Vivekanand Education Society's Institute of Technology
Department of Computer Engineering

Subject: -CSS

Class:- T.E. (D12) **Semester:- VI** **Div:- A**

Roll No: 21	Name: AMIT JOSHI		
Exp. No: 1	Title: Assignment -1		
DOP:		DOS:	07/03/2021
GRADE:	LAB OUTCOMES :	SIGNATURE:	

CLASSMATE
Date :
Page :

CSS Assignment-1

Q1) a) Vulnerability is a weakness in the security system. eg: in procedures, design and implementation that might be exploited to cause loss or harm.
Threat to the computer system is a set of circumstances that has potential to cause loss or harm. Control is an action, device procedure or technique that removes vulnerability, threat is blocked by control of vulnerability.

b) Symmetric key cryptography is method of using the same cryptographic keys for both encryption of plain text and decryption of ciphertext. It has faster execution speed and simple since only one key is used in both operations.
Asymmetric key cryptography is a method of using a pair of keys, the pubic key, which is disseminated widely and a private key, which is known only to owner. It is more complex as it uses operate keys for both operations.

c) Block cipher is a type of symmetric key cipher that converts the plain text block wise at a time. Involves in dividing the plain text to large blocks to convert it into cipher text.
Stream cipher is a type of symmetric key cipher that converts the plain text to cipher text by converting one byte of plain text at a time.
It is complex than block cipher.

Q2) In cryptography, product cipher combines 2 or more transformations in a manner intending that the resulting cipher is more secure than individual components to make it resistant to crypt analysis. It combines a sequence of simple transformations such as substitution (S-box) permutation (p box) and modular ~~architecture~~ arithmatic

Eg: plain text: WE ARE DISCOVERED, SAVE YOURSELF.

I] substitution array.

	A	D	F	G	V	X
A	C	O	8	X	F	4
D	M	K	3	A	Z	9
F	N	W	L	O	J	D
G	5	S	I	Y	H	V
V	P	1	V	B	6	R
X	E	Q	7	T	2	G

immediate cipher text:-

FDXADGVXXAFXGFGDAADD
VFXAVXXAFXGDDGVFXA
GGADGXVXGDXAFFAV.

II) Transposition matrix.

A	V	T	H	O	R
1	6	5	2	3	4
F	D	X	A	D	6
V	X	X	A	F	X
G	F	G	D	A	A
A	D	V	F	X	A
V	X	X	A	F	X
G	D	D	G	V	F
X	A	G	G	A	D
G	X	V	X	G	D
X	A	F	F	A	V

Cipher text: FVGAV GXGXA ADFAG GXFDF
XAFVA GAGXA AXFFDD VXXGV
XD6VF DXFDX DAXA

Q3)

Three main goals associated with security are:-

i) Confidentiality: It is common aspect of information security. ai we need to protect our confidential information from getting leaked into public.

ii) Integrity: In information security, integrity means maintaining and assuring accuracy and completion of data over it is entire life cycle. It means that changes can be done only by authorised mechanism and authorized entities.

iii) Availability: Availability of information refers to ensuring that authorised entities gets information when needed. An information which is stored and maintained is useless if its not available when needed.

* Attacks threating confidentiality :-

- Snooping : The unauthorised interception of information is a form of disclosure. It is passive, suggesting that some entity is listening to communications.
- Traffic analysis : It is the process of interception and examining messages in order to deduce info from patterns in communication.

* Attacks threatning integrity :-

- Modification : is after intercepting or accepting info the interceptor modifies the info to make it beneficial to itself.
- Masquerading or spoofing : happens when the attacker impersonated somebody else.
- Replaying : is an attack in which a service already authorised and completed is forged by another. "duplicate request" in an attempt to repeat authorized commands.
- Repudiation : is a type of attack is different from others because it is performed by one of the parties in communication.

* Attacks threatning availability :-

- Denial of service attack : It is an attack to make a machine or network resource unavailable to its intended user. The denial may occour at the source, at the destination or along the intermediate path.

