Institute of Information Technology

Jahangirnagar University

জাহাঙ্গীরনগর বিশ্ববিদ্যালয়

IT-4259: Computer Network Security

for

4th Year 2nd Semester of B.Sc (Honors) in IT (5th Batch)

Lecture: 04

Cryptography-A Security Mechanism-1

Prepared by:

K M Akkas Ali

akkas_khan@yahoo.com, akkas@juniv.edu

Associate Professor

Institute of Information Technology (IIT)

Jahangirnagar University, Dhaka-1342

Objectives of this Lecture:

- To emphasize traditional symmetric-key substitution ciphers.
- **To illustrate some monoalphabetic ciphers:**
  - Additive cipher
  - Shift and Caesar cipher
  - Multiplicative cipher
  - Affine cipher
- **To illustrate some polyalphabetic ciphers:**
  - Autokey cipher
  - Playfair cipher
  - Vigenere cipher
  - One-time Pad
  - Hill cipher

Prepared by: K M Akkas Ali, Associate Professor, IIT, JU

Traditional Symmetric- Key Ciphers

Traditional symmetric-key ciphers can be classified into two broad categories:

1. Substitution Ciphers

- A substitution cipher replaces one symbol with another. For example, we can replace letter A with letter D, and letter T with letter Z. If the symbols are digits, we can replace 3 with 7, 2 with 6.
- Substitution ciphers can be categorized as either monoalphabetic ciphers or polyalphabetic ciphers.

2. Transposition Ciphers

- A transposition cipher does not substitute one symbol for another, instead it changes the location of the symbols.
- A symbol in the first position of the plaintext may appear in the ninth position of the ciphertext. A symbol in the eighth position of the plaintext may appear in the first position of the ciphertext. For example, the plaintext characters "***hello***" may be encrypted as "***elhol***".
- There are three types of transposition cipher:
  - Keyless Transposition Ciphers
  - Keyed Transposition Ciphers
  - Keyed Columnar Transposition Ciphers or Columnar Transposition Ciphers

Prepared by: K M Akkas Ali, Associate Professor, IIT, JU

Traditional Symmetric- Key Ciphers

Monoalphabetic Ciphers

- In monoalphabetic substitution, the relationship between a symbol in the plaintext to a symbol in the ciphertext is always one-to-one.
- That is, a character or symbol in the plaintext is always changed to the same character or symbol in the ciphertext regardless of its position in the text.
- For example, if letter A in the plaintext is changed to letter D, every letter A is changed to letter D.
- Additive cipher, Caesar cipher, multiplicative cipher, affine cipher etc. are some examples of monoalphabetic ciphers.

Example:

The following shows a plaintext and its corresponding ciphertext. The cipher is probably monoalphabetic because both *l*'s (els) are encrypted as *O*'s.

Plaintext: hello	**Ciphertext: KHOOR**

Prepared by: K M Akkas Ali, Associate Professor, IIT, JU

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.
- For example, if letter "a" could be enciphered as "D" in the beginning of the text, but as "N" at the middle.
- Polyalphabetic ciphers have the advantage of hiding the letter frequency of the undelying language. Eve cannot use the single-letter frequency statistics to break the ciphertext.
- Autokey cipher, playfair cipher, vigenere cipher, Hill cipher etc. are some examples of polyalphabetic ciphers.

Example:

The following shows a plaintext and its corresponding ciphertext. The cipher is polyalphabetic because each *l* (el) is encrypted by a different character. The first *l* (el) is encrypted as N; the second as Z.

Plaintext: hello	Ciphertext: ABNZF

Prepared by: K M Akkas Ali, Associate Professor, IIT, JU

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.
- Assume that the plaintext consists of lowercase letters (a to z), and that the ciphertext consists of uppercase letters (A to Z).
- To be able to apply mathematical operations on the plaintext and ciphertext, we assign numerical values to each letter as shown in the figure below.

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 →	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
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Figure : *Plaintext and ciphertext in Z_{26}*

Note:

- Each character (uppercase or lowercase) is assigned an integer in Z_{26}. The secret key between Alice and Bob is also an integer in Z_{26}.
- For simplicity, lowercase characters are used as plaintext and uppercase characters are used as ciphertext.

