CMR
INSTITUTE OF
TECHNOLOGY

USN | | | | | | | | | |

Internal Assesment Test – I March 2019

Sub:	Cyptography, Network Security & Cyber Law							Code:	15CS61
Date:	**05 / 03 / 2019**	Duration:	90 mins	Max Marks:	50	Sem:	**VA,B & C**	Branch:	**CSE**
Note: Answer any 5 full questions (Including minimum 1 question from Module-2)									

	Module-1	Marks	OBE CO	OBE RBT
1	Explain different common cyber attacks	[10]	CO1	L1
2	Explain different defense strategies and techniques against cyber attacks	[10]	CO1	L1
3 a)	Find gcd (2940, 1760) with the help of Euclid's algorithm	[4]	CO2	L3
b).	Find the inverse of 15 modulo 26 with Extended Euclid's algorithm	[6]	CO2	L3
4a)	i). Find 15^{18} mod 17 using Fermat's Little theorem. ii). Find whether $\langle Z_9^*, *_9 \rangle$ is a group or not? Justify your answer.	[2+4]	CO2	L3,L4
b)	Define Cyclic group. Check whether 5 is a generator for $\langle Z_{13}^*, *_{13} \rangle$ under multiplication mod 13.	[4]	CO2	L3
5 a).	Encrypt the plaintext "CRYPTOGRAPHY" using Hill cipher with the key $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$	[5]	CO2	L3

CMR
INSTITUTE OF
TECHNOLOGY

USN | | | | | | | | | |

Internal Assesment Test – I March 2019

Sub:	Cyptography, Network Security & Cyber Law							Code:	15CS61
Date:	**05 / 03 / 2019**	Duration:	90 mins	Max Marks:	50	Sem:	**VA,B & C**	Branch:	**CSE**
Note: Answer any 5 full questions (Including minimum 1 question from Module-2)									

	Module-1	Marks	OBE CO	OBE RBT
1	Explain different common cyber attacks	[10]	CO1	L1
2	Explain different defense strategies and techniques against cyber attacks	[10]	CO1	L1
3 a)	Find gcd (2940, 1760) with the help of Euclid's algorithm	[4]	CO2	L3
b).	Find the inverse of 15 modulo 26 with Extended Euclid's algorithm	[6]	CO2	L3
4a)	i). Find 15^{18} mod 17 using Fermat's Little theorem. ii). Find whether $\langle Z_9^*, *_9 \rangle$ is a group or not? Justify your answer.	[2+4]	CO2	L3,L4
b)	Define Cyclic group. Check whether 5 is a generator for $\langle Z_{13}^*, *_{13} \rangle$ under multiplication mod 13.	[4]	CO2	L3
5 a).	Encrypt the plaintext "CRYPTOGRAPHY" using Hill cipher with the key $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$	[5]	CO2	L3

b).	Find the value of x by solving the following congruent equations using Chinese Remainder Theorem. $$x \equiv 1 \ mod\ 5$$ $$x \equiv 2 \ mod\ 7$$	[5]	CO2	L3
6	With a neat diagram, explain the single round of DES Encryption Model	[10]	CO2	L2
	Module-2			
7	Encrypt the message 001010111 applying RSA Encryption technique where p=3, q=7	[10]	CO3	L3
8a)	Explain how Secret key and public key can be combined to create session key encryption	[5]	CO3	L2
b)	Explain how side channel attacks exploit timing or power characteristics of RSA implementation.	[5]	CO3	L2

b).	Find the value of x by solving the following congruent equations using Chinese Remainder Theorem. $$x \equiv 1 \ mod\ 5$$ $$x \equiv 2 \ mod\ 7$$	[5]	CO2	L3
6	With a neat diagram, explain the single round of DES Encryption Model	[10]	CO2	L2
	Module-2			
7	Encrypt the message 001010111 applying RSA Encryption technique where p=3, q=7	[10]	CO3	L3
8a)	Explain how Secret key and public key can be combined to create session key encryption	[5]	CO3	L2
b)	Explain how side channel attacks exploit timing or power characteristics of RSA implementation.	[5]	CO3	L2

1 **Explain different common cyber attacks** **[10]**

Common Attacks

Some of the high-profile attacks are discussed below :-

① Phishing and pharming attacks:

These attacks attempt to retrieve personal information from an individual. In phishing attack, the attacker directs its victims to a fake website (eg: banking site) which has the look and feel of authentic site where the victim has to share his credentials (username / password) which are then passed on to the attacker.

