CSS Assignment 1

1) Compare

(a) Vulnerability, threat and control

→ Vulnerability

It is a weakness in the security system, for example in procedures, design or implementation that might be exploited to cause loss or harm. A particular system may be vulnerable to unauthorized data manipulation because system does not verify users identity before allowing data access.

Threat

A threat to a computing system is a set of circumstances that has the potential to cause loss or harm. There are many threats to a computer system, including human initiated and computer initiated ones. Examples of threats include virus, trojan horse, Denial of surface etc.

Control

It is used as a protective measure. Control can be a action, device, procedure or technique that removes or reduces vulnerability. Threat is blocked by control of vulnerability.

Teacher's Sign.: _____

b] Symmetric key vs Assymmetric key

Symmetric key	Assymmetric key
① It only requires one key	① It requires two keys
② The size of cipher text is same or smaller than original plain text	② The size of cipher text is same or larger than original plain text
③ Encryption process is very fast	③ Encryption process is slower.
④ It only provides confidentiality	④ It provides confidentiality and authenticity
⑤ Eg: AES, DES	⑤ Eg: RSA, Deffie Hellman

c] Block & stream cipher

Block Cipher	Stream Cipher
① Data is processed in blocks	① Data is processed bit by bit
② Slower processing	② Faster processing
③ Requires more resources	③ Requires fewer resources
④ Rely on stateful & stateless modes of operation such as ECB, CBC	④ It can be either synchronous or asynchronous

Teacher's Sign.: _____

④ Eg: AES, DES, Blowfish ⑤ Eg: RCY, AS

Q2] Explain product cipher in Detail

→ 1) Product cipher is Data encryption scheme in which the cipher text produced by encrypting a plain text document is subjected to further encryption by combining two or more simple transposition or substitution ciphers.

2) Examples of modern day ciphers include LUCIFER, DES, LOKI etc.

3) Fiestel ciphers are a class of product ciphers which operate on one half of the cipher text at each round, then swap the ciphertext halves after each round

4) In the days of manual cryptography, product cipher were useful device for cryptographies and in fact double transposition or product ciphers on keyword based rectangular matrices were widely used

Q3] what are system security goals? Explain the balance among different goals is needed. Describe in detail attacks threatening to security goals?

→ 1) The three security goals are:

→ Confidentiality

→ Integrity

→ Availability

1] Confidentiality

→ The term confidentiality determine the secrecy of information.

→ The main principle of confidentiality is that only the sender and reciever will be able to access the information i.e only authorized parties have the acess.

→ Confidentiality can be defined as an act of protecting information from unauthorised person

→ Data encryption is used to prevent hacking is example of confidentiality

2] Integrity

→ Integrity is defined as act of protecting information from unauthorised modification by an entity

→ Main principle of integrity is that data should not be modified and kept in original form.

→ Attacks against integrity are called alteration attacks

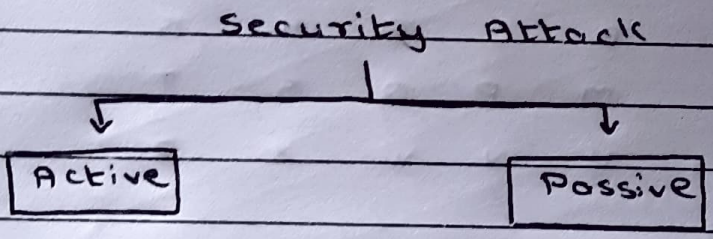
3] Availability

→ It can be defined as a act of protecting info from unauthorised destruction by an entity

→ Main principle of availability is that resources must be available to authorised party at all times

→ System should have sufficient availability of info to satisfy user request
→ Attacks against availability are destruction attack

★ Security Attacks
→ An attack is when the security of a system is compromised by some action of a perpetrator.
→ Attack is classified into four types
① Interception ③ Modification
② Fabrication ④ Interruption



