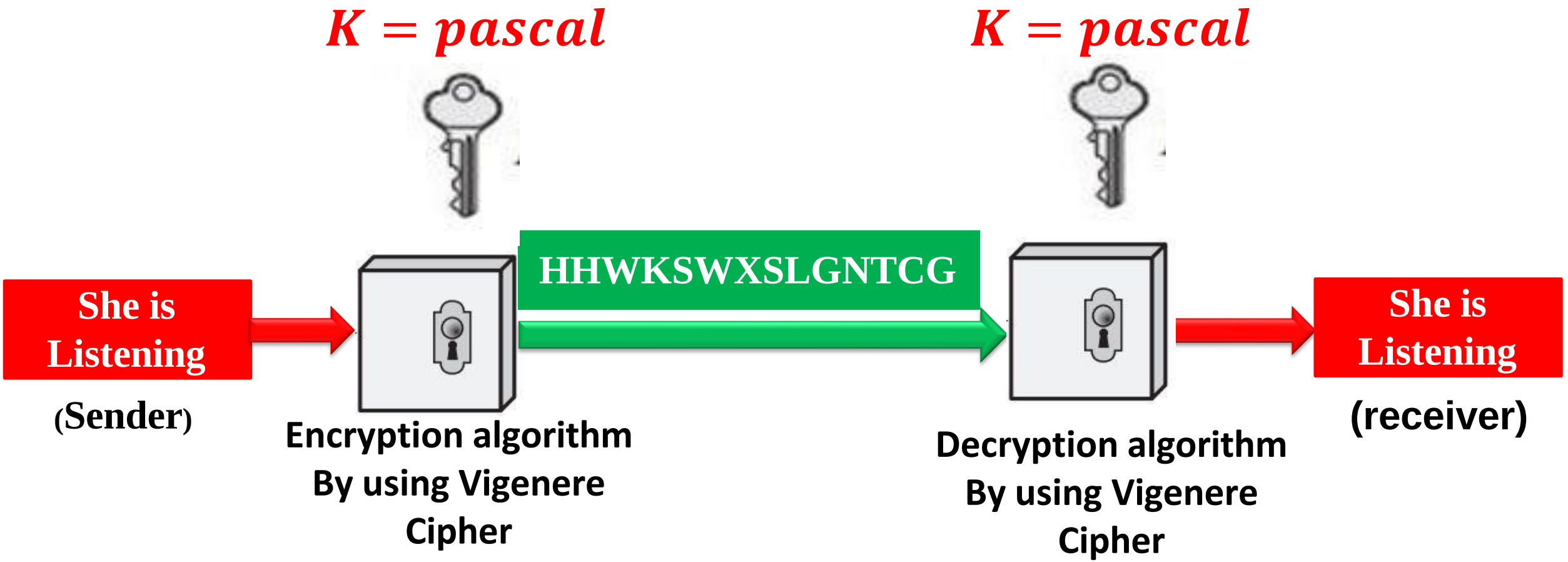
The **Cipher text** is "**HHWKSWXSLGNTCG**"

2. Decryption Algorithm

$$P_i = (C_i - K_i) \bmod 26$$

Cipher text	H	H	W	K	S	W	X	S	L	G	N	T	C	G
Cipher text Value	7	7	22	10	18	22	23	18	11	6	13	19	2	6
Key Stream	p	a	s	c	a	l	p	a	s	c	a	l	p	a
Key Value	15	0	18	2	0	11	15	0	18	2	0	11	15	0
$P_i = (C_i - K_i) \, mod \, 26$	18	7	4	8	18	11	8	18	19	4	13	8	13	6
Plaintext	s	h	e	i	s	l	i	s	t	e	n	i	n	g

The **Plaintext** is "**she is listening**"


$K = pascal$
$K = pascal$
She is Listening
(Sender)
HHWKSWXSLGNTCG
Encryption algorithm By using Vigenere Cipher
Decryption algorithm By using Vigenere Cipher
She is Listening
(receiver)

Autokey Cipher

Alice

Sender

Bob

Receiver

$C_i=(P_i + K_i) \bmod 26$ ← K

Encryption

K → $P_i=(C_i - K_i) \bmod 26$

Decryption

Cipher text

Example 2

Encrypt and decrypt for the Plaintext **"She is Listening"** by using **Autokey Cipher** by using the Key = **PASCAL**

Ans:-

1. Encryption Algorithm

$$C_i = (P_i + K_i)\ mod\ 26$$

Plaintext	s	h	e	i	s	l	i	s	t	e	n	i	n	g
Plaintext Value	18	7	4	8	18	11	8	18	19	4	13	8	13	6
Key Stream	p	a	s	c	a	l	s	h	e	i	s	l	i	s
Key Value	15	0	18	2	0	11	18	7	4	8	18	11	8	18
$C_i = (P_i + K_i)\ mod\ 26$	7	7	22	10	18	22	0	25	23	12	5	19	21	24
Cipher text	H	H	W	K	S	W	A	Z	X	M	F	T	V	Y

