define systematic way of defining & providing security mechanism

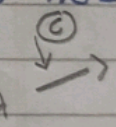
(x.800) The OSI Architecture (ITU-T international telecom union - telecommunication)

OSI security Architecture (open system interconnect)

security attack	security mechanism	security service
Attack when security of system is compromised by some action of a illegle activity.	it is to detect or prevent the attack	↳ A service that enhance the security of the data processing system & the info. transfers of an organization the services make use of one or more security mechanisms.

eg: Passive & Active

Passive:- Attempts to learn or make use of information from the system but does not affect system resources. (only observe)
system is monitored and sometimes scanned.



Types 1) The release of msg content
2) Traffic analysis. (when msg is encrypt find origin of msg or way of msg)
3) eg: telephonic conversation, mail msg.

Active:- observe + read + write + modify
Active attacks involve some modification of the data. or a creation of a false stream and can be subdivided into four categories

1) masquerade (get username & password and sends msg to B) (one entity pretends to diff entity)
2) replay (retransmission after some time)
3) modification of msg (modify actual data)
4) danial of service (generate traffic)

Handling Attack (Mechanisum)

1) Passive attacks - focous on prevention
   - easy to stop
   - Hard to detect

2) Active attacks - focous on Detection and Recovery
   - Hard to stop
   - Easy to detect.

Symmetric key :-
same key, single key , primary key

Asymmetric key:-
Two key / Public key.

security service:-
- Authentication:- credentials provided are compared with local database of auth user if match then user granted.
- Access control - Prevention to use resource
- Data confidentiality :- Protection of data from unauthuser
- Data integrity - assurance that data is received.

security services:-
Digital signature

Date 3/Feb

substitution Technique:- (monoalphabetic)

1) Geasar Ciphex
   LHEL for L every time N
   key 2

$C = (P+K) \bmod 26$ (encryption)

P = Plain text
C = Ciphex text

P = NEP K = 2
C = PGR

For (Decryption)

$P = (C-K) \bmod 26$

general : $C = E(K,P) = (P+K) \bmod 26$ (encrypt)

$C = E(K,P) = (C-K) \bmod 26$ (decrypt)

2) Playfair Ciphex (multiple -letter) (polyalphabetic)
   one → many

eg:
key : monarchy
Plaintext: instruments.

based on 5*5 matrix of key

m	o	n	a	y
c	h	y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

- Plaintext is split into pairs of two letters (diagrams)
- if there is an odd no of letter, a 'z' is added to the last letter

1) PT: instruments

'in' 'st', 'ru', 'me', 'nt' 'sz'

Algo: To encrypt it
eg. matrix above

1) if both the letters are in the same col Take the letter below each one (going back to the left most

eg me → 1st col
m → c e → L

2) 11th For row

St → 4th row
s → t t → L

3) not col & row (Form Rectangle with two letter and take the letters on opposite corner)

eg nt

n → x , t → q

n → t
↓ ↑
t ← t

instruments (PT)
+L mz cL rq T (ET)

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

eg Technology (PT)

"Te" , ch, no, lo, gy
LK hy an pm qg decryption opposite same

Hill Cipher:- (Polyalphabetic)
it is based on linear algebra

eg: input: PT: ACT
key: GYBNQKURP

For Encryption

key matrix n=3 (ACT) matrix ACT

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \qquad \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$$

multiply

$$\begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} \pmod{26}$$

then Remainder Matrix

$$\begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix}$$

= POH

$A^{-1} = \frac{1}{|A|} \times$

Decryption:-

Take inverse matrix of key

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}^{-1} = \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix}$$

Adj =

	1st	2nd			
	6	24	1	6	24
	13	16	10	13	16
	20	17	15	20	17
1st row	6	24	1	6	24
2nd row	13	16	10	13	16

$$\begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix}$$

$$\begin{bmatrix} 260 \\ 574 \\ 539 \end{bmatrix} \pmod{26}$$

$$= \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$$

then original plan text : AGT

Polyalphabetic Substitution Ciphers:-

Vigenere Ciphers :-

Eencrypt — repeate key

key: d e c e p t i v e d e c e p t i v e d e c e p t i v e

plaintext: w e a r e d i s c o v e r e d s a v e y o u r s e l f

ciphertext : z I G V T W Q N G R Z G V T W A H . . .

Hello

H 10

decrypt :- Key — ~~Plaintext~~ C.T.

Transposition Technique:

1) Rail fence technique

PT : " meet me after the toga party "

depth - 2 (rows = 2)

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

Depth - 3

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

ciphertext : mm th gr et afe te oa ate artpy

2) Message Rectangle technique:-

key: 4 8 1 2 5 6 7

PT : "attack postponed until two am"

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

CT: t t h a a p t m t s u o a o d w c o i x k n l y p e t z

1 col — 2nd col

multiple stages of encryption can produce algorithm ... independent. more difficult to cryptanalyze. it is substitution tech it consis rotar cylinders each cylinder has 26 input pins and 26 output pins each input pin to a unique output pin

1) Rotax Machine (substitution technique)
2) Steganography technique involve hiding sensitive info within ordinary non-secrcate file so it will not be detected
types:- text- data hidden in words, Image:- data in form of pixels are having data audio, video etc.

Stream Cipher Vs block Ciphes

1) Stream Ciphes:-
encrypt data stream one bit or one byte at a time

2) block cipher:-

DES (Data encryption std) with diagram

PT: 64 bit block C.T. = 64 bit block
key: 56 bit (64-8)

based on block Cipher technique

64 bit input ——> 64 bit output

Decryption: same step, same key

64 bit input

64 bit key

Permuted choice 1

56 (key)

initial permutation

64

Round 1 ← 48 (K1) ← Permuted choice 2 ← 56 ← left circular shift

2

16

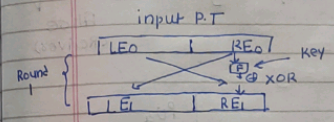
32-bit swap

inverse →

Strength of DES
1) The use 56 bit key
2) strong DES Algorithm: Rounds
3) Resistant to timing attack

Design principle:-
1) No. of Rounds
2) Design function F eg:
3) key schedule algorithm.

Feistel ciphes structure. (Algorithm for DES) Round



Unit 2

symmetric key (conventional Encry)	Asymmetric key (Public key)
same algo for encry & Decry	one algo for encryption and another for decryption
same key	Pair of keys