→ Active Attack - It is a type of attack in which the hacker attempts to transform to change the contents of message or information
→ Passive Attack - It is a type of attack in which attacker observes all the messages and copies content of messages

Q4 ① Affine cipher

$$C = (K_1 \times p + K_2) \bmod n$$

Encrypt "Cipher"

$K_1 = 5$ $K_2 = 8$ $n = 26$

Plaintext	C	i	p	h	e	r
	02	08				
p	~~00~~	~~05~~	15	07	04	17
$K_1 \times p + K_2$	18	48	83	43	28	93
$(K_1 p + K_2) \bmod 26$	18	22	05	17	02	15
Ciphertext	S	W	F	R	C	P

(b) key = "Royal Enfield"

message = "Academic committe will meet today"

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

Block	AC	AD	EM	IC	CO	MX	MI	TX	TE
Cipher	OH	LI	BU	NH	PN	PS	SE	MS	MD

EW	JL	LM	EX	ET	TO	DA	VX	
FU	DA	RT	FM	DM	PL	IL	FM	

Ciphertext: OHLIBUNH PNPSSEMSMD FUDART FMDM PLILFM

Teacher's Sign.: _____

(c) Vignere cipher

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

Key = "BEST"

Plaintext	c	i	p	h	e	r
P	02	08	15	07	04	17
Key	B	E	S	T	B	E
K	01	04	18	19	01	04
P+K	03	12	33	26	05	21
(P+K) mod 26	3	12	7	1	5	21
Ciphertext	D	M	H	B	F	V

Cipher = "DMHBFV"

(d) Hill Cipher

→ we live in an insecure world

3	2
5	7

P = W L V I A I S C R W R D
E I E N N N E U E O L

$$P = \begin{bmatrix} 22 & 11 & 21 & 08 & 00 & 08 & 18 & 02 & 17 & 22 & 17 & 03 \\ 04 & 08 & 04 & 13 & 13 & 13 & 04 & 20 & 04 & 14 & 11 & \end{bmatrix}$$

$$P.K = \begin{bmatrix} 86 & 73 & 83 & 89 & 65 & 89 & 74 & 106 & 71 & 136 & 106 & 9 \\ 72 & 78 & 70 & 107 & 91 & 107 & 64 & 144 & 62 & 142 & 111 & \end{bmatrix}$$

$$(P.K) \bmod 26 = \begin{bmatrix} 4 & 21 & 5 & 11 & 1 & 11 & 11 & 1 & 19 & 3 & 1 & 9 \\ 10 & 0 & 9 & 3 & 1 & 3 & 6 & 7 & 5 & 6 & 7 & \end{bmatrix}$$

∴ C = EK VAFJ LD BB 1DLGBHTF DGBHJ

Teacher's Sign.: _____

5] RSA

$e = 7$, $n = 187$ $\therefore p = 17$ $q = 11$

$\phi(n) = (17-1)(11-1) = 160$

q	r_1	r_2	r	t_1	t_2	$t_1 - qt_2$
22	160	7	6	0	1	-22
1	7	6	1	1	-22	23
6	6	1	0	-22	23	-160

1) $\therefore d = \underline{23}$

2) $M = C^d \bmod 26$

$= 11^{23} \bmod 26$

$= \underline{18}$

3) Approaches to defeat RSA

→ Brute force

→ Mathematical attack

→ Timing attacks

4) $e = 13$, $n = 77$ $\therefore p = 11$ $q = 7$

$\phi(n) = 60$

q	r_1	r_2	r	t_1	t_2	$t_1 - qt_2$
4	60	13	8	0	1	-4
1	13	8	5	1	-4	5
1	8	5	3	-4	5	-9
1	5	3	2	5	-9	14
1	3	2	1	-9	14	-23
2	2	1	0	14	-23	60