Q4) b). R O Y A L
E N F I D
B C G H J/X
K M P Q S
T U V W Z

ac ad em ic com x
mi tx te cu il lm
en et tx cd ay

AC = OH	EW = IT
AD = LI	IL = DA
EM = NK	LM = DS
IC = NH	EX = DB
CO = MN (both in same col)	ET = BR (both in same col)
MX = SC	TX = ZB
MI = GN	OD = LN
TX = ZB	AY = LA (both in same row)
TE = RB (both in same col)	

∴ The encrypted text is "OHLINKNHMNSCGNZBRBITDADSDBBRZB LNLA"

d) $K = \begin{pmatrix} 3 & 2 \\ 5 & 7 \end{pmatrix}$

We live in an insecure world

as key has 2 columns grouping will be of 2

$= \binom{W}{E}\binom{L}{I}\binom{V}{E}\binom{I}{N}\binom{N}{N}\binom{S}{E}\binom{C}{U}\binom{R}{E}\binom{W}{O}\binom{R}{L}\binom{D}{X}$

$= \binom{22}{4}\binom{11}{8}\binom{21}{4}\binom{8}{13}\binom{13}{13}\binom{13}{13}\binom{18}{4}\binom{2}{20}\binom{17}{4}\binom{22}{14}\binom{17}{11}\binom{3}{23}$

∴ $K \cdot \binom{22}{4} = \binom{73}{138} \bmod 26 = \binom{22}{8} = WI$

$K\binom{11}{8} = \binom{49}{111} \bmod 26 = \binom{23}{7} = XH$

$K\binom{24}{4} = \binom{71}{133} \bmod 26 = \binom{19}{3} = TD.$

$K\binom{8}{13} = \binom{50}{131} \bmod 26 = \binom{24}{1} = YB.$

$K.\begin{pmatrix}18\\4\end{pmatrix} = \begin{pmatrix}82\\118\end{pmatrix} \bmod 26 = \begin{pmatrix}10\\14\end{pmatrix} = KO.$

$K\begin{pmatrix}2\\20\end{pmatrix} = \begin{pmatrix}46\\150\end{pmatrix} \bmod 26 = \begin{pmatrix}20\\20\end{pmatrix} = UU$

$K\begin{pmatrix}17\\4\end{pmatrix} = \begin{pmatrix}59\\113\end{pmatrix} \bmod 26 = \begin{pmatrix}7\\9\end{pmatrix} = HJ$

$K\begin{pmatrix}22\\14\end{pmatrix} = \begin{pmatrix}94\\208\end{pmatrix} \bmod 26 = \begin{pmatrix}16\\0\end{pmatrix} = QA$

$K\begin{pmatrix}17\\11\end{pmatrix} = \begin{pmatrix}73\\162\end{pmatrix} \bmod 26 = \begin{pmatrix}21\\6\end{pmatrix} = VG$

$K\begin{pmatrix}3\\23\end{pmatrix} = \begin{pmatrix}55\\176\end{pmatrix} \bmod 26 = \begin{pmatrix}3\\20\end{pmatrix} = DU$

Encrypted text is "WJXHIDYBANYBKOUUHJQAVGDU"

Q5) a) ① $e = 7, n = 187$

$\phi(n) = \phi(11) \times \phi(17) = 10 \times 16 = 160$

By extented Euclidian theorem.

q	r_1	r_2	r	t_1	t_2	$t_.$
21	160	7	6	0	1	-22
1	7	6	1	1	-22	23
6	1	1	0	-22	23	-160
–	1	0	–	23	-160	–

$\therefore d = 23$

$e = 7, d = 23, n = 187$

private key: (23, 187)

public key: (7, 187)

$\therefore c = 11$ (given)

$\therefore m = c^d \bmod N = 11^{23} \bmod 187 = 88$

b) There are 2 possible approaches to defeating the RSA algorithm. The 1st is the brute force approach try all possible private key. Thus, the larger the no. of bits in e and the more secure the algorithm. Cycle attack is very to guessing the value of d. The idea is that we encrypt the cipher text repeatedly counting the

iterations until the original text appears. This no of recycles will decrypt any cipher text.

b) A: public key = (13, 77)

A: $e = 13, n = 77$

$\phi(n) = \phi(7) \times \phi(11) = 6 \times 10 = 60$

q	r_1	r_2	r	t_1	t_2	t_i
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
	1	0		-23	60	

$\therefore d = 60 - 23 = 37$

A = private key = (37, 77)