Personal information may also be leaked out from credit cards, smart cards, ATM cards through a variety of skimming attacks in which third-party card reading device will be installed near card reading terminal.

(redirecting a website's traffic to other website.)

Pharming attacks try to deduce sensitive information from lost or stolen smart cards.

Eaves dropping is another attack where leakage of information takes place on the link between communicating parties.

② Password-guessing attacks:

These attacks attempt to intrude into a computer system. This is a special case of dictionary attack in which attacker tries to break in to a system by trying hundreds of words in a dictionary.

2 Explain different defense strategies and techniques against cyber attacks [10]

③ Impersonation / Masquerade is another attack in which the attacker pretends to be an authorized user of a system inorder to gain access to it or to gain their privileges to make on-line purchases, initiate banking transactions etc.

④ Denial of Service (DoS) :- These attacks are meant to exhaust the computing power, memory capacity or bandwith and make the service interrupted. It usually slows down the system.

⑤ Worms, Viruses & Malwares :- A virus spreads from one computer to another, leaving infections as it travels. A worm is a stand-alone program and it self-replicates. Malware is the malicious software designed to damage a system such as worms, virus, trojan, spyware

Trojan is a kind of malware which is disguised as a legitimate software.

Spyware, installed on a machine can be used to monitor user activity, and as a key logger.

2 **Explain different defense strategies and techniques against cyber attacks** **[10]**

Defence Strategies & Techniques

* **Access Control – Authentication and Authorization:-**

The first defence strategy to prevent intrusions is access control. The first step in access control is to permit or deny entry into the system. It involves some form of authentication — a process of recognizing a user's identity. eg: Password. The user first enters his/her username and password. The system proves user's identity by checking if the entered credentials match with the stored credentials. After successful authentication, user may need to access several resources. The authorization process determines whether the user is allowed to access various resources based on the user's identity.

eg: "Is Rajeev allowed to write into file, CS649 Grades?"

There are atleast 3 parameters to such an access control decision:

(i) the subject or principal, Rajeev,
(ii) the object or resource, CS649 Grades,
(iii) the access mode or operation, write.

* **Data Protection:-**

The data in transit or in storage need to be protected. Data protection mainly

mplies data confidentiality and data integrity.
Confidentiality → Data should not be readable by an intruder.
Integrity → Data intransit should not be tampered with or modified without being detected.
Cryptographic techniques are the best known ways to protect confidentiality & integrity of data. In cryptography, the sender performs encryption on the message to disguise it, while the receiver performs decryption to recover the message. Cryptographic checksum is an integrity check technique.

* Prevention and Detection:— Access control and message encryption are preventive strategies. Authentication keeps intruders out, while authorization limits what can be done by those who have been allowed in. Encryption prevents intruders from eavesdropping on messages. Checksum detects tampering of messages.
Code testing such as black box testing is used to detect vulnerabilities in the domain of software security. White box testing is employed when the source code of a program is easily available.

Intrusion prevention may not always be practical or affordable. Continuous monitoring of network logs and OS logs are a good starting point. Intrusion detection systems also look for certain patterns of behaviour.

* Response, Recovery & Forensics
Response measures should be taken once an attack has been detected, like shutting down all or part of the system. During worm epidemic, the infected part should be quarantined & necessary patches should be applied. Cyberforensics is an area with a set of tools that help trace back the attackers.

3 a)	Find gcd (2940, 1760) with the help of Euclid's algorithm	[4]
b).	Find the inverse of 15 modulo 26 with Extended Euclid's algorithm	[6]

a) GCD ((2940, 1760) with the help of Euclid's algorithm

Step 1: 2940 = 1 * 1760 + 1180

Step 2: 1760 = 1* 1180 + 580

Step 3: 1180 = 2 * 580 + 20

Step 4: 580 = 29*20 + 0

So the GCD (2940, 1760) = 20

b). 8a) Explain how Secret key and public key can be combined to create session key encryption

15^{-1} mod 26

c b

b'	c'	q	r	o1	n1	o2	n2
26	15		2	1	0	0	1
15	11	1	11	0	1	1	-1
11	4	1	4	1	-1	-1	2
4	3	2	3	-1	3	2	-5
3	1	1	1	3	-4	-5	7

Inverse = 7

ie, 15x7 mod 26 = 1

8) a) Explain how Secret key and public key can be combined to create session key encryption [5]

b) Explain how side channel attacks exploit timing or power characteristics of RSA implementation [5] a)

Drawback of :-

Secret key → key Management

Public key → speed.

To combine the speed of secret key & convenience of public key, a session key is employed.

