Roll Number:- 2105048
Name:-Manav Jain
Date:- 26/07/2023

Lab Assignment No:-4

Aim:- Implementation and analysis of RSA cryptosystem and digital signature scheme using RSA

Lab Outcome Attained :- LO2

Theory:-

Explain the steps of RSA key generation

The following are the steps in the generation of an RSA key:

1) Create the two huge primes p and q.

2) Determine the modulus n as follows: n = p * q.

3) Use the formula (n) = (p - 1)(q - 1) to calculate the totient.

4) Select an integer e such that gcd((n), e) = 1 and 1 e (n).

5) Use the formula d = e(-1) mod n to calculate the private exponent.

6) The pair (n, e) represents the public key, while the pair (n, d) represents the private key.

Eg:-

Assume p = 7 and q = 11. So n = p * q = 77. (p - 1)(q - 1) = 6 * 10 = 60 is the totient (n). e = 5 is an integer that meets the conditions 1 e (n) and gcd((n), e) = 1. The private exponent d is calculated using the formula d = e(-1) mod (n) = 3.

The public key is represented by the pair (n, e) = (77, 5). The private key is represented by the pair (n, d) = (77, 3).

In this example, the public key is (77, 5) and the private key is (77, 3). These keys can both encrypt and decode messages.

To encrypt a communication, the sender would use the public key. The private key would then be used by the receiver to decrypt the message.

To encrypt the message "hello" using the public key (77, 5), for example, the sender would first convert the message to a number. In this situation, the answer is 104. The sender would then use the public key to encrypt the number. 525 is the encrypted number.

The receiver would then use the private key (77, 3) to decrypt the number. The decrypted number would be 104. The receiver would then convert the number back to the message, which would be "hello".

Explain the steps of digital signature verification and generation process .

steps in generating and verifying a digital signature :

1. Generate the public and private keys.

The public and private keys are generated using the RSA key generation algorithm. The public key is made public, while the private key is kept secret.

2. Create a hash of the message.

A cryptographic hash function is used to hash the message to be signed. The hash function generates a fixed-length number known as the hash digest that uniquely reflects the message.

3. Encrypt the hash digest with the private key.

The hash digest is encrypted with the private key. The encrypted hash digest is the digital signature.

4. Send the message and the digital signature to the recipient.

The sender sends the message and the digital signature to the recipient.

5. Verify the digital signature.

The recipient decrypts the digital signature with the public key. The decrypted hash digest is compared to the hash of the message. If the two hashes match, then the signature is valid.

overview of the steps involved in generating and verifying a digital signature:

Generation

Generate the public and private keys.

Create a hash of the message.

Encrypt the hash digest with the private key.

Verification

Decrypt the digital signature with the public key.

Compare the decrypted hash digest to the hash of the message.

Output Screenshot:-

1) RSA key generation and decode

Plaintext (string):

hello this is implementation of rsa algorithm

encrypt

Ciphertext (hex):

```
469f99c7c7bd6eb33fb07b16aa06cbdbb8dc4ba02bcc9abb46de3ba1e5110ed4
3a6851ca040fb6114e8b8e2306dd1b55d7fcf2d89990b5f62eee8a9806b8f263
```

decrypt

Decrypted Plaintext (string):

hello this is implementation of rsa algorithm

Status:

Decryption Time: 5ms

RSA private key

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

Modulus (hex):

```
BC86E3DC782C446EE756B874ACECF2A115E613021EAF1ED5EF295BEC2BED899D
26FE2EC896BF9DE84FE381AF67A7B7CBB48D85235E72AB595ABF8FE840D5F8DB
```

Public exponent (hex, F4=0x10001):

```
3
```

Private exponent (hex):

```
7daf4292fac82d9f44e47af87348a1c0b9440cac1474bf394a1b929d729e5bbc
f402f29a9300e11b478c091f7e5dacd3f8edae2effe3164d7e0eeada87ee817b
```

P (hex):

```
ef3fc61e21867a900e01ee4b1ba69f5403274ed27656da03ed88d7902cce693f
```

Q (hex):

```
c9b9fcc298b7d1af568f85b50e749539bc01b10a68472fe1302058104821cd65
```

D mod (P-1) (hex):

```
9f7fd9696baefc6009569edcbd19bf8d576f89e1a439e6ad4905e50ac8899b7f
```

D mod (Q-1) (hex):

```
867bfdd7107a8bca39b503ce09a30e267d567606f02f7540cac03ab5856bde43
```

1/Q mod P (hex):

```
412d6b551d93ee1bd7dccafc63d7a6d031fc66035ecc630ddf75f949a378cd9d
```

2)Digital Signature (hash key generation)

Digital Signatures Scheme

Digitally sign the plaintext with Hashed RSA.

Plaintext (string):

hello this is generation of digital signature SHA-1

Hash output(hex):

5d41539793f25323c88168be360b2969d153514b

3)Digital Signature(generation)

Input to RSA(hex):

5d41539793f25323c88168be360b2969d153514b Apply RSA

Digital Signature(hex):

```
5ce2601899d9c6fcdc5173556d9a8615d4fb021dabdde2337c2fbb4750bcf2f2
5d8f38e2a3e865a91b554ce7237aabb11b322760febc5ba53dfb7cbb6dee1632
531c478a491963bb50fb98328eb198f4a4cf54232cb1683424fa38d1f879e177
dae72e12b5c9cb41556644febdec9eba0d04eb79d1cd87540cf7b02893aa62b0
```

Digital Signature(base64):

```
XOJgGJnZxvzcUXNVbZqGFdT7Ah2r3eIzfC+7R1C88vJdjzjio+hlqRtVTOcjequx
GzInYP68W6U9+3y7be4WMlMcR4pJGWO7UPuYMo6xmPSkz1QjLLFoNCT6ONH4eeF3
2ucuErXJy0FVZkT+veyeug0E63nRzYdUDPewKJOqYrA=
```

Status:

Time: 2ms

RSA public key

Public exponent (hex, F4=0x10001):

3

Modulus (hex):

```
ABC30681295774F7CECA691EC17F4E762DA6DE70F198EAEE3CCE3A435FC006B9
71DC24E55904F1D2705758C041C2B0B18E8BFAE2C9CD96B50082D7D8C7342CBA
B7F6E0622DA53B8B56DBDB24174F00173263CFECAE604795CDA2A037BC3A69B7
C0090AA2DE1568998BCD6D70CC2E0574755B9F7986AE01CE8714A26144279CDB
```

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

Conclusion:-

Learned about the RSA scheme and the RSA cryptosystem, investigated the stages involved in digital key generation and verification, developed and verified digital signatures using software, and implemented the RSA scheme.