Name: Pankaj Parihar

Roll No.: 74

Batch: T21

Assignment – 4

Aim : To implement and analyze RSA cryptosystem and Digital signature scheme using RSA.

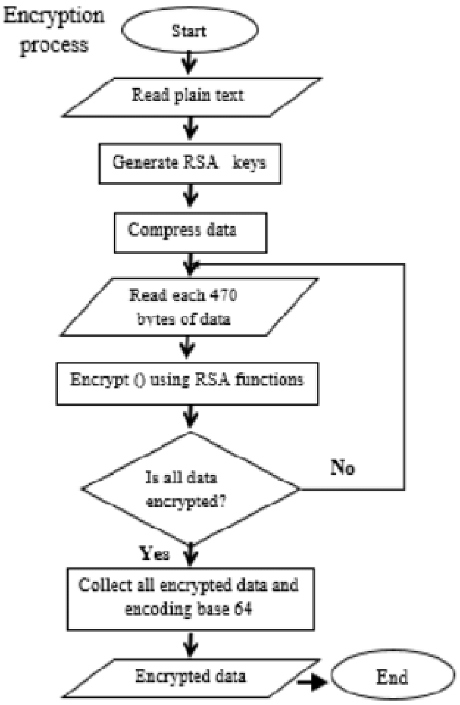
Theory :

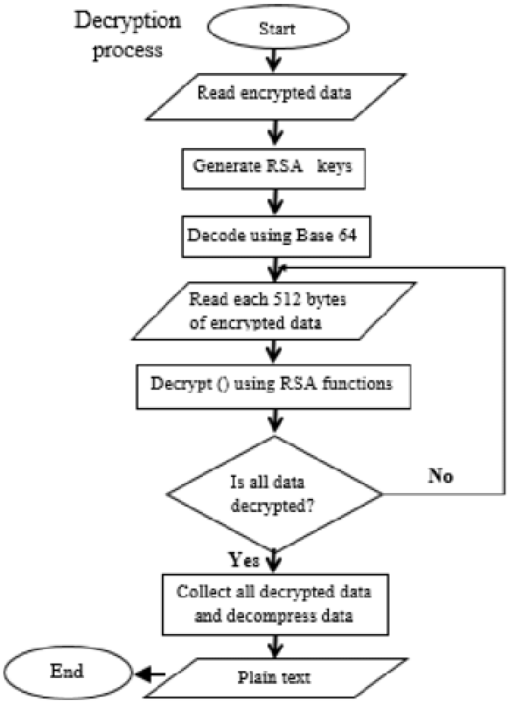
RSA and digital signatures are crucial elements in modern cybersecurity. RSA, a widely used encryption algorithm, ensures secure data transmission by encrypting and decrypting information. Digital signatures, on the other hand, authenticate the identity of the sender and guarantee the integrity of the message. Together, RSA and digital signatures provide a robust framework for secure communication, protecting sensitive data from unauthorized access and ensuring that messages are not tampered with during transmission.

These technologies are essential in various applications, from online banking to secure email communication, making them vital components in the digital world. In this article, we will learn about the RSA signature scheme, Attacks on the RSA Digital Signature Scheme, and the steps of digital signature process creation.

What is RSA?

It is the most popular asymmetric cryptographic algorithm. It is primarily used for encrypting messages but can also be used for performing digital signatures over a message. RSA is a widely used encryption algorithm that ensures secure data transmission by encrypting and decrypting information. It relies on a pair of keys, a public key for encryption and a private key for decryption, to protect sensitive data from unauthorized access. RSA is essential in many applications, such as online banking and secure email communication, providing a robust framework for secure interactions in the digital world.





