2K17/MC/87

ASSIGNMENT - 1

Cryptography and Network Security

1) Types of attack threatning the Confidentiality of Informat:

(i) Packet Capturing (Packet Sniffing) :- In this type of attack the Attacker Capture the data packets in travel. Once the data is captured, the attacker use it to read sensitive information like password or Card Number.

(ii) Password Attacks :- Password based attacks are used to hack the password of target computer to grab access. The attacker may use all the words of Dictionary or some common passwords (called Dictionary attack) or the attacker can simply try all possible combinations

(iii) Dumpster Diving :- Dumpster Diving is Searching through the company dumpsters for any information that can be useful for an attacker for attacking a network.

(iv) Wiretapping :- wire tapping is a type of Network attack that runs in where the Attacker hacks the telecommuni cation devices, listen to phone calls of others

(v) Keylogger :- keylogger is a programme that runs in background of a Computer, logging the users keystrokes. After a user Enters a password, it is stored in the log created by keylogger & forwarded to the Attacker.

(vi) Phising & Pharming :- phising is an attempt to hack sensitive information by sending associated emails with fake URL's. Pharming is another network attack. aimed at indirecting the traffic of one website to another website.

(VII) Social Engineering :- Social Engineering is a type of attack in which someone with very good interactive skills manipulates others into revealing info about network can be used to steal data.

2.) Security Services defined by ITU (X800)

(I) Authentication :- These services for the Authentication of a communicating peer entity of source of data.

- Peer Entity Authentication :- This service, when provided by the (N)-layer provides corroboration to (N+1)-entity that the peer Entity is claimed (N+1)-entity.
- Data Origin Authentication :- This service when provided by the (N) layers provides corporation to an (N+1) entity that the source of the data is claimed.

(II) Acess Control :- This service provides protection against unauthorized use of sources availble via OSI

(III) Data Integrity :- The service counters active threats and may take one of the forms described below..

- Connection Integrity with recovery

This service provides for the integrity of all (N)-user data of an (N)-connection & detects any modification, insertion, deletion or replay of any data within an entire SDU sequence.

- Connection Integrity without recovery

Same as previous but with no recovery attempted.

- Non-Repudation

This service may take one or both of two forms.

(i) Non repudation with proof of origin.

(ii) Non repudation with proof of delivery.

3) Security Mechanism to provide Security Services

(i) Digital Signature : It's a mathematical scheme to verify the Authenticity of digital message Documents.

(ii) Encipherment : Process of making data Unreadable to Unauthorized identities by using cryptographic algo.

(iii) Access Control : regulates who or what can view use resource in a Computing environment.

(i) Physical access control : limits access to Campus, building, room & physical IT assets.

(ii) logical assets control : limits connections to Computer networks system files on data.

(iv) Data Integrity : maintainence the assurence of accuracy & Consistency of data over it's entire life cycle and is a critical aspect of design.

(v) Traffic padding : mechanisms that are used to protect against traffic analysis attack.

4) Affine Caesar Cipher is defined as:

$$C = E([x, b], p) = (xp + b) \bmod 26.$$

now in order for it to be one to one x & 26 should be so co-prime or inverse of x modulus 26 should exist.

$\Rightarrow$ x cannot be a multiple of 2 & 13.

$\Rightarrow$ values of x not allowed are - {2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26}

5.)

M	P	H	Y	K
O	N	Q	R	T
Z	V	W	X	Y
E	L	A	B	G
D	S	F	I/J	C

P: must See you over the Cadogan west Coming out Cadogan holding the plain text in group of four alphabets.

P: MU ST SE EY OU ER CA DO GA NW ES IC OM

C: U2 7B DL G2 PN NW LG 7G TU ER OV LD UH

JN GA TO NC EX

FF ED HW DS R2

Cipher text :- U27BDLG2PNNWLG7GTUERDOULDDSUHFFFDHWDSR2

6). i (i) In play/air cipher we use a 5x5 matrix So on ignoring the fact that some keys might produce identical results, we can have 25! different keys.

→ as for 1st letter we have 25 options, for 2nd with have 24 options.

$25C_1 \times 25 \times 24C_1 \times 24 \cdots = 25!$

(ii) Now we note that any notation along the rows or the columns leads to an equivalent key i.e. the cipher texts would be the same for such keys.

So the Equivalent is $= \frac{25!}{5 \times 5} = 24!$

7) Given plaintext = Explanation & key = leg, applying w/g rule cipher algo

P: E X P L A N A T I O N

K: L E G L E G L E G L E

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

P	K	C	
E (4)	L (11)	11+4 = 25 mod 26	= 15 (P)
X (23)	E (4)	23+4 = 27 %. 26	= 1 (B)
P (15)	G (6)	15+6 = 21 %. 26	= 21 (V)
C (11)	L (11)	11+11 = 22 %. 26	= 22 (W)
A (0)	E (4)	4+0 = 4 %. 26	= 4 (E)
N (13)	G (6)	6+13 = 19 %. 26	= 19 (T)
A (0)	L (11)	11+0) = 11 %. 26	= 11 (L)
T (19)	E (4)	19+4 = 23 %. 26	= 23 (X)
I (18)	G (6)	18+6 = 24 %. 26	= 14 (O)
O (14)	L (11)	11+14 = 25 %. 26	= 25 (Z)
M (13)	E (4)	13+4 = 17 %. 26	= 17 (R)

Cipher text : PBVW ET LXUZR.

8). K = GUIDENCE, Using this keyword to make matrix, we get

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

Now plain given, plain text = G The key is hidden under the splitting P into digraphs & applying algo, we get.

P : TH EP EY IS HI DX DE NU EP TH ED OX

C : PO VU OZ DR LG IY EG CG BG IT PO GE

OR PA DX

LZ LT RN

PO VU OZ DR LG IY EG CE BG IT PO GE LZ IT RN IY.

