Topic 2
Symmetric Ciphers
Classical Encryption Techniques

TERM	DEFINITION
Plaintext	An original message
Ciphertext	The coded message
Enciphering/Encryption	The process of converting plaintext to ciphertext
Deciphering/Decryption	Restoring the plaintext from ciphertext
Cryptography	Area of study of the many schemes used for encryption
Cryptographic System/Cipher	A scheme used for encryption
Cryptanalysis	Techniques used for deciphering a message without any knowledge of the enciphering details
Cryptology	The areas of cryptography and cryptanalysis

- **CRYPTOGRAPHY**

Cryptographic systems are characterized along three independent dimensions:

The number of keys used	**Symmetric** – If both sender and receiver use the same key, the system is referred to as symmetric, single-key, secret-key, or conventional encryption. **Asymmetric** – If the sender and receiver use different keys, the system is referred to as asymmetric, two-key, or public-key encryption.
The type of Operations used for transforming plaintext to ciphertext	**Substitution** – each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element. **Transposition –** elements in the plaintext are rearranged.
The way in which the plaintext is processed	**Block Cipher** – processes the input one block of elements at a time, producing an output block for each input block. **Stream Cipher** – processes the input elements continuously, producing output one element at a time, as it goes along.

- **SYMMETRIC CIPHER MODEL**

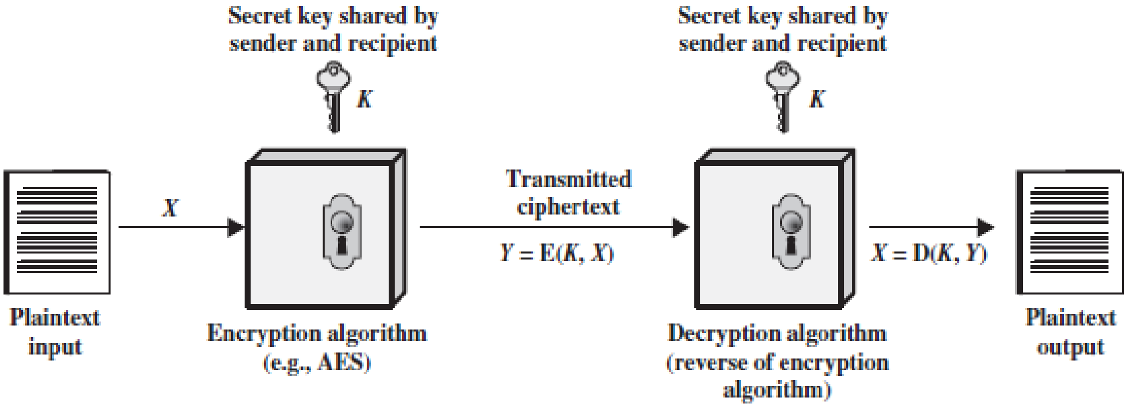
Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E(K, X)
X = D(K, Y)
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Figure: Simplified Model of Symmetric Encryption

