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

Theory:-

1. Explain the steps of RSA key generation.

The computational steps for key generation are

- Generate two different primes including p and q.
- Compute the modulus $n = p \times q$
- Compute the totient $\phi(n) = (p - 1) \times (q - 1)$
- Select for public exponent an integer e such that $1 < e < \phi(n)$ and $\gcd(\phi(n), e) = 1$.
- Compute for the private exponent a value for d such that $d = e-1 \bmod \phi(n)$
- Public Key = [e, n]
- Private Key = [d, n]

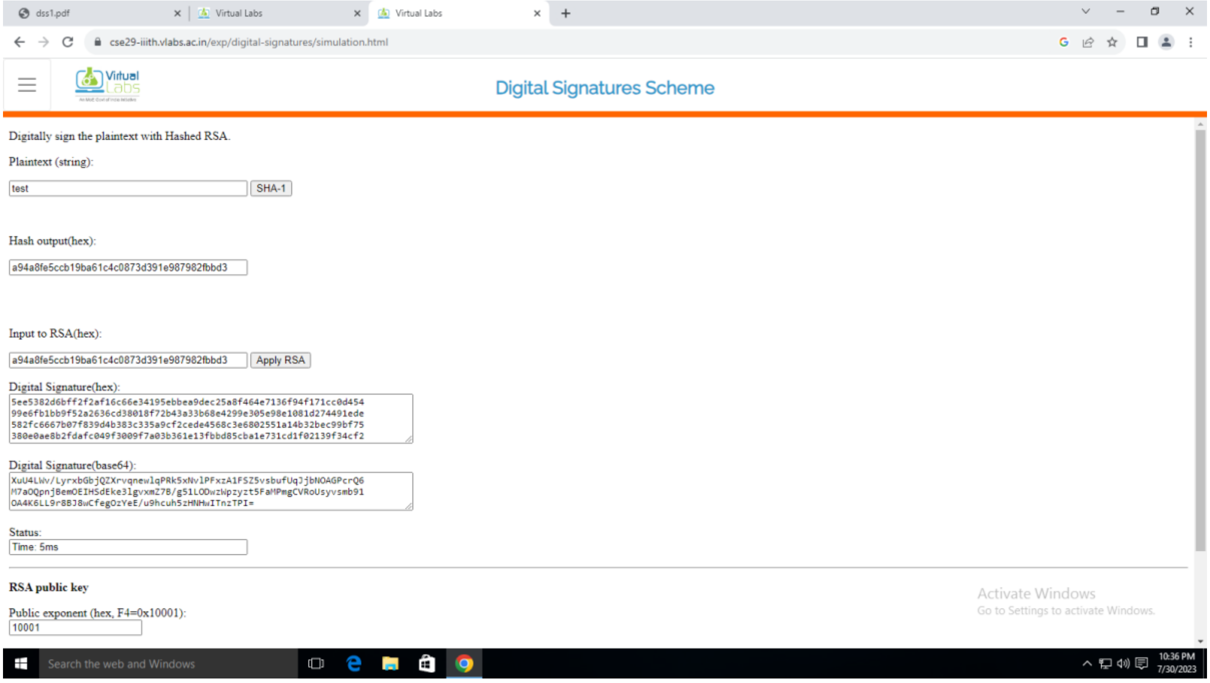
2. Explain the steps of Digital signature generation and verification process.

You send a document to Person B with both the Public and Private key. Remember that the verifier needs the Public key to verify the signature and also assurances that the private key is actually owned by the originator of the document.

The next step is to verify the public key. The verifier can use the Certifying Authority to ensure the validity and the public key. The CA will also help the verifier authenticate the identity of the sender, ensure that they are who they say they are.

If the authenticity of the public key is confirmed, you can then enter the secret private key to decrypt the document and the document is signed. If the private key is incorrect the signature of the document cannot be verified. This is why it is essential to verify the identity of the sender with the Certificate Authority.

Output:-



dss1.pdf
Virtual Labs
Virtual Labs
cse29-iiith.vlabs.ac.in/exp/digital-signatures/simulation.html
Virtual Labs

Digital Signatures Scheme

Digitally sign the plaintext with Hashed RSA.

