FUNDAMENTALS OF CRYPTOGRAPHY
(INFO 4221)

Time Allotted : 2½ hrs **Full Marks : 60**

Figures out of the right margin indicate full marks.

Candidates are required to answer Group A and any 4 (four) from Group B to E, taking one from each group.

Candidates are required to give answer in their own words as far as practicable.

Group – A

1. Answer any twelve: **12 × 1 = 12**

Choose the correct alternative for the following

(i) Which cipher uses 6×6 matrix?
(a) Playfair (b) Monoalphabetic
(c) Vernam (d) None of the above

(ii) What is a combination of Cryptography and Cryptanalysis?
(a) Linear Cryptanalysis (b) Differential Cryptanalysis
(c) Cryptology (d) None of the above

(iii) What suffers from Meet in the Middle attack?
(a) Double DES (b) Triple DES
(c) RSA (d) SSL

(iv) Brute-Force attack is applicable in which of the following algorithm?
(a) RSA (b) DES
(c) MD2 (d) Both (a) and (b)

(v) Which algorithm uses 16 rounds of encryption?
(a) RC5 (b) IDEA
(c) RSA (d) DES

(vi) Which authentication mechanism is associated with FAR and FRR?
(a) Certificate based authentication (b) Biometric authentication
(c) Token based authentication (d) None of the above

(vii) Which of the following uses transformed key?
(a) PEM (b) SSL
(c) HMAC (d) None of the above

(viii) What is the position of SSL in TCP/IP model?
(a) Between Transport and Application (b) Between Transport and Network
(c) Between Transport and Physical (d) None of the above

(ix) Which firewall configuration has 3 level of defence?
(a) Screened Host Firewall Single Homed Bastion
(b) Screened Host Firewall Dual Homed Bastion
(c) Screened Subnet Firewall
(d) None of the above

(x) Which firewall suffers from Tiny Fragmentation attack?
(a) Application level Gateway (b) Packet Filter router
(c) Circuit level gateway (d) None of above

Fill in the blanks with the correct word

(xi) _____ guarantees, there is no modification to message contents.

(xii) The process of writing the text as diagonals and reading it as sequence of rows is called as _____.

(xiii) Key size in Double DES is _____ bits.

(xiv) _____ is an email security protocol that does not require canonical conversion.

(xv) SSL makes use of _____ sub protocols.

Group - B

2. (a) Explain the principles of Network Security. Differentiate between Masquerade and DNS spoofing. *[(CO1) (Understand/LOCQ) (Analyze/IOCQ)]*
(b) Develop the cipher text for the plain text "***fundamentals of cryptography***" using (i) Caesar cipher technique with key= 4 and (ii) Rail Fence technique. *[(CO2) (Evaluate/HOCQ)]*

(6 + 2) + 4 = 12

3. (a) Differentiate between Brute force attack and Cryptanalysis. *[(CO1) (Analyze/IOCQ)]*
(b) Develop the cipher text for the plain text "**11, Harihar road, Kolkata-700132**" using Playfair substitution technique. Keyword to be used is **NETWORK CRYPTANALYSIS.** *[(CO2) (Evaluate/HOCQ)]*
(c) Develop the cipher text for the plain text "***fundamentals of cryptology***" using Simple Columnar Transposition technique for 4 rounds. Keys for First round (3, 2, 1, 4), Second round (4, 1, 3, 2), Third round (2, 1, 3, 4) and Fourth round (1, 2, 3, 4).reference architecture. *[(CO2) (Evaluate/HOCQ)]*

2 + 6 + 4 = 12

Group - C

4. (a) Explain Diffie-Hellman key exchange algorithm. *[(CO3) (Understand/LOCQ)]*
(b) Justify by illustration that Key shifting is not required in first round, fourth round and eighth round of IDEA encryption algorithm. *[(CO3) (Evaluate/HOCQ)]*

4 + 8 = 12

5. (a)

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

From the above S-Box, calculate the output for the following inputs:
(i) 101101(ii) 100110 (iii) 111111. *[(CO3)(Analyze/IOCQ)]*

(b) Explain the working mechanism of Double DES and Triple DES with neat diagrams. *[(CO3)(Understand/LOCQ)]*

6 + 6 = 12

Group - D

6. (a) Differentiate between Certificate based authentication and Biometric authentication. *[(CO5)(Analyze/IOCQ)]*

(b) Discuss three properties of Digital Signature. *[(CO4)(Understand/LOCQ)]*

(c) Discuss five requirements of Hash function. *[(CO4)(Understand/LOCQ)]*

4 + 3 + 5 = 12

7. (a) Explain RSA algorithm in detail. Solve and calculate public key and private key for p=5 and q=13 using RSA algorithm. *[(CO3)(Understand/LOCQ/Analyse/IOCQ)]*

(b) Explain the working of Authentication token. Differentiate between Challenge-Response token and Time based token. *[(CO5)(Understand/LOCQ/Analyze/IOCQ)]*

(2 + 4) + (2 + 4) = 12

Group - E

8. (a) Explain with neat sketch, the working of Alert protocol in SSL. Discuss three limitations of Firewall. *[(CO6)(Understand/LOCQ)]*

(b) Explain DMZ architecture of firewall with neat diagram. Discuss the characteristics of firewall. *[(CO6)(Understand/LOCQ)]*

(3 + 3) + (3 + 3) = 12

9. (a) Consider the 24 bit binary stream, [011101000101011110111010]. Deduce the hexadecimal printable characters from the above binary stream using Base 64 encoding technique. *[(CO6)(Evaluate/HOCQ)]*

(b) Explain with neat sketch, the working mechanism of PEM mail security protocol. *[(CO6)(Understand/LOCQ)]*

6 + 6 = 12

(Necessary table given)

Tabel: Base-64 encoding mapping table

6-bit value	*Character*	*6-bit value*	*Character*	*6-bit value*	*Character*	*6-bit value*	*Character*
0	A	16	Q	32	G	48	W
1	B	17	R	33	H	49	X
2	C	18	S	34	I	50	Y
3	D	19	T	35	J	51	Z
4	E	20	U	36	K	52	0
5	F	21	V	37	L	53	1
6	G	22	W	38	M	54	2
7	H	23	X	39	N	55	3
8	I	24	Y	40	O	56	4
9	J	25	Z	41	P	57	5
10	K	26	A	42	Q	58	6
11	L	27	B	43	R	59	7
12	M	28	C	44	S	60	8
13	N	29	D	45	T	61	9
14	O	30	E	46	U	62	+
15	P	31	F	47	V	63	/
						(Padding)	=

Cognition Level	LOCQ	IOCQ	HOCQ
Percentage distribution	37	33	30