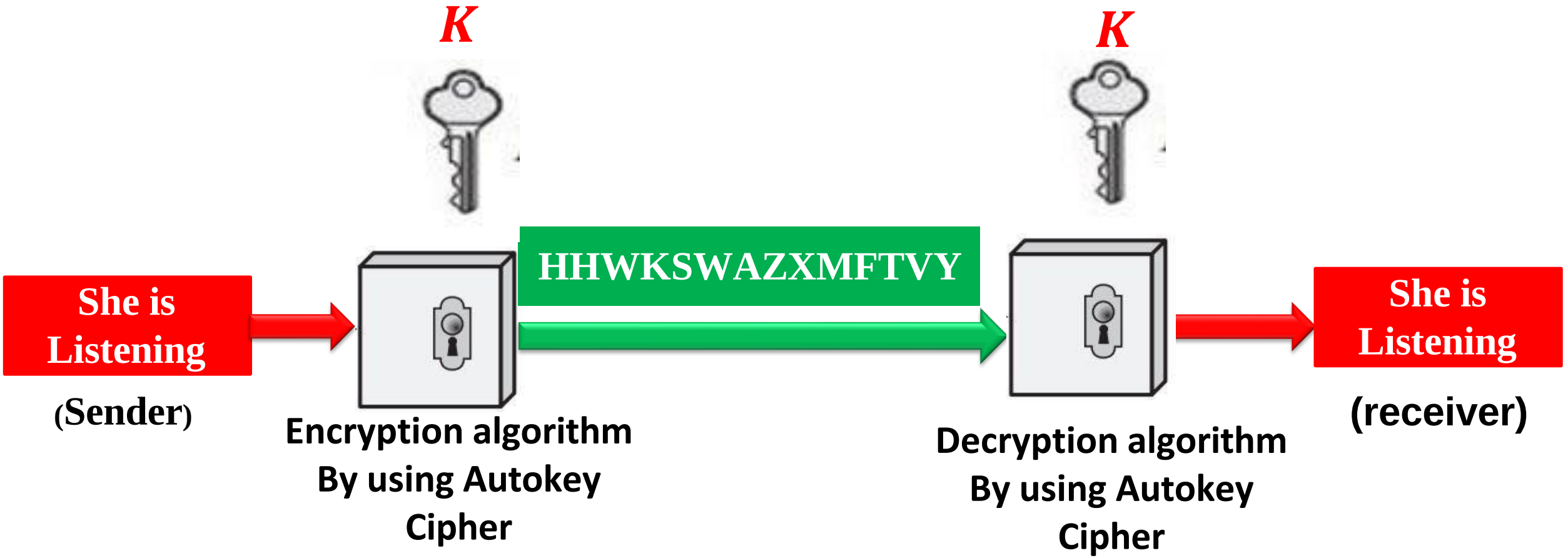
The **Cipher text** is "**HHWKSWAZXMFTVY**"

2. Decryption Algorithm

$$P_i = (C_i - K_i)\ mod\ 26$$

Cipher text	H	H	W	K	S	W	A	Z	X	M	F	T	V	Y
Cipher text Value	7	7	22	10	18	22	0	25	23	12	5	19	21	24
Key Stream	p	a	s	c	a	l	s	h	e	i	s	l	i	s
Key Value	15	0	18	2	0	11	18	7	4	8	18	11	8	18
$P_i = (C_i - K_i)\ mod\ 26$	18	7	4	8	18	11	8	18	19	4	13	8	13	6
Plaintext	s	h	e	i	s	l	i	s	t	e	n	i	n	g

The **Plaintext** is "**she is listening**"


K
K
She is Listening
(Sender)
HHWKSWAZXMFTVY
Encryption algorithm
By using Autokey
Cipher
Decryption algorithm
By using Autokey
Cipher
She is Listening
(receiver)

Example 2

Find decrypt for Ciphertext "**LLPWZ**" by using **Autokey Cipher** by using the Key = **4**

Ans:-

Decryption Algorithm $P_i = (C_i - K_i)\ mod\ 26$

Cipher text	L	L	P	W	Z
Cipher text Value	11	11	15	22	25
Key Value	4	7	4	11	11
$P_i = (C_i - K_i)\ mod\ 26$	7	4	11	11	14
Plaintext	h	e	l	l	o

The Plaintext is "hello"

Homework

1. By using Vigenere Cipher, encrypt the word “Explanation” using the key "hello"

2. Find the Ciphertext of the Plaintext “we are discovered save yourself” by using Autokey system with the keyword “deceptive”