E 00000CS409121902 Pages: 2

Reg No.:_______________ Name:__________________________

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

Seventh semester B.Tech examinations (S), September 2020

Course Code: CS409

Course Name: CRYPTOGRAPHY AND NETWORKSECURITY

Max. Marks: 100 Duration: 3 Hours

PART A

Answer all questions, each carries 4 marks. Marks

1 Which parameters and design choices determine the actual algorithm of a Fiestel Cipher. (4)

2 Encrypt the message **"the house is being sold tonight"** using Vigenere cipher with key "*dollars*". Ignore the space between words. Decrypt the message to get the plain text. (4)

3 Compare stream cipher and block cipher with example. (4)

4 Find gcd(252,105). (4)

5 List different types of attacks addressed by message authentication. (4)

6 Illustrate Needham and Schroedor protocol for mutual authentication. (4)

7 Compare transport mode and tunnel mode functionalities in IPSec. (4)

8 List out the five header fields and their meaning defined in MIME. (4)

9 What are the steps involved in the SSL record protocol transmission? (4)

10 Compare SSL and TLS. (4)

PART B

Answer any two full questions, each carries 9 marks.

11 a) Discuss about different polyalphabetic cipher substitution techniques. (4)

b) Explain single round of DES algorithm. (5)

12 a) Differentiate between Confusion and Diffusion. (4)

b) Explain the key generation in IDEA. (5)

13 Explain AES algorithm in detail. (9)

PART C

Answer any two full questions, each carries 9 marks.

14 a) Alice and Bob agreed to use RSA algorithm for the secret communication. Alice securely choose two primes, p=5 and q=11 and a secret key d=7. Find the corresponding public key. Bob uses this public key and sends a cipher text 18 to Alice. Find the plain text. (6)

b) State and prove Euler's theorem. (3)

15 a) Explain three different Arbitrated Digital Signature Techniques. (9)

16 a) What is suppress replay attack in authentication? Explain the protocol used to eliminate this attack. (4)

b) Explain the key exchange procedure using Elliptic Curves. (5)

PART D

Answer any two full questions, each carries 12 marks.

17 a) Explain the sequence of steps involved in the message generation and reception in PGP with block diagrams. (8)

b) List out the benefits of IPSec. (4)

18 a) Explain the features of any two types of firewalls. (6)

b) Explain the sequence of operations required for Secure Electronic Transaction. (6)

19 a) Explain the format of IPSec ESP Packet. (6)

b) Illustrate the overall operation of SSL Record Protocol. (6)

****