B. E. Electronics and Telecommunication Engineering 4th Year 1st Semester Examination- 2024
Cryptography and Network Security

Time: 3 Hours **Full Marks: 100**

Answer all the parts of a question in the same place

Module-I [Answer question no. 1 (1× 10) =10] CO1

1. a) What do you mean by cryptography and cryptanalysis?
   b) Suppose the key (k) for a shift cipher is 13 and the plaintext is as follows.
   WEWILLMEETATMIDNIGHT
   Convert each letter of plaintext to a sequence of integers and find the corresponding ciphertext.
   c) Why classical cryptosystems are not suitable for practical applications?

(4+4+2)

Module-II [Answer *any two* questions (2×20) = 40] CO2

2. a) Evaluate GCD (24140, 16762) using Euclidean algorithm
   b) What do you mean by Field? Define finite Field and give an example.
   c) Define irreducible polynomial and primitive polynomial.
   d) A is an element of GF(2^4) and 4-tuple representations of A is (a_3 a_2 a_1 a_0). Derive a simplified expression for A^2, where the field is defined by the polynomial $p(x) = x^4 + x + 1$
   e) Describe the basic design principles of modern block cipher.

(3+5+4+4+4)

3. a) What do you mean by block cipher mode of operation?
   b) How you can convert a block cipher into a stream cipher by using counter mode? Describe using a neat sketch.
   c) Why byte substitution operation is required in AES block cipher? Also explain why mixcloumns operation is not used in the last round of AES.
   d) Write the relative merits and demerits of SPN-type structure over Feistel structure for designing modern block cipher.
   e) Why block cipher Rijndael was accepted as Advanced Encryption Standard?

(3+7+5+3+2)

4. a) Write the basic principles of linear cryptanalysis and differential cryptanalysis.
   b) Why One-Time Pad based encryption scheme is perfectly secure? What do you mean by pseudorandom number generator? Write its importance for designing stream cipher.
   c) Write the merits and demerits of RC4 stream cipher.
   d) What do you mean by authentication? Draw a neat sketch and explain briefly a message authentication scheme without encryption/decryption function.

(6+5+3+6)

Module-III [Answer *any two* questions (2×15) = 30] CO3

5. a) How one-time key (K) is generated in Elgamal cryptosystem?
   b) Briefly describe the encryption and decryption processes in Elgamal cryptosystem.
   c) Suppose multiple blocks of a message are encrypted employing single one-time key (K) in Elgamal cryptosystem. Explain how it will affect the security of the system.
   d) Consider an Elgamal cryptosystem with a common prime q = 19 and a primitive root $\beta = 3$. Suppose Bob wants to send the message M = 13 to Alice, the private key of Alice is 5 and Bob selects a random integer 6. Determine the ciphertext and output after decryption.

(3+4+3+5)

6. a) Define Euler's totient function (ϕ). Calculate the value of ϕ (440).
   b) Briefly describe the key generation, encryption and decryption processes in RSA cryptosystem. Write the applications of RSA cryptosystem.
   c) Assume an elliptic curve equation $y^2 = x^3 + x + 1$ over GF (19). Determine R = P + Q, where P = (4, 2) and Q = (10, 6) are two points on the curve.

(4+7+4)

7. a) Why public key encryption is suitable for short message?
   b) Describe one scheme for distribution of secret key with confidentiality and authentication.
   c) Write the role of Certificate authority for key distribution process. Why timestamp is required during generation of certificate? Briefly describe a secure public-key distribution scheme.

(2+6+7)

Module-IV [Answer *any two* questions (2×10) = 20] CO4

8. a) Explain how Kerberos provides authenticated services.
   b) Write the security services provided by PGP. Why compression is done before encryption in PGP?

(5+5)

9. a) Explain the importance of cryptography in network security.
   b) Describe briefly about signed-data content type, enveloped-data content type and digested-data content type in S/MIME

(4+6)

10. a) State different IPSec services.
    b) With a neat sketch briefly describe about SSL protocol stack.
    c) What do you mean by payment gateway and dual signature?

(2+4+4)