E **10000CS409122002** **Pages: 2**

Reg No.:_______________ Name:__________________________

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

Seventh Semester B.Tech Degree Regular and Supplementary Examination December 2021 (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 Encrypt the plain text "short example" using hill cipher with key $\begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix}$ (4)

2 Differentiate between monoalphabetic substitution and polyalphabetic substitution with example. (4)

3 Explain the key generation of AES algorithm. (4)

4 Using extended Euclidian algorithm find the gcd of(161,28).Also find two integers s,t such that $s \times 161 + t \times 28 = gcd(161,28)$. (4)

5 State Fermat's theorem and find the result of 3^{12}mod11 using Fermat's theorem. (4)

6 What are the requirements for the practical application of a hash function? (4)

7 List the services included in the operation of PGP. (4)

8 Write down the steps for preparing enveloped data MIME entity. (4)

9 Name the participants included in the secure electronic transaction (SET) system. (4)

10 What are the protocols used in SSL two layer protocol stack? (4)

PART B

Answer any two full questions, each carries 9 marks.

11 a) Explain the structure of DES with the help of a neat diagram. How S boxes in DES converts a 6 bit input to a 4 bit output? (6)

b) Encrypt the plain text "instruments" using play fair cipher with key "monarchy". (3)

12 a) Explain how round transformation is performed in IDEA. (5)

b) Illustrate key scheduling algorithm and pseudo random generation algorithm in RC4. (4)

13 a) Explain the transformations of AES with suitable examples. (6)

b) Using vigenere cipher encrypt the message "she is listening" using the key word "pascal". (3)

PART C

Answer any two full questions, each carries 9 marks.

14 a) In an RSA cryptosystem user A uses two prime numbers p=13 and q=17 to generate private and public keys. If the public key of A is 35,calculate the private key of A. (4)

b) Explain Diffie-Hellman key exchange algorithm with suitable example. (5)

15 a) Explain the working of SHA-1 secure hash algorithm. (9)

16 a) Explain the key generation, signing and verification of DSA digital signature algorithm. (5)

b) Give the encryption/decryption procedures using Elliptic Curve Cryptography. (4)

PART D

Answer any two full questions, each carries 12 marks.

17 a) Discuss the format of transmitted message of PGP. (6)

b) Explain Oakley key determination protocol for IPSec. (6)

18 a) Explain SSL record protocol services and operations. (6)

b) Write notes on various types of firewalls. (6)

19 a) Explain the role of Security Association and SA selectors in IPSec. (6)

b) Explain the phases of SSL handshake protocol with diagram. (6)

****