CMR INSTITUTE OF TECHNOLOGY

USN | | | | | | | | | | |

Internal Assesment Test – I

Sub:	NETWORK SECURITY			Sec	A & B			Code:	10EC832
Date:	12 / 03 / 2018	Duration:	90 mins	Max Marks:	50	Sem:	VIII	Branch:	TCE

Note: Answer any five full questions.

			Marks	OBE CO	OBE RBT
1		Define passive and active security attacks. Discuss the functioning of the following attacks	02	CO1	L1
	a.	Masquerade.	02	CO1	L1
	b.	Replay.	02	CO1	L1
	c.	Modification of messages.	02	CO1	L1
	d.	Denial of service.	02	CO1	L1
2		Decrypt the cipher text *"**BNCYZXQF**"* using Hill cipher technique with key. $K = \begin{bmatrix} 3 & 4 \\ 19 & 11 \end{bmatrix}$	10	CO2	L3
3		Using play fair cipher, encipher the message "**bassoon guitar**" with key "**MONARCHY**".	10	CO2	L3
4		Explain SDES encryption/decryption and key generation using necessary diagrams.	10	CO2	L3
5		Explain the operation of Caesar Cipher with the algorithm. Decipher "***WKHTXLFNEURZQIRAMXPSVRYHUWKHODCBGRJ***" using Caesar Cipher.	10	CO2	L3
6		Using SDES the key "**1010101110**" find the Sub-keys K_1 *and* K_2 with the permutations as shown in the table below.	10	CO2	L3
7	a.	Given cipher text "***NTSGYCNXEAKIETTHMAOT***" decrypt it using single round transposition technique if $K = 31452$.	5	CO1	L1
	b.	Write a model for network security and explain it in details.	5	CO1	L1

P10	3	5	2	7	4	10	1	9	8	6
P8	6	3	7	4	8	5	10	9		

Solution

1. A passive attack attempts to learn or make use of information from the system but does not affect system resources. An active attack attempts to alter system resources or affect their operation.

a) Passive Attacks **[2 marks]**

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Two types of passive attacks are release of message contents and traffic analysis. Passive attacks are very difficult to detect because they do not involve any alteration of the data. Typically, the message traffic is sent and received in an apparently

normal fashion; neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern. However, it is feasible to prevent the success of these attacks, usually by means of encryption. Thus, the emphasis in dealing with passive attacks is on prevention rather than detection.

b) Active Attacks

Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service.

i. A **masquerade** takes place when one entity pretends to be a different entity (Figure a). A masquerade attack usually includes one of the other forms of active attack. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges. **[2 marks]**

ii. **Replay** involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect (Figure b). **[2 marks]**

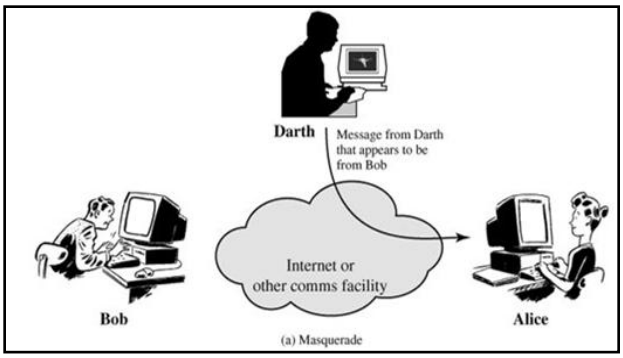
iii. **Modification of messages** simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect (Figure c). For example, a message meaning "Allow John Smith to read confidential file *accounts*" is modified to mean "Allow Fred Brown to read confidential file *accounts.*"