Prepared by: K M Akkas Ali, Associate Professor, IIT, JU

Additive Cipher

- When the cipher is additive, the plaintext, ciphertext, and key are integers in Z_{26}.
- The encryption algorithm adds the key to the plaintext character; the decryption algorithm subtracts the key from the ciphertext character. That is, encryption and decryption are inverse of each other.
- Figure below shows the process of additive cipher.

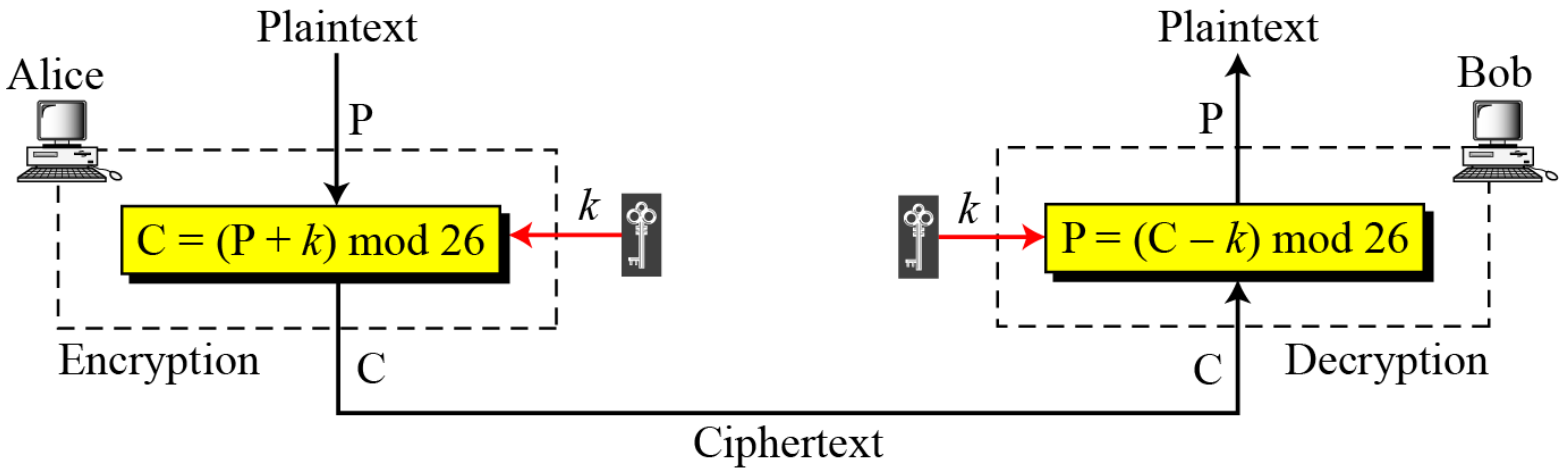

Figure: ***Additive cipher***

Additive Cipher

Example:

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

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

- The result is 'WTAAD'.
- Note that two instances of the same plaintext character (*l*) are encrypted as the same character (*A*). Hence additive cipher is monoalphabetic.

Additive Cipher

Example:

Use the additive cipher with key = 15 to decrypt the message "WTAAD".

Solution:

We apply the decryption algorithm to the plaintext character by character:

Ciphertext: W $\rightarrow$ 22	Decryption: (22 – 15) mod 26	Plaintext: 07 $\rightarrow$ h
Ciphertext: T $\rightarrow$ 19	Decryption: (19 – 15) mod 26	Plaintext: 04 $\rightarrow$ e
Ciphertext: A $\rightarrow$ 00	Decryption: (00 – 15) mod 26	Plaintext: 11 $\rightarrow$ l
Ciphertext: A $\rightarrow$ 00	Decryption: (00 – 15) mod 26	Plaintext: 11 $\rightarrow$ l
Ciphertext: D $\rightarrow$ 03	Decryption: (03 – 15) mod 26	Plaintext: 14 $\rightarrow$ o

- The result is 'hello'.
- Note that the operation is in modulo 26, which means that a negative result needs to be mapped to Z_{26}. (for example, -15 becomes 11).

Prepared by: K M Akkas Ali, Associate Professor, IIT, JU

Shift and Caesar Cipher

Shift Cipher:

- Historically, additive ciphers are called shift ciphers. Because, the encryption algorithm can be interpreted as "shift key character down" and the decryption algorithm can be interpreted as "shift key character up" .
- For example, if the key=15, the encryption algorithm shifts 15 character down. The decryption algorithm shifts 15 character up.

