Course: Cryptography and Network Security
Code: CS-34310
Branch: M.C.A - 4th Semester

Lecture – 6 : Symmetric-Key Ciphers – Part-2

Faculty & Coordinator : Dr. J Sathish Kumar (JSK)

Department of Computer Science and Engineering

Motilal Nehru National Institute of Technology Allahabad,
Prayagraj-211004

Monoalphabetic Substitution Cipher

- In this method, it 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.

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

An example key for monoalphabetic substitution cipher

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

ICFVQRVVNEFVRNVSIYRGAHSLIOJICNHTIYBFGTICRXRS

Cryptanalysis

- The size of the key space for the monoalphabetic substitution cipher is 26! .
- This makes a brute-force attack extremely difficult for Eve even if she is using a powerful computer.
- However, she can use statistical attack based on the frequency of characters.
- The cipher does not change the frequency of characters.
- The monoalphabetic ciphers do not change the frequency of characters in the ciphertext, which makes the ciphers vulnerable to statistical attack.

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.
- Polyalphabetic ciphers have the advantage of hiding the letter frequency of the underlying language.
- Eve cannot use single-letter frequency statistic to break the ciphertext.

Autokey Cipher

- In this cipher, the key is a stream of subkeys, in which each subkey is used to encrypt the corresponding character in the plaintext.
- 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 and 25).
- The third subkey is the value of the second plaintext. And so on.

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

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

Autokey Cipher

- However, it is still as vulnerable to the brute-force attack as the additive cipher.

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**

However, it is still as vulnerable to the brute-force attack as the additive cipher.

Playfair Cipher

- Playfair cipher used by the British army during World War I.
- The secret key in this cipher is made of 25 alphabet letters arranged in a 5 × 5 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.
- The letters dropped in the matrix diagonally starting from the top right-hand corner.
- Before encryption,
  - if the two letters in a pair are the same, a bogus letter is inserted to separate them.
  - After inserting bogus letters, if the number of characters in the plaintext is odd, one extra bogus character is added at the end to make the number of characters even.

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

Playfair Cipher

- The cipher uses three rules for encryption:

  a. If the two letters in a pair are located in the same row of the secret key, 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).

  b. If the two letters in a pair are located in the same column of the secret key, 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).

  c. If the two letters in a pair are not in the same row or column of the secret, 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

$P = P_1P_2P_3 \ldots$ $C = C_1C_2C_3\ldots$ $k = [(k_1, k_2), (k_3, k_4), \ldots]$

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

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

Let us encrypt the plaintext "hello" using the key in Figure

When we group the letters in two-character pairs, we get "he, ll, o".
We need to insert an x between the two l's (els), giving "he, lx, lo".

he → EC lx → QZ lo → BX
Plaintext: hello Ciphertext: ECQZBX

Cryptanalysis of a Playfair Cipher

- Obviously a brute-force attack on a Playfair cipher is very difficult.
  - The size of the key domain is 25!
- However, the frequencies of diagrams are preserved (to some extent because of filler insertion), so a cryptanalyst can use a ciphertext-only attack based on the digram frequency test to find the key.

One-Time Pad

- One of the goals of cryptography is perfect secrecy.
- A study by Shannon has shown that perfect secrecy can be achieved if each plaintext symbol is encrypted with a key randomly chosen from a key domain.
- For example, an additive cipher can be easily broken because the same key is used to encrypt every character.
- However, even this simple cipher can become a perfect cipher if the key that is used to encrypt each character is chosen randomly from the key domain (00, 01, 02, …, 25) - that is, if the first character 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 idea is used in a cipher called one-time pad, invented by Vernam.
- In this cipher, the key has the same length as the plaintext and is chosen completely in random.

One-Time Pad

- A one-time pad is a perfect cipher, but it is almost impossible to implement commercially.
- If the key must be newly generated each time, how can Alice tell Bob the new key each time she has a message to send?
- However, there are some occasions when a one-time pad can be used.
- For example, if the president of a country needs to send a completely secret message to the president of another country, she can send a trusted envoy with the random key before sending the message.

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 tenth position of the ciphertext.
- A symbol in the eighth position in the plaintext may appear in the first position of the ciphertext.
- In other words, a transposition cipher reorders (transposes) the symbols.

Keyless Transposition Ciphers

- Simple transposition ciphers, which were used in the past, are keyless.
- There are two methods for permutation of characters.
- In the first method, the text is written into a table column by column and then transmitted row by row.
- In the second method, the text is written into the table row by row and then transmitted column by column.

Keyless Transposition Ciphers
Rail fence cipher

- In this cipher, the plaintext is arranged in two lines as a zigzag pattern (which means column by column);
- The ciphertext is created reading the pattern row by row.
- For example, to send the message “Meet me at the park” to Bob, Alice writes

m ↘ e ↗ e ↘ t ↗ m ↘ e ↗ a ↘ t ↗ t ↘ h ↗ e ↘ p ↗ a ↘ r ↗ k

- She then creates the ciphertext “MEMATEAKETETHPR” by sending the first row followed by the second row.
- Bob receives the ciphertext and divides it in half (in this case the second half has one less character).
- The first half forms the first row; the second half, the second row. Bob reads the result in zigzag.

Keyless Transposition Ciphers
Transposition cipher

- Alice and Bob can agree on the number of columns and use the second method.
- Alice writes the same plaintext, row by row, in a table of four columns.
- She then creates the ciphertext “MMTAEEHREAEKTTP” by transmitting the characters column by column.
- Bob receives the ciphertext and follows the reverse process.
- He writes the received message, column by column, and reads it row by row as the plaintext.

m	e	e	t
m	e	a	t
t	h	e	p
a	r	k	

Keyless Transposition Ciphers
Transposition cipher

- The following figure shows the permutation of each character in the plaintext into the ciphertext based on the positions.