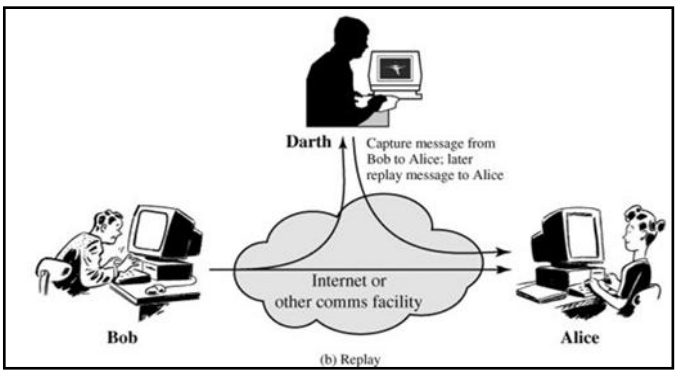
[2 marks]

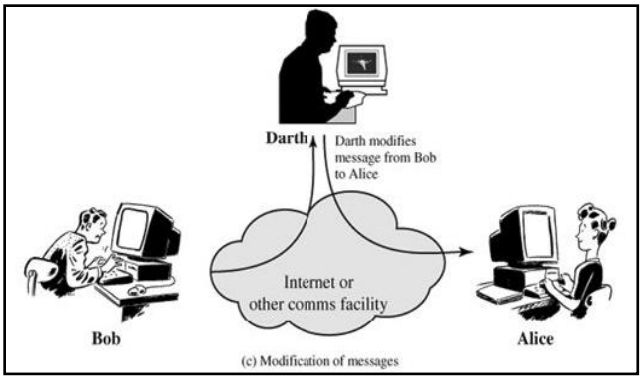
iv. The **denial of service** prevents or inhibits the normal use or management of communications facilities (Figure d). This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination (e.g., the security audit service). Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance. **[2 marks]**

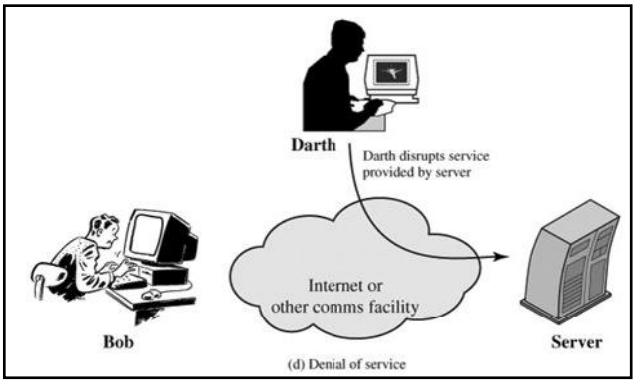
Active attacks present the opposite characteristics of passive attacks. Whereas passive attacks are difficult to detect, measures are available to prevent their success. On the other hand, it is quite difficult to prevent active attacks absolutely, because of the wide variety of potential physical, software, and network vulnerabilities. Instead, the goal is to detect active attacks and to recover from any disruption or delays caused by them. If the detection has a deterrent effect, it may also contribute to prevention.

Figure Active Attacks









2.

$Cipher\ Text = \boldsymbol{BNCYZXQF}$

$$Cipher\ Text = \begin{bmatrix}B\\N\end{bmatrix}\begin{bmatrix}C\\Y\end{bmatrix}\begin{bmatrix}Z\\X\end{bmatrix}\begin{bmatrix}Q\\F\end{bmatrix} = \begin{bmatrix} B & C & Z & Q \\ N & Y & X & F \end{bmatrix} = \begin{bmatrix}1 & 2 & 25 & 16\\13 & 24 & 23 & 5\end{bmatrix}$$ **[1 mark]**

$Plain\ Text = K^{-1}C$

$$[K]^{-1} = \begin{bmatrix} 3 & 4 \\ 19 & 11 \end{bmatrix}^{-1} = \frac{Adj\ [K]}{Det\ [K]}$$