(session key → secret key)

At sender (A)

- Choose random s
- Encrypt msg $E_s(m)$
- Encrypt session key $E_{B.pu}(s)$
- Send $E_s(m)$ & $E_{B.pu}(s)$

At receiver (B)

- Decrypt $E_{B.pu}(s)$ to s, using private key.
- Decrypt $E_s(m)$ to get m, using s

Session key → valid for duration of a session & destroyed thereafter.

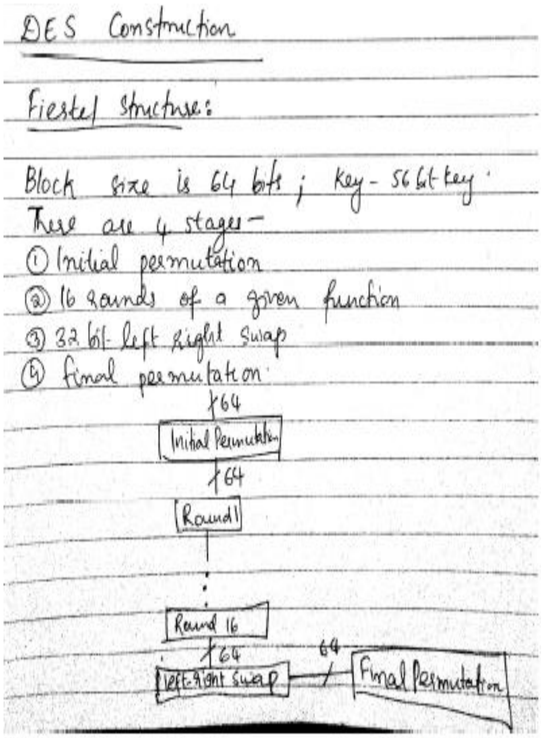
b) Side Channel attack to RSA

→ Attacks based on monitoring timing or power measurements of algorithm. This is especially the case for embedded devices such as smart cards.

Smart card can be stolen by attackers. They can induce the card to perform some cryptographic tasks involving the private key stored in card. They connect smart card via probes to equipment that can accurately monitor variables such as timing & power measurements. [Refer text book - pg 83 for details]

Radioactive particles produced by heavy metals such as uranium caused hardware to malfunction. Other techniques at injecting faults manipulate voltage supply or clock to smart card. Glitches in execution may occur when very high or low clock frequencies are applied or when spikes in voltage supply are introduced.

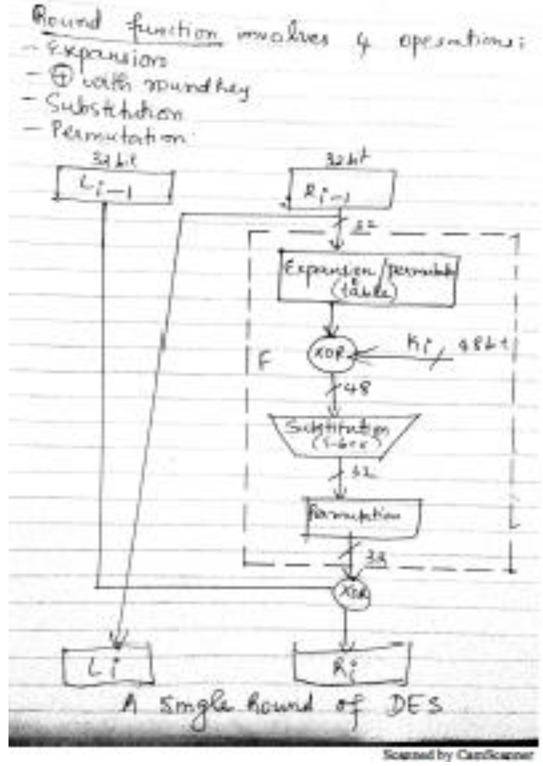
6) With a neat diagram, explain the single round of DES Encryption Model [10]



