NETWORK SECURITY AND CRYPTOGRAPHY
(IOT2105)

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) The process to discover plain text or key is known as
(a) cryptanalysis (b) crypto design
(c) crypto processing (d) crypto graphic

(ii) GCD(n,n+1) = 1 always
(a) true (b) false (c) maybe (d) can't be said

(iii) The Data Encryption Standard (DES) follows
(a) Hash Algorithm (b) Caesars Cipher
(c) Feistel Cipher Structure (d) SP Networks

(iv) Which symmetric key encryption algorithm was widely used in the past but is now considered insecure due to its short key length?
(a) DES (b) AES (c) 3DES (d) RSA

(v) In the RSA algorithm, we select 2 random large values 'p' and 'q'. Which of the following is the property of 'p' and 'q'
(a) P and q should be divisible by Φ(n) (b) P and q should be co-prime
(c) P and q should be prime (d) p/q should give no remainder

(vi) SHA-1 produces a hash value of
(a)256 bits (b)160 bits (c)180 bits (d)128 bits

(vii) Which of the following is not a property of public key cryptography?
(a) Uses different keys
(b) Every user has a unique private key
(c) Public key can be same for number of users
(d) Cannot deduce private key from public key

(viii) Which helps in ensuring non-fraudulent transactions on the web
(a) certificate authority (b) digital authority
(c) dual authority (d) digital signature

(ix) A proxy firewall filters at the
(a) physical layer (b) application layer
(c) data link layer (d) network layer

(x) What is the primary purpose of an email security standard like PGP or S/MIME?
(a) To prevent spam
(b) To filter out malicious software
(c) To encrypt and digitally sign emails for privacy and integrity
(d) To speed up email delivery

Fill in the blanks with the correct word

(xi) _____ means that a sender must not be able to deny sending a message that he sent.

(xii) The _____ attack can endanger the security of the Diffie-Hellman method if two parties are not authenticated to each other.

(xiii) In _____, the cryptographic algorithms and secrets are sent with the message.

(xiv) IPSec defines two protocols: _____ and _____.

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

Group - B

2. (a) Prove the following: [(a mod n) (b mod n)] mod n = (a b) mod n. *[(CO2)(Analyse/IOCQ)]*

(b) State and illustrate the Chinese Remainder Theorem with an example. *[(CO2)(Remember/LOCQ)]*

(c) Find the primitive root of 7. *[(CO2)(Apply/IOCQ)]*

5 + 5 + 2 = 12

3. (a) What are the basic principles of information security? How do these principles guide the design of secure systems and protocols? *[(CO1)(Remember/LOCQ)]*

(b) What is steganography? How does it differ from cryptography? Discuss the applications and limitations of steganography. *(CO1)(Remember/LOCQ)]*

6 + 6 = 12

Group - C

4. (a) State the principles of diffusion and confusion. What is cryptology? *[(CO3)(Remember/LOCQ)]*

(b) Discuss Meet in the Middle attack with suitable numeric example. *[(CO3)(Remember/LOCQ)]*

(c) Explain the drawback of DES and Double DES algorithm and state the concept of Triple DES algorithm. Use suitable diagrams as necessary. *[(CO3)(Analyse/IOCQ)]*

(2 + 1) + 4 + 5 = 12

5. (a) Discuss the working of a stream cipher. Discuss how it differs from a block cipher in terms of speed, error propagation, and usage scenarios. *[(CO3)(Understand/LOCQ)]*

(b) Discuss the encryption and decryption processes of a Feistel cipher with a block diagram. Why is it invertible even if the round function is not? *[(CO2)(Understand/LOCQ)]*

6 + 6 = 12

Group - D

6. (a) Calculate the cipher text (encryption) and the consequent plain text (decryption) using the RSA algorithm, for the following: p = 7; q = 11, e = 17; M = 8. *[(CO4)(Apply/IOCQ)]*

(b) Users A and B use the Diffie-Hellman key exchange technique with a common prime q = 71 and a primitive root a = 7. (i) If user A has private key XA = 5, what is A's public key YA? (ii) If user B has private key XB = 12, what is B's public key YB? What is the shared secret key? *[(CO4)(Apply/IOCQ)]*

6 + 6 = 12

7. (a) When a combination of symmetric encryption and an error control code is used for message authentication, in what order must the two functions be performed? *[(CO4)(Remember/HOCQ)]*

(b) What properties a digital signature should have? What requirements should a digital signature scheme satisfy? *[(CO4)(Remember/IOCQ)]*

(c) What characteristics are needed in a secure hash function? *[(CO4)(Remember/LOCQ)]*

4 + (2 + 4) + 2 = 12

Group - E

8. (a) Explain the NAT with suitable diagram. *[(CO5)(Remember/LOCQ)]*

(b) State the limitations of a firewall. *[(CO6)(Remember/LOCQ)]*

(c) Explain the working of IPSec. *[(CO5)(Remember/IOCQ)]*

3 + 3 + 6 = 12

9. (a) Explain establish security capabilities phase of handshake protocol in SSL. Explain server authentication and key exchange phase of handshake protocol in SSL. *[(CO6)(Remember/LOCQ)]*

(b) Explain client authentication and key exchange phase of handshake protocol in SSL. *[(CO6)(Remember/IOCQ)]*

4 + 4 + 4 = 12

Cognition Level	LOCQ	IOCQ	HOCQ
Percentage distribution	54.16	41.67	4.17