CRYPTOGRAPHY AND NETWORK SECURITY
(CSEN 4162)

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) This is the hiding of a secret message within an ordinary message and the extraction of it at its destination.
(a) message queuing (b) spyware
(c) bytecode (d) steganography.

(ii) .....is an encryption method used to offer secure communication by email:
(a) Mail server (b) PGP
(c) SSL (d) None of the above.

(iii) The minimum positive integer p such that 3^p modulo 17 = 1 is
(a) 5 (b) 8 (c) 12 (d) 16.

(iv) AES uses a .....bit block size and a key size of ----------bits.
(a) 128; 128 or 256 (b) 64; 128 or 192
(c) 256; 128,192 or 256 (d) 128; 128,192 or 256.

(v) Hash function is used for:
(a) message authentication (b) producing fingerprint of a file
(c) both (a) and (b) (d) None of the above.

(vi) RSA algorithm uses variable sized key that is usually between.....and ..... bits.
(a) 256,1048 (b) 256, 2048
(c) 512, 1048 (d) 512, 2048.

(vii) The input block length in AES is:
(a) 56 bits (b) 64 bits (c) 112 bits (d) 128 bits.

(viii) If an efficient algorithm for factoring large number is discovered, which of the following schemes will be known to be not secure?
(a) Diffle-Hellman (b) RSA
(c) AES (d) None of the above.

(ix) SSL layer is located between
(a) transport layer and network layer
(b) application layer and transport layer
(c) data link layer and physical layer
(d) network layer and data link layer.

(x) In the DES algorithm, although the key size is 64 bits, only 48 bits are used for the encryption procedure, the rest are parity bits.
(a) True (b) False
(c) May be (d) Can't say.

Group - B

2. (a) Discuss the concept of Caesar cipher. Use Caesar cipher with key =15 to encrypt the message "GOOD MORNING".

(b) Find the values of (i) 7^7 mod 9 and (ii) 3^{110} mod 13.

(c) Explain the Diffie-Hellman key exchange algorithm. Alice and Bob want to establish a secret key using the Diffie-Hellman key exchange algorithm. Assuming the values as n = 11, g = 5, x = 2 and y = 3. find out the values of the secret keys K1 and K2.

3 + (2 + 2) + 5 = 12

3. (a) State Euler's theorem with example. Find Euler's totient function of n=91.

(b) What is mono-alphabetic cipher? How it is different from Caesar cipher? Explain brute-force attack in this context.

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

Group - C

4. (a) What are the four main stages of AES operation? What would be the following state matrix after the shift row operation?

ac	21	34	ec
02	76	ea	02
13	50	46	a4
92	76	ab	Ba

(b) Explain the encryption process of cipher feedback (CFB) mode using suitable diagram.

(3 + 6) + 3 = 12

5. (a) Explain single round of DES algorithm with flowchart.

(b) Explain the one-time initialization in AES algorithm.

9 + 3 = 12

Group - D

6. (a) Describe MD5 algorithm in detail. Compare its performance with SHA-1.

(b) Briefly discuss the operation of Kerberos authentication protocol with suitable diagram.

5 + (3 + 4) = 12

7. (a) Write an algorithm to generate a digital signature using the RSA algorithm.

(b) State the possible attacks on RSA signature.

(c) State how DSA can be used to generate the digital signature.

5 + 3 + 4 = 12

Group - E

8. (a) What are the different modes of operation of IPSec.

(b) Write a short note on Oakley key determination protocol.

(c) State the limitations of a firewall.

4 + 4 + 4 = 12

9. (a) Describe in brief the proxy firewall.

(b) Discuss ESP header.

(c) Why is the SSL layer positioned between the application layer and the transport layer? What is the purpose of the SSL alert protocol?

4 + 3 + (2 + 3) = 12