DES Construction

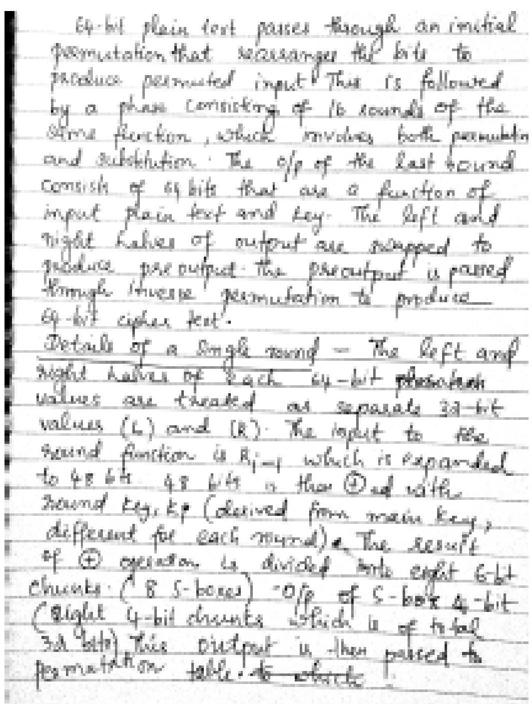
Fiestel Structure:

Block size is 64 bits ; Key - 56 bit key.
There are 4 stages -
① Initial permutation
② 16 rounds of a given function
③ 32 bit left right swap
④ final permutation.



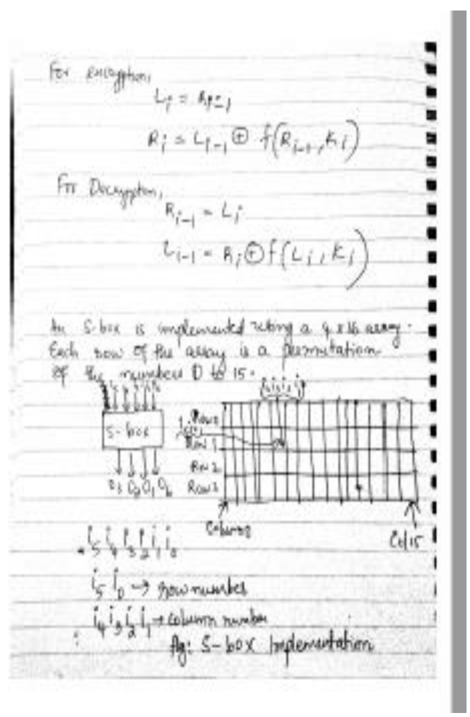
Round function involves 4 operations:
- Expansion
- ⊕ with round key
- Substitution
- Permutation

A Single Round of DES



64-bit plain text passes through an initial permutation that rearranges the bits to produce permuted input. This is followed by a phase consisting of 16 rounds of the same function, which involves both permutation and substitution. The o/p of the last round consists of 64 bits that are a function of input plain text and key. The left and right halves of output are swapped to produce the preoutput. The preoutput is passed through inverse permutation to produce 64-bit cipher text.

Details of a single round - The left and right halves of each 64-bit ~~plaintext~~ values are treated as separate 32-bit values (L) and (R). The input to the round function is R_{i-1} which is expanded to 48 bit. 48 bits is then ⊕ed with the round key, K_i (derived from main key, different for each round). The result of ⊕ operation is divided into eight 6-bit chunks (8 S-boxes). O/p of S-box 4-bit (eight 4-bit chunks which is of total 32 bits). This output is then passed to permutation table. ~~to which~~



For encryption,

$L_i = R_{i-1}$

$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$

For Decryption,

$R_{i-1} = L_i$

$L_{i-1} = R_i \oplus f(L_i, K_i)$

An S-box is implemented using a 4×16 array. Each row of the array is a permutation of the numbers 0 to 15.

Fig: S-box Implementation

4) i). Find 15^{18} mod 17 using Fermat's Little theorem [2]

$$m^{n-1} \bmod n = 1 \text{ (if } n\text{-prime)}$$

$$\Rightarrow 15^{16} \bmod 17 = 1$$

$$(15^{16}) \cdot 15^{2} \bmod 17$$

$$= 1 \cdot 15^{2} \bmod 17$$

$$= 125 \bmod 17$$

$$\underline{\underline{= 4}}$$

Find the value of x by solving the following equations using Chinese Remainder problem.

$$x \equiv 1 \bmod 5$$
$$x \equiv 2 \bmod 7$$

So, $a_1 = 1$, $a_2 = 2$, $m_1 = 5$, $m_2 = 7$.

Step 1: Find $M = m_1 * m_2 = 5 * 7 = 35$.

Step 2: Find $M_1 = M/m_1 = 35/5 = 7$ $\quad$ $M_2 = M/m_2 = 35/7 = 5$.

Step 3: Multiplicative inverses of:

$M_1^{-1} * 7 \bmod 5 = 1$, $\quad$ $M_2^{-1} * 5 \bmod 7 = 1$.

