FUNDAMENTALS OF CRYPTOGRAPHY
(INFO 4221)

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 Meet in the Middle attack.
(a) Double DES (b) Triple DES (c) RSA (d) SSL

(ii) _____ is an encryption algorithm that uses 8 rounds of encryption.
(a) One time pad cipher (b) DES
(c) IDEA (d) All of these

(iii) _____ is a principle of security that ensures sender's identity.
(a) Integrity (b) Authentication
(c) Confidentiality (d) None of these

(iv) _____ mode suffers from message stream modification attack.
(a) CFB (b) OFB (c) Both (a) and (b) (d) None of these

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

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

(vii) _____ is an attack in authentication.
(a) Fabrication (b) Modification (c) Interruption (d) None of these

(viii) _____ is a firewall architecture that makes servers publicly available.
(a) DMZ (b) DES (c) DMQ (d) All of these

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

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

Group - B

2. (a) (i) State the cipher text for the plain text "**19, Hazra road, Kolkata-700029**" using Playfair Substitution technique. Keyword to be used is **Network cryptology**.
(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 Masquerade and DNS spoofing. *[(CO1)(Understand/LOCQ)]*

(6 + 4) + 2 = 12

3. (a) Differentiate between Brute force attack and Cryptanalysis. *[(CO1)(Analyze/IOCQ)]*

(b) Construct a vigenere table for polyalphabetic substitution technique. Using the table develop the cipher text for plain text **"network security"**. Key to be used is **cryptography**. *[(CO2)(Create/HOCQ)]*

(c) Develop the cipher text for the plain text "***fundamentals of security***" using Simple Columnar Transposition technique for 4 rounds. Keys for First round (3,2,1, 4), Second round (3,1,2,4), Thirdround (4,1,3,2) and Fourth round (1,3,2,4).
[(CO2)(Evaluate/HOCQ)]
(*Step detailing and diagrams are mandatory for above problems.*)

(d) Differentiate between Pharming attack and Replay attack. *[(CO1)(Analyze/IOCQ)]*

2 + 4 + 4 + 2 = 12

Group - C

4. (a) Explain the following algorithm modes with neat diagram:
(i) Counter mode
(ii) Cipher Block chaining mode
(iii) Cipher Feedback mode. *[(CO2)(Understand/LOCQ)]*

(b) Differentiate between Double DES and Triple DES with suitable diagrams.
[(CO2)(Analyze/IOCQ)]

(2 + 3 + 4) + 3 = 12

5. (a) 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)]

(b) Illustrate Key Shifting mechanism in IDEA encryption algorithm from first round to Output transformation round. *[(CO2)(Evaluate/HOCQ)]*

6 + 6 = 12

Group - D

6. (a) Define Authentication token. Solve and calculate public key and private key for p = 7 and q = 13 using RSA algorithm. *[(CO5)(Remember/LOCQ)(CO3)(Apply/IOCQ)]*

(b) Explain the working of Authentication token. Discuss the working of Challenge-Response authentication token. *[(CO5)(Understand/LOCQ)][(Understand/LOCQ)]*

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

7. (a) Differentiate between MAC and Message Digest. Explain the working of HMAC algorithm in detail with neat diagram. *[(CO3)(Analyze/IOCQ)(CO4)(Understand/LOCQ)]*

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

   (c) Explain any two requirements of Hash function. *[(CO3)(Understand/LOCQ)]*

(2 + 4) + 4 + 2 = 12

Group - E

8. (a) Differentiate between Hardware firewall and Software firewall. Differentiate between Packet filtering router and Application-level gateway. *[(CO6)(Analyze/IOCQ)(Analyze/IOCQ)]*

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

(3 + 4) + 5 = 12

9. (a) Explain with neat sketch, the working of Record protocol in SSL. *[(CO3)(Understand/LOCQ)]*

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

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

5 + 3 + 4 = 12

Cognition Level	*LOCQ*	*IOCQ*	*HOCQ*
Percentage distribution	*43.75*	*31.25*	*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.*