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 <u>any 5 (five)</u> from Group B to E, taking <u>at least one</u> 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) In cryptography, the order of the letters in a message is rearranged by
(a) transpositional ciphers
(b) substitution ciphers
(c) both transpositional ciphers and substitution ciphers
(d) none of the (a),(b),(c).

(ii) An attack on a cipher text message where the attacker attempts to use all possible permutations and combinations is called:
(a) Brute-Plaintext attack (b) Birthday attack
(c) Known-Plaintext attack (d) Chosen-plaintext attack.

(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 256128; (d) 128,192 or 256.

(v) The number of tests required to break the DES algorithm is
(a) 2.8×10^{14} (b) 4.2×10^{9}
(c) 1.84×10^{19} (d) 7.2×10^{16}.

(vi) Kerberos is an authentication scheme that can used to implement:
(a) Public key cryptography
(b) Digital signature
(c) Hash function
(d) Single sign on.

(vii) Using public key cryptography, X adds a digital signature α to message M, encrypts , and sends it to Y, where it is decrypted. Which one of the following sequences of keys is used for the operations?

(a) Encryption: X's private key followed by Y's private key; Decryption: X's public key followed by Y's public key

(b) Encryption: X's private key followed by Y's public key; Decryption: X's public key followed by Y's private key

(c) Encryption: X's public key followed by Y's private key; Decryption: Y's public key followed by X's private key

(d) Encryption: X's private key followed by Y's public key; Decryption: Y's private key followed by X's public key

(viii) Suppose that everyone in a group of *N* people wants to communicate secretly with the *N*-1 others using symmetric key cryptographic system. The communication between any two persons should not be decodable by the others in the group. The number of keys required in the system as a whole to satisfy the confidentiality requirement is.

(a) 2N (b) N(N-1) (c) N(N-1)/2 (d) $(N-1)^2$.

(ix) SSL layer is located between

(a) transport layer, network layer

(b) application layer, transport layer

(c) data link layer, physical layer

(d) network layer, data link layer.

(x) Which of the following is not a block cipher operating mode?

(a) ECB (b) CBF (c) OFB (d) CBC

Group – B

2. (a) Explain the Diffie Hellman Key-Exchange Algorithm with suitable diagram and example.

(b) Can the Diffie Hellman Key-Exchange Algorithm fall prey to the man-in-the-middle attack? Explain with suitable example.

(c) State the encryption process of Playfair Cipher. What will be the ciphered text if the string "CRYPTOGRAPHY EXAM" is given as input to the code of playfair cipher with keyword as "SECRET" (assuming j is combined with i)?

4 + 4 + 4 = 12

3. (a) Evaluate 3^{21} mod 11 using Fermat's theorem.

(b) Solve using play-fair cipher. Encrypt the word "Semester Result" with the keyword "Examination". List the rules used. Discuss ARP Spoofing.

3 + (7 + 2) = 12

Group – C

4. (a) What do you understand by the terms "diffusion" and "confusion" in context of Cryptography?

(b) Can you state the names of any 2 algorithms for each of these 2 categories and explain them?

(c) Explain the 2 variants of the Triple DES algorithm using suitable block diagrams.

2 + 6 + 4= 12

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

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

9 + 3 = 12

Group – D

6. (a) Define MAC. Compare MD5 with SHA-1.

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

(2 + 3) + 7 = 12

7. (a) Discuss about X.509 authentication service in detail.

(b) Explain digital signature with ElGamal Public key cryptosystem.

6 + 6 = 12

Group – E

8. (a) Explain the NAT with suitable diagram.

(b) State the limitations of a firewall.

(c) Explain the working of IPSec.

3 + 3 + 6= 12

9. (a) Explain the role of PGP in authentication with suitable diagram.

(b) Write a short note on SSL.

6 + 6 = 12