Roll no. : 53
Name: Shreya Kamath
Date: 31st July, 2023.

LAB ASSIGNMENT NO. 4

AIM: Implementation and analysis of RSA cryptosystem and Digital signature scheme using RSA.

LAB OUTCOME ATTAINED:

LO 2: Demonstrate Key management, distribution and user authentication.

THEORY:

RSA

RSA is a widely used public-key encryption algorithm. It involves key generation with two large prime numbers, calculating the modulus and totient, and choosing public and private exponents. The security relies on the difficulty of factoring the large modulus, ensuring secure communication and data encryption. The public key is used for encryption, while the private key is used for decryption.

Steps for Key Generation in RSA

Step 1: Choose Two Large Prime Numbers
Select two distinct prime numbers, typically denoted as "p" and "q." These prime numbers should be large to enhance the security of the RSA key. The product of "p" and "q" is used to calculate the modulus "n" (n = p * q).

Step 2: Calculate the Modulus "n"
Compute the modulus "n" by multiplying the two selected prime numbers: n = p * q.

Step 3: Calculate the Totient of "n" (φ(n))
The totient of "n," denoted as φ(n), is calculated as φ(n) = (p-1) * (q-1). The totient function counts the number of positive integers that are coprime (relatively prime) to "n."

Step 4: Choose the Public Exponent (e)
Select a small public exponent "e" (usually a prime number), where 1 < e < φ(n), and "e" is coprime with φ(n) (i.e., gcd(e, φ(n)) = 1). The public key is represented by (e, n).

Step 5: Calculate the Private Exponent (d)
Compute the private exponent "d" such that (d * e) % φ(n) = 1. In other words, "d" is the modular multiplicative inverse of "e" modulo φ(n). The private key is represented by (d, n).

Step 6: Public and Private Key Generation
The generated public key is (e, n), and the corresponding private key is (d, n).

The security of RSA relies on the difficulty of factoring the large modulus "n" into its prime factors "p" and "q." The larger the prime numbers used, the more secure the RSA key. The public key (e, n) is used for encryption, while the private key (d, n) is kept secret and used for decryption.

Roll no. : 53
Name: Shreya Kamath
Date: 31st July, 2023.

DIGITAL SIGNATURE

A digital signature is a cryptographic technique used to verify the authenticity and integrity of digital messages or documents. It involves the use of a private key to encrypt a unique hash of the message, creating a digital signature. The recipient can then use the corresponding public key to decrypt the signature and verify the message's origin and content.

Digital Signature Generation Process:

1. Hashing: The signer creates a hash (fixed-size digital fingerprint) of the message using a cryptographic hash function (e.g., SHA-256). This produces a unique representation of the message.

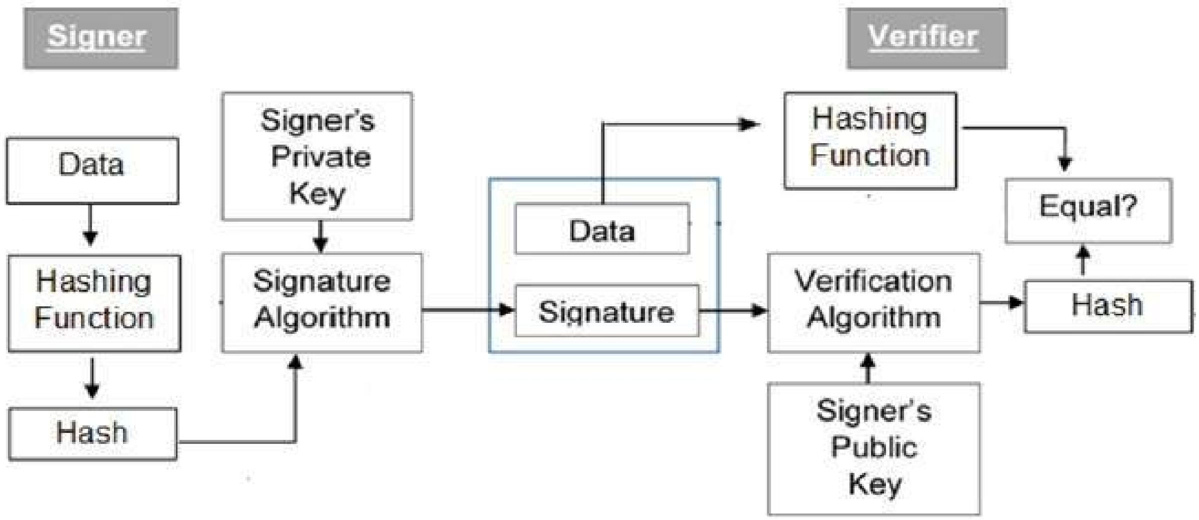
2. Private Key Encryption: The signer encrypts the hash using their private key (from their public-private key pair) to create the digital signature. This ensures that only the signer's private key can produce the signature for that specific message.

Digital Signature Verification Process:

1. Hashing: The recipient of the message computes the hash of the received message using the same cryptographic hash function used by the signer.

2. Public Key Decryption: The recipient decrypts the received digital signature using the signer's public key (obtained from a trusted source like a digital certificate).

3. Comparison: The recipient compares the computed hash with the decrypted signature. If they match, it confirms the integrity and authenticity of the message, as only the signer's private key could have produced the matching signature for that specific message.



By using digital signatures, the recipient can verify the origin and integrity of the message, ensuring that it has not been altered in transit and came from the claimed sender.

Roll no. : 53
Name: Shreya Kamath
Date: 31st July, 2023.

OUTPUT:
RSA

Plaintext (string):

shreya kamath

encrypt

Ciphertext (hex):

```
38c8cd63b594936af48200940978d7dd719edcbf42a91f7775da45f33b26d6b5
4d7cc0ef5b060bd188b79eec06022ee0aab1e2e6e5baf155497b7cae007d64d0
```

decrypt

Decrypted Plaintext (string):

shreya kamath

Status:

Decryption Time: 1ms

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
```

Roll no. : 53
Name: Shreya Kamath
Date: 31st July, 2023.

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

DIGITAL SIGNATURE

Plaintext (string):

shreyakamath SHA-1

Hash output(hex):

7b1da690f567252df0b030a76b9f8f0e3b8b7771

Input to RSA(hex):

7b1da690f567252df0b030a76b9f8f0e3b8b7771 Apply RSA

Digital Signature(hex):

09e02be0837d0407bd718f959df06efaf3e882910f20a99016349a47d2e78b85
969b45e00cecc8f0902900f552f518f22857ce411e301a08810d6588e1ba1ef1

Digital Signature(base64):

CeAr4IN9BAe9cY+VnfBu+vPogpEPIKmQFjSaR9Lni4WWm0XgDOzI8JApAPVS9Rjy
KFfOQR4wGgiBDWWI4boe8Q==

Status:

Time: 2ms

RSA public key

Public exponent (hex, F4=0x10001):

3

Modulus (hex):

BC86E3DC782C446EE756B874ACECF2A115E613021EAF1ED5EF295BEC2BED899D
26FE2EC896BF9DE84FE381AF67A7B7CBB48D85235E72AB595ABF8FE840D5F8DB

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

CONCLUSION:

Hence, we successfully implemented the RSA cryptosystem and the digital signature scheme. Through the secure key management and authentication processes, we established a robust encryption system and a reliable method to verify message authenticity, ensuring secure communication and data integrity.