Teacher's Sign.: _____

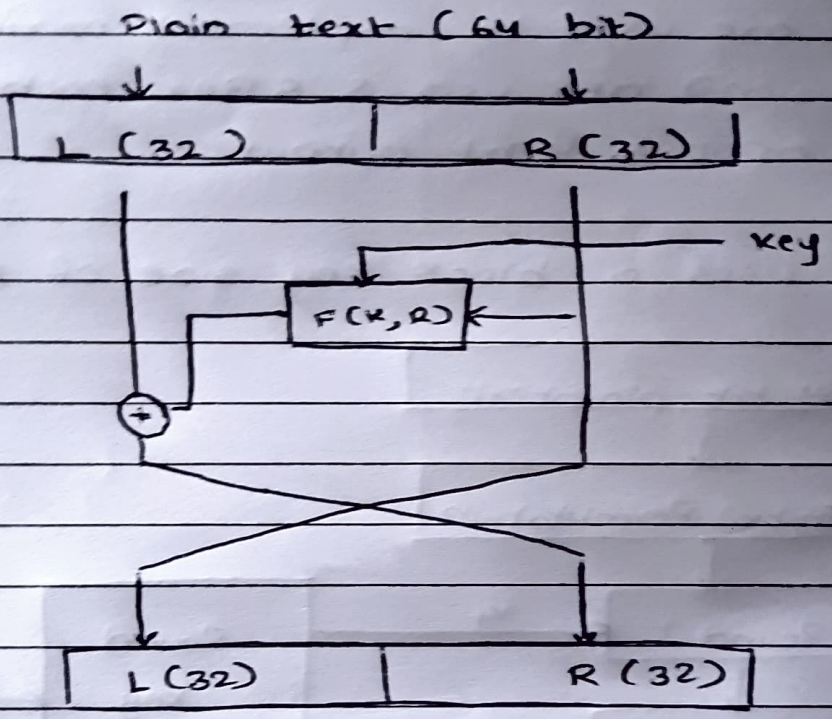
$\therefore d = 37$

$C = 26$

$\therefore M = 26^{37} \bmod 26$

$= 0$

6] a) Fiestel Structure

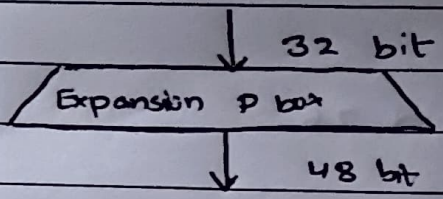


Fiestel Structure encrypts plain text in several rounds, where it applies substitution and permutation to data. Each round uses a different key for encryption, and some key for decryption

b) There is extra swap in the 16th round of DES algorithm in order to ensure symmetry.

