CRYPTOGRAPHY & NETWORK SECURITY

MC-407

ASSIGNMENT - 1

AIMAN SIDDIQUA - 2K18/MC/008

(1.) Different types of attack threatening the confidentiality of information :-

(i) SNOOPING

Snooping refers to unauthorized access to or interception of data. For example, a file transferred through the internet may contain confidential information. An unauthorized entity may intercept the transmission and use the contents for their own benefit. To prevent snooping, the data can be nonintelligible to the intercepter by using enchipherment techniques.

(ii) TRAFFIC ANALYSIS

Although encipherment of data may make it nonintelligible for the interceptor, she can obtain some other type of information by monitoring online traffic. For example, she can find the electronic address (like email address) of the sender or the receiver. She can collect pairs of requests and responses to help her guess the nature of transaction.

Scanned with CamScanner

(2) Security services defined by ITU-T (X.800) ~~to~~ related to ~~provide~~ the security goals and attacks:-

(i) DATA CONFIDENTIALITY

It is designed to protect data from disclosure attack. The service as designed by X.800 is very broad and encompasses confidentiality of the whole message or a part of the message and also protection against traffic analysis. That is, it is designed to prevent snooping & traffic analysis attacks.

(ii) DATA INTEGRITY

It is designed to protect data from modification, insertion, deletion and replaying by an adversary. It may protect the whole message or a part of the message.

(iii) AUTHENTICATION

This service provides the authentication of the party at the other end of the line. In connection oriented communication, it provides authentication of the sender or receiver during the connection establishment (peer entity authentication). In connectionless communication, it authenticates the source of data (data origin authentication).

(iv) NON REPUDIATION

This service protects against repudiation by either the sender or the receiver of the data.

Scanned with CamScanner

In nonrepudiation with proof of origin, the receiver of the data can later prove the identity of the sender if denied. In nonrepudiation with proof of delivery, the sender of data can prove that data were delivered to the intended receiver.

(v) ACCESS CONTROL

It provides protection against unauthorized access to data. The term access is very broad and can involve reading, writing, modifying, executing programs and so on.

(3.) Security mechanism recommended by ITU-T (X.800) to provide the security services are:

(i) Encipherment - Hiding or covering of data can provide confidentiality. Two techniques - cryptography & steganography are used for encipherment.

(ii) Data Integrity - The mechanism ~~depen~~ appends to the data a short checkvalue that has been created by a specific process from the data itself. If the checkvalue created by receiver matches, the integrity of data is preserved.

(iii) Digital Signature - It is a means by which the sender can electronically sign the data and the receiver can electronically verify the signature.

Scanned with CamScanner

(iv) Authentication Exchange - In this two entities exchange some messages to prove their message identity to each other. For example, one entity can prove that she knows a secret that only she is supposed to know.

(v) Traffic Padding - It means inserting some bogus data into the data traffic to thwart the adversary's attempt to use the traffic analysis.

(vi) Routing Control - It means selecting and continuously changing different available routes between the sender and the receiver to prevent the opponent from eavesdropping on a particular route

(vii) Notarization - It means selecting a third trusted party to control the communication between two entities. This can be done to prevent repudiation.

(viii) Access Control - It uses method to prove that a user has access right to the data or resources owned by a system. Examples passwords & PINs.

(4.) Playfair Matrix:

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

Scanned with CamScanner

Plaintext :- "Must see you over Cadogan West Coming at once." (Add bogus 'x' at the end)

Encrypted Text :
APTLCNYGNPNHPGDYTUQU OFNCLDPHFPQY
WHESUK

(5.) i) We use a 5x5 matrix. Ignoring the fact that some keys may produce identical results we have 25! different keys.

ii) For any notation along the rows or the columns lead to an equivalent key.
Equivalent value is $\frac{25!}{5 \times 5} = 24!$

(6.) Vigenere Cipher :-
Keyword :- "LEG" Plaintext :- "start ieambush"

P= STARTTHEAMBUSH
K= LEGLEGLEGLEGLE

$C_i = (P_i + K_i) \bmod 26$

P_i	K_i	C_i	
S	L	$(18+11) \bmod 26 = 3$	(D)
T	E	$(19+4) \bmod 26 = 23$	(X)
A	G	$(0+6) \bmod 26 = 6$	(G)