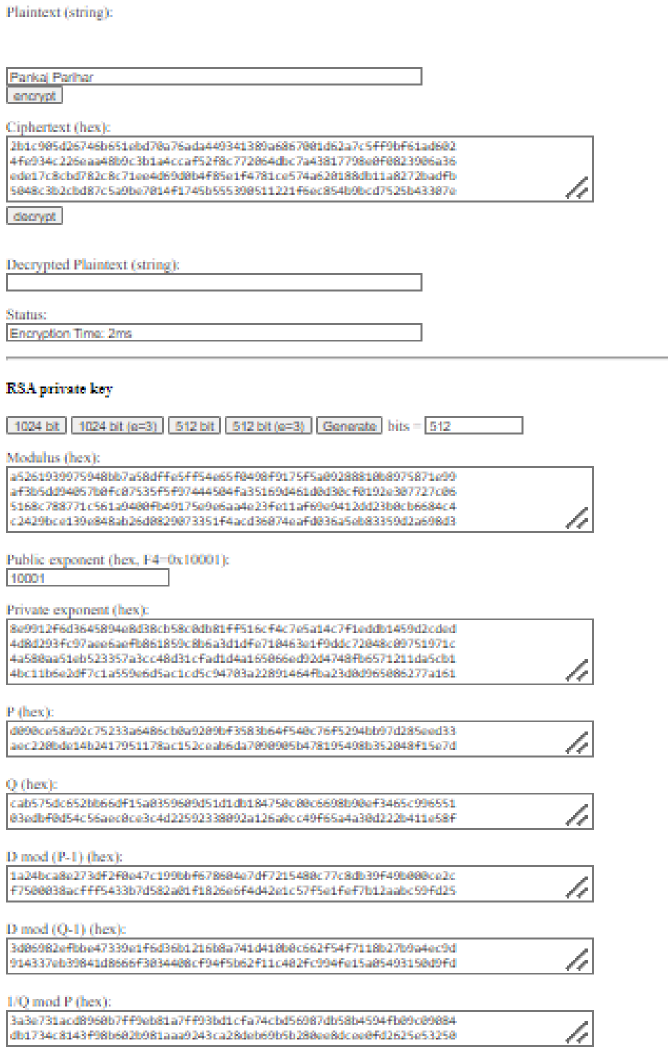
What is Digital Signature?

As the name sounds are the new alternative to signing a document digitally. It ensures that the message is sent by the intended user without any tampering by any third party (attacker). In simple words, digital signatures are used to verify the authenticity of the message sent electronically.

Digital signatures authenticate the identity of the sender and guarantee the integrity of the message. By using a private key to create a unique signature and a public key to verify it, digital signatures ensure that messages are not tampered with during transmission. This technology is vital for ensuring trust and security in various online transactions and communications, making it an indispensable tool in modern cybersecurity.

Output:

Encryption:



Plaintext (string):

Pankaj Parihar

Ciphertext (hex):

```
2b1c905d26746b651ebd70a76ada449341380a6867001d62a7c5ff9bf61ad602
4fe934c226eaa48b9c3b1a4ccaf52f8c772864dbc7a43817798e0f0823906a36
ede17c8cbd782c8c71ee4d69d0b4f85e1f4781ce574a620188db11a8272badfb
5048c3b2cbd87c5a9be7014f1745b555390511221f6ec854b0bcd7525b43387e
```

Decrypted Plaintext (string):

Status:

Encryption Time: 2ms

RSA private key

bits = 512

Modulus (hex):

```
a5261939975948bb7a58dffe5ff54e65f0498f9175f5a09288810b8975871e99
af3b5dd94057b0fc87535f5f97444504fa35169d461d0d30cf0192e307727c06
5168c788771c561a9400fb49175e9e6aa4e23fe11af69e9412dd23b0cb6684c4
c2429bce139e848ab26d8829073351f4acd36074eafd036a5eb83359d2a698d3
```

Public exponent (hex, F4=0x10001):

10001

Private exponent (hex):

```
8e9912f6d3645894e8d38cb58c0db81ff516cf4c7e5a14c7f1eddb1459d2cded
4d8d293fc97aee6aefb861859c8b6a3d1dfe718463e1f9ddc72848c09751971c
4a580aa51eb523357a3cc48d31cfad1d4a165066ed92d4748fb6571211da5cb1
4bc11b6e2df7c1a559e6d5ac1cd5c94783a22891464fba23d0d965086277a161
```

