CRYPTOGRAPHY & NETWORK SECURITY
(CSEN 4132)

Time Allotted : 2½ hrs **Full Marks : 60**

Figures out of the right margin indicate full marks.

Candidates are required to answer Group A and any 4 (four) from Group B to E, taking one from each group.

Candidates are required to give answer in their own words as far as practicable.

Group – A

1. Answer any twelve: **12 × 1 = 12**

Choose the correct alternative for the following

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

(ii) The multiplicative Inverse of 1234 mod 4321 is
(a) 3239 (b) 3213 (c) 3242 (d) Does not exist.

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

(iv) In RSA, Φ(n) = _____ in terms of p and q, where n = pq
(a) (p)/(q) (b) (p)(q) (c) (p-1)(q-1) (d) (p+1)(q+1)

(v) What type of encryption does DES use?
(a) Asymmetric encryption (b) Symmetric encryption
(c) Hashing (d) Digital signatures.

(vi) 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

(vii) Which of the following properties is essential for a good cryptographic hash function?
(a) The hash function must be reversible
(b) It should produce a fixed-size hash output
(c) The hash value must be the same for different inputs
(d) It should be easy to find two different inputs with the same hash value.

(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) Which protocols are part of IPsec?
(a) ESP and AH (b) TCP and UDP
(c) HTTP and HTTPS (d) SSH and TLS.

(x) A firewall that uses two TCP connections is
(a) Bastion (b) Applicaton Gateway
(c) Circuit level Gateway (d) Packet Filter.

Fill in the blanks with the correct word

(xi) When two different message-digests have the same value, it is called _____.

(xii) In the digital signature technique, the sender of the message uses _____ to create cipher text.

(xiii) Symmetric key cryptography uses the same key for both encryption and _____.

(xiv) The RSA algorithm is a widely used _____ key cryptographic algorithm for secure data transmission.

(xv) The Diffie-Hellman key exchange protocol allows two parties to securely agree on a shared _____ over an insecure channel.

Group - B

2. (a) Evaluate gcd(1398,324) using Extended Euclidian algorithm. *[(CO2)(Evaluate/IOCQ)]*
(b) Using Fermat's theorem find the value of 5158 mod 11. Find 27^{-1} mod 41(multiplicative inverse) using Fermat's theorem. *[(CO2)(Remember)/LOCQ)]*
(c) State Euler's theorem. Determine Φ(27) and Φ(240) using Euler's totient function. *[(CO2)(Apply/IOCQ)]*

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

3. (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? *[(CO1)(Understand/LOCQ))]*
(b) Define Euler's totient function and its application. *[(CO2)(Apply/IOCQ)]*
(c) Discuss the pros and cons of symmetric and asymmetric key cryptography. *[(CO1)(Understand/LOCQ)]*

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

Group - C

4. (a) 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 q = 11 and a primitive root alpha=7, find out the values of the secret keys K1 and K2. *[(CO5)(Evaluate/HOCQ)]*
(b) Draw the steps involved in the encryption of the Cipher Block Chaining (CBC) mode. *[(CO3)(Remember/LOCQ)*]
(c) Explain the Key Generation Process of DES with suitable diagram. *[(CO3)(Analyze/IOCQ)]*

5 + 2 + 5 = 12

5. (a) What requirements must a public key cryptosystem have to fulfil to a secured algorithm?
Perform encryption and decryption using RSA algorithm for the following. P=7; q=11; e=17; M=8. *[(CO3)(Apply/IOCQ)]*

(b) Explain the steps of the AES algorithm with suitable diagram. *[(CO3)(Understand/LOCQ)]*

(4 + 4) + 4 = 12

Group - D

6. (a) Describe the process of digital signature generation and verification using the Digital Signature Algorithm (DSA). *[(CO6)(Apply/HOCQ)]*

(b) Discuss the role of the hash function in this process. *[(CO4)(Remember/LOCQ)]*

6 + 6 = 12

7. (a) What do you understand by two-factor authentication method? *[(CO4)(Understand/LOCQ)]*

(b) Explain the Kerberos third-party authentication model with suitable diagram. *[(CO4)(Understand/LOCQ)]*

(c) What is digital signature? Write a short note on the Digital Signature Algorithm (DSA). *[(CO6)(Describe/LOCQ)]*

3 + 4 + (2 + 3) = 12

Group - E

8. (a) What are different types of firewalls? Briefly explain the working principle of each. *[(CO6)(Remember/LOCQ)]*

(b) Briefly explain the Handshake Protocol of SSL. *[(CO5)(Analyze/LOCQ)]*

(2 + 4) + 6 = 12

9. (a) What are the different types of firewalls? List and briefly describe each type. *[(CO5)(Remember/LOCQ)]*

(b) How do you perform regular maintenance on a firewall? *[(CO5)(Analyze/LOCQ)]*

(c) Discuss the potential security vulnerabilities associated with using VPNs and how they can be mitigated. *[(CO5)(Analyze/IOCQ)]*

4 + 4 + 4 = 12

Cognition Level	LOCQ	IOCQ	HOCQ
Percentage distribution	59.5	29	11.5