EXPERIMENT NO: -6

Aim – Implementation and analysis of RSA cryptosystem and Digital signature scheme using RSA.

Theory – RSA: 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 RSA algorithm is named after those who invented it in 1978: Ron Rivest, Adi Shamir, and Leonard Adleman.

Asymmetric Key Cryptography: Asymmetric cryptography, also known as public- key cryptography, is a process that uses a pair of related keys -- one public key and one private key -- to encrypt and decrypt a message and protect it from unauthorized access or use. A public key is a cryptographic key that can be used by any person to encrypt a message so that it can only be deciphered by the intended recipient with their private key. A private key -- also known as a secret key -- is shared only with key's initiator.
When someone wants to send an encrypted message, they can pull the intended recipient's public key from a public directory and use it to encrypt the message before sending it. The recipient of the message can then decrypt the message using their related private key. On the other hand, if the sender encrypts the message using their private key, then the message can be decrypted only using that sender's public key, thus authenticating the sender. These encryption and decryption processes happen automatically; users do not need to physically lock and unlock the message.
Many protocols rely on asymmetric cryptography, including the transport layer security (TLS) and secure sockets layer (SSL) protocols, which make HTTPS possible. The encryption process is also used in software programs -- such as browsers -- that need to establish a secure connection over an insecure network like the Internet or need to validate a digital signature.
Increased data security is the primary benefit of asymmetric cryptography. It is the most secure encryption process because users are never required to reveal or share their private keys, thus decreasing the chances of a cybercriminal discovering a user's private key during transmission.

RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e., **Public Key** and **Private Key.** As the name describes that the Public Key is given to everyone and Private key is kept private.

RSA Algorithm

RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e., Public Key and Private Key. As the name describes that the Public Key is given to everyone and Private key is kept private.

The RSA algorithm holds the following features:

- RSA algorithm is a popular exponentiation in a finite field over integers including prime numbers
- The integers used by this method are sufficiently large making it difficult to solve
- There are two sets of keys in this algorithm: private key and public key.

RSA Key Generation:

- Choose two large prime numbers p and q
- Calculate n=p*q
- Select public key e such that it is not a factor of (p-1) *(q-1)
- Select private key d such that the following equation is true (d*e) mod(p-1) (q-1) =1 or d is inverse of E in modulo (p-1) *(q-1)

Digital Signature: Digital signatures are the public-key primitives of message authentication. In the physical world, it is common to use handwritten signatures on handwritten or typed messages. They are used to bind signatory to the message.

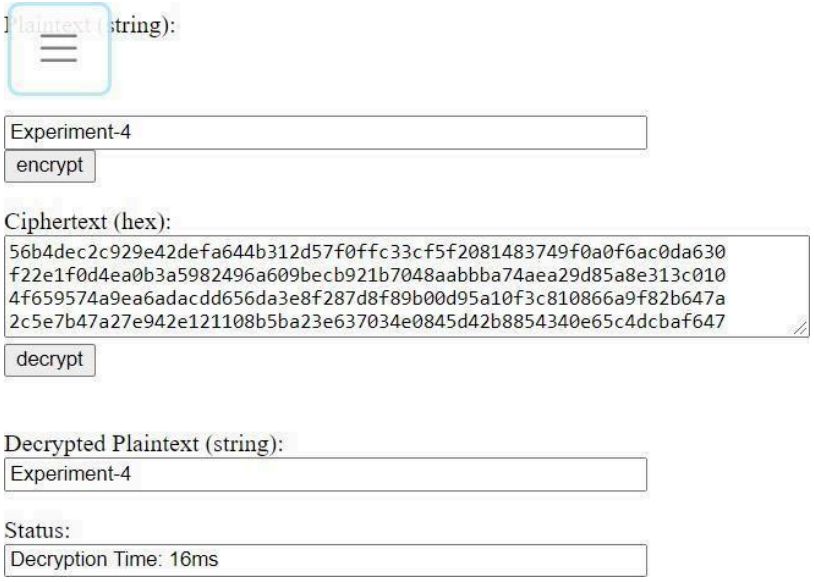
Similarly, a digital signature is a technique that binds a person/entity to the digital data. This binding can be independently verified by receiver as well as any third party.

Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.

In real world, the receiver of message needs assurance that the message belongs to the sender and he should not be able to repudiate the origination of that message. This requirement is very crucial in business applications, since likelihood of a dispute over exchanged data is very high.

Conclusion: In this experiment we learned about RSA and Digital Signature. RSA algorithm is a public key encryption technique and is considered as the most secure way of encryption.

