Roll No: 09
Name: Shreya Bagade
Date: 28/07/2023

LAB ASSIGNMENT NO:04

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

Lab Outcome Attained: Demonstrate Key management, distribution and user authentication.

Theory:

Explain the steps of RSA key generation.

RSA is a cryptosystem for public-key encryption, and is broadly used for securing responsive information, specifically when being sent over an insecure network including the Internet.

In RSA cryptography, both the public and the private keys can encrypt a message; the inverse key from the one used to encrypt a message is used to decrypt it. This attribute is one reason why RSA has developed into the most broadly used asymmetric algorithm. It supports an approach of assuring the confidentiality, integrity, authenticity and non-reputability of digital connection and data storage.

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 $d = e^{-1} \mod \phi(n)$
- Public Key = [e, n]
- Private Key = [d, n]

Roll No: 09
Name: Shreya Bagade
Date: 28/07/2023

Explain the steps of Digital signature generation and verification process.

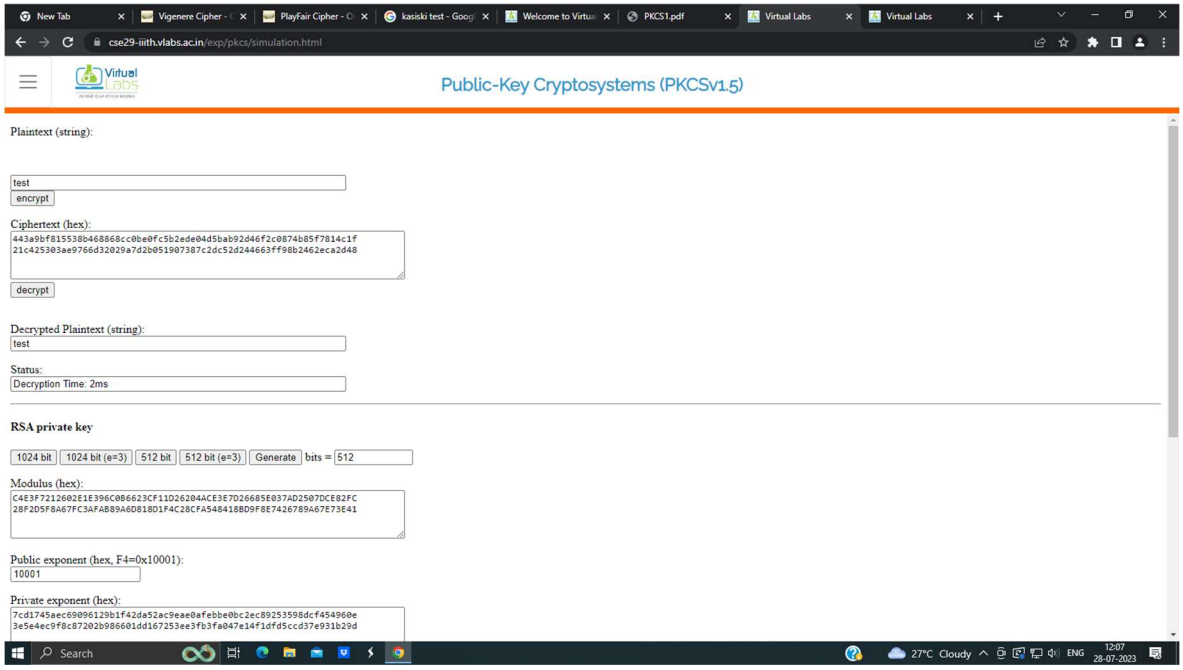
Digital signatures are the public-key primitives of message authentication. In the physical world, it is common to use handwritten signatures on handwritten or typed messages. They are used to bind signatory to the message.