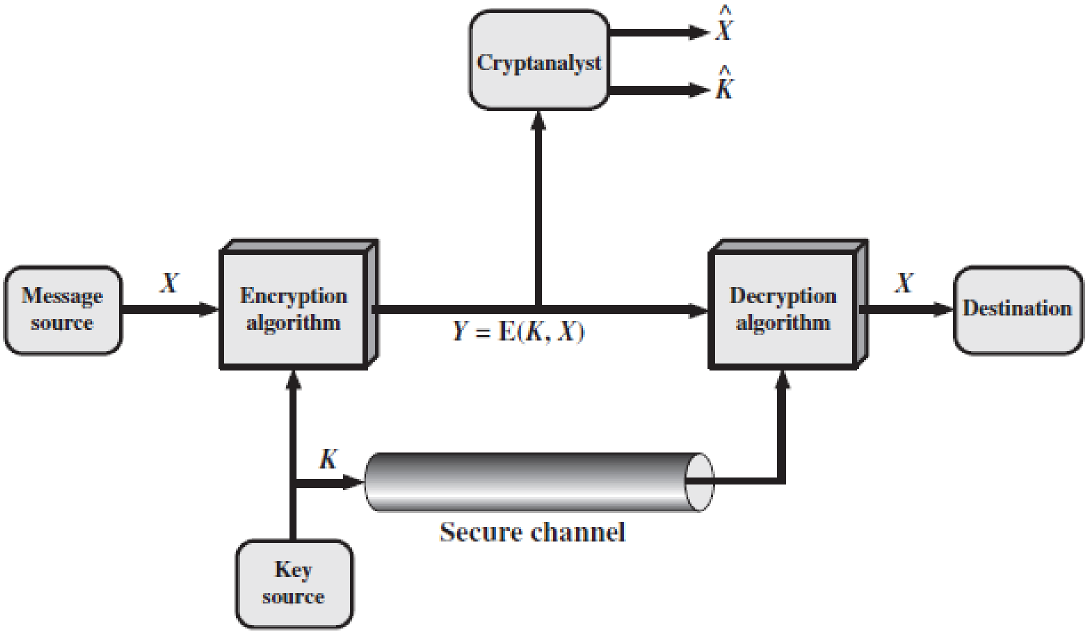

Figure: Model of Symmetric Cryptosystem

- **ENCRYPTION SCHEME SECURITY**

Unconditionally Secure	- No matter how much time an opponent has, it is impossible to decrypt the ciphertext simply because the required information is not there
Computationally Secure	- The cost of breaking the cipher exceeds the value of the encrypted information - The time required to break the cipher exceeds the useful lifetime of the information

- **SYMMETRIC ENCRYPTION**

Substitution Techniques	• Caesar Cipher • Monoalphabetic Cipher • Playfair Cipher • Polyalphabetic Cipher • Vigenère Cipher • One Time Pad
Transposition Techniques	• Rail Fence Cipher • Row Transposition Cipher

Substitution Ciphers

- **Caesar Cipher**
  - Simplest and earliest known use of a substitution cipher used by Julius Caesar
  - Involves replacing each letter of the alphabet with the letter standing three places further down the alphabet. Alphabet is wrapped around so that the letter following Z is A.

Example:

Plain : `meet me after the toga party`
Cipher : `PHHW PH DIWHU WKH WRJD SDUWB`

Encryption algorithm: $c = \mathrm{E}(3, p) = (p + 3) \bmod 26$

A shift may be of any amount, so that the general
Encryption algorithm: $c = \mathrm{E}(k, p) = (p + k) \bmod 26$ [where k takes on a value in the range 1 to 25]
Decryption algorithm: $p = \mathrm{E}(k, c) = (c - k) \bmod 26$

Weakness: only 25 keys to attempt.

- **Monoalphabetic Cipher**
  - Rather than a constant shift of the alphabet, could shuffle the letters arbitrarily.
  - The key can be any permutation of the 26 alphabetic characters. There are 26! possible keys .

Example:

Plain	:	abcdefghijklmnopqrstuvwxyz
Key	:	DKVQFIBJWPESCXHTMYAUOLRGZN

Plaintext	:	ifwewishtoreplaceletters
Ciphertext	:	WIRFRWAJUHYFTSDVFSFUUFYA

Weakness: Easy to break because they reflect the frequency data of the original alphabet.

- **Playfair Cipher**
  - Best known multi-letter encryption cipher. Treats digrams (two-letter combination) as single units and translates these units into ciphertext digrams.
  - Based on the use of a 5 x 5 matrix of letters constructed using a keyword.