Caesar Cipher

- Additive ciphers are also called Caesar cipher. Because, Julius Caesar used this cipher to communicate with his officers.
- Caesar used a key of 3 for his communications. That is, the cipher involves replacing each letter of the plaintext with the letter standing three places further down the alphabet. For example,

Plaintext	**:**	**Meet**	**me**	**after**	**the**	**lunch**
Ciphertext	:	PHHW	PH	DIWHU	WKH	OXQFK

Multiplicative Cipher

In a multiplicative cipher-

- The encryption algorithm specifies multiplication of the plaintext by the key.
- The decryption algorithm specifies division of the ciphertext by the key. In other words, decryption algorithm means multiplication of the ciphertext by the multiplicative inverse of the key.
- The plaintext and ciphertext are integers in Z_{26}, but the key is an integer in Z_{26}^*.
- Encryption and decryption are inverse of each other.
- Figure below shows the process of multiplicative cipher.

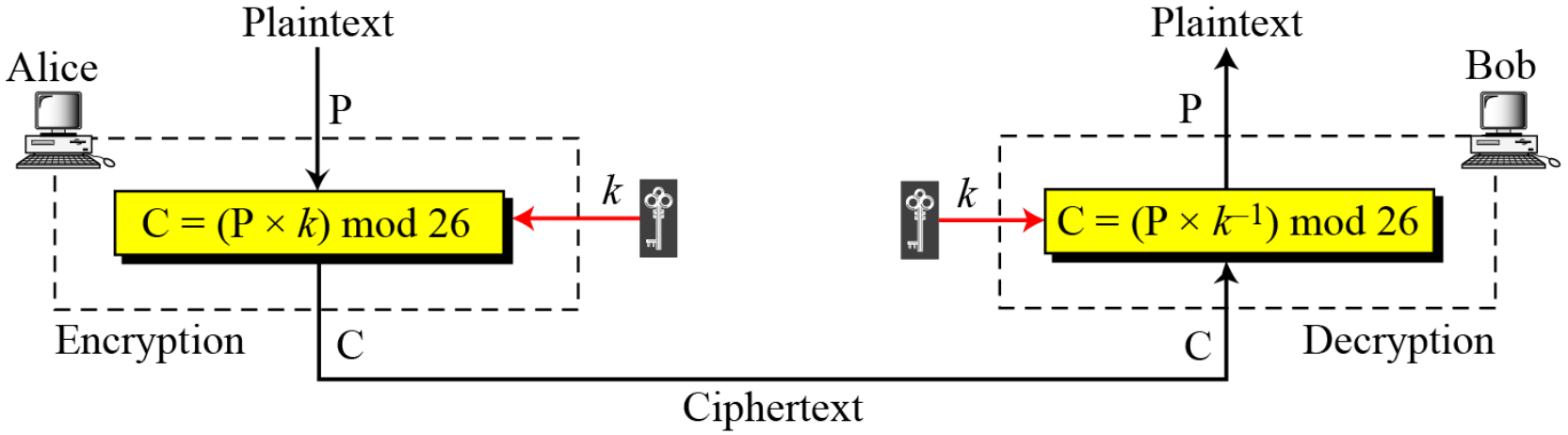

Figure: Multiplicative cipher

Multiplicative Cipher

Example:

What is the key domain for any multiplicative cipher?

Solution:

The key needs to be in Z_{26}^*. This set has only 12 members: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25.

Note:

- We can find the key domain for any multiplicative cipher using Euler's Phi-function, sometimes called the Euler's Totient function.

Example:

Encrypt the message "hello" with a key of 7 using multiplicative cipher.

Solution:

We apply the following encryption algorithm to the plaintext character by character: C=(Pxk)mod 26

Plaintext: h $\rightarrow$ 07	Encryption: $(07 \times 07) \bmod 26$	ciphertext: 23 $\rightarrow$ X
Plaintext: e $\rightarrow$ 04	Encryption: $(04 \times 07) \bmod 26$	ciphertext: 02 $\rightarrow$ C
Plaintext: l $\rightarrow$ 11	Encryption: $(11 \times 07) \bmod 26$	ciphertext: 25 $\rightarrow$ Z
Plaintext: l $\rightarrow$ 11	Encryption: $(11 \times 07) \bmod 26$	ciphertext: 25 $\rightarrow$ Z
Plaintext: o $\rightarrow$ 14	Encryption: $(14 \times 07) \bmod 26$	ciphertext: 20 $\rightarrow$ U

The ciphertext is "XCZZU".

