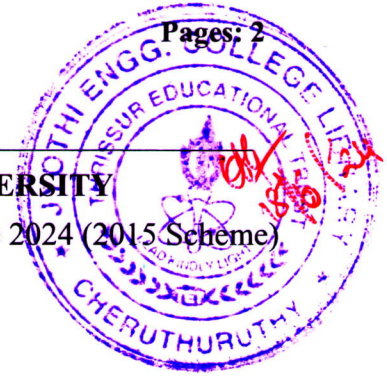


Reg No.: \_\_\_\_\_

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

**APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY**

B.Tech Degree S7 (S, FE) / S7 (PT) (S, FE) Examination May/June 2024 (2015 Scheme)

**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  | Differentiate between cryptography and steganography.                                                                          | (4) |
| 2  | Prove that Vigenere cipher is a polyalphabetical cipher by converting the plaintext "HELLO" to ciphertext using the key "CSE". | (4) |
| 3  | With neat diagram, explain the single round of IDEA.                                                                           | (4) |
| 4  | What is Euler's Totient function? Find $\phi(35)$ .                                                                            | (4) |
| 5  | Brute force attack is difficult in hash functions. True or false? Justify your answer.                                         | (4) |
| 6  | How signature is generated and verified using Digital Signature algorithm?                                                     | (4) |
| 7  | What are the steps for transmission and reception of PGP messages?                                                             | (4) |
| 8  | Write notes on anti-replay mechanism in IP Security.                                                                           | (4) |
| 9  | List out the parameters defined for SSL connection state.                                                                      | (4) |
| 10 | What is the need for dual signature in SET? How is it generated?                                                               | (4) |

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

- |    |                                                                                                                               |     |
|----|-------------------------------------------------------------------------------------------------------------------------------|-----|
| 11 | a) Describe the rules for encryption in playfair ciphers. Using this, encrypt the message "GOODMORNING" with the key "MUSIC". | (6) |
|    | b) Explain how multi stage encryption is done using rotor machines.                                                           | (3) |
| 12 | a) Compare and contrast cipher feedback mode and output feedback modes of operation of DES.                                   | (5) |
|    | b) What are the primitive operations of RC4? How RC4 algorithm works?                                                         | (4) |

- 13 Explain in detail the transformation functions in one round of AES encryption. (9)

**PART C**

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

- 14 a) What are the properties of modular arithmetic defined on a set of nonnegative integers ( $Z_n$ )? Find the additive and multiplicative inverses modulo 7. (5)
- b) Discuss the key generation, encryption and decryption procedure in RSA. (4)
- 15 a) Explain Diffie- Hellman key exchange protocol. Assume  $\alpha=5$ ,  $q=23$ ,  $X_A=4$ ,  $X_B=3$ . Find the values of  $Y_A$ ,  $Y_B$ , and  $K$ . (5)
- b) With neat diagram, explain how private key and public key encryption provides confidentiality, authentication and signature to the messages. (4)
- 16 Discuss MD5 algorithm steps in detail. (9)

**PART D**

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

- 17 a) What are the header fields in MIME? Elaborate on MIME content types. (8)
- b) Give the format of ESP packet in IPSec. (4)
- 18 a) Write brief note on Oakley key management protocol for IPSec and mention its important features. (6)
- b) Explain how the client server authentication is carried out using SSL handshake protocol? (6)
- 19 a) Explain various types of firewalls with advantages and disadvantages of each. (8)
- b) Write notes on Transport layer security. (4)

\*\*\*\*