$Det\ [K] = -43\ mod\ 26 = -17\ mod\ 26 = 9$ **[1 mark]**

$\frac{1}{9}\ mod\ 26 = 9^{-1}\ mod\ 26$

$r = r_1 - qr_2 \quad and \quad t = t_1 - qt_2$

q	r_1	r_2	r	t_1	t_2	t
2	26	9	8	0	1	-2
1	9	8	1	1	-2	3
8	8	1	0	-2	3	-26
	1	0		3	-26	

$9^{-1}\ mod\ 26 = 3$ **[2 marks]**

$Adj\ [K] = \{Cofactor\ [K]\}^T$

$$Cofactor\ [K] = \begin{bmatrix} 11 & -19 \\ -4 & 3 \end{bmatrix} \quad Adj\ [K] = \begin{bmatrix} 11 & -4 \\ -19 & 3 \end{bmatrix} \qquad [\mathbf{2\ marks}]$$

$$[K]^{-1} = \frac{Adj\ [K]}{Det\ [K]} = (3)\begin{bmatrix} 11 & -4 \\ -19 & 3 \end{bmatrix} = \begin{bmatrix} 33 & -12 \\ -57 & 9 \end{bmatrix} mod\ 26 = \begin{bmatrix} 7 & 14 \\ 21 & 9 \end{bmatrix} \quad [\mathbf{2\ marks}]$$

$$Plain\ Text = K^{-1}C = \begin{bmatrix} 7 & 14 \\ 21 & 9 \end{bmatrix}\begin{bmatrix} 1 & 2 & 25 & 16 \\ 13 & 24 & 23 & 5 \end{bmatrix} = \begin{bmatrix} 189 & 350 & 497 & 182 \\ 138 & 258 & 732 & 381 \end{bmatrix} mod\ 26$$

$$Plain\ Text = \begin{bmatrix} 7 & 12 & 3 & 0 \\ 8 & 24 & 4 & 17 \end{bmatrix} = \begin{bmatrix} h & m & d & a \\ i & y & e & r \end{bmatrix} = hi\ my\ dear \quad [\mathbf{2\ marks}]$$

3. **[5 marks]**

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

Plain Text: **bassoon guitar**

Encryption Rules:

1. Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last.
2. Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last.
3. Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter.

Plain Text:	ba	sx	so	on	gu	it	ar
Rule	2	2	3	1	3	3	1
Cipher Text:	IB	XA	PA	NA	EW	KS	RM

Cipher Text: **IBXAPANAEWKSRM** **[5 marks]**

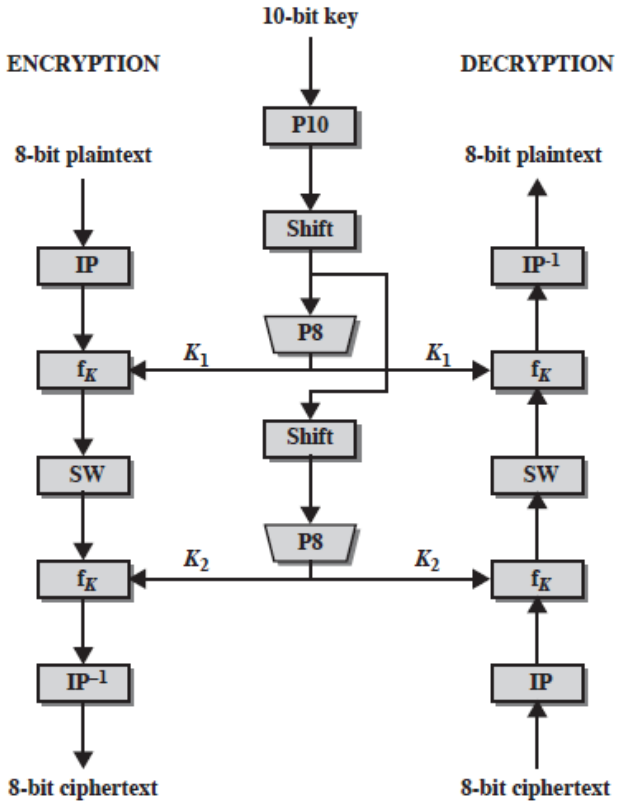
4. **Simplified Data Encryption Standard (S-DES):**

