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) Key used in the symmetric key cryptography is called
(a) Public Key (b) Permanent Key
(c) Session Key (d) Private Key.

(ii) What is data encryption standard (DES)?
(a) Block cipher (b) Stream cipher
(c) Bit cipher (d) None of the mentioned.

(iii) In MD-5 the length of the message digest is
(a) 160 (b) 128 (c) 64 (d) 54.

(iv) We require _____ to verify digital signature
(a) receiver's public key (b) sender's private key
(c) sender's public key (d) receiver's private key.

(v) RC4 is an example of
(a) Hash Algorithm (b) Stream Cipher
(c) Block Cipher (d) All of the above.

(vi) ElGamal encryption system is
(a) symmetric key encryption algorithm
(b) asymmetric key encryption algorithm
(c) not an encryption algorithm
(d) none of the mentioned.

(vii) The Authentication Header (AH) protocol, part of IPsec, provides which of the following security functions?
(a) Source authentication
(b) Data integrity
(c) Data confidentiality
(d) Source authentication and data integrity.

(viii) The Secure Socket Layer (SSL) provides
(a) encryption for messages sent by both client and server
(b) server authentication
(c) optional client authentication
(d) all of the above.

(ix) If an efficient algorithm for factoring large number is discovered which of this following schemes will be known to be not secure?
(a) AES (b) Diffle-Hellman
(c) RSA (d) EI Gammal.

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

Group – B

2. (a) Discuss the concept of Vernam cipher. What will be the output of the following plain text if Vernam cipher technique is used to encode it? Assume the one time pad is NCBTZQARX.
Plain Text: How are you?

(b) Define Euler's totient function and its application.

(c) Evaluate gcd(1547,560) using Euclid's algorithm.
(2 + 3) + (2 + 2) + 3 = 12

3. (a) Using Fermat's theorem find the value of 5^{158} mod 11?

(b) What do you mean by confidentiality and authentication? Discuss various types of active attacks.

(c) What do you mean by transposition technique? What will be the output of the following plain text if simple columnar transposition technique is used to encode it?
Plain Text: Hello World.
2 + (2 + 4) + (1 + 3) = 12

Group – C

4. (a) Discuss the pros and cons of symmetric and asymmetric key cryptography.

(b) Explain the RSA Algorithm. What is the real crux of RSA?

(c) Consider a plain text alphabet ***G***. Using RSA algorithm and the values of E, D and N as 3, 11 and 15 find out the encrypted cipher text. Verify that on decryption, the cipher text transforms back to the plain text ***G***.

3 + (3 + 2) + 4 = 12

5. (a) What are the disadvantages with ECB mode of operation?

(b) Explain the steps of the AES Algorithm with suitable diagram.

(c) What is triple DES? Explain it with suitable block diagram. Explain why it is more secure than DES algorithm.

2 + 4 + (3 + 3) = 12

Group – D

6. (a) Describe the role of Ticket Granting Ticket and service granting Ticket in Kerberos.

(b) Describe SHA-1 algorithm in detail.

(c) Compare and contrast MD-5 and SHA-1 algorithms.

4 + 5 + 3 = 12

7. (a) What do you understand by two-factor authentication method?

(b) Explain the Kerberos third-party authentication model with suitable diagram.

(c) What is digital signature? Write a short note on the Digital Signature Algorithm (DSA).

3 + 4 + (2 + 3) = 12

Group – E

8. (a) Differentiate between transport and tunnel modes of operation of IPsec.

(b) What are the different security services provided by PGP?

(c) Explain how PGP provides confidentiality and authenticity of electronic mails. Explain the necessity of base-64 conversion in PGP.

4 + 2 + (4 + 2) = 12

9. (a) "ISAKMP agrees to create exchanges for the SA establishment and keying material". What are the different exchange types?

(b) Explain the working of the OAKLEY key determination protocol.

(c) What advancement does the OAKLEY key determination protocol provide over the Diffie-Hellman Key exchange algorithm?

5 + 4 + 3 = 12