$M_1^{-1} = 3$. $\quad$ $M_2^{-1} = 3$

Step 4: $x = (a_1 * M_1 * M_1^{-1} + a_2 * M_2 * M_2^{-1}) \bmod 35$

$= (1 * 7 * 3 + 2 * 5 * 3) \bmod 35$

$= (21 + 30) \bmod 35$

$= (51) \bmod 35 = 16$.

So we get the solution $16 \equiv 1 \bmod 5$

$16 \equiv 2 \bmod 7$.

7) Encrypt the msg 001010111 by RSA.

$P = 3,\ q = 7$

step 1: $n = P * q = 3 * 7 = 21$

step 2: $\phi(n) = (P-1)(q-1) = (3-1)(7-1) = 2 * 6 = 12$

Step 3: Block Size $\log_2 21 = 5$

Step 4: $1 < e < \phi(n)$ $\gcd(e, \phi(n)) = 1$, so $e = 5$

Step 5: Encryption key = $(5, 21)$

Step 6: To find $d = e^{-1} \bmod \phi(n) \Rightarrow d * 5 \bmod 12 = 1$

so $d = 5$

Step 7: Decryption key $(5, 21)$

Step 8: To encrypt we have to divide the msg in blocks of size 5 ← Padding 0

So we got $m_1 = 00101$ $m_2 = 00111$

$c_1 = (00101)^5 \bmod 21$
$= 5^5 \bmod 21$
$= 17$

$c_2 = (00111)^5 \bmod 21$
$= 7^5 \bmod 21$
$= 7$

Step 9: Now for decryption:

$m_1 = (17)^5 \bmod 21$
$= 5$

$m_2 = (7)^5 \bmod 21$
$= 7$

So the encrypted msg is: 100010111
And Decrypted msg is: 001010111

4b) To check 5 is the generator for the group $\langle Z_{13}^*, *_{13} \rangle$

we do: $P = 13$ The distinct prime factor of $(p-1)$ i.e 12

is 3, 2.

$p_1 = 3$, $p_2 = 2$.

To test if 5 is the generator for $\langle Z_{13}^*, *_{13} \rangle$.

P2: i) $5^{12/2} \bmod 13 = 5^6 \bmod 13 = 12$.

P1: ii) $5^{12/3} \bmod 13 = 5^4 \bmod 13 = 1$.

As 5 has not passes the test for $p_1 = 3$ so 5 is not the generator for $\langle Z_{13}^*, *_{13} \rangle$.

a) ii) Find whether $\langle Z_9^*, *_9 \rangle$ is a group or not? Justify

The group and the operation table is

	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
3	3	6	3	6	3	6
4	4	8	7	2	5	
5	5	1	2	7	8	4

1) So it is closed

2) $(2 *_9 4) *_9 5 == 2 *_9 (4 *_9 5)$

associative property and we are getting

iii) Identity element e=1 (as multiplication mod operation)

But It is following the inverse property. As gcd(i , 9) is always 1, (as <Z9* ,*9> contains the elements which are co- prime with 9) so definitely for all the elements inverse exists.
So it is a group.

5)a) Encrypt the plainText CRYPTOGRAPHY using Hill cipher with the Key $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$

Soln : Key = $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}_{2\times 2}$ So P.T divided into block of size 2

So b_1 = CR, b_2 = YP, b_3 = TO, b_4 = GR, b_5 = AP, b_6 = HY

$c_1 = [2 \;\; 17] \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$

$= [2*9 + 17*5 \quad 2*4 + 17*17] = [103 \quad 303] \bmod 26$

$= [25 \quad 17] = [Z R]$

$c_2 = [24 \quad 15] \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} = [24*9 + 15*5 \quad 24*4 + 15*7]$

$= [291 \quad 201] \bmod 26 = [5 \quad 19] = [F T]$

$c_3 = [19 \quad 14] \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} = [19*9 + 14*5 \quad 19*4 + 14*7]$

$= [241 \quad 174] \bmod 26 = [7 \quad 18] = [H S]$

$c_4 = [6 \quad 17] \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} = [6*9 + 17*5 \quad 6*4 + 17*7]$

$= [139 \quad 143] \bmod 26 = [9 \quad 13] = [J N]$

$c_5 = [0 \quad 15] \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} = [15*5 \quad 15*7] = [75 \quad 105] \bmod 26$

$= [23 \quad 1] = [X B]$

$c_6 = [7 \quad 24] \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} = [7*9 + 24*5 \quad 7*4 + 24*7]$

$= [183 \quad 196] \bmod 26 = [1 \quad 14] = [B O]$

So the ciphertext is : ZRFTHSJNXBBO