Unit I

Q.1. List & briefly define categories of security services

→ 1] Authentication -
The assurance that the communicating entity is the one that it claims to be.

① Peer entity authentication -
used in association with a logical connection to provide confidence in the identity of the entities connected.

② Data-origin authentication -
It is connectionless transfer, provides assurance that the source of received data is as claimed.

2] Access control -
The prevention of unauthorized use of a resource.
This service controls who can have access to a resource, under what conditions access can occur.

3] Data confidentiality -
The protection of data from unauthorized disclosure

① connection confidentiality -
The protection of all user data on a connection.

② connectionless confidentiality -
The protection of all user data in a single data block.

③ selective field confidentiality -
The confidentiality of selected fields within the user data on a connection or in a single data block.

④ traffic flow confidentiality -
The protection of the info that might be derived from observation of traffic flows.

4) data integrity -
The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, replay).

① connection integrity with recovery -
Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion or replay of any data within an entire data sequence, with recovery attempted.

② connection integrity without recovery -
provides only detection without recovery.

③ selective - field connection integrity -
Provides for the integrity of selected fields within the user data of a data block transferred over a connection.

④ connectionless integrity -
Provides for the integrity of a single connectionless data block & may take the form of detection & data modification.

⑤ selective - field connectionless integrity -
Provides for the integrity of selected field within a single connectionless data block.

5] Non - repudiation -
Provides protection against denial by one of entities involved in communication of having participated in all or part of communication.

Q.2. Explain X.800 security mechanism.

→ 1. A service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers.

2. Divided into - ① specific security mechanisms.
② pervasive security mechanisms.

3. specific security mechanism -
- May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.
- Encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization.

4. Pervasive security mechanism -
- Mechanism that are not specific to any particular OSI security service or protocol layer.
- Trusted functionality, security labels, event detection, security audit trails, security recovery.

5. Encipherment - The use of mathematical algo. to transform data into a form that is not readily intelligible.

6. access control - a variety of mechanisms that enforce access rights to resources.

7. data integrity - a variety of mechanisms used to assure the integrity of data unit or stream of data units.

8. authentication exchange -
A mechanism intended to ensure the identity of an entity by means of info exchange.

9. Traffic padding -
The insertion of bits into gap in a data stream to frustate traffic analysis attempts.

10. & Trusted functionality -
That which is perceived to be correct w.r.t some criteria.

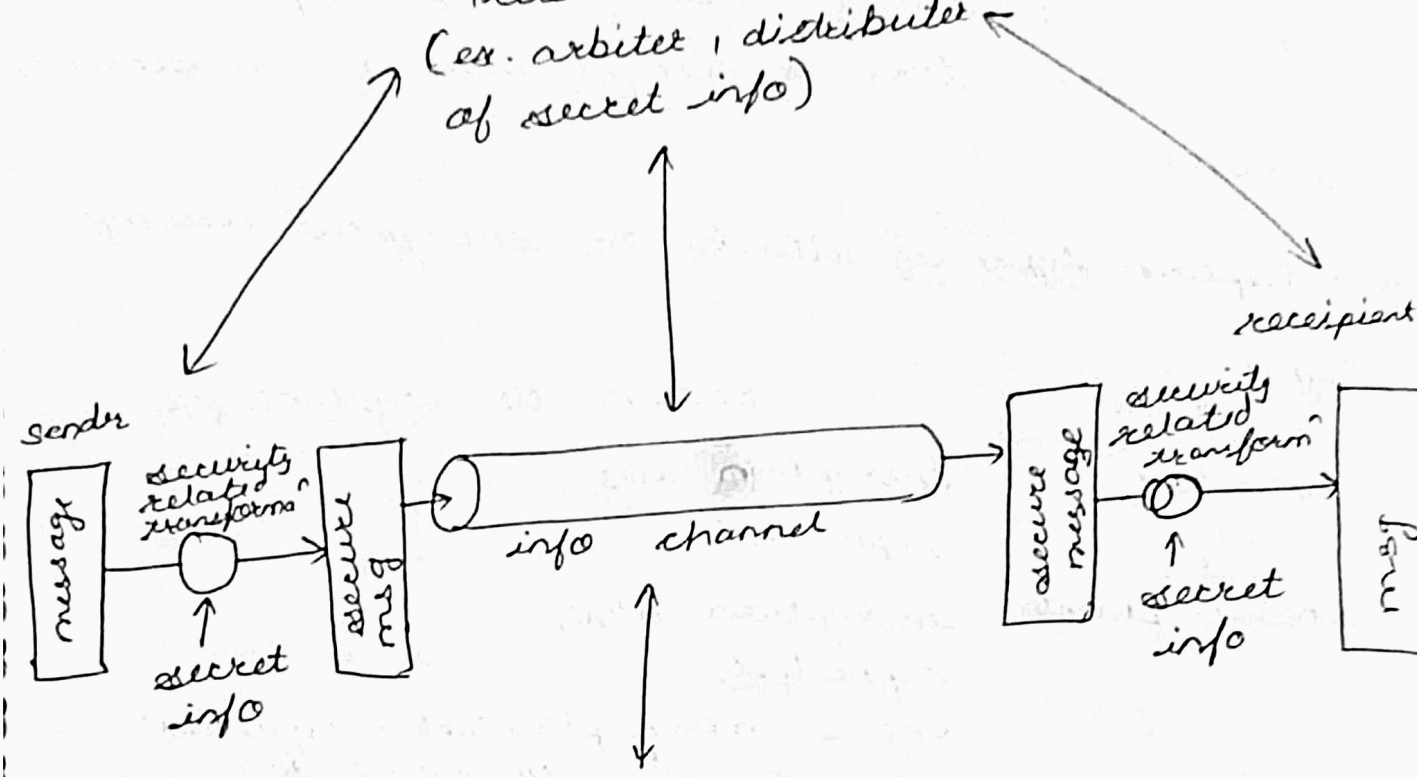
11. security label -
The marking bound to a resource that names or designates the security attributes of that resource.

