Name: Harsh Mishra
Roll no: 64
Batch: T21

Aim : To implement and analyze RSA cryptosystem and Digital signature scheme using RSA.

Theory :

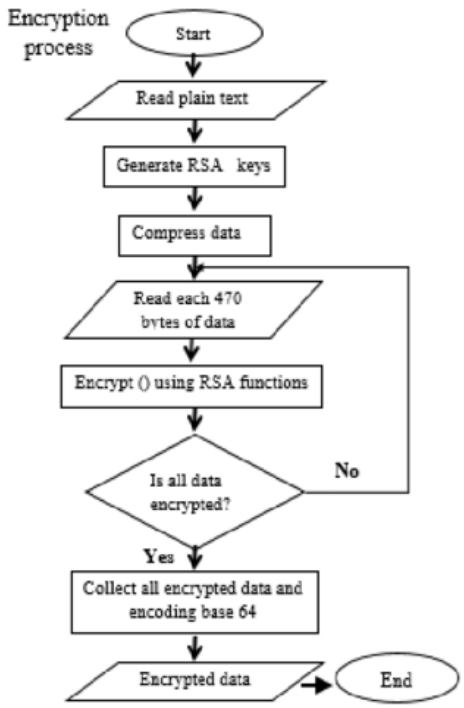
RSA and digital signatures are crucial elements in modern cybersecurity. RSA, a widely used encryption algorithm, ensures secure data transmission by encrypting and decrypting information. Digital signatures, on the other hand, authenticate the identity of the sender and guarantee the integrity of the message. Together, RSA and digital signatures provide a robust framework for secure communication, protecting sensitive data from unauthorized access and ensuring that messages are not tampered with during transmission.

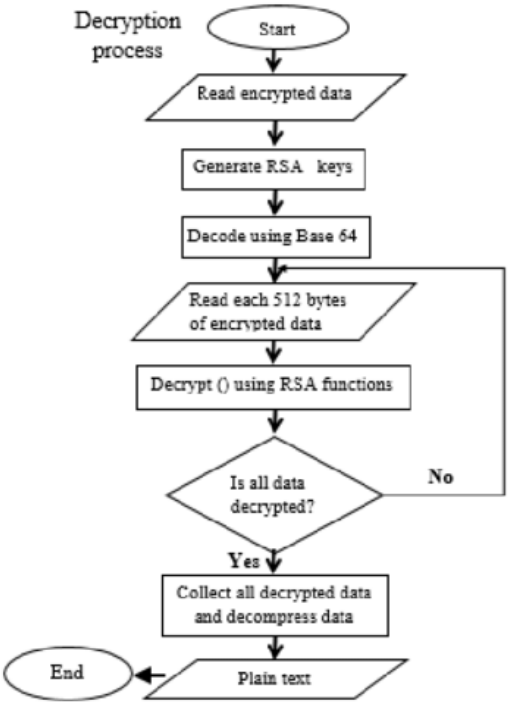
These technologies are essential in various applications, from online banking to secure email communication, making them vital components in the digital world. In this article, we will learn about the RSA signature scheme, Attacks on the RSA Digital Signature Scheme, and the steps of digital signature process creation.

What is RSA?

It is the most popular asymmetric cryptographic algorithm. It is primarily used for encrypting messages but can also be used for performing digital signatures over a message. RSA is a widely used encryption algorithm that ensures secure data transmission by encrypting and decrypting information. It relies on a pair of keys, a public key for encryption and a private key for decryption, to protect sensitive data from unauthorized access. RSA is essential in many applications, such as online banking and secure email communication, providing a robust framework for secure interactions in the digital world.

Name: Harsh Mishra
Roll no: 64
Batch: T21





What is Digital Signature?

