

Reg No.: \_\_\_\_\_

Name: \_\_\_\_\_

**APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY**  
**SEVENTH SEMESTER B.TECH DEGREE EXAMINATION(S), MAY 2019**

**Course Code: CS409**

**Course Name: CRYPTOGRAPHY AND NETWORK SECURITY**

Max. Marks: 100

Duration: 3 Hours

**PART A**

*Answer all questions, each carries 4 marks.*

Marks

- |    |  |     |
|----|--|-----|
| 1  | How the nonlinearity is achieved in DES.   | (4) |
| 2  | Differentiate Confusion and Diffusion.   | (4) |
| 3  | Discuss the key expansion procedure in AES   | (4) |
| 4  | State and prove Fermat's Theorem   | (4) |
| 5  | In a public key system using RSA, you intercept the cipher text C=8 sent to a user whose public key is e=13, n=33. What is the plain text M? | (4) |
| 6  | Compare the strength of MAC and Encryption against brute-force attack  | (4) |
| 7  | Give the header format of ESP in IPSec   | (4) |
| 8  | Give the authentication methods used in Oakley algorithm   | (4) |
| 9  | What are the services provided by Record Layer Protocol for Secure Socket Layer connections?   | (4) |
| 10 | What are the characteristic features of stateful inspection firewall?  | (4) |

**PART B**

*Answer any two full questions, each carries 9 marks.*

- |    |   |     |
|----|---|-----|
| 11 | a) Differentiate between monoalphabetic ciphers and polyalphabetic ciphers and give one example for each.     | (5) |
|    | b) Give different techniques used in steganography  | (4) |
| 12 | a) How key generation is performed in IDEA  | (4) |
|    | b) Discuss Mix Column transformation in AES   | (5) |
| 13 | a) Using rail fence cipher, encrypt the text <i>meet me after the toga party</i> using the key 4 3 1 2 5 6 7. | (4) |
|    | b) Illustrate inverse S box creation in AES.  | (5) |

**PART C**

*Answer any two full questions, each carries 9 marks.*

- |    |  |     |
|----|--|-----|
| 14 | a) Find gcd(240, 46) using Extended Euclid's Algorithm       | (4) |
|    | b) Discuss the key exchange procedure using Elliptic Curves. | (5) |

- 15 Illustrate MD 5 hash algorithm in detail (9)
- 16 a) Consider a Diffie Hellman scheme with a common prime  $q = 11$  and primitive root  $\alpha = 2$ . (5)
- i. Show that 2 is a primitive root of 11.
  - ii. If user A has public key  $Y_A = 9$ , what is A's private key?
  - iii. If user B has public key  $Y_B = 3$ , what is the shared secret key K, shared with A
- b) Discuss Digital Signature Algorithm (4)

**PART D**

*Answer any two full questions, each carries 12 marks.*

- 17 a) What are the steps used for preparing an enveloped data and signed data in MIME entity? (6)
- b) Discuss the message format of PGP. (3)
  - c) How the integrity is achieved using ICV in Authentication Header. (3)
- 18 a) Illustrate the relevance of dual signature in SET. (4)
- b) Discuss SSL record protocol operations. (6)
  - c) What are the requirements of Encrypted Tunnels? (2)
- 19 a) Give the significance of SA selectors in IPSec. (4)
- b) Why compression is done before encryption in PGP? (2)
  - c) Discuss different Firewall configurations. (6)

\*\*\*\*\*