

JK Lakshmipat University Jaipur
INSTITUTE OF ENGINEERING AND TECHNOLOGY

End Term Examination, December 2022

B. Tech. (CSE), Semester V

Roll No.....

CS1214: CRYPTOGRAPHY

Time: 2 hours

Max. Marks: 30

Instructions to students:

1. Do not write anything other than your roll number on question paper.
 2. Mention all the assumptions for your answers clearly.
-

1. Why we need authentic encryption? Compare SSL, IPsec and SSH in terms of security. Which one is more secure MAC then Encrypt, Encrypt then MAC and MAC and Encrypt? Justify your answer. [2+2+3]
(CO4)
 2. Describe Markel Puzzle in details. Prove that there is a quadratic gap between complexity at users end and complexity at attacker's end. [4+3]
(CO5)
 3. Prove that, text book RSA (without trapdoor) is insecure. Describe RSA with trapdoor permutation for key exchange in a public key encryption system. [4+4]
(CO7)
 4. What is public key cryptography? Describe Diffie Hellman protocol and include detail explanation of modular arithmetic. How Diffie Hellman key establishment protocol can be used to set up a public key encryption system? [2+4+2]
(CO6)
-