ADMISSION NUMBER

School of Computing Science and Engineering

Bachelor of Technology in Computer Science and Engineering

Mid Term Examination - May 2024

Duration : 90 Minutes
Max Marks : 50

Sem VI - R1UC613C - Cryprography and Network Security

General Instructions

Answer to the specific question asked
Draw neat, labelled diagrams wherever necessary
Approved data hand books are allowed subject to verification by the Invigilator

1) Compare Vignere and Vernam ciphers K2 (2)

2) Define a state in AES. How many states are there in each version of AES? K1 (3)

3) Explain different types of attacks that are addressed by encryption K2 (4)

4) In a cipher, S-boxes can be either static or dynamic. The parameters in a static S-box do not depend on the key. a. State some advantages and some disadvantages of static and dynamic S-boxes. b. Are the S-boxes (substitution tables) in AES static or dynamic? K2 (6)

5) Find the integer X that satisfies the equation $7x \equiv 4 (\text{mod } 9)$. K3 (6)

6) Find the result of multiplying P_1=x^5+x^2+x by P_2=x^7+x^4+x^3+x^2+x in GF(28) with irreducible polynomial x^8+x^4+x^3+x+1 using the algorithm described above. (KL-3, Unit 1) K3 (9)

7) Distinguish between the group, ring and a field. K4 (8)

8) In RSA: a. Given n = 221 and e = 5, find d. b. Given n =3937 and e =17, find d. c. Given p = 19, q = 23, and e = 3, find n, φ(n), and d. Examine K4 (12)

OR

In RSA, given e = 13 and n = 100 Encrypt the message “HOW ARE YOU” using 00 to 25 for letters A to Z and 26 for the space. Use different blocks to make P < n. Examine. K4 (12)