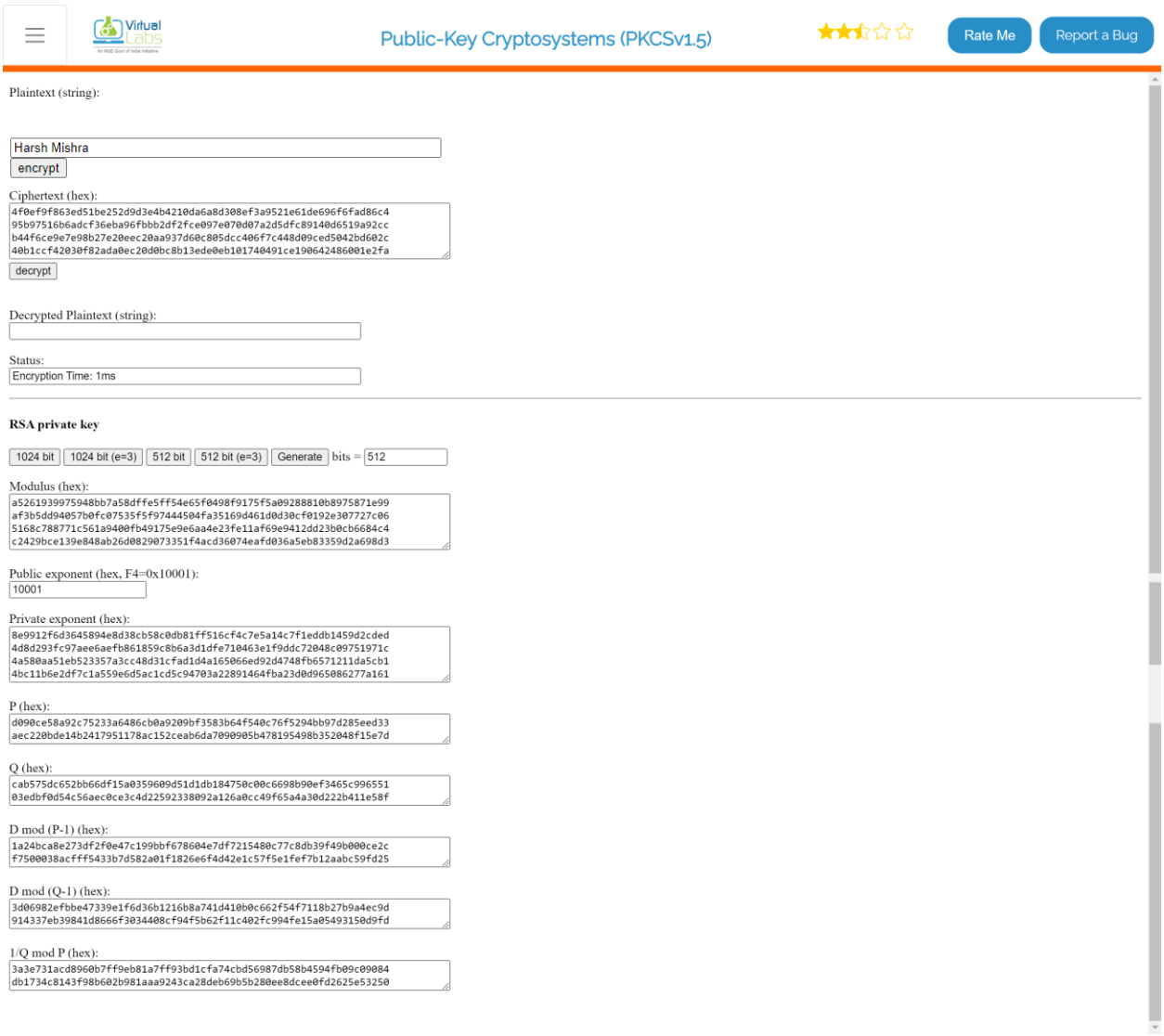
As the name sounds are the new alternative to signing a document digitally. It ensures that the message is sent by the intended user without any tampering by any third party (attacker). In simple words, digital signatures are used to verify the authenticity of the message sent electronically.

Digital signatures authenticate the identity of the sender and guarantee the integrity of the message. By using a private key to create a unique signature and a public key to verify it, digital signatures ensure that messages are not tampered with during transmission. This technology is vital for ensuring trust and security in various online transactions and communications, making it an indispensable tool in modern cybersecurity.