Scanned with CamScanner

R	L	(17+11) mod 26 = 2	(C)
T	E	(19+4) mod 26 = 23	(X)
T	G	(19+6) mod 26 = 25	(Z)
H	L	(7+11) mod 26 = 18	(S)
E	E	(4+4) mod 26 = 8	(I)
A	G	(0+6) mod 26 = 6	(G)
M	L	(12+11) mod 26 = 23	(X)
B	E	(1+4) mod 26 = 5	(F)
U	G	(20+6) mod 26 = 0	(A)
S	L	(18+11) mod 26 = 3	(D)
H	E	(7+4) mod 26 = 11	(L)

Ciphertext: DXGCXZSIGXFADL

(7.) Using the Keyword PLAYFAIR to generate the matrix

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

Plaintext: THE KEY IS HIDDEN UNDER THE DOOR PAD.

Ciphertext:
QMGMKPCNEBCZIMUPTIGIQMMISV
VGLYCZ.
(using 'x' as bogus letter)

Scanned with CamScanner

(8.) (a) Since everyone has access to plaintext and ciphertext, therefore it is a plaintext attack.

(b)

P:	A	B	C	D	E	F	G	H	I	J
C:	C	A	B	D	E	H	F	G	I	J

1	2	3	4	5
3	1	2	4	5

Key = [3 1 2 4 5]

The size of permutation Key is 5.

(9.) The occurency frequency analysis of the given cipher text.

Alphabet	No. of occurence	Percentage frequency
C	37	14.45%
G	24	9.38%
S	20	7.81%
K	18	7.03%
Y	15	5.86%
I	15	5.47%
U	14	5.08%
N	13	5.07%
Z	13	5.07%
E	12	4.7%
O	10	3.9%
F	9	3.52%
D	8	3.125%

Scanned with CamScanner

L	7	2.73%
X	7	2.73%
J	6	2.34%
P	6	2.34%
W	5	1.95%
M	5	1.95%
H	5	1.95%
A	5	1.95%
Q	1	0.39%

Based on frequencies, we can make a guess for key. Like, in the cipher, C is the most common letter so we can replace C by E (which is generally the most frequent letter in plain english text).

Proceeding in this manner:

Key: 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 X M L N U Y O Z T Q G P R H

Using the decryption key:

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

Scanned with CamScanner

(10) P: LET US MEET NOW
C: HBC DF NOPI KLB

P: 11 4 19 20 18 12 4 4 19 13 14 22
C: 7 1 2 3 5 13 14 15 8 10 11 1

In hill cipher
$C = PK \bmod 26$

let $m=2$, $E_K(11,4) = (7,1)$
$E_K(19,20) = (2,3)$

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

$$K = \frac{1}{144}\begin{bmatrix} 20 & -4 \\ -19 & 11 \end{bmatrix}\begin{bmatrix} 7 & 1 \\ 2 & 3 \end{bmatrix} = \frac{1}{144}\begin{bmatrix} 132 & 8 \\ -111 & 14 \end{bmatrix}$$

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

$C = PK \bmod 26$
$K = P^{-1}C$

let $P = (11 \times 20) - (4 \times 19) = 144 \bmod 26 = 14$
As inverse of 14 doesn't exist, $m \neq 2$

$E_K(11, 4, 19) = (7, 1, 2)$
$E_K(20, 18, 12) = (3, 5, 13)$
$E_K(4, 4, 14) = (14, 15, 8)$

$K = PC$
$|P| = 2058 \bmod 26 = 4$

Scanned with CamScanner

Key doesnt exist for 3x3

For m=4 we dont have enough data,

(11.) K= 9, 0, 1, 7, 23, 15, 21, 14, 11, 11, 2, 8, 9

P= SEND MORE MONEY

P_i	K_i	C_i
S (18)	9	(18+9) mod 26 = 1
E (4)	0	(4+0) % 26 = 4
N (13)	1	(13+1) % 26 = 14
D (3)	7	(3+7) % 26 = 10
M (12)	23	(12+23) % 26 = 9
O (14)	15	(14+15) % 26 = 3
R (17)	21	(17+21) % 26 = 12
E (4)	14	(4+14) % 26 = 18
M (12)	11	(12+11) % 26 = 23
O (14)	11	(14+11) % 26 = 25
N (13)	2	(13+2) % 26 = 15
E (4)	8	(4+8) % 26 = 12
Y (24)	9	(24+9) % 26 = 7

C: BEOKJDMSXZPMH

Scanned with CamScanner