Output:


Plaintext (string):
Experiment-4
encrypt
Ciphertext (hex):
56b4dec2c929e42defa644b312d57f0ffc33cf5f2081483749f0a0f6ac0da630
f22e1f0d4ea0b3a5982496a609becb921b7048aabbba74aea29d85a8e313c010
4f659574a9ea6adacdd656da3e8f287d8f89b00d95a10f3c810866a9f82b647a
2c5e7b47a27e942e121108b5ba23e637034e0845d42b8854340e65c4dcbaf647
decrypt
Decrypted Plaintext (string):
Experiment-4
Status:
Decryption Time: 16ms

RSA private key

1024 bit | 1024 bit (e=3) | 512 bit | 512 bit (e=3) | Generate | bits = 512

Modulus (hex):

```
ABC30681295774F7CECA691EC17F4E762DA6DE70F198EAEE3CCE3A435FC006B9
71DC24E55904F1D2705758C041C2B0B18E8BFAE2C9CD96B50082D7D8C7342CBA
B7F6E0622DA53B8B56DBDB24174F00173263CFECAE604795CDA2A037BC3A69B7
C0090AA2DE1568998BCD6D70CC2E0574755B9F7986AE01CE8714A26144279CDB
```

Public exponent (hex, F4=0x10001):

```
3
```

Private exponent (hex):

```
728204561b8fa34fdf319b69d654def973c4944b4bbb47497dded1823fd559d0
f692c34390adf68c4ae4e5d5812c75cbb45d51ec86890f2355ac8fe5da22c87b
62449e2aa754422bc43d3ca32efa866227ad58178e7803897d074f1312740aa7
61cfc7ed753bb829d7a2ab091289d1676809bfd61276b43bb3a395714f167beb
```

P (hex):

```
e200731c6e934a0fdc1d5ce5f66d08ba9478280f46e9cbed777029dd4811a7cd
4aa66ad8365c5aa67b06b97e54ee8fec03adb2134f7359a427c7ffc468ef0231
```

Q (hex):

```
c28f8005c4138e39d462a3495a6a2dc96267a3ba11c2765a1aa77fbdd87ab1ef
62aaf3e677df79b44d52b364db70bb6d559f4da51b8899d0d1d74272e496e0cb
```

D mod (P-1) (hex):

```
96aaf76849b786b53d68e8994ef35b270da5700a2f4687f3a4f5713e300bc533
87199c90243d91c452047ba98df45ff2ad1e76b78a4ce66d6fdaaa82f09f56cb
```

D mod (Q-1) (hex):

```
81b50003d80d097be2ec6cdb919c1e86419a6d26b681a43c11c4ffd3e5a7214a
41c74d444fea5122de3722433cf5d248e3bf8918bd05bbe08be4d6f7430f4087
```

1/Q mod P (hex):

```
a318fb95d3b10d6cfb0096fc3a3173377cf0952bf5d50fd3ccf678dd636ca1a1
aeed8da416c8fba4395b00dc3e22823d1b2add8a4e1222d562af11bd6c78ad94
```

RSA DIGITAL SIGNATURE

gn the plaintext with Hashed RSA.

tring):

test | SHA-1

Hash output(hex):

```
a94a8fe5ccb19ba61c4c0873d391e987982fbbd3
```

Input to RSA(hex):

a94a8fe5ccb19ba61c4c0873d391e987982fbbd3 | Apply RSA

Digital Signature(hex):

```
5ac483d7ec6a76b6d53046c4dd439dcc95179983de793e0060b0f4942b30bff7
4d1fcd54494765544f9863c3425bb28b313610726ea089c04202155efad34340
0f5b5afc7a59777c9e035edb20c529664087b63380c0d4af8ef617b4c3f08529
d227643cad3f0e0d2217ef460cb5427607b32c1f8a20309c1580601b20867054
```

Digital Signature(base64):

```
Ws5D1+xqdrbVMEbE3UOdzJUXmYPeeT4AYLD01Cswv/dNH81USUd1VE+YY8NCW7KL
MTYQcm6gicBCAhVe+tNDQA9bWvx6WXd8ngNe2yDFKWZAh7YzgMDUr472F7TD8IUp
01dkPK0/Dg01F+9GDLVCdgezLB+KIDCcFYBgGyCGcFQ=
```

Status:

Time: 6ms

RSA public key

Public exponent (hex, F4=0x10001):

10001

Modulus (hex):

```
a5261939975948bb7a58dffe5ff54e65f0498f9175f5a09288810b8975871e99
af3b5dd94057b0fc07535f5f97444504fa35169d461d0d30cf0192e307727c06
5168c788771c561a9400fb49175e9e6aa4e23fe11af69e9412dd23b0cb6684c4
c2429bce139e848ab26d08290733351f4acd36074eafd036a5eb83359d2a698d3
```

1024 bit | 1024 bit (e=3) | 512 bit | 512 bit (e=3)