**MSc -2nd Semester**

**Mid-semester 2022**

**Cryptography and Network security (CSMC-204)**

1. **Explain the use of S-box in DES algorithm.**

**Ans:** S-boxes are used to perform substitution operations, which are crucial part of the encryption process in DES. The algorithm’s other operations are linear and easy to analyze, but the primary purpose of S-boxes is to introduce non-linearity into the encryption process. The non-linearity makes it more difficult to apply cryptanalysis techniques, thus enhancing the security of the algorithm.

1. **State the primary difference between symmetric and asymmetric key cryptography.**

**Ans:** Symmetric encryption uses a single key that needs to be shared among the people who need to receive the message while asymmetric encryption uses a pair of a public key and a private key to encrypt and decrypt messages when communication. Asymmetric key cryptography eliminates the need to share the key.

Symmetric key cryptography is much faster than asymmetric key cryptography.

1. **Find the value of x and y for a=5, b=10, which satisfy the equation ax + by = gcd (a, b).**

**Ans:**

From extended Euclidian Algorithm,

(S\*n) + (b\*t) = gcd(n, b) = gcd (b, n)

r1 = b; r2 = n;

r1 = 10, r2 = 5, t1 = 0, t2 = 1;

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **q** | **r1** | **r2** | **r** | **t1** | **t2** | **t** |
| 2 | 10 | 5 | 0 | 0 | 1 | -2 |
|  | 5 | 0 |  | 1 | -2 |  |

Therefore,

5 = 5x+10y

* 5 = 5x + 10
* 5x = - 5
* x = -1

1. **What is the substitution in cryptography?**