P (hex):

```
d090ce58a92c75233a6486cb0a9289bf3583b64f540c76f5294bb97d285eed33
aec220bde14b2417951178ac152ceab6da7090905b478195498b352848f15e7d
```

Q (hex):

```
cab575dc652bb66df15a0359609d51d1db184750c00c6608b90ef3465c996551
03edbf0d54c56aec8ce3c4d22592338892a126a0cc49f65a4a30d222b411e58f
```

D mod (P-1) (hex):

```
1a24bca8e273df2f0e47c199bbf678604e7df7215480c77c8db39f49b000ce2c
f7500038acfff5433b7d582a01f1826e6f4d42e1c57f5e1fef7b12aabc59fd25
```

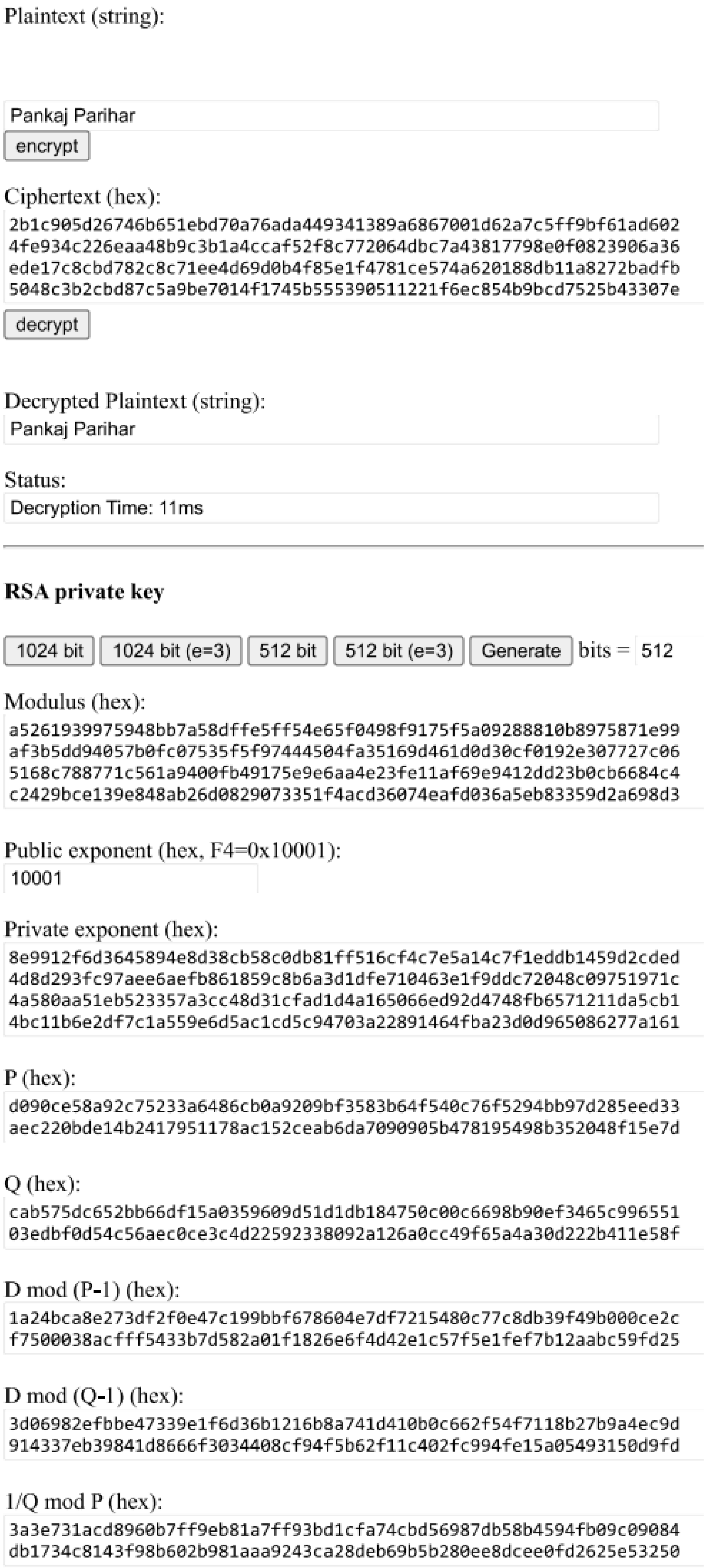
D mod (Q-1) (hex):

```
3d06982efbbe47339e1f6d36b1216b8a741d410b0c662f54f7118b27b9a4ec9d
914337eb39841d8666f3034408cf94f5b62f11c402fc994fe15a05493150d9fd
```