Plaintext (string):

test [SHA-1]

Hash output(hex):

a94a8fe5ccb19ba61c4c0873d391e987982fbbd3

Input to RSA(hex):

a94a8fe5ccb19ba61c4c0873d391e987982fbbd3 [Apply RSA]

Digital Signature(hex):

```
5ee5382d6bff2f2af16c66e34195ebbea9dec25a8f464e7136f94f171cc0d454
99e6fb1bb9f52a2636cd38018f72b43a33b68e4299e305e98e1081d274491ede
582fc6667b07f839d4b383c335a9cf2cede4568c3e6802551a14b32bec99bf75
380e0ae8b2fdafc049f3009f7a03b361e13fbbd85cba1e731cd1f02139f34cf2
```

Digital Signature(base64):

```
XuU4LWv/LyrxbGbjQZXrvqnewlqPRk5xNvlPFxzA1FSZ5vsbufUqJjbNOAGPcrQ6
M7aOQpnjBemOEIHSdEke3lgvxmZ7B/g51LODwzWpzyzt5FaMPmgCVRoUsyvsmb91
OA4K6LL9r8BJ8wCfegOzYeE/u9hcuh5zHNHwITnzTPI=
```

Status:

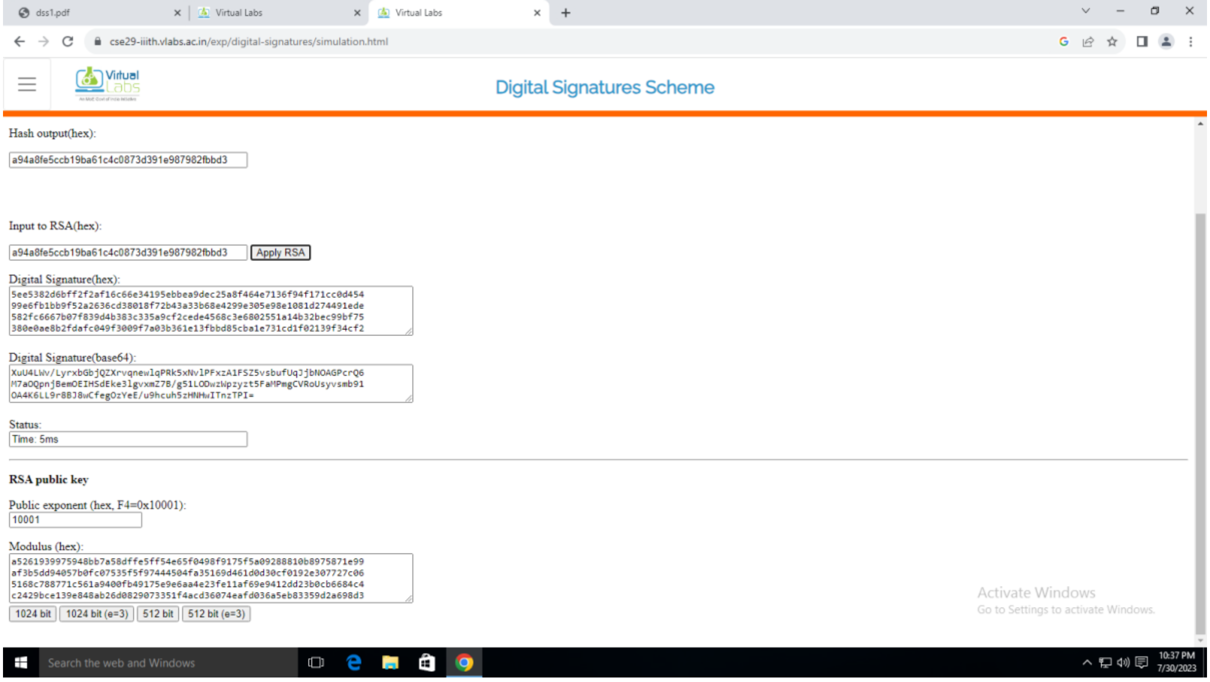
Time: 5ms

RSA public key

Public exponent (hex, F4=0x10001):

10001

Activate Windows
Go to Settings to activate Windows.
Search the web and Windows
10:36 PM
7/30/2023



dss1.pdf
Virtual Labs
Virtual Labs
cse29-iiith.vlabs.ac.in/exp/digital-signatures/simulation.html
Virtual Labs

Digital Signatures Scheme

Hash output(hex):

a94a8fe5ccb19ba61c4c0873d391e987982fbbd3

Input to RSA(hex):

a94a8fe5ccb19ba61c4c0873d391e987982fbbd3 [Apply RSA]

