B.TECH/ECE/8TH SEM/INFO 4281/2022

FUNDAMENTALS OF CRYPTOGRAPHY
(INFO 4281)

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) __________ firewall does not hinders system performance.
(a) Hardware (b) Software (c) Hybrid (d) None of these

(ii) __________ is a unconditionally secure encryption algorithm.
(a) One time pad cipher (b) DES (c) IDEA (d) All of these.

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

(iv) __________ mode cannot be used for transmitting long messages.
(a) ECB (b) CBC (c) None of these (d) All of these.

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

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

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

(viii) __________ is susceptible to Bucket Brigade attack.
(a) Diffie-Hellman (b) Double DES
(c) Both (a) and (b) (d) None of These

(ix) Mathematical attack is associated with __________ algorithm.
(a) PEM (b) RSA (c) SSL (d) None of these

(x) Digital Certificate is applicable with __________
(a) Certificate Authentication (b) Biometric Authentication
(c) Fabrication (d) None of these.

Group- B

2. (a) Develop the cipher text for the plain text "*network security*" using the following techniques:
(i) Playfair cipher technique with keyword = CRYPTOGRAPHY
(ii) Simple Columnar Transposition technique up to 3 rounds with keys for First round (3,2,1) Second
round (1,2,3) and Third round(2,1,3)
(*Step detailing and diagram mandatory for above problem.*)
[(CO2)(Create/HOCQ)]

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

(4 + 3) + 5 = 12

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

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

(c) Differentiate between Denial of Service attack and Replay attack. [(CO1)(Analyze/IOCQ)]

(3 + 3) + 4 + 2 = 12

Group - C

4. (a) Differentiate between Confusion and Diffusion. Explain Meet in the Middle attack. [(CO2)(Analyze/IOCQ)(CO2)(Understand/LOCQ)]

(b) Discuss Single round encryption of IDEA algorithm in detail including Output transformation round. [(CO2)(Understand/LOCQ)]

(2 + 2) + 8 = 12

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

(b) Differentiate between Algorithm types and modes. Explain Counter mode with neat diagram. [(CO2)(Analyze/IOCQ)(Understand/LOCQ)]

5 + (2 + 5) = 12

Group - D

6. (a) 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)]

(b) Explain Biometric Authentication in detail. Differentiate between Challenge-Response token and Time based token. [(CO4)(Understand/LOCQ)][(CO4)(Analyze/IOCQ)]

(2 + 4) + (2 + 4) = 12

7. (a) Explain the working of HMAC algorithm in detail with neat diagram. [(CO3)(Understand/LOCQ)]

   (b) State any five requirements of Digital Signature. [(CO3)(Remember/LOCQ)]

7 + 5 = 12

Group - E

8. (a) Differentiate between Software firewall and Hardware firewall. Explain different types of firewall configuration with neat diagram. [(CO5)(Analyze/IOCQ)][(CO5)(Understand/LOCQ)]

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

(2 + 6) + 4 = 12

9. (a) Explain the working of Handshake protocol in detail with neat diagrams. [(CO3)(Understand/LOCQ)]

   (b) Discuss the attacks possible on Packet Filtering router. [(CO5)(Understand/LOCQ)]

8 + 4 = 12

Cognition Level	LOCQ	IOCQ	HOCQ
Percentage distribution	65.64	16.66	17.70

Course Outcome (CO):

After the completion of the course students will be able to:

1. Define the concepts of Network security and identify different types of attack on Network security. Recall the principles of security.
2. Classify different kinds of Substitution techniques and Transposition techniques and discuss the concepts of Symmetric key cryptography and Asymmetric key cryptography. Explain in detail DES, RSA and IDEA algorithm.
3. Prepare and practice numerical module based on DES and RSA. Illustrate the concept of SSL, PEM, Authentication token and Digital Signature. Explain Message Digest and Hash function in accordance with the prescribed syllabus.
4. Analyze Certificate based Authentication, Biometric Authentication and differentiate between different types of Authentication tokens.
5. Explain concepts of Firewall (including types of Firewall), DMZ Network and comparing between different Firewall Configurations.

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