12. Event detection -
detection of security relevant events.

13. security audit trail -
Data collected & potentially used to facilitate a security audit, which is an independent review and examination of system records & activities.

14. security recovery -
Deals with requests from mechanisms, such as event handling & takes recovery actions.

Q.3. Explain model for network security.



- All the techniques for providing security have two components:-

1. A security related transformation on the info to be sent. Ese include the encryption of msg & the addition of a code to verify the identity of sender.
2. Some secret info shared by the two principals and it is hoped, unknown to the opponent.
   Ex - encryption key is used.

- Using this model requires us to:-

1, design a suitable algo. for the security transformation.

2. generate the secret info used by algo.

3. develop methods to distribute & share secret info.
4. specify a protocol enabling the principals to use the transformation & secret info for a security service.

Q.4. Explain types of attacks on encrypted message.

Types of attack	known to cryptanalyst
ciphertext only	encryption algo, ciphertext
known plaintext	encryption algo, ciphertext, one or more plaintext - ciphertext pairs formed with secret key
chosen plaintext	encryption algo, ciphertext, plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
chosen ciphertext	encryption algo, ciphertext, ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with secret key.
chosen text	encrypted algo, ciphertext, plaintext msg chosen by cryptanalyst, together with its corresponding ciphertext generated with secret key,

ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key.

Q.5. List & briefly define types of cryptanalytic attacks based on what is known to the attacker.

→ same as Q.4.

Q.6 Explain substitution ciphers ceaser, monoalphabetic, playfair & hill.

→ 1) <u>ceasar cipher</u>

1. ciphertext letter = plaintext letter + 3 (mark)
2. It is the earliest known substitution cipher by Julius Caesar.
3. first attested use in military affairs.
4. replaces each letter by 3rd letter on
5. Ex - meet me after toga party
   PHHW PH DIWHU WRJD SDUWB
6. can define transformation as :-

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U

s	t	u	v	w	x	y	z
V	W	X	Y	Z	A	B	C

7. Mathematically give each letter a number

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

q	r	s	t	u	v	w	x	y	z
16	17	18	19	20	21	22	23	24	25

2. Then have caesar cipher as:-

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

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

where p - plain text letter
k - position down the alphabet value in the range 1 to 25.

3) Monoalphabetic cipher

1. Arbitary substitution of letters
2. rather than just shifting the alphabet could shuffle (jumble) the letters arbitarily.
3. Each plaintext letter maps to a different random ciphertext letter.
4. here key is 26 letters long
5. Number of keys $26 \times 25 \times \ldots \times 1 = 26! = 4 \times 10^{26}$
6. Regularities in the language can be exploided
7. transformation -

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

8. Eg -
plaintext - if we wish to replace letters
ciphertext - W Z R F R W A J U H Y F T S D V F S F U U F Y A

9. There are total $26! = \approx 4 \times 10^{26}$ keys, but even with so many keys. it would not be secure
10. Problem is language characteristics.

11. Letters like z, j, k, q, x are rarely used whereas other letters like a, e, are mostly used.
12. Monoalphabetic substitution ciphers do not change with relative letter frequencies.
13. Calculate letter frequency for ciphertext, compare counted plate against known rules.
14. For monoalphabetic must identify each letter - tables of common double/triple letters help.
15. Monoalphabetic ciphers are easy to break because they reflect the frequency of data of the original text.

