M.TECH/CSE/2ND SEM/CSEN 5234/2015
2015

Cryptography & Network Security
(CSEN 5234)

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 x 1=10**

(i) What will be the value of φ (147)

(a) 72 (b) 84 (c) 128 (d) 112.

(ii) ……..is generally used in ECB, CBC or CFB mode.

(a) RSA (b) DES
(c) AES (d) IDEA.

(iii) Which of the following technology is based on IDEA algorithm?

(a) S/MIME (b) SET
(c) SSL (d) PGP.

(iv) The Secure Socket Layer provides

(a) encryption for messages sent by both client server
(b) server authentication
(c) optional client authentication
(d) all of these.

(v) If the sender encrypts the message with her private key, it achieves the purpose of

(a) confidentiality
(b) confidentiality and authentication
(c) confidentiality and not authentication
(d) authentication.

(vi) SSL layer is located between ---------- and ---------- layer

(a) transport and network layer (b) application and transport layer
(c) network and data link layer (d) data link and physical layer.

(vii) MD5 produces ----------bits of message digests :

(a) 124 (b) 160
(c) 1024 (d) 256.

(viii) The ---------- attack is related to confidentiality.

(a) interception (b) fabrication
(c) modification (d) interruption.

(ix) The CA signs a digital certificate with

(a) the user's public key (b) the user's private key
(c) owner's private key (d) owner's public key.

(x) Which of the following is passive attack?

(a) Masquerade (b) Traffic Analysis
(c) Replay attack (d) Denial of service.

Group – B

2.(a) State Fermat's little theorem and explain its application. Find the results of 6^{10} mod 11 and 3^{12} mod 11.

(b) User A and B exchange the key using Diffie-Hellman Algorithm. Assume α=5, q=11, X_a=2, X_b=3. Find the value of Y_a, Y_b and K. "For its effectiveness Diffie Hellman depends on the difficulty of computing discrete logarithms" - Justify the statement.

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

3.(a) Discuss the DES algorithm in details with explanation of each step and with diagram.

(b) Using Rail fence Technique encrypt the following message.

Must see you over Cadogan West

(c) Explain RSA algorithm with example.

7+2+3=12

Group – C

4.(a) Perform encryption and decryption using RSA algorithm for the following: P=7, q=11, e=17, M=8.

(b) Explain the term (i) Integrity (ii) Authentication (iii) Non-Repudiation in Network Security.

(c) Explain digital envelop and digital signature.

2+(3X2)+(2X2)=12

5.(a) Define an elliptic curve and explain their applications in cryptography.

(b) On the elliptic curve $y^2 = x^3 - 36x$ let P = (-3, 9) and Q = (-2, 8). Find P + Q and 2P.

(3+3)+6=12

Group – D

6.(a) Explain briefly the handshake and the record protocol of SSL.

(b) What are the different security services provided by PGP? Describe the role of the Ticket Granting Ticket and Service Granting Ticket in Kerberos.

6+(3+3)=12

7.(a) What is a message digest? What is the difference between Message digest and Message Authentication Code?

(b) Write down MD5 algorithm with explanation. Briefly compare its performance with SHA – 1.

(2+3)+7=12

Group – E

8.(a) What are the difference between SSL version 3 and TLS? What is the ElGamal Cryptosystem?

(b) Compare and contrast key management in PGP and S/MIME.

(3+3)+6=12

9.(a) What is a firewall? Name different types of firewall? Briefly explain the working principle of each.

(b) What are the limitations of firewall?

(2+7)+3=12