CRYPTOGRAPHY & NETWORK SECURITY
(INFO 3233)

Time Allotted : 3 hrs **Full Marks : 70**

Figures out of the right margin indicate full marks.

Candidates are required to answer Group A and any 5 (five) from Group B to E, taking at least one from each group.

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

Group – A
(Multiple Choice Type Questions)

1. Choose the correct alternative for the following: **10 × 1 = 10**

(i) ..... suffers from Man in the Middle attack.
(a) Double DES (b) Triple DES
(c) Diffie-Hellman Key Exchange Algorithm (d) SSL

(ii) ..... Firewall does not hinder system performance.
(a) Hardware (b) Software (c) Hybrid (d) None of these

(iii) ..... cipher facilitate one to one substitution.
(a) Polyalphabetic (b) Polygram
(c) Homophonic (d) Monoalphabetic.

(iv) ..... mode can be used for transmission of long messages.
(a) CFB (b) OFB (c) CBC (d) None of these

(v) Canonical conversion is related to .....
(a) PEM (b) RSA (c) SSL (d) None of these.

(vi) ..... is an attack in availability.
(a) Fabrication (b) Modification
(c) Interruption (d) None of these

(vii) ..... algorithm produces 160 bit hash value.
(a) MD5 (b) SHA-1 (c) All of these (d) None of these

(viii) ..... signature is a bit pattern signature.
(a) Manual (b) Digital (c) Rectangular (d) None of these

(ix) ..... is used to generate unique password in Authentication Token.
(a) Seed (b) Clock (c) Battery (d) None of these

(x) FAR and FRR are applicable with .....
(a) Certificate Authentication (b) Biometric Authentication
(c) SSL Authentication (d) None of these.

Group - B

2. (a) (i) State the cipher text for the plain text "**11, Harish Road, Kolkata-700023**" using Playfair Substitution technique. Keyword to be used is **CRYPTOGRAPHY.**
(ii) State the cipher text for the plain text "***fundamentals of cryptography***" using (i) Caesar cipher technique with key = 5 and (ii) Rail Fence technique
(*Step detailing and diagram mandatory for above problems.*) *[(CO2)(Evaluate/HOCQ)]*
(b) Differentiate between Trojan Horse and DNS spoofing. *[(CO1)(Understand/LOCQ)]*
(6 + 4) + 2 = 12

3. (a) Construct a vigenere table for polyalphabetic substitution technique. Using the table develop the cipher text for plain text **"network analysis"**. Key to be used is **cryptography.** *[(CO2)(Create/HOCQ)]*
(b) Differentiate between Phishing and Replay attack. *[(CO1)(Analyze/IOCQ)]*
(c) Develop the cipher text for the plain text "***fundamentals of security***" using Simple Columnar Transposition technique for 3 rounds. Keys for First round (3,2,1, 4), Second round (1,2,3, 4), Thirdround (2,3,1, 4). *[(CO2)(Evaluate/HOCQ)]*
(*Step detailing and diagrams are mandatory for above problems.*)
(3 + 3) + 3 + 3 = 12

Group - C

4. (a) Explain the following algorithm modes with neat diagram:
(i) Electronic Code Book Mode
(ii) Cipher Block chaining mode
(iii) Cipher Feedback mode. *[(CO2)(Understand/LOCQ)]*
(b) Differentiate between Confusion and Diffusion. *[(CO2)(Analyze/IOCQ)]*
(3 + 3 + 4) + 2 = 12

5. (a) Explain Sub Key generation algorithm of RC5 with neat diagram.
[(CO2) (Understand/LOCQ)]
(b) Demonstrate Man in the Middle attack with attached 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) Briefly discuss Single round encryption of IDEA algorithm.
[(CO2)(Understand/LOCQ)]
4 + 4 + 4 = 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 MD5 algorithm in detail with neat diagram. Discuss the working of Time based authentication token.

[(CO4)(Understand/LOCQ)][(CO5)(Understand/LOCQ)]

(1 + 5) + (4 + 2) = 12

7. (a) Differentiate between MAC and Message Digest. Explain the working of Biometric authentication. *[(CO3)(Analyze/IOCQ)(CO5)(Understand/LOCQ)]*

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

(c) Explain HMAC algorithm with neat diagram. *[(CO4)(Understand/LOCQ)]*

(3 + 3) + 2 + 4 = 12

Group - E

8. (a) Explain data transmission between two networks using VPN architecture with suitable diagram. Differentiate between Packet filtering router and Application-level gateway. *[(CO3)(Understand/LOCQ)(CO6)(Analyze/IOCQ)]*

(b) Explain with neat sketch, the working of PGP mail security protocol.

[(CO3)(Understand/LOCQ)]

(5 + 3) + 4 = 12

9. (a) Explain with neat sketch, the working of Record protocol in SSL.

[(CO3)(Understand/LOCQ)]

(b) Explain with neat sketch, the working of PEM mail security protocol.

[(CO3)(Understand/LOCQ)]

(c) Explain DMZ architecture of firewall with neat diagram.

[(CO6)(Understand/LOCQ)]

5 + 4 + 3 = 12

Cognition Level	*LOCQ*	*IOCQ*	*HOCQ*
Percentage distribution	*56.25*	*23.96*	*19.79*

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 and illustrate the concepts of Symmetric key cryptography and Asymmetric key cryptography. Discuss in detail DES, RSA, IDEA and RC5 algorithm.
3. Solve numerical based on DES and RSA. Analyze the concept of SSL, PGP and PEM. Explain VPN. Compare MAC, Message Digest and Hash function.
4. Analyze MD5 Message Digest algorithm and HMAC algorithm. Illustrate 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.*