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 of the following is a computationally secure encryption algorithm?
(a) DES (b) RC5
(c) IDEA (d) All the above

(ii) Which of the following is an unconditionally secure encryption algorithm?
(a) Vernam Cipher (b) DES
(c) IDEA (d) All of these

(iii) Which rounds do not require key shifting in IDEA?
(a) 2 and 3 (b) 5 and 1
(c) 1, 4 and 8 (d) 4 and 8

(iv) Which mode can be used for transmitting long messages?
(a) CBC (b) OFB
(c) ECB (d) None of above

(v) Which algorithm is susceptible to Bucket Brigade attack?
(a) Double DES
(b) Triple DES
(c) Diffie-Hellman Key Exchange algorithm
(d) None of the above

(vi) What is used to generate unique password in Authentication Token?
(a) Processor (b) Battery
(c) Keyboard (d) Seed

(vii) Which of the following has Record protocol as sub-protocol?
(a) DES (b) IDEA
(c) SSL (d) RSA

(viii) 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

(ix) Which encryption algorithm is used by PGP?
(a) DES (b) IDEA
(c) RC5 (d) All of the above

(x) Which principle of security ensures sender's identity?
(a) Confidentiality (b) Modification
(c) Authentication (d) All of the above

Fill in the blanks with the correct word

(xi) An attack in confidentiality is called _____.

(xii) A person who attempts to break cryptography solutions is called _____.

(xiii) DES encrypts blocks of _____ bits.

(xiv) When two different message digests have the same value, it is called as _____.

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

Group - B

2. (a) Develop the cipher text for the plain text "***cryptography and cryptology***" using the following techniques:
(i) Playfair substitution technique with keyword= **NETWORK SECURITY**
(ii) Simple Columnar Transposition technique up to 3 rounds with keys for First round (3, 2, 1, 4), Second round (4, 3, 2, 1) and Third round (2, 4, 1, 3).
[(CO2) (Evaluate/HOCQ)]

(b) Discuss different types of attack on an encrypted text performed by Cryptanalyst.
[(CO1) (Understand/LOCQ)]

(5 + 3) + 4 = 12

3. (a) State the cipher text for the plain text "**19, Hazra avenue, Kolkata-700019**" using Playfair Substitution technique. Keyword to be used is **Network cryptology.**
State the cipher text for the plain text "***fundamentals of cryptography***" using (i) Caesar cipher technique with key=9 and (ii) Rail Fence technique.
[(CO2) (Evaluate/HOCQ)]

(b) Differentiate between IP Spoofing and Masquerade. *[(CO1) (Analyze/IOCQ)]*

(6 + 4) + 2 = 12

Group - C

4. (a) Explain Digital Envelope in detail. *[(CO3) (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].

[(CO3) (Apply/IOCQ)]

6 + 6 = 12

5. (a) Alice and Bob want to establish a secret key using the Diffie-Hellman Key exchange algorithm. Assuming the values as n=11, g=5, x=2 and y=3, find out the values of A, B, K1 and K2. *[(CO3)(Apply/IOCQ)]*

(b)

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

From the above S-Box, calculate the output for the following inputs:
(i) 101001 (ii) 000111 (iii) 010101. *[(CO3)(Analyze/IOCQ)]*

6 + 6 = 12

Group - D

6. (a) In an RSA cryptosystem, a particular A uses two prime numbers p = 13 and q =17 to generate her public and private keys. If the public key of A is 35, calculate the private key of A. *[(CO3)(Apply/IOCQ)]*

(b) Explain the working mechanism of Certificate based Authentication in detail. *[(CO5)(Understand/LOCQ)]*

(c) Discuss the properties of Message authentication code. *[(CO4)(Understand/LOCQ)]*

4 + 5 + 3 = 12

7. Calculate the Message digest for the following sets of original messages:
(i) 7391742 (ii) 6476797 (iii) 2766893 (iv) 9553737. *[(CO4)(Apply/IOCQ)]*

(4 × 3) = 12

Group - E

8. (a) Differentiate between Circuit level-gateway and Application-level gateway. *[(CO6)(Analyze/IOCQ)]*

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

5 + 7 = 12

9. (a) Justify the statement "Positioning of SSL layer is perfect in TCP/IP model". *[(CO6)(Analyze/IOCQ)]*

(b) Define Bastion Host. Discuss five properties of Bastion Host. *[(CO6)(Remember/Understand/LOCQ)]*

5 + (2 + 5) = 12

Cognition Level	LOCQ	IOCQ	HOCQ
Percentage distribution	33.33	47.92	18.75