Batch: A3	**Roll No.: 16010121045**
Experiment No.	

Title: study and Generation of Digital signatures using virtual labs

Objective:

Expected Outcome of Experiment:

CO	Outcome
CO3	Comprehend cryptographic hash functions, Message Authentication Codes and Digital Signatures for Authentication

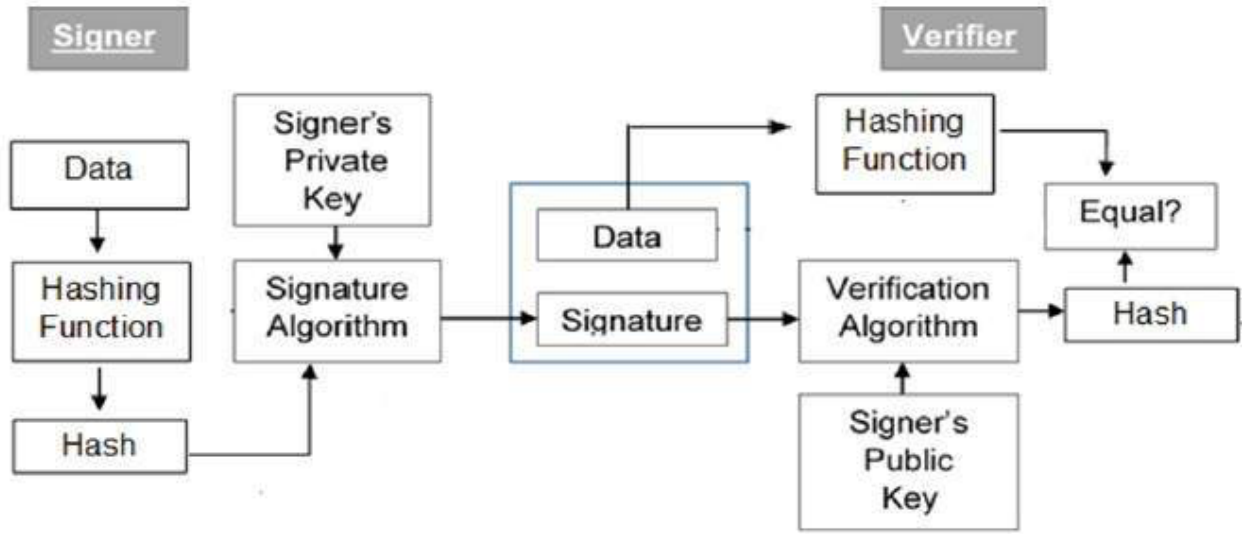
Books/ Journals/ Websites referred:

1. https://www.ques10.com/p/33840/rsa-digital-signature-scheme-1/
2. https://cse29-iiith.vlabs.ac.in/exp/digital-signatures/simulation.html

Abstract:-
(Digital signatures, Digital certificates)

