C 16000EC468062301 Pages: 2

JYOTHI ENGG. COLLEGE LIBRARY
THRISSUR EDUCATIONAL TRUST
CHERUTHURUTHY
OK 20/6/23

Reg No.:_______________ Name:__________________________

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

B.Tech Degree S8 (S, FE) / S8 (PT) (R, S) Examination June 2023 (2015 Scheme)

Course Code: EC468

Course Name: SECURE COMMUNICATION

Max. Marks: 100 Duration: 3 Hours

PART A

Answer any two full questions, each carries 15 marks. Marks

1 a) Explain the security services defined by ITU-T related to network security goals. (8)

b) Discuss the attacks on integrity. (7)

2 a) Give the properties of group, ring and field (9)

b) Define linear congruence. Apply linear congruence concept to solve the equation $3x+4 \equiv 6 \pmod{13}$ (6)

3 a) Find whether set of rational numbers is an abelian group under addition. Justify your answer. (9)

b) Differentiate between active attack and passive attack (6)

PART B

Answer any two full questions, each carries 15 marks.

4 a) Use Playfair Cipher with key ENGINEERING to encrypt the message TEST THIS PROCESS. (8)

b) Explain one time pad (OTP) with an example. Mention its advantages and disadvantages (7)

5 a) Differentiate between confusion and diffusion (6)

b) Explain DES encryption with a neat sketch. (9)

6 a) Explain differential cryptanalysis and how it differs from linear cryptanalysis. (7)

b) Use hill cipher to encrypt the plain text "PAY MORE MONEY" using the key (8)

$$\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

PART C

Answer any two full questions, each carries 20 marks.

7 a) Explain the requirements of RSA public key cryptosystem? Using RSA algorithm encrypt a plaintext value of M = 10 for the parameters p =7, q = 13 and e = 5. (10)

b) Write notes on Honey pot in network security (5)

c) Explain proactive password checking. (5)

8 a) Discuss the password management in UNIX (10)

b) Explain the Public Key Cryptosystem with neat block diagram. (10)

9 a) Consider Diffie- Hellman key exchange scheme with common prime q=83 and a primitive root α= 5. If the user A has private key X_A= 6, Find A's public key. If the user B has private key X_B= 10, find B's public key. Also find the shared secret key (10)

b) Explain the architecture of Distributed Intrusion Detection with neat sketch. (10)

****