C **H1076** **Pages: 2**

Reg No.:_______________ Name:__________________________

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

EIGHTH SEMESTER B.TECH DEGREE EXAMINATION, MAY 2019

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) Differentiate between active and passive attacks. (5)

b) Solve the equation $3x+4 \equiv 6(\text{mod } 13)$. (5)

c) Give different types of attacks in a cryptosystem. (5)

2 a) It is told in arithmetic that the remainder of an integer divided by 4 is the same as the remainder of division of the two rightmost digits by 4. Use the properties of mod operator to prove this claim. (5)

b) Differentiate between group, ring, abelian group and field with examples. (10)

3 a) Find whether the set of whole numbers is an Abelian Group under addition. Justify. (5)

b) Define the inverse and identity elements for any operation in a group. (5)

c) Discuss attacks on integrity. How it can be prevented? (5)

PART B

Answer any two full questions, each carries 15 marks.

4 a) Discuss the properties of an ideal cryptographic system. (5)

b) Using the Key: **PAY,** do OTP for **LAY.** (5)

c) Give the basic permutations and substitution in DES. (5)

5 a) Discuss four transformations used in Advanced Encryption Standard. (10)

b) Give the advantages of Poly Alphabetic Cipher. (5)

6 a) Explain Diffie- Hellman public key cryptosystem with an example. (10)

b) Encrypt the word SECURE using Key as 3 using Ceaser Cipher. (5)

PART C

Answer any two full questions, each carries 20 marks.

7 a) Explain RSA algorithm with parameters $p = 3$, $q = 11$, $e = 7$ and $M = 5$. (15)

b) Give the requirements of a secure password. (5)

8 a) What are the advantages of Honey pot? (5)

b) How does distributed intrusion detection work? (10)

c) Write note on password protection. (5)

9 a) Using Key analogy, explain Public Key Cryptosystem. (10)

b) Give applications of PKCS. (5)

c) Discuss the techniques for intrusion detection. (5)

****

C **H192077** **Pages: 1**

Reg No.:_______________ Name:__________________________

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

EIGHTH SEMESTER B.TECH DEGREE EXAMINATION(S), OCTOBER 2019

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 attacks. (5)

b) Differentiate between privacy, integrity and authentication in security services. (5)

c) Differentiate security mechanisms in detail. (5)

2 a) Discuss the properties of Group, Ring and Field. Give examples. (10)

b) Discuss about GF(2). (5)

3 a) Discuss Euclidean algorithm. (10)

b) Discuss attacks on availability. (5)

PART B

Answer any two full questions, each carries 15 marks.

4 a) Encrypt the word COMMUNICATION with key as CRYPTO using Play fair cipher. (5)

b) Discuss the security of OTP. (5)

c) Explain differential cryptanalysis. (5)

5 a) With necessary diagrams, explain AES. (15)

6 a) Discuss any poly-alphabetic cipher with an example. (5)

b) Encrypt the word CRYPTO with key as 4 using Ceaser Cipher. (5)

c) Discuss any transposition cipher with an example. (5)

PART C

Answer any two full questions, each carries 20 marks.

7 a) Explain PKDS with PKCS. Give comparison. (10)

b) What is the difference between symmetric encryption and asymmetric encryption? (5)

8 a) Discuss the steps for RSA. Perform the encryption and decryption for $p = 7, q = 11, e = 4$ and $M = 5$. (15)

b) Explain statistical anomaly detection. (5)

9 a) Give a few password selection strategies. (5)

b) How is Public Key Certificates Validated? (5)

c) Discuss intrusion detection exchange format. (10)

****