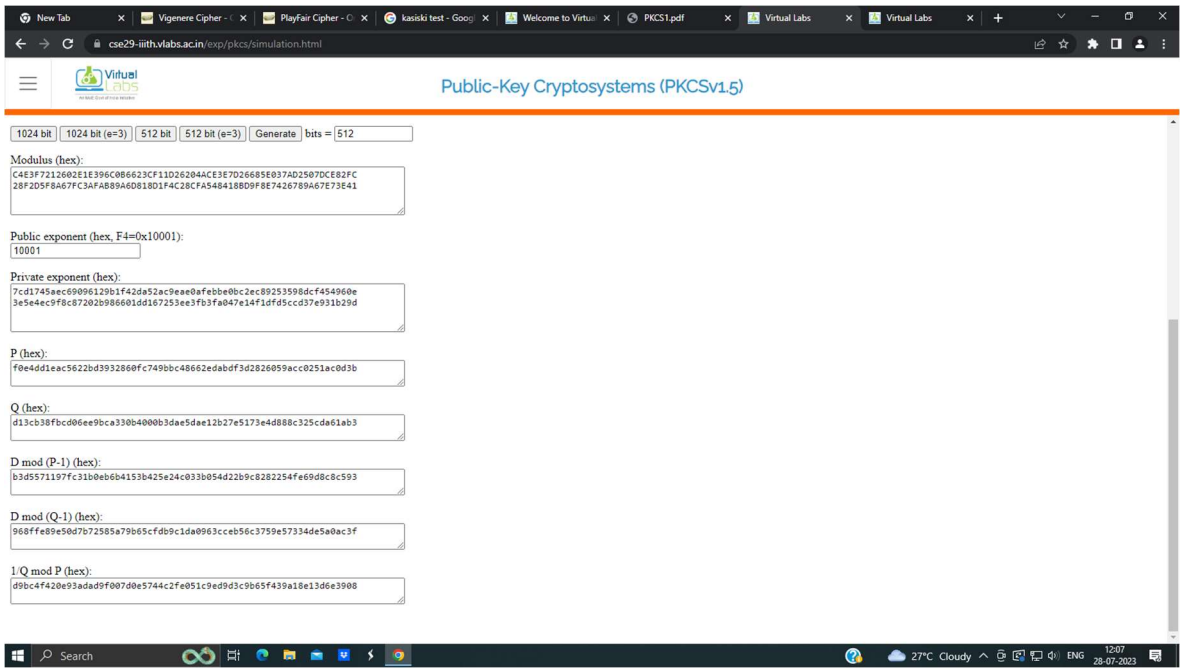
The steps followed in creating digital signature are**:**

1. Message digest is computed by applying hash function on the message and then message digest is encrypted using private key of sender to form the digital signature. (digital signature = encryption (private key of sender, message digest) and message digest = message digest algorithm(message)).
2. Digital signature is then transmitted with the message.(message + digital signature is transmitted)
3. Receiver decrypts the digital signature using the public key of sender.(This assures authenticity, as only sender has his private key so only sender can encrypt using his private key which can thus be decrypted by sender's public key).
4. The receiver now has the message digest.
5. The receiver can compute the message digest from the message (actual message is sent with the digital signature).
6. The message digest computed by receiver and the message digest (got by decryption on digital signature) need to be same for ensuring integrity.

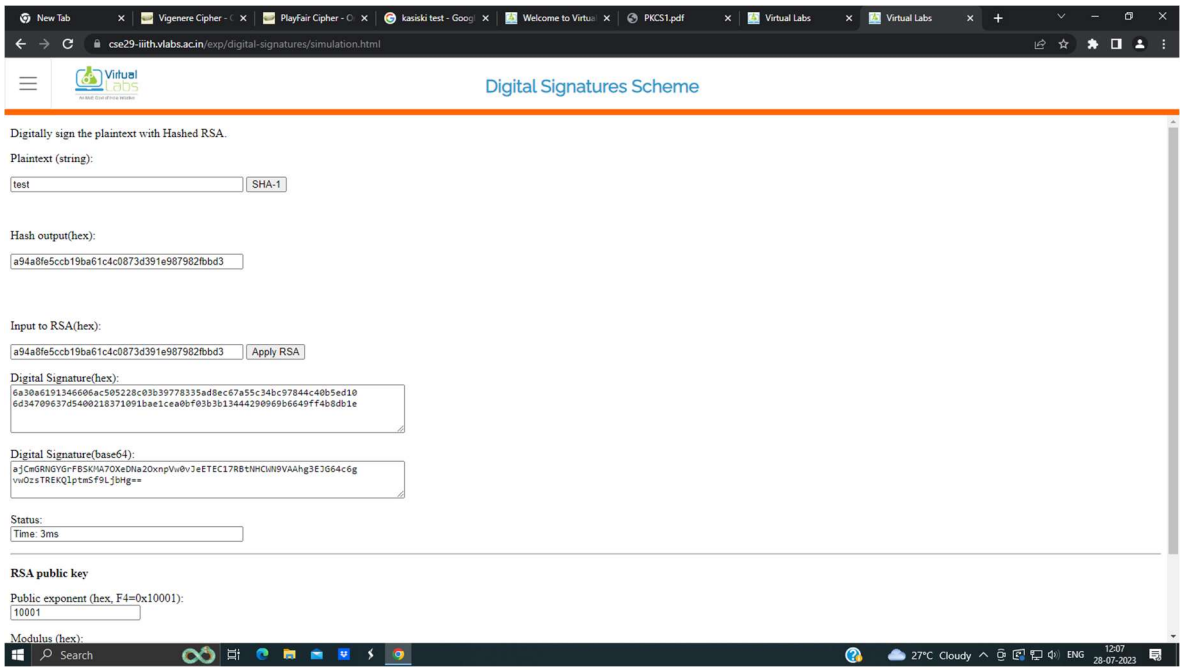
Roll No: 09
Name: Shreya Bagade
Date: 28/07/2023

