Practical No. 8

Aim:- To write a progeam to implement RSA key cryptogeaphy.

Theory:- RSA encryption algoeithm is a type of public-key encryption algoeithm. It is implemented using Public key encryption algoeithm which is also called asymmeteic algoeithm. These are those algoeithm. in which sender and receiver use different keys foe encryption and decryption. Each sender is assigned a pair of keys.

- Public key — used foe encryption.
- Private key - used foe decryption.

Algoeithm:-

The steps foe RSA algoeithm are as follows:-

1. Select two large prime te numbers, p and q
2. Multiply these numbers to find $n = p \times q$, where n is called the modulus foe encryption and decryption.
3. Choose a number e less than n, such that n is relatively prime to $(p-1) \times (q-1)$. It means that e and $(p-1) \times (q-1)$ have no common Factoe except 1. Choose "e" such that $1 < e < \alpha(n)$ e is prime to $\alpha(n)$ $\gcd(e, d(n)) = 1$.
4. If $n = p \times q$ then the public key is $<e, n>$. A plaintext message m is encrypted using public key $<e, n>$. To find cipher text c foem the plain text following foemula is used to get cipher text C. $C = m^e \bmod n$.
5. To determine the private key, we use the following foemula to calculate the d such that $De \bmod \alpha(n) = 1$.
6. The private key is $<d, n>$. A ciphertext message C is decrypted using private key $<d, n>$. To calculate plain text m foem the ciphertext e following foemula is used to get plaintext m.

$$m = c^d \bmod n$$

Amar KRISH

Teacher's Signature _____

Example:- Step 1:- Select two large prime numbers $p=7$ and $q=11$

Step 2:- Multiply these numbers to find $n=p \times q$ where n is called the modulus for encryption and decryption

$$n = p \times q = 7 \times 11 = 77$$

Step 3:- Choose a number e less than n, such that n is relatively prime to $(p-1) \times (q-1)$

$$\phi(n) = (p-1) \times (q-1) = 6 \times 10 = 60$$

Let us now choose relative prime e of 60 as 7.

Thus public key is $\langle e, n \rangle = (7, 77)$

Step 4:- A plaintext message m is encrypted using public key $\langle e, n \rangle$

Formula to convert plain text to cipher text is

$$C = m^e \bmod n \rightarrow C = 9^7 \bmod 77 \Rightarrow C = 37$$

Step 5:- The private key is $\langle d, n \rangle$. To determine the private key, we use the following formula d such that:-

$$De \bmod \{(p-1) \times (q-1)\} = 1$$

$$1d \bmod 60 = 1, \text{ which gives } d = 43.$$

The private key is $\langle d, n \rangle = (43, 77)$

Step 6:- A cipher text message C is decrypted using private key $\langle d, n \rangle$. To calculate plain text from the cipher text C following formula is used to get plain text m.

$$m = c^d \bmod n$$

$$m = 37^{43} \bmod 77$$

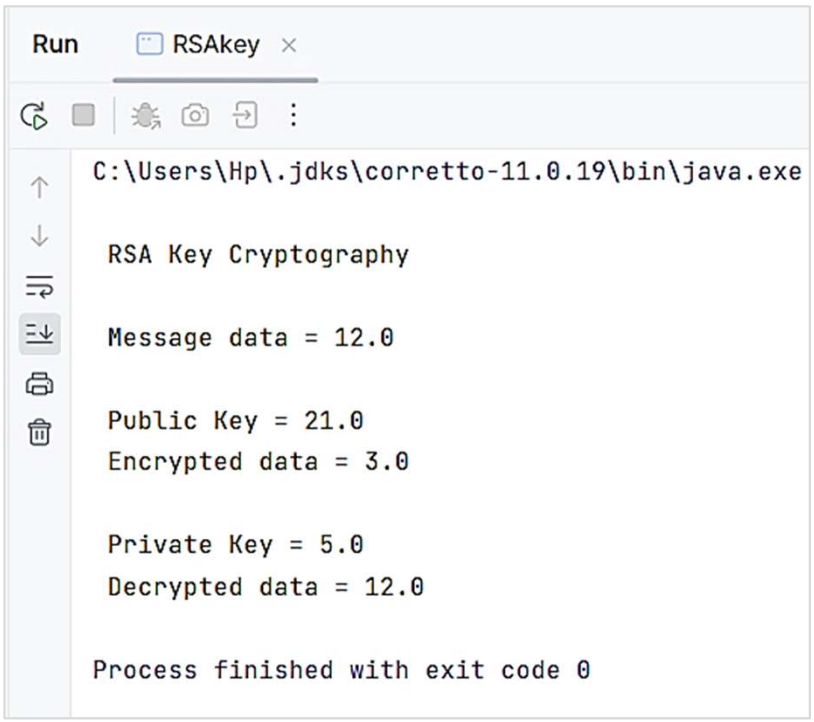
$$m = 9$$

$\therefore$ Plain text = 9 and cipher text = 37.

Program:

```
public class RSAkey {

   public static double gcd(double a, double h) {
      // This function returns the gcd
      double temp;
      while (true) {
         temp = a % h;
         if (temp == 0)
            return h;
         a = h;
         h = temp;
      }
   }

   public static void main(String[] args) {
      double p = 3;
      double q = 7;
      double n = p * q;                    // Public Key

      // Finding the other part of public key.
      double e = 2;
      double phi = (p - 1) * (q - 1);
      while (e < phi) {
         if (gcd(e, phi) == 1)
            break;
         else
            e++;
      }
      double pri = e;                                    // Private Key
      int k = 2;                                         // A constant value
      double d = (1 + (k * phi)) / e;
      double msg = 12;                                   //Encryption Message

      System.out.println("\n RSA Key Cryptography");
      System.out.println("\n Message data = " + msg);
      System.out.println("\n Public Key = " + n);

      double c = Math.pow(msg, e) % n;                   // Encryption
      System.out.println(" Encrypted data = " + c);
      System.out.println("\n Private Key = " + pri);

      double m = Math.pow(c, d) % n;                     // Decryption
      System.out.println(" Decrypted data = " + m);
   }
}
```

Output:


Run
RSAkey
C:\Users\Hp\.jdks\corretto-11.0.19\bin\java.exe
RSA Key Cryptography
Message data = 12.0
Public Key = 21.0
Encrypted data = 3.0
Private Key = 5.0
Decrypted data = 12.0
Process finished with exit code 0