$c = 26$ (given) $\therefore m = c^d \bmod n = 26^{37} \bmod 77$

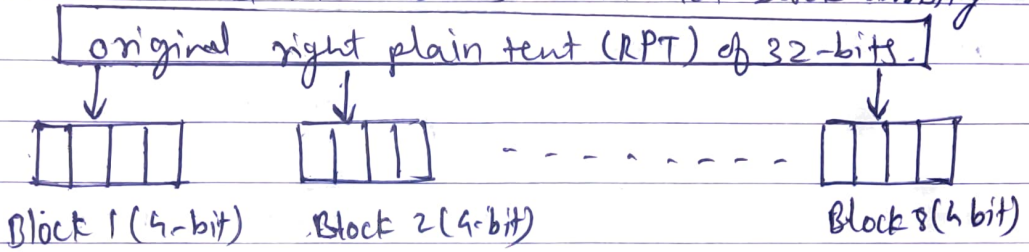
$\therefore m = 5$

$\therefore$ Plain text decrypted by A is 5

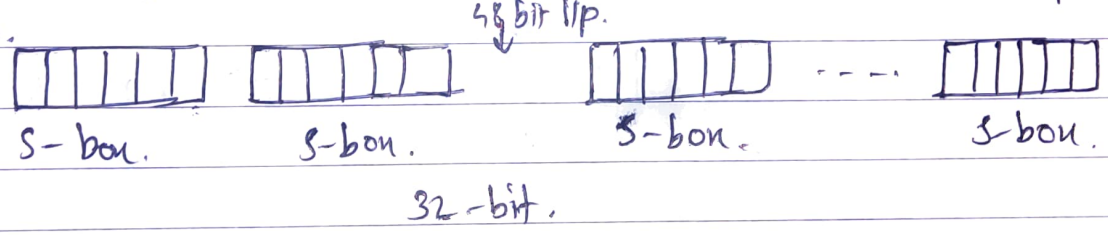
Q6) a). Fiestal cipher is not a specific scheme of block cipher, it is a design model from which many different block ciphers are derived. DES is just one example of fiestal cipher. The encryption uses the fiestal structure consisting multiple rounds of processing of the plain text, each round consisting of a substitution step followed by a permutation step. The process of decryption in fiestal cipher is almost similar. Instead of starting with a block of plain text, the cipher text block is fed into the start of fiestal structure and then the process therefore is exactly the same.

b) Significance of extra swap between left and right half blocks. As mentioned, the final swapping of 'L' and 'R' in the last step of the feistal cipher is essential. If there are not swapped, then the resulting ciphertext could not be decrypted using same DES algorithm.

c) We had two 32 bit plain text areas called as left plain text (LPT) and right plain text (RPT). During the expansion permutation, the RPT is expanded from 32 bits to 48 bits. Bits are permuted as well hence called as expansion permutation. This happens as the 32-bit is divided into 8 blocks with each block consisting 4 bits.



d) Significance of S-box: The Sboxes carry out the real mixing (Confusion). DES uses 8 s-boxes, each with a 6-bit i/p and 4-bit o/p.



Q7). a) DES has 64-bit block length which it divides into 2 parts i.e. "L" (Left plain text) and "R" (Right plain text) each.

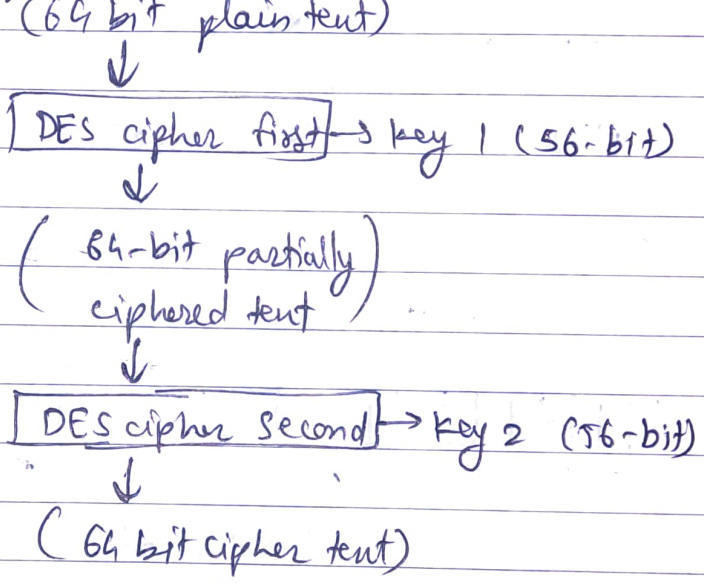
b) DES uses a 64-bit key PKS including 1-bit for parity, so the actual key is 56 bits. 48 bits are selected from the 56 bits of the key. This is Ki. The key bits are selected each round by rotating the keys a select amount and then pulling out of a subset of the necessary bits.