3] playfair cipher -

1. One approach to improving security was to encrypt multiple ~~times~~ letters.
2. Playfair cipher was invented by charles Wheatstone in 1854, but named after his friend Baron Playfair.
3. A 5×5 matrix of letters based on a keyword - fill in letters of keyword - fill rest of matrix with other letters
4. 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

5 - Advantages -

① 26 x 26 diagrams (two letter combinations)

② Possible keys = 25!25! keys.

6 - Disadvantages of -

① leaves much of language structure

② few 100s of ciphertext are enough for cryptanalysis.

7 - Security much improved over monoalphabetic.

8 - it can be broken, given a few hundred letters since still has much of plaintext structure.

4] Hill ciphet -

1. developed by mathematician Lester Hill in 1929.
2. The encryption algo takes m successive plaintext letters & substitutes for them m ciphertext letters
3. The substitution is determined by m linear eq^n in which each character is assigned a numerical value (a=0, b=1, ... z=25).
4. For m=3, the system can be described as -

$$c_1 = (k_{11}p_1 + k_{12}p_2 + k_{13}p_3) \bmod 26$$

$$c_2 = (k_{21}p_1 + k_{22}p_2 + k_{23}p_3) \bmod 26$$

$$c_3 = (k_{31}p_1 + k_{32}p_2 + k_{33}p_3) \bmod 26.$$

This can be expressed in termed of row vectors & matrices -

$$(c_1\ c_2\ c_3) = (p_1\ p_2\ p_3)\begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \bmod 26$$

4. The use of larger matrix hides more frequency info.
5. Thus a 3×3 hill cipher hides not only single-letter but two-letter frequency info.

Q.7. Explain polyalphabetic substitution cipher Vigenere, autokey & one-time pad.

→ i] Vigenere cipher -

1. Simplest polyalphabetic substitution cipher is the Vigenere cipher.
2. Effectively multiple caesar ciphers.
3. Key is multiple letters long $K = K_1 K_2 \ldots K_d$.
4. i^{th} letter specifies i^{th} alphabet to use.
5. Write the plaintext out, write the keyword repeated above it, use each key letter as a caesar cipher key, encrypt the corresponding plaintext letter.
6. Eg - using keyword deceptive.

key - deceptive deceptive deceptive
plaintext - we are discovered save yourself
ciphertext - ZICVTWQNGRZ GVTWAVZHCQYGLMGJ

7. Have multiple ciphertext letters for each plaintext letter.
8. Hence letter frequencies are obscured, but not totally lost.

2] autokey cipher -

1. ideally want a key as long as message.
2. Vigenere proposed the autokey cipher.
3. keyword is prefixed to message as key.
4. Knowing keyword can recover the first few letters.
5. use these in turn on the rest of message.
6. but still have frequency characteristics to attack
7. Ex - given key deceptive.

key :- deceptive we are discovered sav
plaintext :- we are discovered save yourself
ciphertext :- ZICV TWQNGKZEII GASXTSLVVWLA

3] one-time pad -

1. If a truly random key as long as the message is used, the cipher will be secure called one-time pad.
2. It is unbreakable since ciphertext bears no statistical relationship to the plaintext.
3. since for any plaintext & any ciphertext there exist a key mapping one to other., can use only the key once.
4. Problem of -
   ① making large quantities of keys
   ② safe distribution of key.

Q. 11. Explain transposition techniques.

→ 1. Transposition techniques hide the message by rearranging the letter order without altering the actual letters used.

2. can recognise these since have the same frequency distribution as the original text.

3. Perform some permutations on plaintext letters.

4. Ex - ~~Raif~~ Rail fence cipher
transposition matrix.

5. Rail fence cipher

① Write message letters out diagonally over a number of rows.

② then read off cipher row by row.

③ Ex - write message "meet me after toga the party" out as:

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

④ giving ciphertext

MEMATROAHPRYETEFETGTEAT

6. Transposition matrix

① A more complex ~~matrix~~ scheme

② write letters of message out in rows over a specified number of columns.

③ Then reorder the columns according to some key before reading off the rows.

Key:- 4 3 1 2 5 6 7

plaintext:- 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.

(4) More than one stage of transposition.

Q.12. Explain operation of rotor machine.

→ (1) Multiple stages of encryption can produce an algo. that is significantly more difficult to cryptanalyze.

(2) Before DES, rotor machines use multiple stages of encryption.

(3) Machine consist of set of independently rotating cylinders through which electrical pulses can flow.

(4) Each cylinder has 26 input pins & 26 output pins, with internal wiring that connects each input pin to a unique output pin.

(5) single cylinder defines a monoalphabetic substitution

(6) Before modern ciphers, rotor machines were most common product cipher

(7) implemented a very complex, varying substitution cipher

(8) used a series of cylinders, each giving one substitution, which rotated & changed after each letter was encrypted.