Name: Aman Singh
Batch : T23 Roll No: 128

Experiment No 3

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

Lab Outcome :

LO2 : Demonstrate Key management, distribution and user authentication.

Theory :

1. Explain the steps of RSA key generation?

RSA (Rivest-Shamir-Adleman) is a widely used asymmetric cryptographic algorithm that relies on a pair of keys: a public key and a private key. RSA key generation involves a series of steps that ensure secure communication and data encryption. Below, I'll provide a detailed explanation of the key generation process:

1. Choosing Prime Numbers (p and q): The first step in RSA key generation is to select two distinct prime numbers, usually denoted as p and q. These prime numbers are critical to the security of the algorithm. They need to be large and chosen randomly to prevent attackers from factoring the modulus and breaking the encryption.

2. Calculating Modulus (n): The modulus (n) is computed as the product of the two prime numbers: n = p * q. The modulus is used in both the public and private keys. It provides the size of the "space" in which the encryption operates, making the encryption stronger with larger values of n.

3. Calculating Euler's Totient Function (φ(n)): Euler's totient function (φ(n)) is calculated as φ(n) = (p - 1) * (q - 1). This function is crucial for ensuring that the public and private keys are relatively prime. φ(n) represents the count of numbers less than n that are coprime to n.

4. Selecting Public Exponent (e): The public exponent (e) is a small odd integer that is coprime to φ(n). A common choice for e is 65537 (2^16 + 1). This choice of e provides good security properties while ensuring efficient encryption and decryption operations.

5. Calculating Private Exponent (d): The private exponent (d) is computed as the modular multiplicative inverse of e modulo φ(n). In other words, it satisfies the equation (e * d) % φ(n) = 1. The private exponent d is what allows the decryption of messages encrypted with the public key.

Name: Aman Singh
Batch : T23 Roll No: 128

6. Public Key Generation: The public key consists of the pair (e, n). It is distributed to anyone who wishes to send an encrypted message to the key owner. The public key is used for encrypting messages, ensuring only the private key holder can decrypt them.

7. Private Key Generation: The private key consists of the pair (d, n). This key must be kept secret and secure. The private key is used for decrypting messages encrypted with the corresponding public key. Losing the private key could compromise the security of encrypted communications.

The RSA key generation process is fundamental to the security and effectiveness of RSA encryption. It leverages the mathematical properties of prime numbers and modular arithmetic to create a secure communication channel between parties. The strength of RSA lies in the difficulty of factoring large semiprime numbers (the product of two large prime numbers), which makes it practically impossible for attackers to deduce the private key from the public key.

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

Digital signatures play a crucial role in ensuring data integrity, authenticity, and nonrepudiation in the digital world. They provide a way to verify that a digital document or message was indeed generated by a specific sender and has not been tampered with during transmission. The process involves two main steps: digital signature generation and digital signature verification.

Digital Signature Generation:

1. Hashing the Message: The sender begins by creating a cryptographic hash of the message they want to sign. A hash function, such as SHA-256, is used to produce a fixed-size digest that uniquely represents the content of the message.

2. Private Key Encryption: The sender then encrypts the hash value using their private key. This encrypted hash forms the digital signature. The use of the private key ensures that only the sender, who possesses the corresponding private key, can create the signature.

3. Attaching the Signature: The encrypted hash (digital signature) is attached to the original message. This combination forms the digitally signed message. Any alteration to the message will result in a different hash, making it evident that the message has been tampered with.

Digital Signature Verification:

Name: Aman Singh
Batch : T23 Roll No: 128

1. Hashing the Received Message: The recipient of the digitally signed message starts by computing the hash value of the received message using the same hash function as the sender. This generates a digest that represents the content of the received message.

2. Public Key Decryption: The recipient then decrypts the digital signature using the sender's public key. This process yields the original hash value that the sender encrypted using their private key during the signature generation.

3. Comparing Hashes: The recipient compares the decrypted hash value with the hash value they calculated from the received message. If the two hash values match, it indicates that the message has not been tampered with and that the signature is valid. A mismatch suggests either tampering or the use of an incorrect signature.

