**NIRMA UNIVERSITY**

**Institute of Technology**

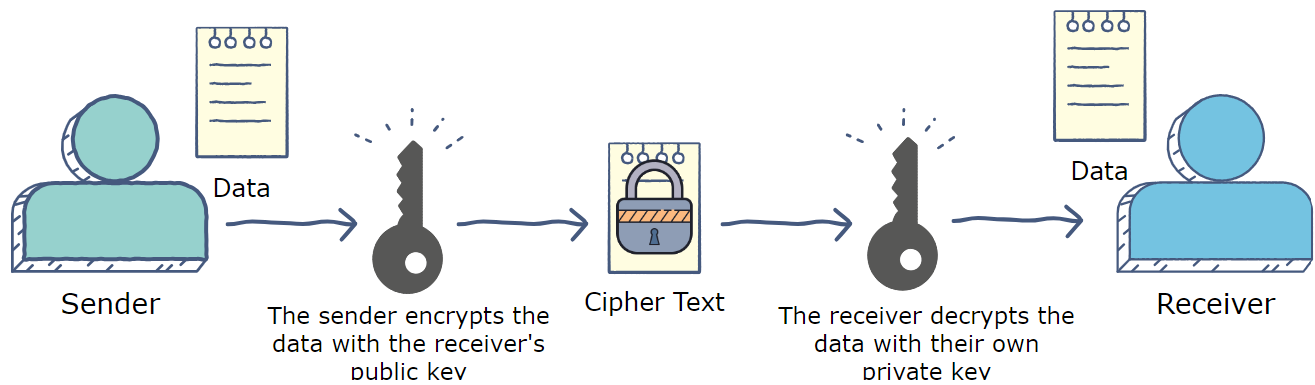
**B.Tech. Computer Science and Engineering**

**2CSDE54 Information and Network Security**

**Implementation of RSA Algorithm.**

The RSA algorithm is an asymmetric cryptography algorithm; this means that it uses a public key and a private key (i.e two different, mathematically linked keys). As their names suggest, a public key is shared publicly, while a private key is secret and must not be shared with anyone.

The following illustration highlights how asymmetric cryptography works:



**How it works**

The RSA algorithm ensures that the keys, in the above illustration, are as secure as possible. The following steps highlight how it works:

**1. Generating the keys**

1. Select two large prime numbers, ***p*** and ***q***. The prime numbers need to be large so that they will be difficult for someone to figure out.
2. Calculate ***n*= *p x q*.**
3. Calculate the Eulers ***totient*** function; ***ϕ*(*n*)=(*p*−1)(*q*−1)**.
4. Select an integer *e*, such that *e* is ***co-prime*** to ***ϕ*(*n*)** and **1<*e* < *ϕ*(*n*).** The pair of numbers **(*n*,*e*)** makes up the public key.
5. Calculate ***d*** such that ***e . d=1 mod ϕ(n) i.e. (e . d) mod ϕ(n)= 1***

*d* can be found using the ***extended euclidean algorithm***. The pair (*n*,*d*) makes up the private key. i.e. we need to find multiplicative inverse of ***e mod ϕ(n)***

### 2. Encryption

Given a plaintext *M*, represented as a number, the ciphertext *C* is calculated as: **C=Me mod n.**

### 3. Decryption

Using the private key (*n*,*d*), the plaintext can be found using: **P=Cd mod n**.

**Example:**

Choose p = 3 and q = 11

Compute n = p \* q = 3 \* 11 = 33

Compute φ(n) = (p - 1) \* (q - 1) = 2 \* 10 = 20

Choose e such that 1 < e < φ(n) and e and φ (n) are coprime. Let e = 7

Compute a value for d such that (d \* e) % φ(n) = 1. One solution is d = 3 [(3 \* 7) % 20 = 1]

Public key is (e, n) => (7, 33)

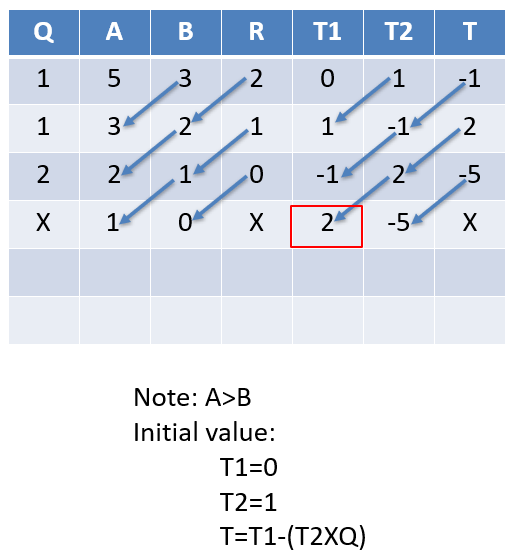
Private key is (d, n) => (3, 33)

The encryption of m = 2 is c = 27 % 33 = 29

The decryption of c = 29 is m = 293 % 33 = 2

How to find multiplicative inverse ***e mod ϕ(n)***

**In the below example we have calculated for 3 mod 5**

******

Note: A>B

Initial value:

T1=0

T2=1

T=T1-(T2XQ)

**Q**

**A**

**B**

**R**

**T1**

**T2**

**T**

5

3

2

0

1

-

1

3

2

1

1

-

1

2

2

1

0

-

1

2

-

5

1

0

X

2

-

5

X