Prepared by: K M Akkas Ali, Associate Professor, IIT, JU

Multiplicative Cipher

Example:

Decrypt the message "XCZZU" with a key of 7 using multiplicative cipher.

Solution:

We apply the following decryption algorithm to the ciphertext character by character: $P=(C \times k^{-1}) \bmod 26$, where k^{-1} is the multiplicative inverse of k. Here the multiplicative inverse of 7 is 15 in z_{26}.

Ciphertext: X→23	Decryption: (23x15) mod 26	Plaintext: 05→h
Ciphertext: C→02	Decryption: (02x15) mod 26	Plaintext: 04→e
Ciphertext: Z→25	Decryption: (25x15) mod 26	Plaintext: 11→l
Ciphertext: Z→25	Decryption: (25x15) mod 26	Plaintext: 11→l
Ciphertext: U→20	Decryption: (20x15) mod 26	Plaintext: 14→o

- The result is 'hello'.

Prepared by: K M Akkas Ali, Associate Professor, IIT, JU

Affine Cipher

- It is the combination of additive and multiplicative ciphers with a pair of keys.
- The first key is used with the multiplicative cipher which comes from Z_{26}*. This set has only 12 members: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25.
- The second key is used with the additive cipher which comes from Z_{26}. This set has only 26 members: 0, 1, 2, 3, 4, 5, ……, 25.
- Therefore, the size of the key domain for any Affine cipher is

$$26 \times 12 = 312.$$

Affine Cipher

- Figure below shows that Affine cipher is actually two ciphers, applied one after another.
- In Affine cipher, the encryption and decryption algorithms are based on the following two formulas:

$$C = (P \times k_1 + k_2) \bmod 26 \qquad P = ((C - k_2) \times k_1^{-1}) \bmod 26$$

where k_1^{-1} is the multiplicative inverse of k_1 and $-k_2$ is the additive inverse of k_2

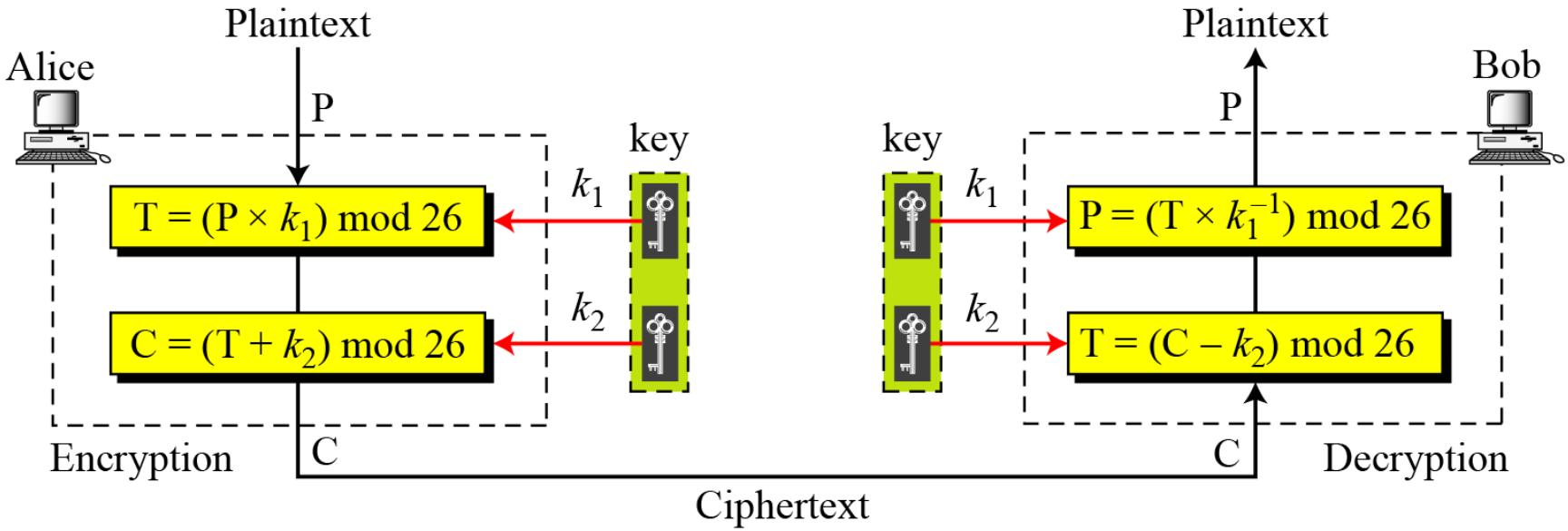

Figure: Affine cipher

Affine Cipher

Example:

Use an affine cipher to encrypt the message "hello" with the key pair (7, 2) in modulo 26.

