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

(ii) _____ is a Computationally secure encryption algorithm.
(a) DES (b) BDE
(c) RC5 (d) Both (a) and (c)

(iii) _____ mode can be used for transmitting long messages.
(a) ECB (b) CBC
(c) None of these (d) All of these

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

(v) _____ cipher uses both transposition and substitution.
(a) Combinational (b) Product
(c) Double (d) None of these

(vi) _____ algorithm uses 16 rounds of encryption.
(a) IDEA (b) DES
(c) RSA (d) Both (a) and (c)

(vii) OSI position of _____ is between transport and application.
(a) IPSec (b) SSL
(c) all of these (d) none of these

(viii) Mathematical attack is applicable in _____
(a) RSA (b) DES
(c) MD2 (d) all of these.

(ix) FAR and FRR are applicable with _____
(a) Certificate Authentication (b) Biometric Authentication
(c) Fabrication (d) None of these.

(x) Record protocol is a sub protocol of _____
(a) DES (b) IDEA (c) SSL (d) RSA.

Group- B

2. (a) Develop the cipher text for the plain text "*cryptography and security*" 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)
(*Step detailing and diagram mandatory for above problems.*)
[(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) Construct a vigenere table for polyalphabetic substitution technique. Using the table develop the cipher text for plain text "cryptology and security". Key to be used is cryptography. [(CO2)(Create/HOCQ)]

(b) Develop the cipher text for the plain text "*CRYPTOLOGY SECURITY*" using one time pad technique. Key to be used is "BARCEKAPERALAFRICA".
[(CO2)(Create/HOCQ)]

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

(3 + 3) + 4 + 2 = 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. Explain Meet in the Middle attack. [(CO2)(Analyze/IOCQ)(Understand/LOCQ)]

(3 + 3 + 3) + 3 = 12

5. (a) Explain Diffie-Hellman key exchange algorithm. [(CO2)(Understand/LOCQ)]

(b) Justify by illustrationthat Key shifting is not required in first round, fourth round and eighth round of IDEA encryption algorithm. [(CO2)(Evaluate/HOCQ)]

4 + 8 = 12

Group - D

6. (a) Define Authentication token. Solve and calculate public key and private key for p = 7 and q = 11 using RSA algorithm.
[(CO5)(Remember/LOCQ)(CO3)(Apply/IOCQ)]

(b) Explain RSA algorithm in detail. Solve and calculate public key and private key for p = 5 and q = 13 using RSA algorithm.
[(CO2)(Understand/LOCQ)][(CO3)(Apply/IOCQ)]

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

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

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

(c) Discuss the requirements of Hash function. [(CO3)(Understand/LOCQ)]

3 + (2 + 4) + 3 = 12

Group - E

8. (a) Differentiate between Hardware firewall and Software firewall. Explain different types of firewall with neat diagram.
[(CO6)(Analyze/IOCQ)(Understand/LOCQ)]

(b) Brieflyexplain the working of Record protocol in detail with neat diagram.
[(CO3)(Understand/LOCQ)]

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

(2 + 4) + 3 + 3 = 12

9. (a) Explain with neat sketch, the working of Alert protocol in SSL.
[(CO3)(Understand/LOCQ)(CO6)(Understand/LOCQ)]

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

(c) Define Firewall. Discuss the attacks possible on Packet Filtering router.
[(CO6)(Remember, Understand/LOCQ)]

2 + 2 + 8 = 12

Cognition Level	LOCQ	IOCQ	HOCQ
Percentage distribution	55.21	17.71	27.08

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