Teacher's Sign.: _____

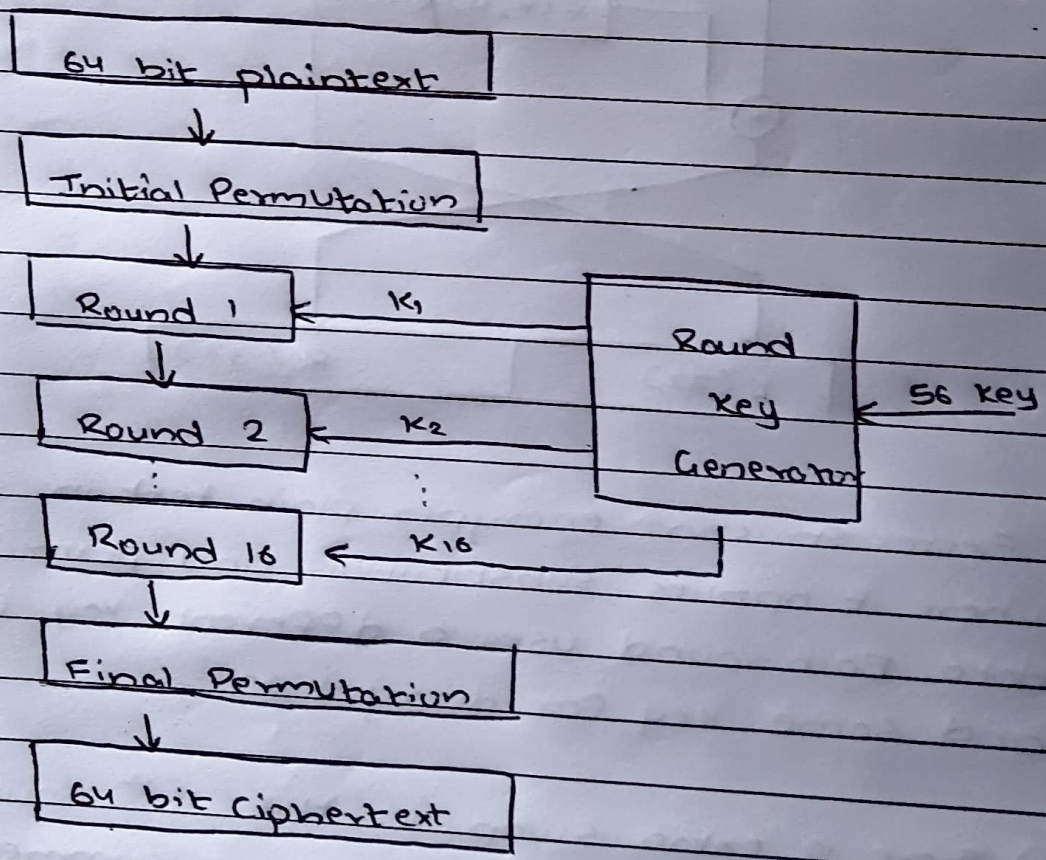
c)



Since input is 32 bit & key is 48 bit, we need to expand input to 48 bits to perform XOR

d) S-box are used to implement mixing (confusion). DES uses 8 SBox, each having 6 bit input & 4 bit output

7] i) DES uses a block key size of 64 bits



DES Structure

Teacher's Sign.: _____

2) DES uses cipher key size of 56 bits
3) DES has 16 rounds
4) Expansion box is needed to increase block size from 32 bit to 48 bit

8] 2 DES :

→ It is a encryption technique which uses two instances of DES on same plain text. In both instances, it uses different keys to encrypt plain text.
→ Both keys are required at time of decryption
→ 64 bit plain text goes into first DES instance which gets converted to middle text using first key & then it goes to second DES instance to get cipher text.
→ Complexity : 2^{57} permutations

3DES :

→ Triple DES is a encryption technique that uses three instances of DES on same plain text.
→ It is vulnerable to meet-in-the-middle attack and it uses 168 bit key
→ Complexity : 2^{112} permutations

AES :

→ AES is a block cipher which can have a key size of 128 \ 256 \ 192 bits.
→ It encrypts data in blocks of 128 bits each
→ It can have either 10 \ 12 \ 14 rounds
→ Operations such as SubBytes, ShiftRows,

Teacher's Sign.: _____

MixColumns, AddRoundKey are used

→ A key algorithm is used to calculate all the round keys from the key.

9] $g = 2 \quad p = 11$

① 2 is a primite root of 11 because

n	g^n	$g^n \bmod P$
1	2	2
2	4	4
3	8	8
4	16	5
5	32	10
6	64	9
7	128	7
8	256	3
9	512	6
10	1024	1
11	2048	2

{$g^n \bmod P$} contains elements which lie in residue set of Z_{11}

② $x_a = a$

$a = g^x \bmod p$

$a = 2^a \bmod 11$

$\therefore a = 6$

③ $y = 3$

$b = g^y \bmod p$

$b = 2^3 \bmod 11$

$\therefore b = 8$

④ $K_1 = b^x \bmod p$

$= 8^a \bmod 11$

$= 7$

$K_2 = a^y \bmod p$

$= 6^3 \bmod 11$

$= 7$

Teacher's Sign.: _____