Solution:

We apply the following encryption algorithm to the plaintext character by character: $C=(P \times k_1 + k_2) \bmod 26$

P: h $\rightarrow$ 07	Encryption: $(07 \times 7 + 2) \bmod 26$	C: 25 $\rightarrow$ Z
P: e $\rightarrow$ 04	Encryption: $(04 \times 7 + 2) \bmod 26$	C: 04 $\rightarrow$ E
P: l $\rightarrow$ 11	Encryption: $(11 \times 7 + 2) \bmod 26$	C: 01 $\rightarrow$ B
P: l $\rightarrow$ 11	Encryption: $(11 \times 7 + 2) \bmod 26$	C: 01 $\rightarrow$ B
P: o $\rightarrow$ 14	Encryption: $(14 \times 7 + 2) \bmod 26$	C: 22 $\rightarrow$ W

The ciphertext is "ZEBBW".

Prepared by: K M Akkas Ali, Associate Professor, IIT, JU

Affine Cipher

Example:

Use the affine cipher to decrypt the message "ZEBBW" with the key pair (7, 2) in modulus 26.

Solution

We apply the following decryption algorithm to the ciphertext character by character: $C=((P - k_2) \times k^{-1}) \bmod 26$, where k^{-1} is the multiplicative inverse of k_1 and $-k_2$ is the additive inverse of k_2. Here additive inverse of 2 is 24 and multiplicative inverse of 7 is 15.

C: Z $\rightarrow$ 25	Decryption: $((25 - 2) \times 7^{-1}) \bmod 26$	P:07 $\rightarrow$ h
C: E $\rightarrow$ 04	Decryption: $((04 - 2) \times 7^{-1}) \bmod 26$	P:04 $\rightarrow$ e
C: B $\rightarrow$ 01	Decryption: $((01 - 2) \times 7^{-1}) \bmod 26$	P:11 $\rightarrow$ l
C: B $\rightarrow$ 01	Decryption: $((01 - 2) \times 7^{-1}) \bmod 26$	P:11 $\rightarrow$ l
C: W $\rightarrow$ 22	Decryption: $((22 - 2) \times 7^{-1}) \bmod 26$	P:14 $\rightarrow$ o

The plaintext is "hello".

Traditional Symmetric- Key Ciphers

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.
- For example, letter "a" could be enciphered as "D" in the beginning of the text, but as "N" at the middle.
- Polyalphabetic ciphers have the advantage of hiding the letter frequency of the undelying language. Eve cannot use the single-letter frequency statistics to break the ciphertext.
- Autokey cipher, playfair cipher, vigenere cipher, Hill cipher etc. are some examples of polyalphabetic ciphers.

Example:

The following shows a plaintext and its corresponding ciphertext. The cipher is polyalphabetic because each *l* (el) is encrypted by a different character. The first *l* (el) is encrypted as N; the second as Z.

Plaintext: hello	**Ciphertext: ABNZF**

Prepared by: K M Akkas Ali, Associate Professor, IIT, JU

Autokey Cipher

- In autokey cipher, the key is a stream of subkeys, in which each subkey is used to encrypt the corresponding plaintext character.
- The first subkey is a predetermined value secretly agreed upon by Alice and Bob.
- The second subkey is the value of the first plaintext character (between 0 to 25).
- The third subkey is the value of the second plaintext character. And so on.
- Encryption and decryption is done using the following formulas.

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

$$\text{Encryption: } C_i = (P_i + k_i) \bmod 26 \qquad \text{Decryption: } P_i = (C_i - k_i) \bmod 26$$

- The name of this cipher as 'autokey' implies that the subkeys are automatically created from the plaintext cipher characters during the encryption process.