1/Q mod P (hex):

```
3a3e731acd8960b7ff9eb81a7ff93bd1cfa74cbd56087db58b4594fb09c09884
db1734c8143f98b602b081aaa9243ca28deb69b5b280ee8dcee0fd2625e53250
```

Decryption:



Plaintext (string):

Pankaj Parihar

Ciphertext (hex):

```
2b1c905d26746b651ebd70a76ada449341389a6867001d62a7c5ff9bf61ad602
4fe934c226eaa48b9c3b1a4ccaf52f8c772064dbc7a43817798e0f0823906a36
ede17c8cbd782c8c71ee4d69d0b4f85e1f4781ce574a620188db11a8272badfb
5048c3b2cbd87c5a9be7014f1745b555390511221f6ec854b9bcd7525b43307e
```

Decrypted Plaintext (string):

Pankaj Parihar

Status:

Decryption Time: 11ms

RSA private key

bits = 512

Modulus (hex):

```
a5261939975948bb7a58dffe5ff54e65f0498f9175f5a09288810b8975871e99
af3b5dd94057b0fc07535f5f97444504fa35169d461d0d30cf0192e307727c06
5168c788771c561a9400fb49175e9e6aa4e23fe11af69e9412dd23b0cb6684c4
c2429bce139e848ab26d0829073351f4acd36074eafd036a5eb83359d2a698d3
```

Public exponent (hex, F4=0x10001):

10001

Private exponent (hex):

```
8e9912f6d3645894e8d38cb58c0db81ff516cf4c7e5a14c7f1eddb1459d2cded
4d8d293fc97aee6aefb861859c8b6a3d1dfe710463e1f9ddc72048c09751971c
4a580aa51eb523357a3cc48d31cfad1d4a165066ed92d4748fb6571211da5cb1
4bc11b6e2df7c1a559e6d5ac1cd5c94703a22891464fba23d0d965086277a161
```

P (hex):

```
d090ce58a92c75233a6486cb0a9209bf3583b64f540c76f5294bb97d285eed33
aec220bde14b2417951178ac152ceab6da7090905b478195498b352048f15e7d
```

Q (hex):

```
cab575dc652bb66df15a0359609d51d1db184750c00c6698b90ef3465c996551
03edbf0d54c56aec0ce3c4d22592338092a126a0cc49f65a4a30d222b411e58f
```

D mod (P-1) (hex):

```
1a24bca8e273df2f0e47c199bbf678604e7df7215480c77c8db39f49b000ce2c
f7500038acfff5433b7d582a01f1826e6f4d42e1c57f5e1fef7b12aabc59fd25
```

D mod (Q-1) (hex):

```
3d06982efbbe47339e1f6d36b1216b8a741d410b0c662f54f7118b27b9a4ec9d
914337eb39841d8666f3034408cf94f5b62f11c402fc994fe15a05493150d9fd
```

1/Q mod P (hex):

```
3a3e731acd8960b7ff9eb81a7ff93bd1cfa74cbd56987db58b4594fb09c09084
db1734c8143f98b602b981aaa9243ca28deb69b5b280ee8dcee0fd2625e53250
```

Conclusion: Demonstrated key management, distribution and user authentication (LO2 is achieved).