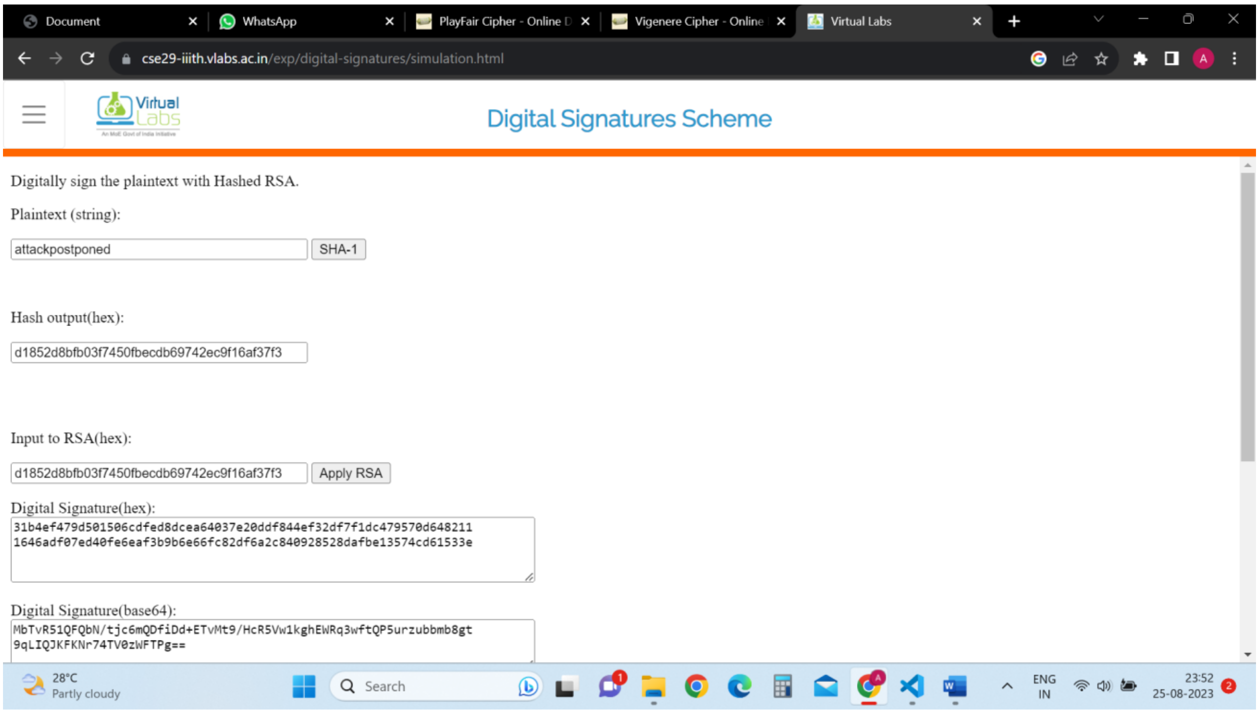
Benefits and Security:

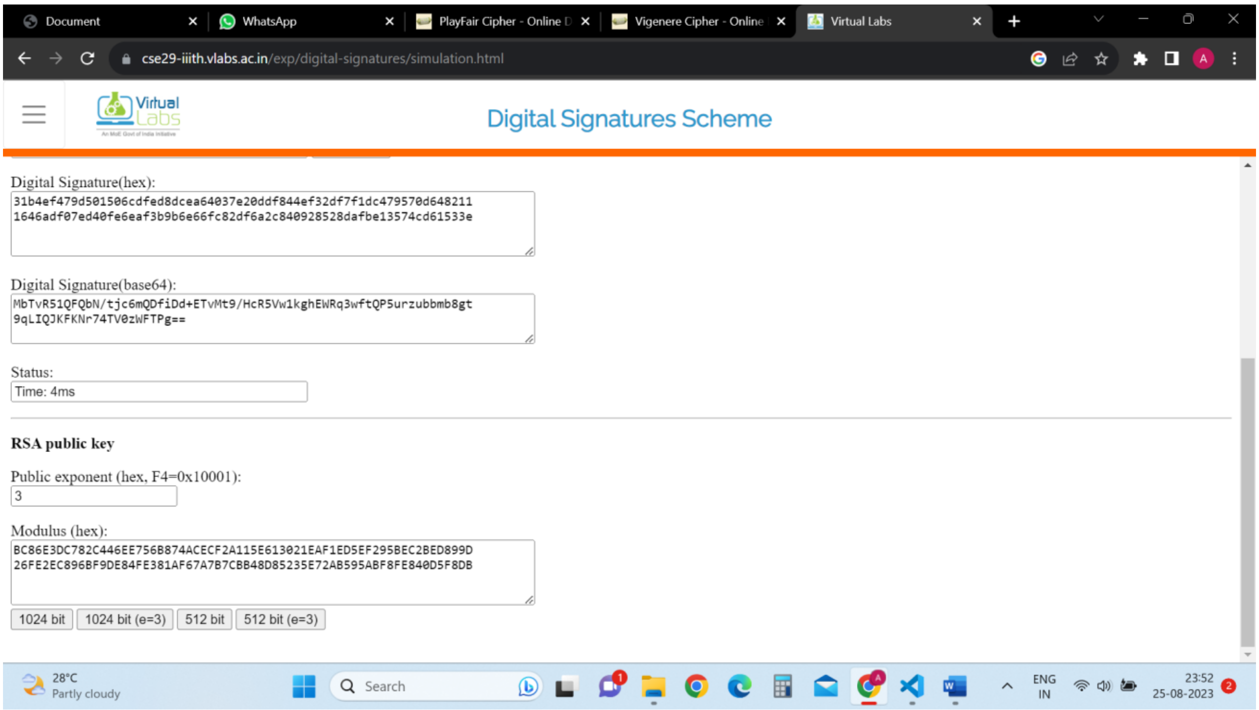
The digital signature process provides several benefits:
- Data Integrity: Any alteration to the message or document will lead to a mismatch between the computed hash and the decrypted hash in the signature.
- Authenticity: The use of the sender's private key ensures that only the sender could have created the signature.
- Non-Repudiation: The sender cannot deny having sent the digitally signed message since the signature is tied to their private key.

Output:

Name: Aman Singh
Batch : T23 Roll No: 128

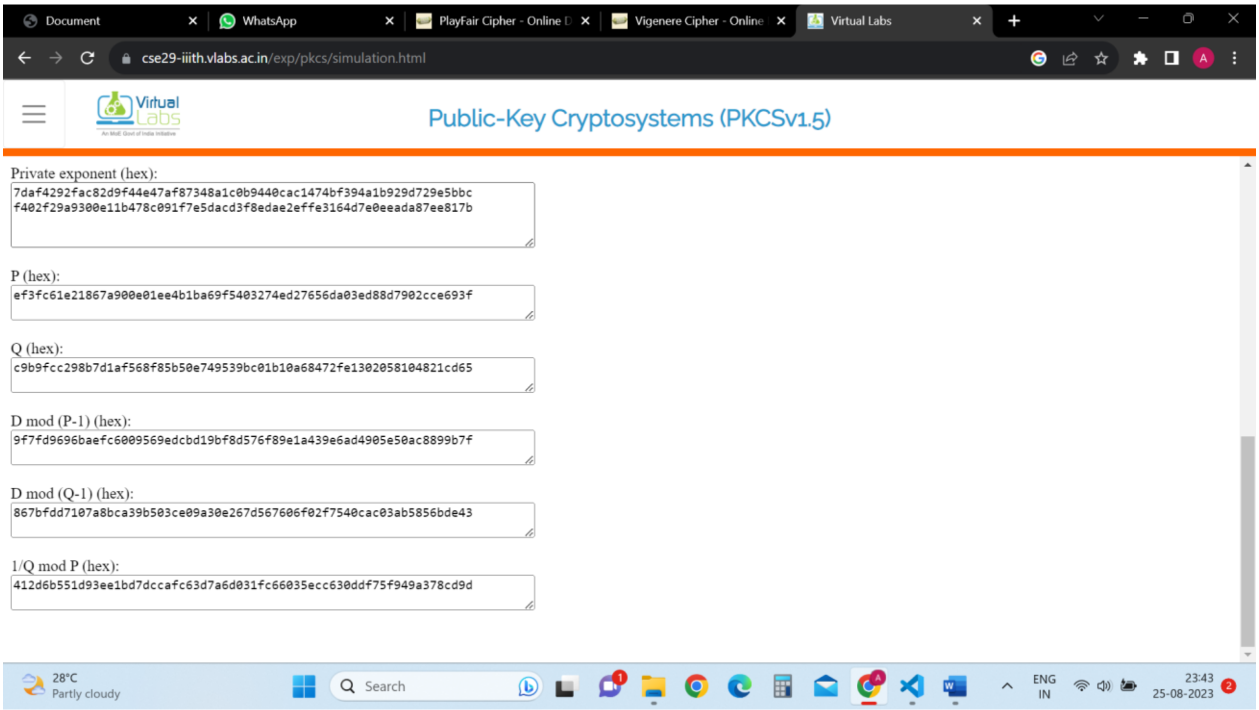
Digital Signature:

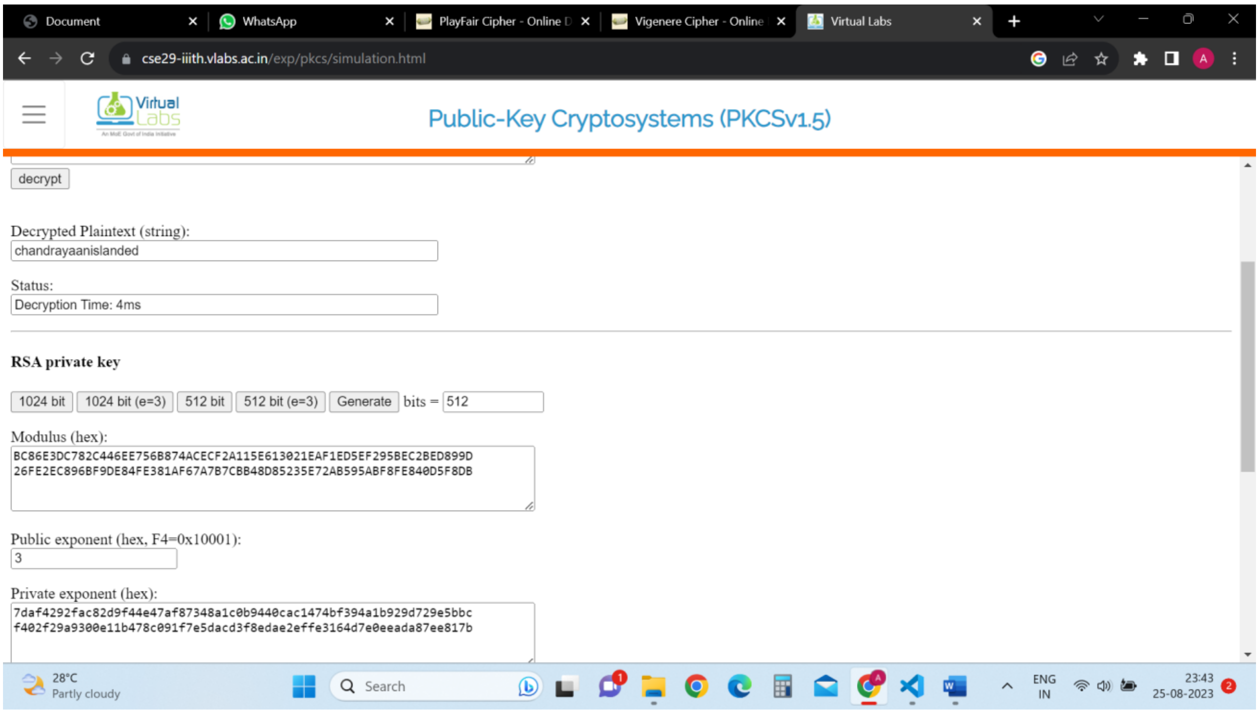




Name: Aman Singh
Batch : T23 Roll No: 128

RSA key generation and decode





Name: Aman Singh
Batch : T23 Roll No: 128

Conclusion:

Learnt about RSA scheme and RSA cryptosystem , explored steps involved in digital key generation and verification , generated and verified digital signature using software and also implemented RSA scheme.

Name: Aman Singh
Batch : T23 Roll No: 128