Block diagram [4 marks] **Description [6 marks]**

1. Simplified DES was developed by Professor Edward Schaefer of Santa Clara University.
2. The S-DES encryption algorithm takes 8-bit block of plain text and 10-bit key and produces 8-bit output.
3. Similarly S-DES decryption algorithm also takes 8-bit cipher text and same 10-bit key to produce the 8-bit plain text.
4. The Encryption algorithm performs 5 functions.
    a) Initial Permutation (IP)

b) Complex Function (f_K)
c) Swapping (SW)
d) Again Complex Function (f_K)
e) Final Permutation (IP^{-1})

5. The figure shown below is the simplified DES. **[4 marks]**



[Simplified DES Scheme]

6. The complex function f_K takes 2 inputs those are 8-bit encrypted data and 8-bit key.
7. From the 10-bit key two 8-bit sub key are generated.
8. We can use 16 bit key, consisting of two 8-bit sub keys, one used for each occurrence. A single 8-bit key could be used twice in the algorithm. A compromise is to use 10-bit key from which two 8-bit key is generated.
9. The 10-bit key is first subjected to a permutation $(P10)$
10. Then shift operation is performed.
11. This shifted output is passed through the permutation $(P8)$ and produce the 8-bit output which is the 1st sub-key$(K1)$. The permuted output is also provided to another shift to produce another instance of $(P8)$ which is the 2nd sub-key $(K2)$
12. The encrypted algorithm is represented as :

$$Cipher\ Text = IP^{-1}.f_{K2}.SW.f_{K1}.IP$$

$$or \quad Cipher\ Text = IP^{-1}\left(f_{K2}\left(SW\left(f_{K1}(IP(Plain\ Text))\right)\right)\right)$$

$$Where\ K_1 = P8\left(Shift\left(P10(Key)\right)\right)$$

$$K_2 = P8\left(Shift\left(Shift\left(P10(Key)\right)\right)\right)$$

$Similarly\ Decryption\ can\ be\ represented\ as$:

$$Plain\ Text = IP^{-1}\left(f_{K1}\left(SW\left(f_{K2}\left(IP(Cipher\ Text)\right)\right)\right)\right)$$

5. **Caesar Cipher** **[2 marks]**

The earliest known use of a substitution cipher, and the simplest, was by Julius Caesar. The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet.

Then the algorithm can be expressed as follows. For each plaintext letter *p*, substitute the ciphertext letter *C*:

C = E(3, *p*) = (*p* + 3) mod 26

A shift may be of any amount, so that the general Caesar algorithm is
C = E(*k*, *p*) = (*p* + *k*) mod 26 **[2 marks]**
where *k* takes on a value in the range 1 to 25. The decryption algorithm is simply
p = D(*k*, *C*) = (*C k*) mod 26 **[2 marks]**

Cipher Text: ***WKHT XLFN EURZ QIRA MXPS VRYH UWKH ODCB GRJ***

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

The plain Text is: **The quick brown fox jumps over the lazy dog** **[4 marks]**

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
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

6. key "**1010101110**"

P10	3	5	2	7	4	10	1	9	8	6
P8	6	3	7	4	8	5	10	9		

Key Generation:

	STEPS	CASE
	10 bit Key	1 0 1 0 1 0 1 1 1 0 1 2 3 4 5 6 7 8 9 10
	P10	1 1 0 1 0 0 1 1 1 0 3 5 2 7 4 10 1 9 8 6