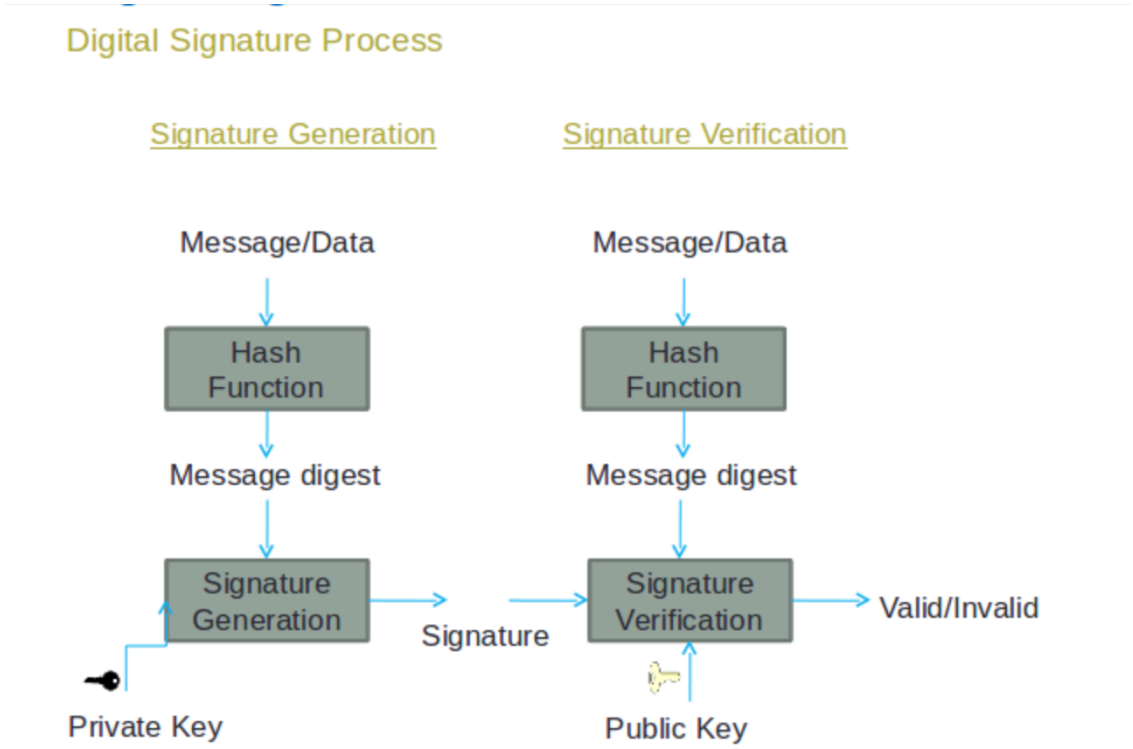
Related Theory: -

Digital signature model



(image source: https://www.tutorialspoint.com/cryptography/cryptography_digital_signatures.htm)

Digital signature process-



Virtual lab screenshots:

Digitally sign the plaintext with Hashed RSA.

Plaintext (string):

This is a plaintext SHA-1

Hash output(hex):

f80f7adecb79b142adf664b84b6446ac4782c7a

Input to RSA(hex):

f80f7adecb79b142adf664b84b6446ac4782c7a Apply RSA

Digital Signature(hex):

```
0995d9a0c54023de264d27f741914e6734f716c447914cc2823e32a9a3adce12
1a729ad7bbdfdd1831192d9b85a39c4772fe56a4e4df2a526a81d1b909bb1d8f
7e109125fd5c892d72f78016e50a54848177d3b9c46aa6ba3c2b08139b261e43
0771db9044580e71d39e84f8aff68d4e8299456ad14571e49def036e7584e2ac
```

Digital Signature(base64):

```
CZXZoMVAI94mTSf3QZFOZzT3FsRHkUzCgj4yqaOtzhIacprXu9/dGDEZLZuFo5xH
cv5WpOTfKlJqgdG5Cbsdj34QkSX9XIktcveAFuUKVISBd9O5xGqmujwrCBObJh5D
B3HbkERYDnHTnoT4r/aNToKZRWrRRXHkne8DbnWE4qw=
```

Status:

Time: 10ms

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)

Assignment:

1. Digital signature can't provide _____ for the message

   (a) Integrity
   (b) Confidentiality
   (c) Non repudiation
   (d) Authentication

2. Digital signature uses _____ for generating valid signature
   (a) Private key
   (b) Public key
   (c) Secret key
   (d) None of the above

3. Verification Algorithm uses _____ for validating digital signature
   (a) Private key
   (b) Public key
   (c) Secret key
   (d) None of the above

4. Is digital signature scheme possible without public key cryptography

   (a) Yes
   (b) No
   (c) May be exist
   (d) None of the above

5. Explain importance of Hashing(using experiment)and explain why Hashing is needed ?

   - Hashing gives a more secure and adjustable method of retrieving data compared to any other data structure. It is quicker than searching for lists and arrays. In the very range, Hashing can recover data in 1.5 probes, anything that is saved in a tree. Hashing, unlike other data structures, doesn't define the speed. A balance between time and space has to be

maintained while hashing. There are two ways of maintaining this balance.

- Controlling speed by selecting the space to be allocated for the hash table
- Controlling space by choosing a speed of recovery
- Hashed passwords cannot be modified, stolen, or jeopardized. No well-recognized and efficient key or encryption scheme exists that can be misused. Also, there is no need to worry if a hash code is stolen since it cannot be applied anywhere else.
- Two files can be compared for equality easily through hashing. There is no need to open the two documents individually. Hashing compares them word-by-word and the computed hash value instantly tells if they are distinct. This advantage can be used for the verification of a file after it has been shifted to a new place. It is an example of SyncBack which is a file backup program.

- In DBMS, hashing is used to search the location of the data without using index structure. This method is faster to search using the short hashed key instead of the original value.

Need for hashing

- Password Verification
- Compiler Operation
- Rabin-Karp Algorithm
- Data Structures
- Message Digest

6. Suggest a scheme that does not use any hashing scheme.

Key wrapping is a separate algorithm and not an application of hash fuctions.

RSA typically refers to a public-key cryptosystem which is widely used for secure data transmission. It uses paired keys where one is used to encrypt messages and the other to decrypt them. RSA is therefore not a hash function. That said, algorithms that use RSA crypto keys often use hashes to sign messages.

7. Explain why digital signature schemes works ?

   Digital signatures work by verifying that a digital message or file was not altered during transmission. They accomplish this by calculating a hash value (a number) based on the data being transmitted. The hash value is encrypted using the recipient's public key. When the receiver decrypts the hash value using his private key, he can verify that the original message hasn't been tampered with.