Digital Signature(hex):

```
5ee5382d6bff2f2af16c66e34195ebbea9dec25a8f464e7136f94f171cc0d454
99e6fb1bb9f52a2636cd38018f72b43a33b68e4299e305e98e1081d274491ede
582fc6667b07f839d4b383c335a9cf2cede4568c3e6802551a14b32bec99bf75
380e0ae8b2fdafc049f3009f7a03b361e13fbbd85cba1e731cd1f02139f34cf2
```

Digital Signature(base64):

```
XuU4LWv/LyrxbGbjQZXrvqnewlqPRk5xNvlPFxzA1FSZ5vsbufUqJjbNOAGPcrQ6
M7aOQpnjBemOEIHSdEke3lgvxmZ7B/g51LODwzWpzyzt5FaMPmgCVRoUsyvsmb91
OA4K6LL9r8BJ8wCfegOzYeE/u9hcuh5zHNHwITnzTPI=
```

Status:

Time: 5ms

RSA public key

Public exponent (hex, F4=0x10001):

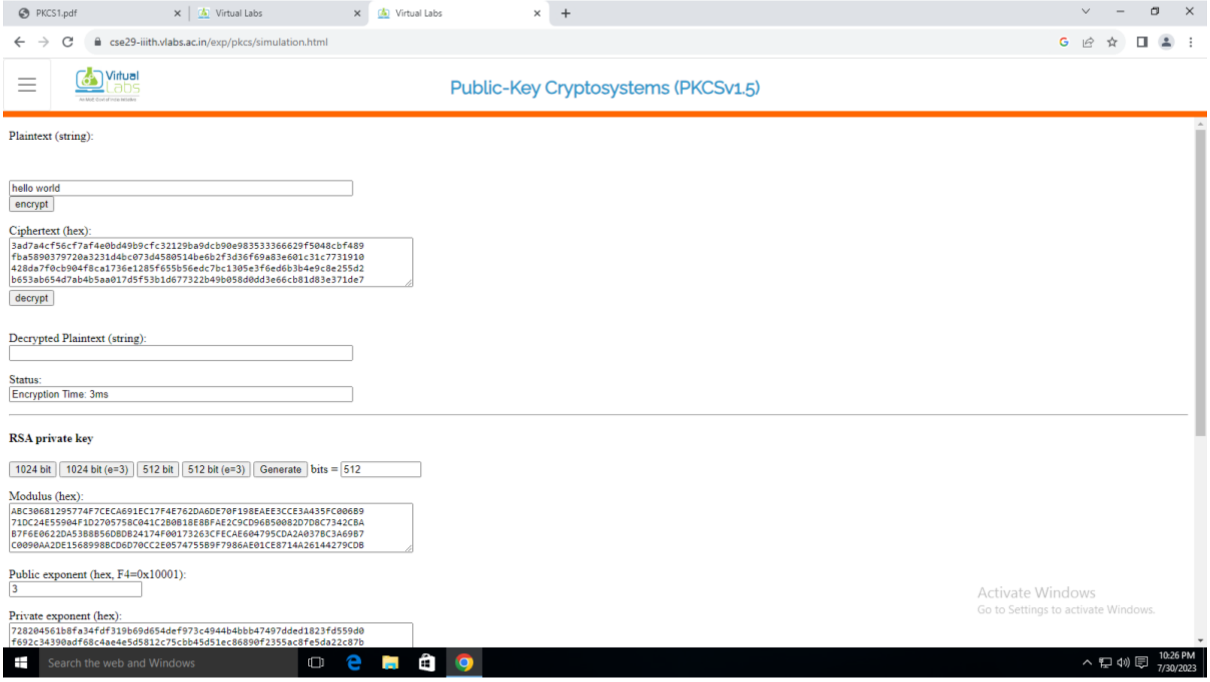
10001

Modulus (hex):

```
a5261939975948bb7a58dffe5ff54e65f0498f9175f5a09288810b8975871e99
af3b5dd94057b0fc07535f5f97444504fa35169d461d0d30cf0192e307727c06
5168c788771c561a9400fb49175e9e6aa4e23fe11af69e9412dd23b0cb6684c4
c2429bce139e848ab26d0829073351f4acd36074eafd036a5eb83359d2a698d3
```

[1024 bit] [1024 bit (e=3)] [512 bit] [512 bit (e=3)]

Activate Windows
Go to Settings to activate Windows.
Search the web and Windows
10:37 PM
7/30/2023