9) (a) Since everyone has acess to both plain text and cipher text therefore it'll be a known plain text attack.

b) P: A B C D E K H J I
C C A B D F H F I J

1	2	3	4	5
2	3	1	4	5

Key → [2 3 1 4 5]

⇒ the size of permutation key is 5.

10) (i) the occurancy / frequency analysis of the given cipher text.

this will given the following result :

Alphabet	# of occurance in P.	frequency.
C	37	14.45 %
G	24	9.38 %
G	20	7.81 %
K	18	7.03 %
Y	15	5.86 %
I	15	5.86 %
U	14	5.47 %
N	13	5.08 %
Z	13	5.08 %
E	12	5.08 %
O	10	
F	→ 9	
D	8	
L, X	→ 7	
J	→ 6	
P, W, M, H	→ 5	
A	→ 1	
Q	→ 1	

(ii) based on the frequencies we can make a guess for the key, like in the cipher text C is the most frequent letter, so we can replace C by E (which is generally the most frequent letter in plain English text.

so, proceeding in this similar manner, we get,

K = 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
V K E B I W A F D C S Y M L N U F Y O 2 T Q G P R H

So, Note Here key refers to the decryption key

Now here is plain text.

I MAY NOT BE ABLE TO GROW FLOWERS BUT MY GARDEN PRODUCES JUST AS MANY DEADLEAVES OLD OVER SHOES PIECES OF ROPE AND BUSH ELSE DEAD GRASS AS ANYBODY SEND TODAY I BAUGHT A WHEEL BARROW TO HELP IN CLEANING IT UP I HAVE ALWAYS LOVE AND RESPECT TO WHEELBARROW IT IS ONE WHEELED VEHICLE OF WHICH IM MASTER.

P → I may not be able to grow flowers but my garden produces just as many dead leaves old over today I baught a wheelbarrow to help in cleaning it up. I have always loved and respected the wheelbarrow. It is one wheeled vehicle of which I'm perfect master.

11). P: LET US MEET NOW
C: H BC DF N OPT K I B

P:	11	4	19	20	1	8	1	2	4	19	13	14	22
C:	7	1	2	3	5	13	14	15	8	10	11		1

in hill cipher, we know.

$C = PK \bmod 26$

let $m = 2$, $E_K(11,4) = (3,1)$

$E_F = (19,20) = (8,23)$

$$\begin{bmatrix} 7 & 1 \\ 2 & 3 \end{bmatrix} = \begin{bmatrix} 11 & 4 \\ 19 & 20 \end{bmatrix} K \Rightarrow K = \begin{bmatrix} 11 & 4 \\ 19 & 20 \end{bmatrix} \begin{bmatrix} 7 & 1 \\ 2 & 3 \end{bmatrix}$$

$$K = \frac{1}{144} \begin{bmatrix} 20 & -4 \\ -19 & 11 \end{bmatrix} \begin{bmatrix} 7 & 1 \\ 2 & 3 \end{bmatrix}$$

$$K = \frac{1}{144}\begin{bmatrix} 20 & -4 \\ -19 & 11 \end{bmatrix}\begin{bmatrix} 7 & 1 \\ 2 & 3 \end{bmatrix}$$

$$k = \frac{1}{144}\begin{bmatrix} 132 & 8 \\ -111 & 14 \end{bmatrix}$$

$$c = \begin{bmatrix} 7 & 1 \\ 2 & 3 \end{bmatrix} \quad P = \begin{bmatrix} 11 & 4 \\ 19 & 20 \end{bmatrix}$$

$C = (PK) \bmod 26$.

$K = P^{-1}C$

$\det P = 11 \times 20 - 4 \times 19 = 144 \bmod 26$

$= 14$

Since inverse of 14 mod 26 doesnot exist.

$\Rightarrow m \neq 2$

let $m = 3$

$F_K(11, 4, 19) = (7, 1, 2)$

$F_K(20, 8, 12) = (3, 5, 13)$

$F_K(4, 4, 14) = (14, 15, 8)$

$$\begin{bmatrix} 7 & 1 & 2 \\ 3 & 5 & 13 \\ 14 & 15 & 8 \end{bmatrix} = \begin{bmatrix} 11 & 4 & 19 \\ 20 & 18 & 12 \\ 4 & 4 & 19 \end{bmatrix}$$

$K = P^{-1}C$

$\det P = 2058 \bmod 26 = 4$

$\Rightarrow$ key doesn't exist for 3×3 even.

since $eP \rightarrow CC$

$e \rightarrow P$

therefore $m \neq 1$

for 2 we don't have sufficient data, for $m > 3$

we calculate for $m > 3$, Allcent different plain text.

12). $k = (9, 0, 1, 7, 23, 15, 21, 11, 11, 2, 8, 9)$

P	k	C
S (18)	9	$18+9 = 27 \bmod 26 =$ B
E (4)	0	$4+0 = 4 \bmod 26$ E
N (13)	1	$13+1 = 14 \bmod 26$ O
D (3)	7	$7+3 = 10 \bmod 26$ K
M (12)	23	$23+12 = 35 \% 26$ J
O (14)	15	$15+14 = 29 \% 26$ D
R (17)	21	$17+21 = 38 \% 26$ M
E (4)	14	$4+14 = 18 \% 26$ S
M (12)	11	$12+11 = 23 \% 26$ X
O (14)	11	$14+11 = 25 \% 26$ Z
N (13)	2	$13+2 = 15 \% 26$ P
E (4)	8	$8+4 = 12 \% 26$ M
Y (24)	9	$9+24 = 33 \% 26$ H

C: BEOKJDMSXZPMH.