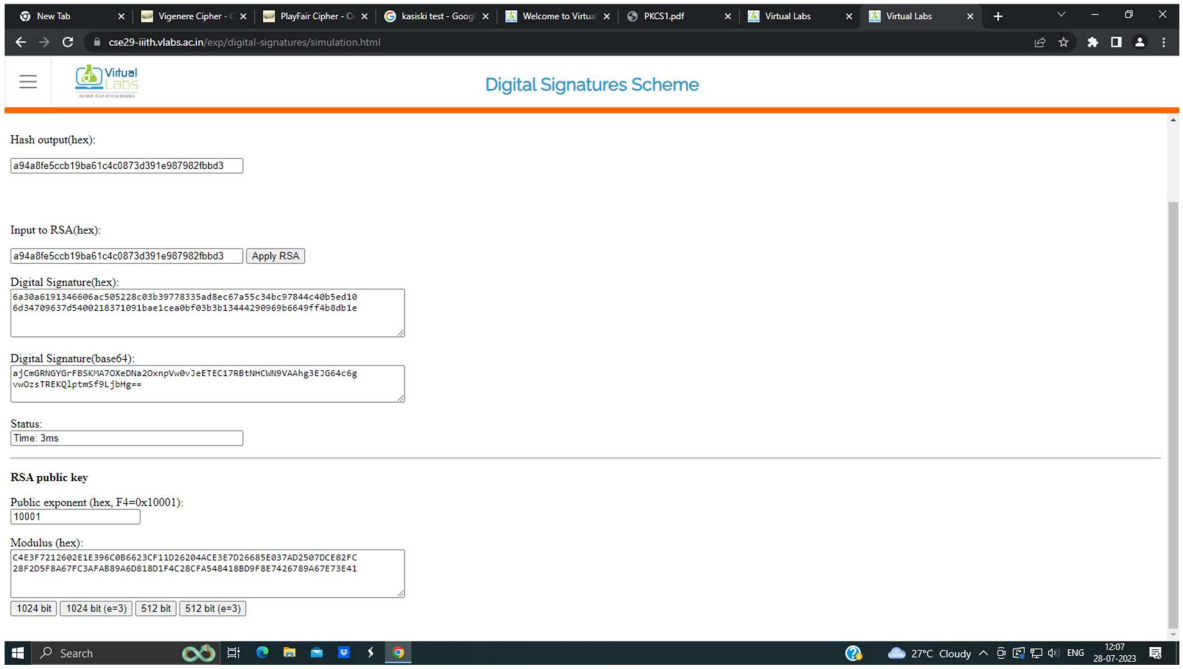
Output Screenshots:





Roll No: 09
Name: Shreya Bagade
Date: 28/07/2023





Roll No: 09
Name: Shreya Bagade
Date: 28/07/2023

Conclusion: We learnt that both RSA encryption and digital signatures offer strong security measures for protecting sensitive data and verifying the legitimacy of digital interactions. The RSA algorithm leverages the mathematical complexity of factoring large prime numbers to create a pair of keys for secure encryption and decryption. Digital signatures, on the other hand, provide a means of ensuring the integrity and authenticity of digital messages.