Example:

Plaintext	:	secret message
Keyword	:	MONARCHY

5x5 Matrix:

1. Fill in letters of keyword (minus duplicates) from left to right and from top to bottom, then fill in the remainder of the matrix with the remaining letters in alphabetic order
2. The letters 'I and J' count as one letter

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

Prepare the message:

1. Must be split into pairs
2. Separate all duplicated letters by inserting letter 'x'
3. If there is an odd letter at the end of message, insert letter 'x'
4. Ignore all spaces

secret message → SE CR ET ME SX SA GE

Encoding Rules:

1. If in same column, move each letter Down ONE. Upon reaching end of table, wrap around.
2. If in same row, move each letter Right ONE. Upon reaching end of table, wrap around.
3. If not in same column or row, form a rectangle and swap the letters with the ones on the end of the rectangle.

SE → LI [Rule 3]
CR → DM [Rule 3]
ET → KL [Rule 1]
ME → CL [Rule 1]
SX → XA [Rule 1]
SA → XB [Rule 1]
GE → IF [Rule 2]
So, the encoded message = LIDMKLCLXAXBIF

- **Polyalphabetic Cipher**
  - Improves on the simple monoalphabetic technique by using different monoalphabetic substitutions as one proceeds through the plaintext message

Example:

Plaintext : bee
Keyword : 54321

1	A	B	C	D	E
2	B	C	D	E	F
3	C	D	E	F	G
4	D	E	F	G	H
5	E	F	G	H	I

b with key 5, intersection is: F
e with key 4, intersection is: H
e with key 3, intersection is: G

Ciphertext : FHG

- **Vigenère Cipher**
  - Best known and one of the simplest polyalphabetic substitution ciphers
  - To encrypt a message, a key is needed that is as long as the message and usually, the key is a repeating keyword.

  Encryption formula : $C_i = (P_i + k_{i \bmod m}) \bmod 26$
  Decryption formula : $P_i = (C_i - k_{i \bmod m}) \bmod 26$

Example:

Plaintext : we are discovered save yourself
Keyword : deceptive

Plaintext : wearediscoveredsaveyourself
Key : deceptivedeceptivedeceptive

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

The cipher character = numeric value of the character + key (shift)

For first plaintext character ‘w’, the cipher = 22 (numeric value of w) + 3 (numeric value of key) = 25 (Z)

Ciphertext : ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Modulo Operation

```
X mod n = X – [int(X/n) x n]

24 mod 26 = 24 – [int(24/26) x 26] = 24 – 0 = 24

48 mod 26 = 48 – [int(48/26) x 26] = 48 – [1 x 26] = 48 – 26 = 22
```

- **One-Time Pad (OTP)**

- Use a random key as long as the message so that the key need not be repeated
- Key is used to encrypt and decrypt a single message and then is discarded
- Each new message requires a new key of the same length as the new message

Strengths

- Scheme is unbreakable as it produces random output that bears no statistical relationship to the plaintext
- Because the ciphertext contains no information whatsoever about the plaintext, there is simply no way to break the code

Weakness

- OTP offers complete security, but in practice has two fundamental difficulties
    - There is the practical problem of making large quantities of random keys. Any heavily used system might require millions of random characters on a regular basis
    - For every message, a key of equal length is needed by both sender and receiver

Transposition Techniques

- **Rail Fence Cipher**

- Simplest transposition cipher
- Plaintext is written down as a sequence of diagonals and then read off as a sequence of rows
- The depth of the matrix is the encryption key

Example:

Plaintext : `meet me after the toga party`
Key : `2`

m		e		m		a		t		r		h		t		g		p		r		y
	e		t		e		f		e		t		e		o		a		a		t	

Ciphertext : `MEMATRHTGPRYETEFETEOAAT`

- **Row Transposition Cipher**

- A more complex transposition
- Write the message in a rectangle row by row. Read the message off column by column as per the key value order.
- Number of rows = message length / key length

Example:

Plaintext : `attackpostponeduntiltwoamxyz`
Key : `4312567`

4	3	1	2	5	6	7
a	t	t	a	c	k	p
o	s	t	p	o	n	e
d	u	n	t	i	l	t
w	o	a	m	x	y	z

Ciphertext : `TTNAAPTMTSUOAODWCOIXKNLYPETZ`