ET/PE/B/T/414/D/2024(S)

# BE Electronics and Telecommunication Engineering 4th Year 1st Semester Supplementary 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 *any three* questions (3×15) = 45] CO1**

1. a) How many transformations are there in AES? Describe briefly each of these transformations. Which of these transformations defined for AES change the content of bytes? Which one does not change the content of the bytes?

(1+12+1+1)

2. a) How many round keys are needed for AES with cipher-key size 128 bits?
b) Write the AES Key Expansion algorithm.
c) How confusion and diffusion are achieved in block cipher AES?
d) AES has a large block size than DES. Is this an advantage or disadvantage?

(1+8+4+2)

3. a) Briefly describe the working principle of block cipher DES.
b) What do you mean by weak keys in DES? Mention some weak keys in DES.
c) Write the relative merits and demerits of triple DES over normal DES.

(9+3+3)

4. a) Briefly describe the Diffie-Hellman key exchange protocol.
b) Consider the RSA scheme, where Bob chooses $p = 7$, $q = 11$ and public key $e = 13$. Determine Bob's private key (d). Now suppose Alice wants to send the plaintext 5 to Bob. Find the ciphertext and decrypted plaintext received by Bob.

(9+6)

[ Turn over

**Module-II [Answer *any one* questions (1×15) =15] CO2**

5. a) Write the Euclidian algorithm and use it to evaluate GCD (980, 560)
   b) What is Euler's totient function? Find the value of Φ (29) and Φ (100)
   c) Find the result of multiplying $P_1(x) = x^5 + x^2 + 1$ by $P_2(x) = x^7 + x^4 + x^3 + x^2 + x$ over GF ($2^8$) with reduction polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$.

(5+5+5)

6. a) Distinguish between differential and linear cryptanalysis. Which one is a chosen-plaintext attack? Which one is known-plaintext attack?
   b) What is double DES? What kind of attack on double DES makes it useless?
   c) Solve the congruence $x^2 \equiv 7 \ mod\ 13$.
   d) How we can find the multiplicative inverse of a number using extended Euclidian algorithm?

(6+2+4+3)

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

7. a) Name three types of messages in PGP and explain their purpose.
   b) What is X.509 Standard?
   c) Explain how Kerberos provides authenticated services.

(6+4+5)

8. a) Briefly describe the different services provided by TLS protocol
   b) Define Encapsulating Security Payload (ESP) and the security services it provides.

(8+7)

9. a) In electronic mail system, what are the role of User Agent, Message Transfer Agent and Message Access Agent.
   b) Explain how Bob finds out what cryptographic algorithms Alice has used when he received an S/MIME message from her.
   c) Write about the threats in web security.

(9+3+3)

**Module-IV [Answer *any one* questions (1×10) = 10] CO4**

10. a) What do you mean by confidentiality, authenticity, and availability?

b) Consider an automated teller machine (ATM) in which users provide a personal identification number (PIN) and a card for account access. Give examples of confidentiality, integrity, and availability requirements associated with the system and in each case, indicate the degree of importance of requirement.

(6+4)

11. a) Assume in an authentication scheme, the hash function used is H and the encryption/decryption function is E/D. Show how the functions will be used to provide authentication as well as confidentiality.

b) Write the key features of secure electronic transaction.

(4+6)