Prepared by: K M Akkas Ali, Associate Professor, IIT, JU

Autokey Cipher

Example for Encryption:

Assume that Alice and Bob agreed to use an autokey cipher with initial key value k_1 = 12. Now Alice wants to send Bob the message "Attack is today".

Solution:

Enciphering is done character by character.

1. Replace each plaintext character by its integer value (e.g *a* with 00, *b* with 01 etc.)
2. Write the 1st subkey (k_1=12) underneath the 1st plaintext character, 2nd subkey (k_2=00, which is the 1st plaintext character) underneath the 2nd plaintext character. And so on.
3. Now encrypt each plaintext character using the formula:

$$C_i=(P_i+k_i) \bmod 26$$

For example, for 3rd plaintext character ***t***, its corresponding ciphertext is-

$C_3=(P_3+k_3) \bmod 26$
$t=(19+19) \bmod 26$
$t=12=M$

Prepared by: K M Akkas Ali, Associate Professor, IIT, JU

Autokey Cipher

Example for Encryption (continue):

Plaintext:	a	t	t	a	c	k	i	s	t	o	d	a	y
P's Values:	00	19	19	00	02	10	08	18	19	14	03	00	24
Key stream:	*12*	*00*	*19*	*19*	*00*	*02*	*10*	*08*	*18*	*19*	*14*	*03*	*00*
C's Values:	12	19	12	19	02	12	18	00	11	7	17	03	24
Ciphertext:	**M**	**T**	**M**	**T**	**C**	**M**	**S**	**A**	**L**	**H**	**R**	**D**	**Y**

The ciphertext is "MTMTCMSALHRDY".

Note:

- We see that autokey cipher is a polyalphabetc cipher because the three occurrence of "a" in the plaintext are encrypted differently. The 1st 'a' is encrypted as M, the 2nd as T, and the 3rd as D.

Prepared by: K M Akkas Ali, Associate Professor, IIT, JU

Autokey Cipher

Example for Decryption:

With initial key value k_1 = 12, use the autokey cipher to decrypt the message sent by Alice to Bob: 'MTMTCMSALHRDY'.

Solution:

Deciphering is done character by character in the reverse direction.

1. Replace each ciphertext character by its integer value (e.g *M* with 12, *T* with 19 etc).
2. Write the 1st subkey (k_1=12) underneath the 1st ciphertext character and then find the first letter of the plaintext using the formula:

   $$P_i=(C_i-k_i) \bmod 26.$$

   For example, for 1st ciphertext character ***M***, its corresponding plaintext is-

   $P_1=(C_1-k_1) \bmod 26$
   $M=(12-12) \bmod 26$
   $M=00=a$
3. Write the integer value of the first plaintext character as the 2nd subkey underneath the 2nd ciphertext character and find the plaintext character using above formula. And so on.

Prepared by: K M Akkas Ali, Associate Professor, IIT, JU

Autokey Cipher

Example for Decryption (continue):

Ciphertext	**:**	**M**	**T**	**M**	**T**	**C**	**M**	**S**	**A**	**L**	**H**	**R**	**D**	**Y**
C's Values	:	12	19	12	19	02	12	18	00	11	07	17	03	24
Key Stream	:	12	00	19	19	00	02	10	08	18	19	14	03	00
P's Values	:	00	19	19	00	02	10	08	18	19	14	03	00	24
Plaintext	:	a	t	t	a	c	k	i	s	t	o	d	a	y

The plaintext is "attack is today".

Prepared by: K M Akkas Ali, Associate Professor, IIT, JU

Playfair Cipher

- The best-known poly-alphabetic cipher is Playfair cipher.
- This cipher is invented by Charles Wheatstone in 1854, but named after his friend Baron Playfair. It was used by the British Army during World War I.
- The secret key in this cipher is made of 25 alphabet letters arranged in a 5x5 matrix (letters I and J are considered the same when encrypting).
- Different arrangements of the letters in the matrix can create many different secret keys. One of the possible arrangement is shown in the figure here.
- Before encryption, the plaintext characters are grouped as two-character pairs.
- If the two letters in a pair are the same, a bogus letter is inserted to separate them.
- After inserting the bogus letters (if any), if the number of characters in the plaintext is odd, then one extra bogus character is added at the end to make the number of characters even.

