Semester	T.E. Semester VI – Computer Engineering
Subject	Cryptography and cyber security
Subject Professor In-charge	Prof. Amit Nerurkar
Assisting Teachers	Prof. Amit Nerurkar
Laboratory	M312B

Student Name	Deep Salunkhe
Roll Number	21102A0014
TE Division	A

Title : **Design and Implementation of RSA algorithm for generating public and private key**

Title:

Design and Implementation of RSA algorithm for generating public and private key

---

Explanation:

1. Definition: A public-key cryptosystem, also known as asymmetric cryptography, is a cryptographic technique that uses two keys - a public key and a private key - to perform encryption and decryption operations.
2. Key Generation:
    - Public Key: The public key is made freely available to anyone and is used for encryption by other parties.
    - Private Key: The private key is kept secret by its owner and is used for decryption. It must never be shared with others.
3. Encryption and Decryption:
    - Encryption: A message or data is encrypted using the recipient's public key. Only the corresponding private key can decrypt the ciphertext.
    - Decryption: The encrypted message is decrypted using the recipient's private key, ensuring that only the intended recipient can access the original plaintext.
4. Security Properties:
    - Confidentiality: Public-key cryptosystems provide confidentiality by ensuring that only the intended recipient, who possesses the corresponding private key, can decrypt and access the original message.
    - Authentication: Public-key cryptosystems enable authentication by allowing users to digitally sign messages using their private keys, which can be verified by anyone using the corresponding public key.
    - Integrity: Digital signatures generated using public-key cryptography also ensure data integrity, as any tampering with the message will result in an invalid signature.

- Non-repudiation: Public-key cryptosystems provide non-repudiation, meaning that a user cannot deny sending a message or creating a digital signature once it has been verified using their public key.

5. Applications:

   - Secure Communication: Public-key cryptosystems are used to establish secure communication channels over insecure networks, such as the internet. Examples include HTTPS for secure web browsing and S/MIME for secure email communication.
   - Digital Signatures: Public-key cryptography is used to generate and verify digital signatures, ensuring the authenticity and integrity of electronic documents, transactions, and messages.
   - Key Exchange: Public-key cryptosystems facilitate secure key exchange protocols, such as Diffie-Hellman key exchange, which allows parties to establish a shared secret key over an insecure channel.

6. Security Considerations:

   - Key Management: Proper key management practices, including key generation, distribution, storage, and revocation, are crucial for the security of public-key cryptosystems.
   - Key Sizes: The security of public-key cryptosystems depends on the size of the keys used. Larger key sizes provide stronger security but may impact performance.
   - Algorithm Selection: Choosing secure and widely-accepted cryptographic algorithms, such as RSA, ECC, or ElGamal, is essential to ensure the security and interoperability of public-key cryptosystems.

Result:

RSA private key

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

Title : Design and Implementation of RSA algorithm for generating public and private key

Roll No: 21102A0014

Plaintext (string):

deep

encrypt

Ciphertext (hex):

```
542132f674bb35f26f56282e21331596837b8cb41c2edacd2439f682cd77011f
17b2eebb8eb10baa4cbad7def3563fe6dab3d0880fdb1f131762d0b96cee9819
c2fec8984a56ceb3f7e1e436df6aa3001621e0b2f507e3c948cea1c91691841b
368e37b408a581b7111379dc6e1f2c0c3afc6a7908688316cc00f32e3139bd3f
```

decrypt

Decrypted Plaintext (string):

deep

Status:

Decryption Time: 6ms

Conclusion:

By understanding these theoretical aspects of public-key cryptosystems, students can gain insights into their principles, functionalities, and applications in cryptography and system security. Lab exercises can involve implementing encryption, decryption, digital signature generation and verification, key exchange protocols, and exploring real-world use cases to reinforce learning and understanding.