E 10000CS409122201 Pages: 2

Reg No.:_______________ Name:________________________

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

Seventh Semester B.Tech Degree (S, FE) Examination January 2023 (2015 Scheme)

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 Using Caeser cipher apply brute force attack on the ciphertext “**xjhwjybwnynsl**” and recover the plaintext and the key (4)

2 Apply the key generation of SDES on the initial 10bit key “1100011110” and compute the sub keys k1 and k2. (Hint: P10 - 3 5 2 7 4 10 1 9 8 6 and P8 - 6 3 7 4 8 5 10 9) (4)

3 Describe the initialization, initial permutation and key stream generation of RC4 (4)

4 Define Euler’s Theorem. Give examples (4)

5 Differentiate Conventional and Public Key Cryptosystem (4)

6 Explain the different message authentication functions (4)

7 List and explain the five header fields supported by MIME (4)

8 Describe the services offered by IPSEC (4)

9 Discuss the various Web security threats (4)

10 Describe the limitations of Firewalls (4)

PART B

Answer any two full questions, each carries 9 marks.

11 Explain the working of DES with relevant figures (9)

12 a) Using Playfair cipher encrypt the data “confidential” with keyword “security” (5)

b) Discuss the primitive operations used in IDEA (4)

13 With neat sketch describe the AES encryption and decryption process (9)

PART C

Answer any two full questions, each carries 9 marks.

14 Discuss the Diffie Hellman Key exchange Algorithm. Explain with an example how it is vulnerable to man-in middle attack. (9)

15 a) Using RSA algorithm find the plaintext if the ciphertext is 58 . Assume the values for p=7 q=11 and e=17 (5)

b) Discuss the basic uses of Message Authentication Codes (4)

16 Explain the Digital Signature Algorithm. With figure describe the signing and verifying process in DSS (9)

PART D

Answer any two full questions, each carries 12 marks.

17 a) List and explain the services offered by PGP (6)

b) With relevant figures explain the cryptographic functions used in Pretty Good Privacy (6)

18 a) With neat sketch describe the working of IPSEC in the network layer (6)

b) Discuss the different types of Firewalls? (6)

19 a) Discuss the services offered by SSL Record Protocol. With figure explain the operation of SSL Record Protocol (6)

b) Describe the working of Secure Electronic Transaction (6)

****