Sir Syed University of Engineering and Technology

Department of Software Engineering

Course Name: Information Security
Submitted By: MUSTAFA
Submitted To: Sir Hassan Zaki
Miss Tahir Aqeel
Batch: 2018
Section: B

ASSIGNMENT # 01

Question # 01:

Search any latest Security attack and briefly describe it in your own words, taking into account the CIA Triad.

Answer # 01:

The latest security attack is ransomware.

Taking into account the CIA tried

The CIA triad is a broadly used data safety model that can information an organization's efforts and policies aimed at retaining its information secure. The model has nothing to do with the U.S. Central Intelligence Agency; rather, the initials stand for the three concepts on which InfoSec based on.

- Confidentiality
- Integrity
- Availability

1. **Confidentiality**: Only licensed users and approaches be capable to get access to or alter data
2. **Integrity**: Data have to be maintained in a right kingdom and no one must be in a position to improperly modify it, both by chance or maliciously
3. **Availability**: Authorized users need to be capable to get access to records each time they want to do so.

So these are the some basic principles which can always remember and keep in mind for any InfoSec professional

Question # 02:

Encrypt and Decrypt your first name using PLAYFAIR Cipher if Key is your father's first name.

Answer # 02:

PLAYFAIR CIPHER

Plaintext: bilquees
Key: AHMED

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

Encryption

Plaintext pair: mu st af ax

So the plain text **"mustafax"** encrypted as **"SD TU BM MV"**

Decryption

So the final result of decryption is 'MUSTAFA'

Question # 03:

Encrypt "wearediscoveredsaveyourself" using VIGENERE Cipher if Key is your first name.

Answer # 03:

VIGENERE CIPHER

Plaintext: wearediscoveredsaveyourself

Key: MUSTAFA

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
0	1	2	3	4	5	6	7	8	9	10	11	12
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
13	14	15	16	17	18	19	20	21	22	23	24	25

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**
P'S Value	22	4	0	17	4	3	8	18	2	14	21	4	17	4	3	18	0	21	4	24	14	20	17	18	4	11	5
Key stream	12	20	18	19	0	5	0	12	20	18	19	0	5	0	12	20	18	19	0	5	0	12	20	18	19	0	5
C's value	8	24	18	10	4	7	8	4	22	6	13	4	22	4	15	12	18	13	4	3	14	6	11	9	23	11	10
Cipher text	I	Y	S	K	E	H	I	E	W	G	N	E	W	E	P	M	S	N	E	D	O	G	L	J	X	L	K

Encryption: ci = (pi +ki) mod 26
CIPHERTEXT:

I	Y	S	K	E	H	I	E	W	G	N	E	W	E	P	M	S	N	E	D	O	G	L	J	X	L	K

Question # 04:

Encrypt and Decrypt any four letter word using HILL Cipher if Key is HILL.

Answer # 04:

Plaintext: bowl
Key: HILL

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
13	14	15	16	17	18	19	20	21	22	23	24	25

Key = $\begin{bmatrix} H & I \\ L & L \end{bmatrix} \longrightarrow \begin{bmatrix} 7 & 22 \\ 11 & 11 \end{bmatrix}$

Plaintext= $\begin{bmatrix} B & W \\ O & L \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & 8 \\ 14 & 11 \end{bmatrix}$

Encryption
C=kp mod 26

$$\begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} \begin{bmatrix} 1 \\ 14 \end{bmatrix}$$

$$\begin{bmatrix} 119 \\ 165 \end{bmatrix} \quad \text{Mod 26}$$

$$\begin{bmatrix} 15 \\ 9 \end{bmatrix}$$

P

$$\begin{bmatrix} \textbf{J} \\ \end{bmatrix}$$

C=kp mod 26

$$\begin{bmatrix} \textbf{7} & \textbf{8} \\ \textbf{11} & \textbf{11} \end{bmatrix} \begin{bmatrix} \textbf{22} \\ \textbf{11} \end{bmatrix}$$

$$\begin{bmatrix} \textbf{144} \\ \textbf{209} \end{bmatrix} \quad \text{Mod 26}$$

$$\begin{bmatrix} \textbf{8} \\ \textbf{25} \end{bmatrix}$$

$$\begin{bmatrix} \textbf{I} \\ \textbf{Z} \end{bmatrix}$$

<u>Cipher text:</u> PJ IZ

<u>Decryption</u>

D=k-1 C mod 26

Find inverse of key notation

k-1=1/|k| adj (k)

Determinant of matrix

$$\begin{bmatrix} \textbf{7} & \textbf{8} \\ \textbf{11} & \textbf{11} \end{bmatrix}$$

= -11

Now find multiplicative inverse of determinant

k-1 =7

Adj of matrix

$$\begin{bmatrix} \textbf{11} & \textbf{-8} \\ \textbf{-11} & \textbf{7} \end{bmatrix}$$

Before decryption we have to remove minus values add 26 on both sides after adding matrix is

$$\begin{matrix} \textbf{11} & \textbf{18} \end{matrix}$$

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

Now k inverse

$$7\begin{bmatrix} 11 & 18 \\ 15 & 7 \end{bmatrix}$$

$$\begin{bmatrix} 77 & 126 \\ 105 & 49 \end{bmatrix} \quad \text{Mod 26}$$

$$\begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix}$$

<u>Cipher text:</u> PJ OB

$$\begin{bmatrix} P \\ J \end{bmatrix} \quad \begin{bmatrix} 15 \\ 9 \end{bmatrix}$$

$$\begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix}\begin{bmatrix} 15 \\ 9 \end{bmatrix}$$

$$\begin{bmatrix} 573 \\ 222 \end{bmatrix}$$

$$\begin{bmatrix} 1 \\ 14 \end{bmatrix}$$

$$\begin{bmatrix} B \\ O \end{bmatrix}$$

$$\begin{bmatrix} I \\ Z \end{bmatrix} \quad \begin{bmatrix} 8 \\ 25 \end{bmatrix}$$

$$\begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix}\begin{bmatrix} 14 \\ 1 \end{bmatrix}$$

$$\begin{bmatrix} 372 \\ 37 \end{bmatrix}$$

$$\begin{bmatrix} \\ \end{bmatrix}$$

22
11

$$\begin{bmatrix} \mathbf{W} \\ \mathbf{L} \end{bmatrix}$$

After Decryption Cipher text: BO WL

Question # 05:

Using ROW TRANSPOSITION Cipher, Encrypt your Postal Address by taking any 6 bit key.

Answer # 05:

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
0	1	2	3	4	5	6	7	8	9	10	11	12
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
13	14	15	16	17	18	19	20	21	22	23	24	25

Plaintext**:** 74700
Key**:** 321654

3	**2**	**1**	**6**	**5**	**4**
7	4	7	0	0	x

Cipher text

1	**2**	**3**	**4**	**5**	**6**
7	4	7	x	0	0
H	E	H	23	A	A

Cipher text:

H	**E**	**H**	**23**	**A**	**A**