Output:

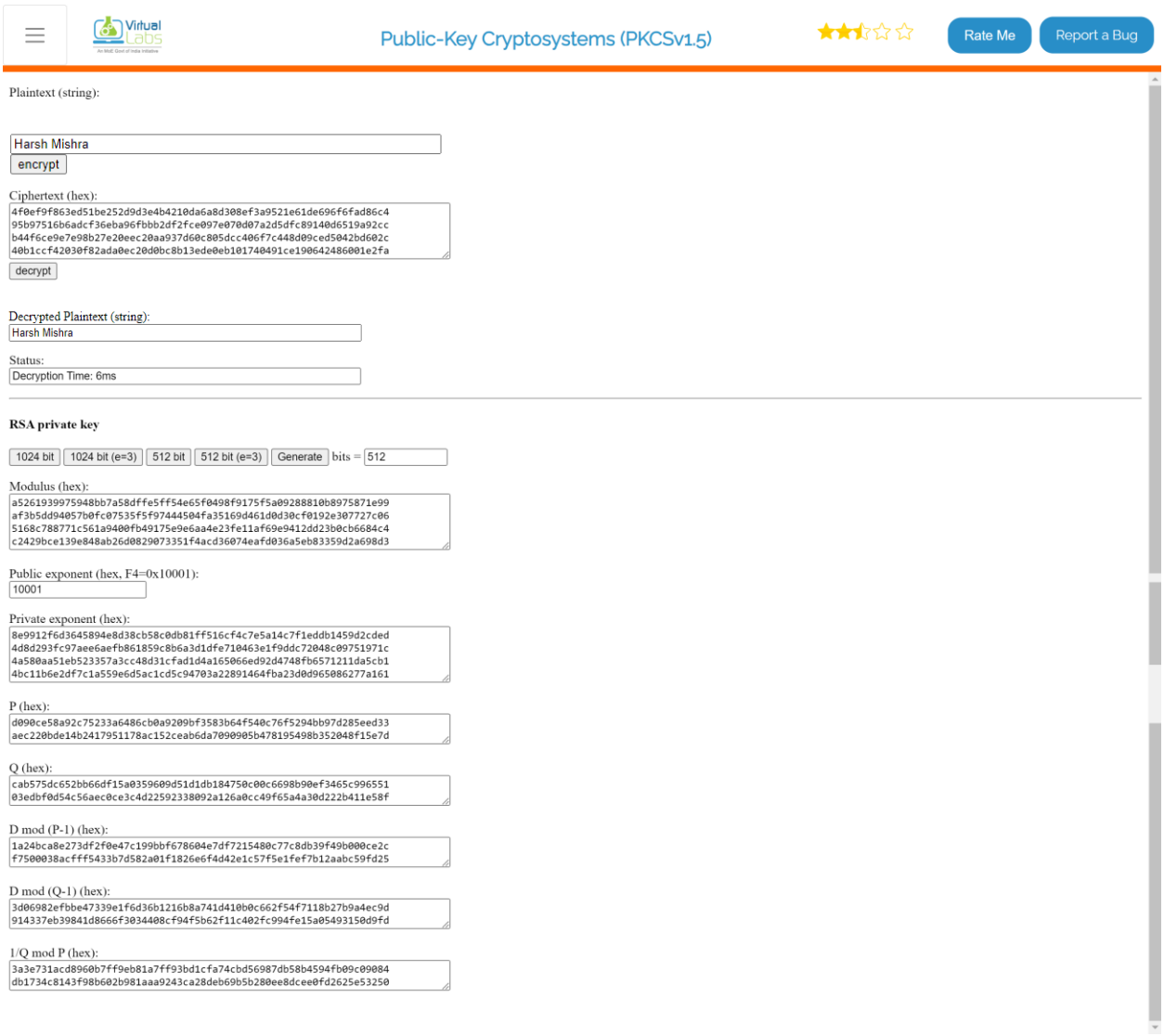
Encryption:

Name: Harsh Mishra
Roll no: 64
Batch: T21



Decryption:

Name: Harsh Mishra
Roll no: 64
Batch: T21



Conclusion: Demonstrated key management, distribution and user authentication (LO2 is achieved).