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

Figure : ***Secret key in Playfair Cipher***

Playfair Cipher

Encryption rule for Playfair Cipher:

The playfair cipher uses three rules for encryption:

1. If the two letters in a pair are located in the same row of the secret key matrix, the corresponding encrypted character for each letter is the next letter to the right in the same row (with wrapping to the beginning of the row if the plaintext letter is the last character in the row).
2. If the two letters in a pair are located in the same column of the secret key matrix, the corresponding encrypted character for each letter is the letter beneath it in the same column (with wrapping to the beginning of the column if the plaintext letter is the last character in the column).
3. If the two letters in a pair are not located in the same row or column of the secret key matrix, the corresponding encrypted character for each letter is a letter that is in its own row but in the same column as the other letter.

Playfair Cipher

Example for Encryption:

Encrypt the plaintext "hello" using the secret key matrix shown in the figure below.

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

Secret Key

Solution:

- We group the plaintext as two-character pairs: "he // o"
- Here, in the second pair, the two letters are the same. So, we insert ***x*** as a bogus letter between the two *l's*. Now we have:

  "***he lx lo***".
- Now encrypt the message using the encryption rules for playfair cipher.

he → EC lx → QZ lo → BX

Plaintext: hello Ciphertext: ECQZBX

We see that playfair cipher is actually a polyalphabetc cipher because the two occurrence of "l" in the plaintext are encrypted differently, such as "Q" and "B".

Prepared by: K M Akkas Ali, Associate Professor, IIT, JU

Playfair Cipher

Decryption rule for Playfair Cipher:

The playfair cipher uses three rules for decryption:

1. If the two ciphertext letters in a pair are located in the same row of the secret key matrix, the corresponding decrypted character for each letter is the previous letter to the left in the same row (with wrapping to the end of the row if the ciphertext letter is the first character in the row).
2. If the two ciphertext letters in a pair are located in the same column of the secret key matrix, the corresponding decrypted character for each letter is the letter above it in the same column (with wrapping to the end of the column if the ciphertext letter is the first character in the column).
3. If the two ciphertext letters in a pair are not located in the same row or column of the secret key matrix, the corresponding decrypted character for each letter is a letter that is in its own row but in the same column as the other letter.

Prepared by: K M Akkas Ali, Associate Professor, IIT, JU

Playfair Cipher

Example for Decryption:

Decrypt the message "ECQZBX" using the secret key matrix shown in the figure below.

Solution:

- We group the ciphertext as two-character pairs: "EC *QZ* BX"
- Now decrypt the message using the decryption rules for playfair cipher.

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

Secret Key

EC → he QZ → lx BX → lo

Ciphertext: ECQZBX Plaintext: hello

Prepared by: K M Akkas Ali, Associate Professor, IIT, JU

Vigenere Cipher

- This cipher was designed by French mathematician Blaise de Vigenere.
- In this cipher, the secret key stream is created by repeating the initial secret key stream as many times as needed.
- The initial secret key stream of length m (where 1<=m<=26) is previously agreed upon by Alice and Bob.
- The cipher can be described as follows:

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

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

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

Here, (k_1, k_2, k_3,….., k_m) is the initial secret key stream

Prepared by: K M Akkas Ali, Associate Professor, IIT, JU

Vigenere Cipher

Example for Encryption:

Encrypt the message "*She is listening*" using Vigenere cipher with the 6-character keyword "PASCAL".

Solution:

1. The initial key stream is "PASCAL" (*15, 0, 18, 2, 0, 11*). The key stream is the repetition of this initial key stream (as many times as needed).
2. Now encrypt each plaintext character using the formula $C_i=(P_i+k_i) \bmod 26$

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**

The ciphertext is "HHWKSWXSLGNTCG".

Prepared by: K M Akkas Ali, Associate Professor, IIT, JU

Vigenere Cipher

Example for Decryption:

Decrypt the message "HHWKSWXSLGNTCG" using Vigenere cipher with the 6-character keyword "PASCAL".

Solution:

1. The initial key stream is "PASCAL" (*15, 0, 18, 2, 0, 11*). The key stream is the repetition of this initial key stream (as many times as needed).
2. Now decrypt each plaintext character using the formula $P_i=(C_i-k_i) \bmod 26$

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

The plaintext is "she is listening".

