**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:**

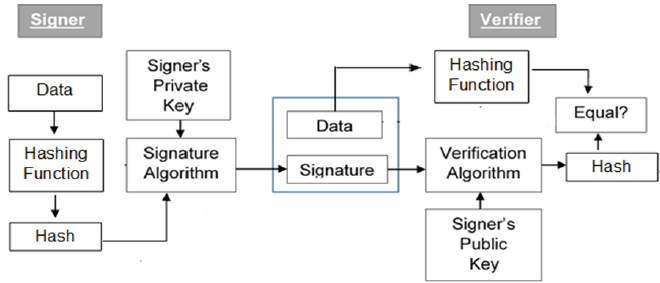
1. [**https://www.ques10.com/p/33840/rsa-digital-signature-scheme-1/**](https://www.ques10.com/p/33840/rsa-digital-signature-scheme-1/)
2. [**https://cse29-iiith.vlabs.ac.in/exp/digital-signatures/simulation.html**](https://cse29-iiith.vlabs.ac.in/exp/digital-signatures/simulation.html)

**Abstract**:-

*(Digital signatures, Digital certificates)*

**Related Theory: -**

**Digital signature model**



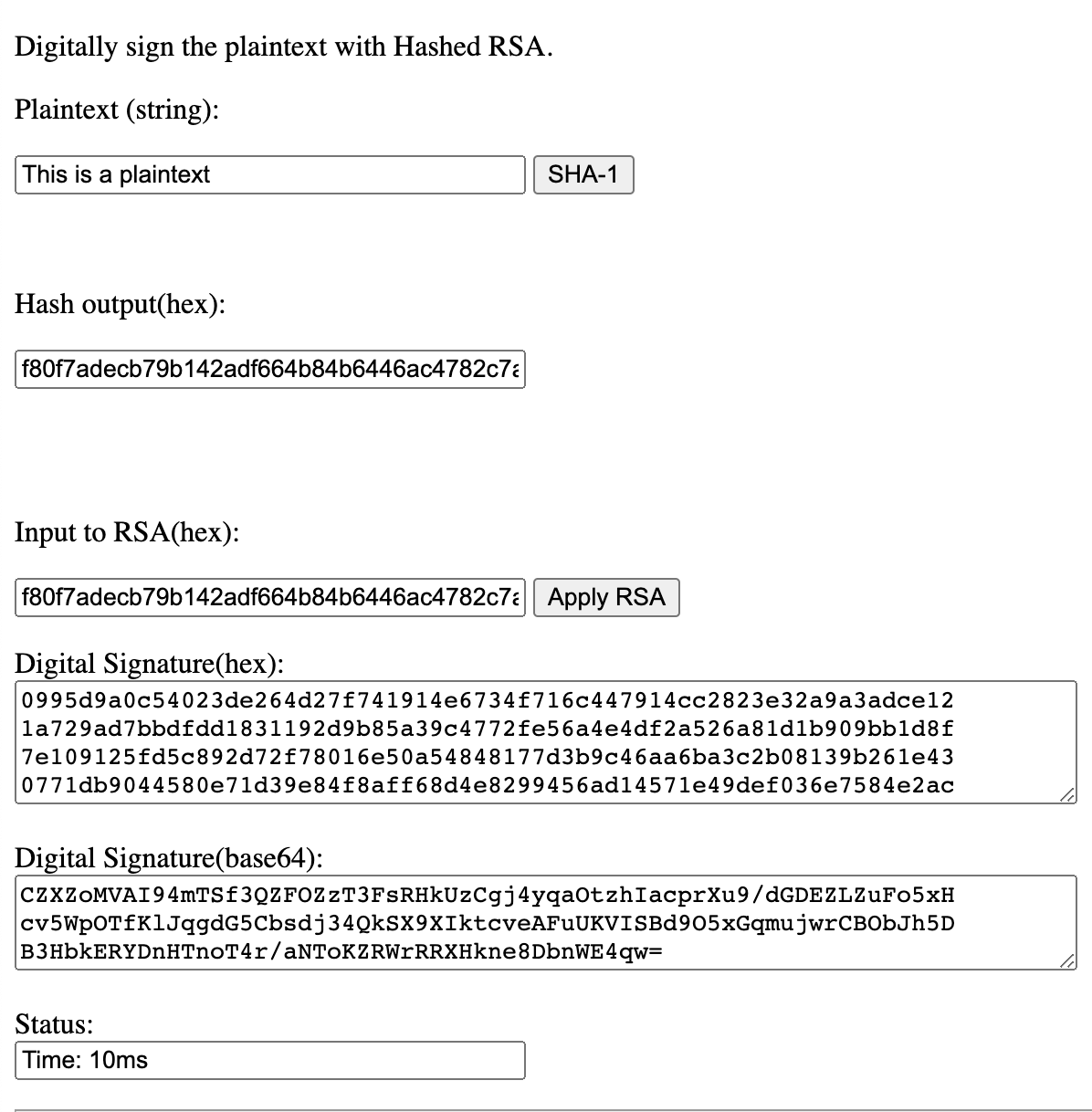
(image source: <https://www.tutorialspoint.com/cryptography/cryptography_digital_signatures.htm>)

**Digital signature process-**

**Diagram

Description automatically generated**

**Virtual lab screenshots:**

Graphical user interface, text, application, email

Description automatically generated

**Assignment:**

1. Digital signature can't provide \_\_\_\_\_\_ for the message

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

1. Digital signature uses \_\_\_\_\_\_ for generating valid signature  
   (a) Private key  
   (b) Public key  
   (c) Secret key  
   (d) None of the above
2. Verification Algorithm uses \_\_\_\_\_\_ for validating digital signature  
   (a) Private key  
   (b) Public key  
   (c) Secret key  
   (d) None of the above
3. Is digital signature scheme possible without public key cryptography

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

1. 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

1. 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.

1. 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.