M. Sc Sem-II, 2022 Mid-semester examination

Full Marks-30 Subject- Cryptography& Network Security (CSMC204) Time - 1 hour

1. **Answer any five.** **[5 x 2 marks = 10 marks]**
   a) Explain the use of S-box in DES algorithm.
   b) State the prime difference between symmetric and asymmetric key cryptography.
   c) Find the value of x and y for a=5, b=10, which satisfy the equation ax+by=gcd(a,b).
   d) What is substitution in cryptography?
   e) What is LFSR?
   f) What is passive attack?
   g) What is monoalphabetic cipher? Give an example. (1+1)

2. **Answer any four.** **[4 x 5 marks = 20 marks]**
   a) State Fermat's Little Theorem for prime numbers. Find an a and p pair such that Fermat's theorem is satisfied, but p is not a prime. (3+2)
   b) Explain the steps of RSA algorithm with an example.
   c) Describe the Diffie-Hellman key exchange protocol.
   d) How can Diffie-Hellman key exchange protocol be vulnerable to the man in the middle attack?
   e) Why is 3-DES more secure than 2-DES?
   f) Find the euler totient function value for 43 and 24. (2+3)