One-Time Pad

- An additive cipher can be easily broken because the same key is used to encrypt each character of the plaintext.
- In one-time pad, each character in the plaintext is encrypted with a key randomly chosen from a key domain (00, 01, 02, 03, …..,25). For example, the first character of the plaintext is encrypted using the key 04, the second character is encrypted using the key 02, the third character is encrypted using the key 21; and so on.
- This type of cipher is invented by Vernam. The key has the same length as the plaintext and is chosen completely in random.
- The same key is used to encrypt and decrypt for each individual character of the message and then discarded. Each new message requires a new key of the same length as the new message.
  - Ciphertext-only attack is impossible for one-time pad.
  - If the sender changes the key sequence randomly each time she sends a message, then other types of attacks are also impossible.
  - One-time pad produces random output that bears no statistical relationship to the plaintext. So, there is simply no way to break the code.
- Though perfect secrecy can be achieved through one-time pad, it has some difficulties:
  - It is almost impossible to implement commercially, because large quantities of random key generation is very difficult.
  - For every message to be sent, a key of equal length is needed by both sender and receiver. How can Alice tell Bob the new key each time she has a message to send? Thus, a mammoth key distribution problem exists.

Prepared by: K M Akkas Ali, Associate Professor, IIT, JU

Hill Cipher

- This cipher was invented by Lester S. Hill.
- In this cipher, the plaintext is divided into equal-size blocks.
- The blocks are encrypted one at a time in such a way that each character in the block contributes to the encryption of other characters in the block.
- In a Hill cipher, the key is a square matrix of size *m x m* in which *m* is the size of the block (i.e. number of characters in each block).
- The key matrix K in the Hill cipher needs to have a multiplicative inverse.

$$\mathrm{K} = \begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1m} \\ k_{21} & k_{22} & \cdots & k_{2m} \\ \vdots & \vdots & & \vdots \\ k_{\mathrm{m1}} & k_{\mathrm{m2}} & \cdots & k_{mm} \end{bmatrix}$$

$$\begin{aligned} \mathrm{C}_1 &= \mathrm{P}_1 k_{11} + \mathrm{P}_2 k_{21} + \cdots + \mathrm{P}_m k_{m1} \\ \mathrm{C}_2 &= \mathrm{P}_1 k_{12} + \mathrm{P}_2 k_{22} + \cdots + \mathrm{P}_m k_{m2} \\ &\cdots \\ \mathrm{C}_\mathrm{m} &= \mathrm{P}_1 k_{1m} + \mathrm{P}_2 k_{2m} + \cdots + \mathrm{P}_m k_{mm} \end{aligned}$$

Figure: ***Key in the Hill cipher***

Hill Cipher

Example: Encrypt the message "code is ready" using Hill cipher.

Solution:

- There are 11 characters in the plaintext message.
- For dividing it into equal-size blocks (here, 3 blocks with 4 characters per block), add an extra bogus character "z" to the last block, and then remove the spaces.
- Thus, the plaintext characters can be represented by a 3 × 4 matrix P.
- Hence, the key will be a 4 x 4 square matrix K.
- The ciphertext is obtained from ciphertext matrix C as "OHKNIHGKLISS".
- Decryption is done using the inverse of the key matrix.

$$P \begin{bmatrix} 02 & 14 & 03 & 04 \\ 08 & 18 & 17 & 04 \\ 00 & 03 & 24 & 25 \end{bmatrix} \quad K \begin{bmatrix} 09 & 07 & 11 & 13 \\ 04 & 07 & 05 & 06 \\ 02 & 21 & 14 & 09 \\ 03 & 23 & 21 & 08 \end{bmatrix} = C \begin{bmatrix} 14 & 07 & 10 & 13 \\ 08 & 07 & 06 & 11 \\ 11 & 08 & 18 & 18 \end{bmatrix}$$

a. Encryption

$$C \begin{bmatrix} 14 & 07 & 10 & 13 \\ 08 & 07 & 06 & 11 \\ 11 & 08 & 18 & 18 \end{bmatrix} \quad K^{-1} \begin{bmatrix} 02 & 15 & 22 & 03 \\ 15 & 00 & 19 & 03 \\ 09 & 09 & 03 & 11 \\ 17 & 00 & 04 & 07 \end{bmatrix} = P \begin{bmatrix} 02 & 14 & 03 & 04 \\ 08 & 18 & 17 & 04 \\ 00 & 03 & 24 & 25 \end{bmatrix}$$

b. Decryption