c) DES with any no of rounds fewer than 16 could be broken with

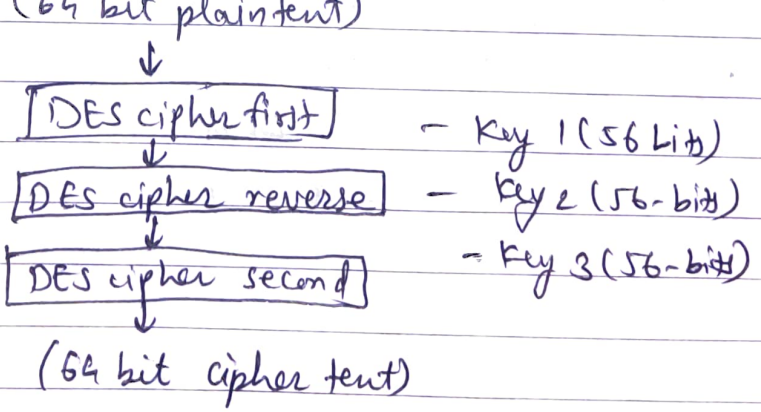
known - plaintext more efficiently than by a brute force attack Hence DES has 16 rounds.

d) Expands from 32 bits to 48 bits. This changes the order of the bits as well as repeating certain bits, it is known as expansion permutation.

Q8) Double DES (2DES): This is an encryption technique which uses 2 instances of DES on same plain text. In both instances it uses different keys to encrypt the plain text. Both keys are required at the time of decryption.



Triple DES: It is an encryption technique which uses 3 instances of DES on same plain text. It uses 3 different types of keys.



AES: stands for advanced encryption standard and is a majorly used symmetric encryption algorithm. It is mostly used for encryption and protection of electronic data. It was used as the better than DES. AES consists of 3 blocks ciphers and these ciphers are used to provide an encryption of data. AES has keys of 3 lengths which are 128, 192 and 256 bits. It provides high security and can prevent many attacks. It consists of 10 rounds of processing for 128 bit key.

Q9) a) $g = 2$, $n = 11$ (given)

since $2^1 \% 11 = 2$ $\quad 2^6 \% 11 = 9$

$2^2 \% 11 = 4$ $\quad 2^7 \% 11 = 7$

$2^3 \% 11 = 8$ $\quad 2^8 \% 11 = 3$

$2^4 \% 11 = 5$ $\quad 2^9 \% 11 = 6$

$2^5 \% 11 = 10$ $\quad 2^{10} \% 11 = 1$

∴ 2 is the primitive root of 11 as well as all the no's from 1-10 occour when we do $2^i \bmod 11$

b) If A has a public key a, what is A's private key.

A has public key = 9

∴ By extended Euclidean method.

q	r_1	r_2	r	t_1	t_2	t
1	11	9	2	0	1	-1
4	9	2	1	1	-1	5
2	2	1	0	-1	5	-11
-	1	0	-	5	-11	-

∴ A's private key = 5.

c) B has public key 3, what is B's private key

∴ By extended Euclidean method.

q	r_1	r_2	r	t_1	t_2	t
3	11	3	2	0	1	-3
1	3	2	1	1	-3	4
2	2	1	0	-3	4	11
-	1	0	-	4	-1	-

∴ B's private key = 4

d) At A:

$A = g^x \bmod n$

$= 2^5 \bmod 11$

$= 10$

$K_1 = B^x \bmod 11$

$= 5^5 \bmod 11$

$= 1$

At B:

$B = g^y \bmod n$

$= 2^4 \bmod 11$

$= 5$

$K_2 = A^r \bmod n$

$= 10^5 \bmod 11$

$= 1$

$\therefore K_1 = K_2 = 1$

Q 10) $x = 10 \bmod 3 \quad x = 11 \bmod 4 \quad x = 12 \bmod 5$

$m_1 = 3 \quad m_2 = 4 \quad m_3 = 5$

$M = m_1 \times m_2 \times m_3 = 3 \times 4 \times 5 = 60$

$M_1 = \frac{M}{m_1} = 20 ; \quad M_2 = \frac{M}{m_2} = 15 ; \quad M_3 = \frac{M}{m_3} = 12$

$M_1^{-1} = 20 \bmod 3 = 2$

$M_2^{-1} = 15 \bmod 4 = 3$

$M_3^{-1} = 12 \bmod 5 = 2$

$\therefore x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$

$x = (480 + 495 + 288) \bmod 60$

$\therefore x = \underline{43}$