Reg No.:_______________ Name:__________________________

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

Eighth semester B.Tech degree examinations, September 2020

Course Code: EC468

Course Name: SECURE COMMUNICATION

Max. Marks: 100 Duration: 3 Hours

PART A

Answer any two full questions, each carries 15 marks. Marks

1 a) Discuss different types of active and passive attacks in cryptography. (7)

b) Discuss about all the five categories of security services (X.800). (8)

2 a) Differentiate between group, ring and field using examples. (10)

b) Solve 9x ≡ 8 (mod 7). (5)

3 a) Give the details of different security mechanisms. (7)

b) Find the multiplicative inverse of $x^3 + x + 1$ in GF(2^4) considering an irreducible polynomial $m(x) = x^4 + x + 1$ (8)

PART B

Answer any two full questions, each carries 15 marks.

4 a) Encrypt 'attack at dawn' using Caesar cipher with key=5 (5)

b) Encrypt 'we are discovered save yourself' using playfair cipher. Use the Keyword 'MONARCHY' for creating the playfair matrix. (5)

c) What are the security issues associated with monoalphabetic/polyalphabetic substitution ciphers? (5)

5 a) Explain about different types of cryptanalytic attacks. (7)

b) Discuss in detail the transformations associated with DES encryption. (8)

6 a) Give the procedure for encryption and decryption of Hill cipher with an example. (7)

b) Explain the steps involved in a single round of AES encryption. (8)

PART C

Answer any two full questions, each carries 20 marks.

7 a) Explain the different steps involved in RSA public key cryptosystem. Encrypt the plaintext 88 using RSA algorithm assuming $p = 17$, $q = 11$ & $e = 7$ (10)

b) What are the requirements for a public key cryptosystem as laid down Diffie and Hellman? (7)

c) How is public key cryptosystem different from symmetric cryptosystem? (3)

8 a) What are the advantages of 'Honeypots' in the context of secure communications? (5)

b) Give the requirements of a strong secure password? Explain the password management system in UNIX. (10)

c) Explain the working of a distributed intrusion detection system. (5)

9 a) Explain Diffie-Hellman Key exchange protocol for public key crypto systems. (10)

b) Explain in detail various intrusion detection techniques. (10)

****