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
01	05	09	13	02	06	10	13	03	07	11	15	04	08	12

m	**e**	**e**	**t**
m	**e**	**a**	**t**
t	**h**	**e**	**p**
a	**r**	**k**	

- The second character in the plaintext has moved to the fifth position in the ciphertext;
- The third character has moved to the ninth position; and so on.
- Although the characters are permuted, there is a pattern in the permutation: (01, 05, 09, 13), (02, 06, 10, 13), (03, 07, 11, 15), and (08,12).
- In each section, the difference between the two adjacent numbers is 4.

Keyed Transposition Ciphers

- The keyless ciphers permute the characters by using writing plaintext in one way (row by row, for example) and reading it in another way (column by column, for example).
- The permutation is done on the whole plaintext to create the whole ciphertext.
- Another method is to divide the plaintext into groups of predetermined size, called blocks, and then use a key to permute the characters in each block separately.

Keyed Transposition Ciphers

- Alice needs to send the message “Enemy attacks tonight” to Bob.
- Alice and Bob have agreed to divide the text into groups of five characters and then permute the characters in each group.
- The following shows the grouping after adding a bogus character at the end to make the last group the same size as the others.

e n e m y	a t t a c	k s t o n	i g h t z

- The key used for encryption and decryption is a permutation key, which shows how the character are permuted.
- For this message, assume that Alice and Bob used the following key

Encryption ↓

3	1	4	5	2
1	2	3	4	5

↑ Decryption

Keyed Transposition Ciphers

- The third character in the plaintext block becomes the first character in the ciphertext block;
- The first character in the plaintext block becomes the second character in the ciphertext block; and so on.
- The permutation yields

E E M Y N	T A A C T	T K O N S	H I T Z G

- Alice sends the ciphertext “EEMYNTAACTTKONSHITZG” to Bob.
- Bob divides the ciphertext into 5-character groups and, using the key in the reverse order, finds the plaintext.

STREAM AND BLOCK CIPHERS

- Symmetric ciphers into two broad categories: stream ciphers and block ciphers.
- Stream Ciphers
  - In a stream cipher, encryption and decryption are done one symbol (such as a character or a bit) at a time.
  - We have a plaintext stream, a ciphertext stream, and a key stream.
  - Call the plaintext stream P, the ciphertext stream C, and the key stream K.

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

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

STREAM AND BLOCK CIPHERS

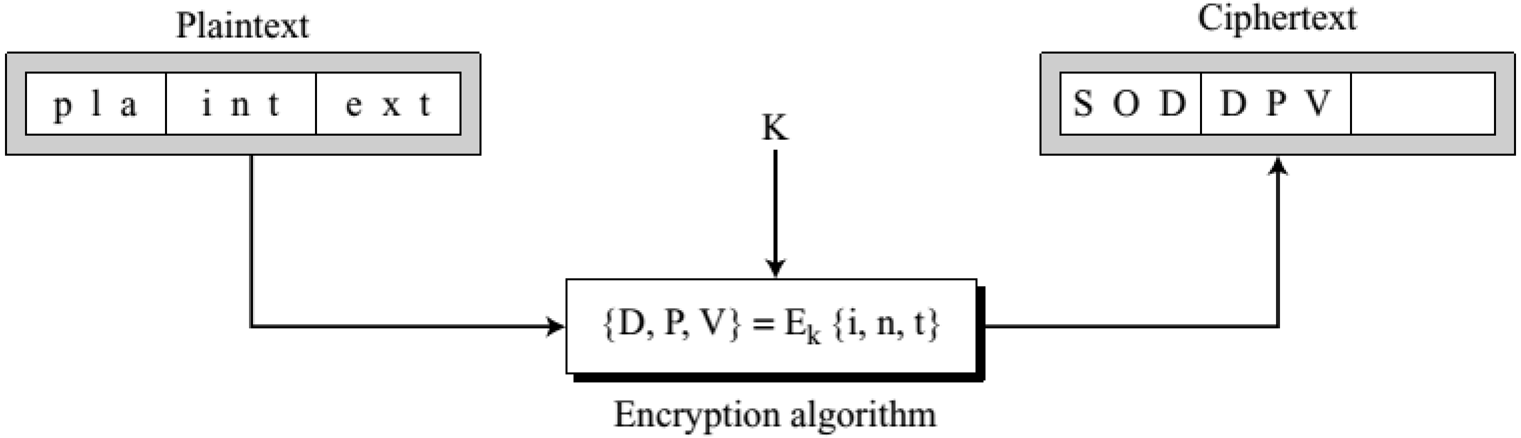
- Symmetric ciphers into two broad categories: stream ciphers and block ciphers.
- Stream Ciphers
  - In a stream cipher, encryption and decryption are done one symbol (such as a character or a bit) at a time.
  - We have a plaintext stream, a ciphertext stream, and a key stream.
  - Call the plaintext stream P, the ciphertext stream C, and the key stream K.

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

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

STREAM AND BLOCK CIPHERS

- 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.
  - Based on the definition, in a block cipher, a single key is used to encrypt the whole block even if the key is made of multiple values.
  - In a block cipher, a ciphertext block depends on the whole plaintext block.



STREAM AND BLOCK CIPHERS

- Stream ciphers

- Additive ciphers
- Monoalphabetic substitution ciphers
- Vigenere ciphers

- Block ciphers

- Playfair ciphers
- Polyalphabetic cipher
- DES and AES