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) For a network with N nodes, how many master keys are present?
(a) N(N-1)/2 (b) N
(c) N(N+1)/2 (d) N/2.

(ii) Find the value of ϕ (21)
(a) 10 (b) 8
(c) 12 (d) 14.

(iii) What is a common vulnerability associated with the Diffie-Hellman key exchange if not properly mitigated?
(a) Man-in-the-Middle attack (b) Replay attack
(c) Cipher text-only attack (d) Chosen-plaintext attack

(iv) How many rounds of processing does AES use for a 256-bit key?
(a) 10 rounds (b) 12 rounds
(c) 14 rounds (d) 16 rounds

(v) In the DES algorithm the round key is _____ bit and the Round Input is _____ bits.
(a) 48, 32 (b) 64,32
(c) 56, 24 (d) 32, 32

(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 cannot be achieved by the digital signature in symmetric key encryption?
(a) Message authentication (b) Data integrity
(c) Non-repudiation (d) Security of the message

(viii) 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.

(ix) Which of the following is a key feature of IPsec?
(a) It operates at the Application layer.
(b) It supports both transport and tunnel modes.
(c) It is exclusively for email encryption.
(d) It is used only for IPv6 networks.

(x) What types of protocols are used in VPNs?
(a) Application level protocols (b) Tunnelling protocols
(c) Network protocols (d) Mailing protocols

Fill in the blanks with the correct word

(xi) In cryptography, the order of the letters in a message is rearranged by _____.

(xii) Digital Signature cannot provide _____ for the message.

(xiii) IP Sec services are available in _____ layer.

(xiv) _____ is an encryption method used to offer secure communication by email.

(xv) _____ masks your IP address.

Group - B

2. (a) Find $8^{-1} \bmod 77$ (multiplicative inverse) using Euler's theorem. *[(CO2)(Apply/IOCQ)]*
(b) Solve x =3(mod 5), x=1(mod 7), x=6(mod 8) using Chinese Remainder Theorem. *[(CO1.CO2)(Anlyze/HOCQ)]*
(c) How many primate roots are there in modulo 7 and modulo 11? 2 is a primitive root modulo 13. What are the other primitive roots modulo 13? *[(CO2)(Remember/LOCQ)]*

3 + 5 + (2 + 2) = 12

3. (a) What do you mean by confidentiality and authentication? Discuss various types of active attacks. *[(CO1)(Remember /LOCQ)]*
(b) 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. *[(CO1)(Understand/LOCQ)]*
(c) What do you understand by the terms "diffusion" and "confusion" in context of Cryptography? *[(CO1)(Remember/LOCQ)]*

(2 + 4) + (1 + 3) + 2 = 12

Group - C

4. (a) Given p=17, q=11, and e=7 Use RSA algorithm to find n, d, Public and Private Key. *[(CO1,CO2)(Evaluate/HOCQ)]*

(b) Explain Round operation of DES algorithm with suitable block diagram. *[(CO4)(Analyze/HOCQ)]*

6 + 6 = 12

5. (a) Explain the attacks on RSA algorithm and discuss its countermeasures. *[(CO3)(Understand/IOCQ)]*

(b) Discuss how different cryptographic algorithms use Fiestel Cipher Structure. How many S boxes are there in AES? How S-box is calculated. *[(CO4) (Explain/LOCQ)]*

5 + (3 + 2 + 2) = 12

Group - D

6. (a) Explain the roll of the Authentication Server (AS) and the Ticket Granting Server (TGS) in Kerberos. *[(CO4)(Analyze/HOCQ)]*

(b) What is a Message digest? Explain HMAC algorithm with a suitable diagram. *[(CO4)(Understand/LOCQ)]*

(3 + 3) + (2 + 4) = 12

7. (a) Explain Key generation, Encryption and Decryption method of El Gamal Cryptosystem? *[(CO6)(Understand/HOCQ)]*

(b) Explain the concept of digital envelope. *[(CO4)(Understand/LOCQ)]*

(c) Write an algorithm to generate a digital signature using the RSA algorithm. *[(CO6)(Remember/LOCQ)]*

4 + 3 + 5 = 12

Group - E

8. (a) How does PGP provide authentication and confidentiality for email services and for file transfer applications? Draw the block diagram and explain the components of PGP. *[(CO5, CO6)(Understand/IOCQ)]*

(b) Explain about IPSec architecture. *[(CO5, CO6)(Understand/LOCQ)]*

(2 + 6) + 4 = 12

9. (a) "ISAKMP agrees to create exchanges for the SA establishment and keying material". What are the different exchange types? *[(CO5)(Understand/LOCQ)]*

(b) Explain the working of the OAKLEY key determination protocol. *[(CO5)(Understand/LOCQ)]*

(c) What advancement does the OAKLEY key determination protocol provide over the Diffie-Hellman Key exchange algorithm? *[(CO6)(Analyze/HOCQ)]*

5 + 4 + 3 = 12

Cognition Level	LOCQ	IOCQ	HOCQ
Percentage distribution	52.08	16.67	31.25