Public-Key Cryptosystems (PKCSv1.5)

Plaintext (string):

```
hello world
```

Ciphertext (hex):

```
3ad7a4cf56cf7af4e0bd49b9cfc32129ba9dcb90e983533366629f5048cbf489
fba5890379720a3231d4bc073d4580514be6b2f3d36f69a83e601c31c7731910
428da7f0cb904f8ca1736e1285f655b56edc7bc1305e3f6ed6b3b4e9c8e255d2
b653ab654d7ab4b5aa017d5f53b1d677322b49b058d0dd3e66cb81d83e371de7
```

Decrypted Plaintext (string):

Status:

```
Encryption Time: 3ms
```

RSA private key

bits = 512

Modulus (hex):

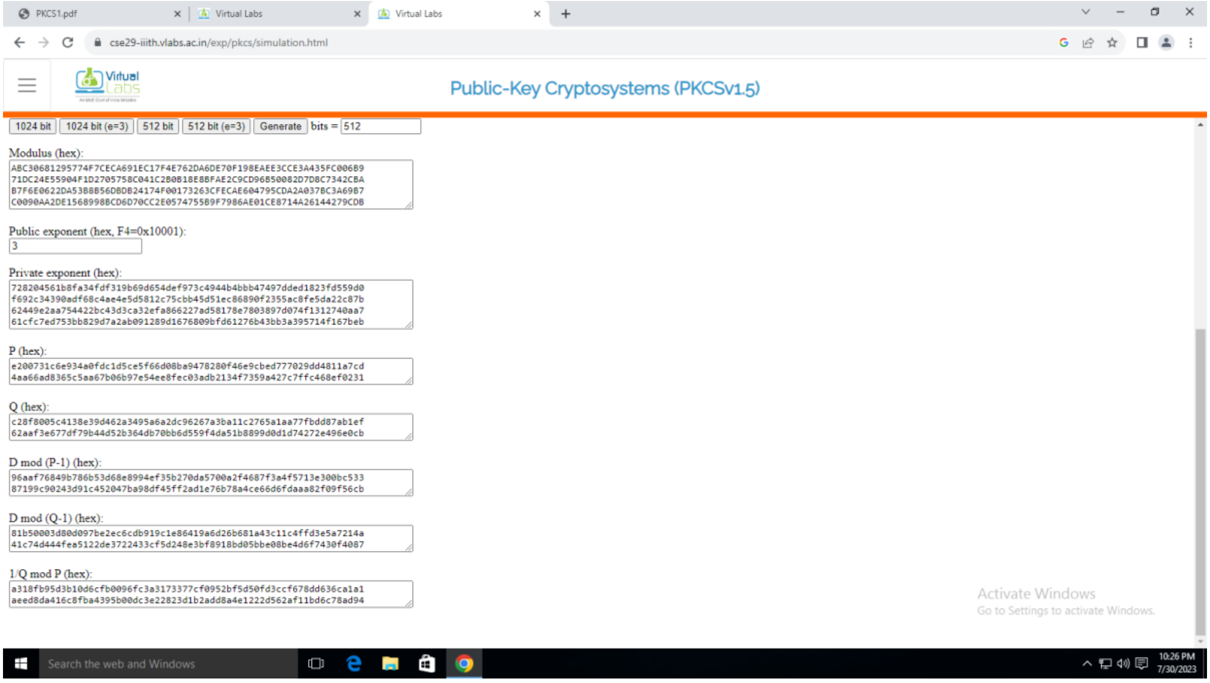
```
ABC30681295774F7CECA691EC17F4E762DA6DE70F198EAEE3CCE3A435FC006B9
71DC24E55904F1D2705758C041C2B0B18E8BFAE2C9CD96B50082D7D8C7342CBA
B7F6E0622DA53B8B56DBDB24174F00173263CFECAE604795CDA2A037BC3A69B7
C0090AA2DE1568998BCD6D70CC2E0574755B9F7986AE01CE8714A26144279CDB
```

Public exponent (hex, F4=0x10001):

```
3
```

Private exponent (hex):

```
728204561b8fa34fdf319b69d654def973c4944b4bbb47497dded1823fd559d0
f692c34390adf68c4ae4e5d5812c75cbb45d51ec86890f2355ac8fe5da22c87b
```



Public-Key Cryptosystems (PKCSv1.5)

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
```

Conclusion:-With This we were able to understand key generation of RSA as well as digital signature