Assignment 3

Aim: Implementation and analysis of RSA cryptosystem and Digital Signature scheme using RSA

Theory:

RSA (Rivest-Shamir-Adleman):

RSA is a widely used public-key cryptosystem for secure data transmission and digital signatures. It's based on the mathematical properties of large prime numbers. RSA involves a pair of keys: a public key for encryption and a private key for decryption. The security of RSA relies on the difficulty of factoring large semiprime numbers.

Algorithm:

1. Key Generation:

   - Choose two distinct prime numbers, p and q.

   - Calculate n = p * q.

   - Compute the totient ϕ(n) = (p - 1) * (q - 1).

   - Choose an integer e (usually a small prime, commonly 65537) that is coprime with ϕ(n).

   - Compute d such that (d * e) % ϕ(n) = 1.

   - Public key: (e, n)

   - Private key: (d, n)

2. Encryption:

   - Convert the plaintext message into a numeric value m.

   - Compute the ciphertext c = (m^e) % n.

3. Decryption:

   - Compute the plaintext message m = (c^d) % n.

Digital Signature:

A digital signature is a cryptographic technique that provides authenticity, integrity, and non-repudiation for digital messages or documents. It involves using a private key to sign the message and a public key to verify the signature. Digital signatures ensure that the sender of a message is authenticated and that the message has not been tampered with during transmission.

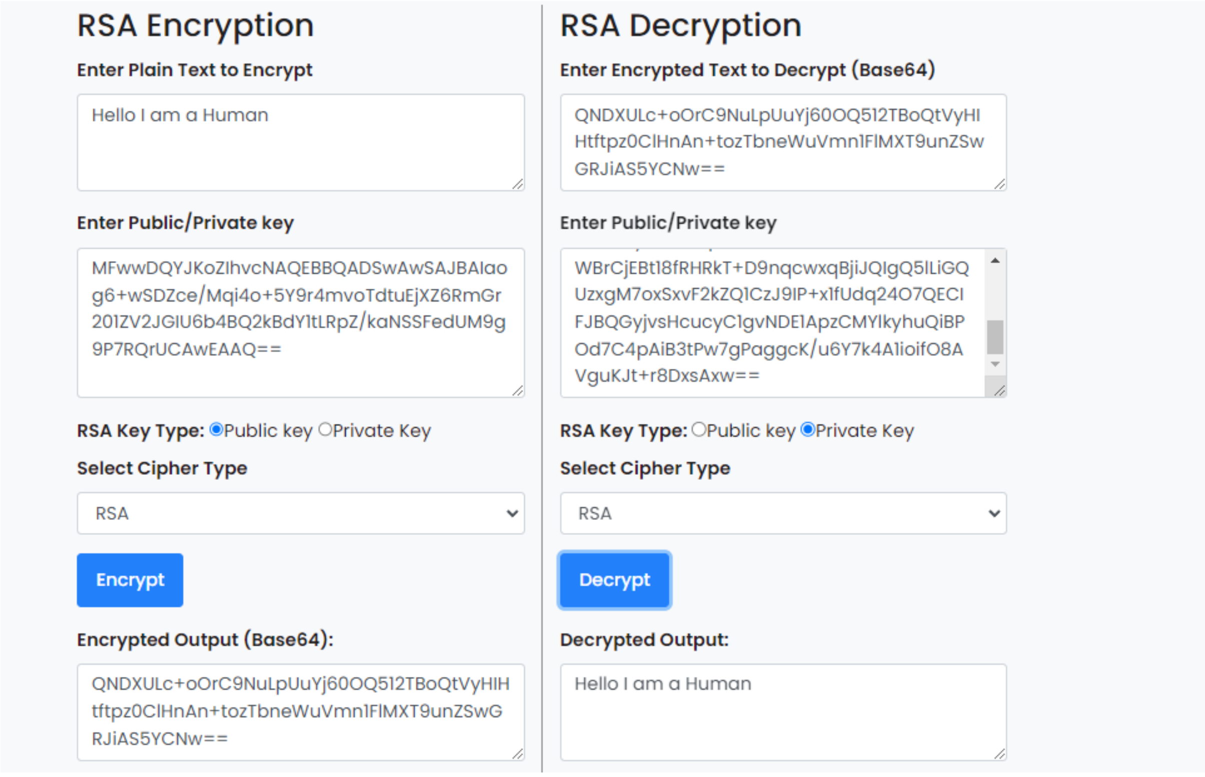
Algorithm:

1. Key Generation:
   - Choose a private key for signing.
   - Compute a corresponding public key for verification.

2. Signing:
   - Hash the message to produce a fixed-length digest.
   - Encrypt the digest using the private key to create the digital signature.

3. Verification:
   - Decrypt the digital signature using the sender's public key to get the digest.
   - Hash the received message to produce a digest.
   - Compare the two digests. If they match, the signature is valid.

Digital signatures are essential for secure communication, online transactions, and authentication of digital documents.



RSA Encryption

Enter Plain Text to Encrypt

Hello I am a Human

Enter Public/Private key

```
MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAIao
g6+wSDZce/Mqi4o+5Y9r4mvoTdtuEjXZ6RmGr
201ZV2JGIU6b4BQ2kBdY1tLRpZ/kaNSSFedUM9g
9P7RQrUCAwEAAQ==
```

RSA Key Type: ● Public key ○ Private Key

Select Cipher Type

RSA

Encrypted Output (Base64):

```
QNDXULc+oOrC9NuLpUuYj60OQ512TBoQtVyHIH
tftpz0ClHnAn+tozTbneWuVmn1FlMXT9unZSwG
RJiAS5YCNw==
```

RSA Decryption

Enter Encrypted Text to Decrypt (Base64)

```
QNDXULc+oOrC9NuLpUuYj60OQ512TBoQtVyHI
Htftpz0ClHnAn+tozTbneWuVmn1FlMXT9unZSw
GRJiAS5YCNw==
```

Enter Public/Private key

```
WBrCjEBt18fRHRkT+D9nqcwxqBjiJQIgQ5lLiGQ
UzxgM7oxSxvF2kZQ1CzJ9IP+x1fUdq24O7QECI
FJBQGyjvsHcucyC1gvNDE1ApzCMYlkyhuQiBP
Od7C4pAiB3tPw7gPaggcK/u6Y7k4A1ioifO8A
VguKJt+r8DxsAxw==
```

RSA Key Type: ○ Public key ● Private Key

Select Cipher Type

RSA

Decrypted Output:

Hello I am a Human

<u>Conclusion:</u> Thus we learnt and implemented RSA and digital signature using RSA