

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) |