<table>
<tr><td></td><td></td><td></td></tr>
<tr><td rowspan="2">Key K1</td><td>Split</td><td><table><tr><td>11010</td><td>01110</td></tr><tr><td>L0</td><td>R0</td></tr></table></td></tr>
<tr><td>LS-1</td><td><table><tr><td>10101
1 2 3 4 5</td><td>11100
6 7 8 9 10</td></tr></table></td></tr>
<tr><td></td><td>P8</td><td><table><tr><td>1</td><td>1</td><td>1</td><td>0</td><td>1</td><td>1</td><td>0</td><td>0</td></tr><tr><td>6</td><td>3</td><td>7</td><td>4</td><td>8</td><td>5</td><td>10</td><td>9</td></tr></table>K1 [5 marks]</td></tr>
<tr><td rowspan="2">Key K2</td><td>LS-2</td><td><table><tr><td>10110
1 2 3 4 5</td><td>10011
6 7 8 9 10</td></tr></table></td></tr>
<tr><td>P8</td><td><table><tr><td>1</td><td>1</td><td>0</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td></tr><tr><td>6</td><td>3</td><td>7</td><td>4</td><td>8</td><td>5</td><td>10</td><td>9</td></tr></table>K2 [5 marks]</td></tr>
</table>

7. (a)

Cipher Text: NTSG YCNX EAKI ETTH MAOT

Encryption Key:

3	1	4	5	2
(1)	(2)	(3)	(4)	(5)

Interchange the index and the value

1	2	3	4	5
3	1	4	5	2

Rearrange it:

2	**5**	**1**	**3**	**4**
1	2	3	4	5

Decryption Key: 2 5 1 3 4 **[2 marks]**

2	5	1	3	4
N	Y	E	E	M
T	C	A	T	A
S	N	K	T	O
G	X	I	H	T

Rearranging:

1	2	3	4	5
E	N	E	M	Y
A	T	T	A	C
K	S	T	O	N
I	G	H	T	X

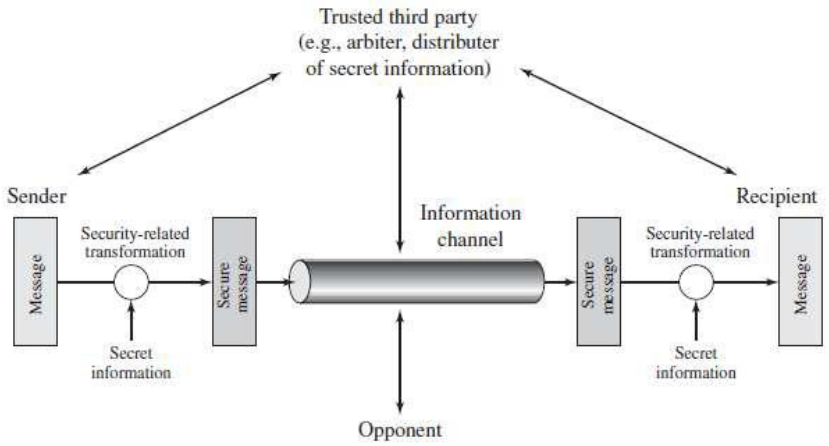
Plain Text: “Enemy attacks tonight” **[3 marks]**

(b) **A Model for Network Security**

Diagram [3 marks] **Explanation [2 marks]**

A model for much of what we will be discussing is captured, in very general terms, in Figure. A message is to be transferred from one party to another across some sort of internet. The two parties, who are the *principals* in this transaction, must cooperate for the exchange to take place. A logical information channel is established by defining a route through the internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals.

Figure. Model for Network Security [3 marks]



Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, and so on. All the techniques for providing security have two components:

- A security-related transformation on the information to be sent. Examples include the encryption of the message, which scrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender.
- Some secret information shared by the two principals and, it is hoped, unknown to the opponent. An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.

A trusted third party may be needed to achieve secure transmission. For example, a third party may be responsible for distributing the secret information to the two principals while keeping it from any opponent. Or a third party may be needed to arbitrate disputes between the two principals concerning the authenticity of a message transmission.

This general model shows that there are four basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.
2. Generate the secret information to be used with the algorithm.
3. Develop methods for the distribution and sharing of the secret information.
4. Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.