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 algorithm suffers from Tiny Fragmentation attack?
(a) Double DES (b) Triple DES
(c) Packet Filtering Router (d) SSL.

(ii) Which are the chief principles of security?
(a) Integrity (b) Authentication
(c) Availability (d) Both (a) and (b).

(iii) What does it indicate if severity field in Alert protocol of SSL has value 2?
(a) Warning (b) Fatal Error
(c) Authentication token (d) None of these.

(iv) IDEA algorithm is used in which of the following cases?
(a) PEM (b) PGP (c) SSL (d) None of these.

(v) Which architecture is used to conduct Recruitment examination?
(a) DMZ (b) DES (c) DMQ (d) All of these.

(vi) Which firewall configuration(s) make(s) use of two packet filtering router?
(a) DMZ
(b) Screened Subnet firewall
(c) Screened host firewall singled home bastion
(d) All of these.

(vii) Which encryption algorithm which is used by PGP?
(a) DES (b) RSA (c) IDEA (d) All of these.

(viii) Which encryption algorithm uses 8 rounds of encryption?
(a) One time pad cipher (b) DES (c) IDEA (d) All of these.

(ix) Which one of the following is a mandatory component in Authentication Token?
(a) Keypad (b) Clock (c) Processor (d) None of these.

(x) Which firewall configuration has 1 level of defence?
(a) Screened Host Firewall Single Homed Bastion
(b) Screened Subnet Firewall
(c) Screened Host Firewall Dual Homed Bastion
(d) None of these.

Fill in the blanks with the correct word

(xi) _____ is the weakest firewall configuration.

(xii) _____ mode is not suitable for transmission of long messages.

(xiii) Alert protocol is a sub protocol of _____

(xiv) _____ authentication makes use of FAR and FRR

(xv) An active attack where DNS Server is hacked is called _____.

Group - B

2. (a) (I) State the cipher text for the plain text "**55, Baikuntha Road, Kolkata-700025**" using Playfair Substitution technique. Keyword to be used is **CRYPTOLOGY.**
(II) State the cipher text for the plain text "***principles of entropy***" using (i) Caesar cipher technique with key=7 and (ii) Rail Fence technique
(*Step detailing and diagram mandatory for above problems.*) *[(CO2)(Evaluate/HOCQ)]*
(b) Differentiate between Virus and Masquerade. *[(CO1)(Analyze/IOCQ)]*
(c) Differentiate between Replay attack and Pharming. *[(CO1)(Understand/LOCQ)(Analyze/IOCQ)]*

(4 + 4) + 2 + 2 = 12

3. (a) Construct a vigenere table for polyalphabetic substitution technique. Using the table develop the cipher text for plain text **"network topology"**. Key to be used is **cryptology**. *[(CO2)(Create/HOCQ)]*
(b) Develop the cipher text for the plain text "***MILD CYCLONE"*** using one time pad technique. Key to be used is "**ACEKBPERALA**". *[(CO2)(Create/HOCQ)]*
(c) Differentiate between unconditionally secure and computationally secure encryption algorithms. *[(CO1)(Analyze/IOCQ)]*
(d) Develop the cipher text for the plain text "***network cryptology***" using Simple Columnar Transposition technique for 3 rounds. Keys for First round (4, 1, 5, 3, 2), Second round (1, 3, 5, 2, 4), Third round (2, 3, 1, 4, 5). *[(CO2)(Evaluate/HOCQ)]*
(*Step detailing and diagrams are mandatory for above problems.*)

(2 + 2) + 3 + 2 + 3 = 12

Group - C

4. (a) Explain Single round encryption of DES algorithm in detail with a neat diagram. *[(CO2)(Understand/LOCQ)]*
(b) Discuss Single round encryption of IDEA algorithm in detail. *[(CO2)(Understand/LOCQ)]*
(c) Differentiate between Algorithm types and Algorithm modes. *[(CO2)(Analyze/IOCQ)]*

5 + 5 + 2 = 12

5. (a) Explain Cipher Block Chaining (CBC) mode and Counter mode in detail with neat diagrams. *[(CO2)(Understand/LOCQ)]*

(b) Demonstrate Man in the Middle attack with the following numerical parameters: [n=11, g=7; x for sender=3; y for receiver=9 and x=4, y=6 for attacker]. *[(CO2)(Apply/IOCQ)]*

(c) Explain the working mechanism of IDEA with a neat block diagram. *[(CO3)(Understand/LOCQ)]*

5 + 4 + 3 = 12

Group - D

6. (a) Define Authentication token. Solve and calculate public key and private key for p=23 and q=13 using RSA algorithm. *[(CO5)(Remember/LOCQ)(CO3)(Apply/IOCQ)]*

(b) Explain the working of HMAC algorithm in detail with neat diagram. *[(CO4)(Understand/LOCQ)]*

(2 + 5) + 5 = 12

7. (a) Differentiate between Certificate based authentication and Biometric authentication. *[(CO4)(Understand/LOCQ)]*

(b) Compare between the working mechanism of Challenge / Response Authentication token and Time based Authentication token. *[(CO5)(Analyze/IOCQ)]*

(c) Discuss two properties of Digital Signature. *[(CO4)(Understand/LOCQ)]*

4 + 4 + 4 = 12

Group - E

8. (a) Consider the 24 bit binary stream, [100111001010110001110101]. Deduce the hexadecimal printable characters from the above binary stream using Base 64 encoding technique. *[(CO3)(Evaluate/HOCQ)]*

(b) Explain with neat sketch, the working of PEM mail security protocol. *[(CO3)(Understand/LOCQ)]*

6 + 6 = 12

9. (a) Explain with neat sketch, the working mechanism of Handshake protocol in SSL. *[(CO6)(Understand/LOCQ)]*

(b) Discuss the attacks possible on Packet Filtering router. *[(CO6)(Understand/LOCQ)]*

6 + 6 = 12

Cognition Level	LOCQ	IOCQ	HOCQ
Percentage distribution	51.04	23.96	25

Course Outcome (CO):

After the completion of the course students will be able to

1. Define the concepts of Network security. Classify different types of attack on Network security. Recall the principles of security.
2. Classify different kinds of Substitution techniques and Transposition techniques. Describe the concepts of Symmetric key cryptography and Asymmetric key cryptography. Discuss in detail DES, RSA and IDEA algorithm.
3. Solve numerical based on DES and RSA. Analyze the concept of SSL, PEM and PGP. Compare MAC, Message Digest and Hash function.
4. Analyze HMAC algorithm. Describe Digital Signature.

5. Explain Authentication token and Classify between different types of Authentication tokens. Compare Certificate based authentication and Biometric Authentication
6. Explain the concepts of Firewall and DMZ Network. Compare between Packet filtering router, Application- level gateway and Circuit-level gateway. Classify between different Firewall Configurations.

**LOCQ: Lower Order Cognitive Question; IOCQ: Intermediate Order Cognitive Question; HOCQ: Higher Order Cognitive Question.*

BASE64 INDEX TABLE

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	/