**PRACTICAL 8**

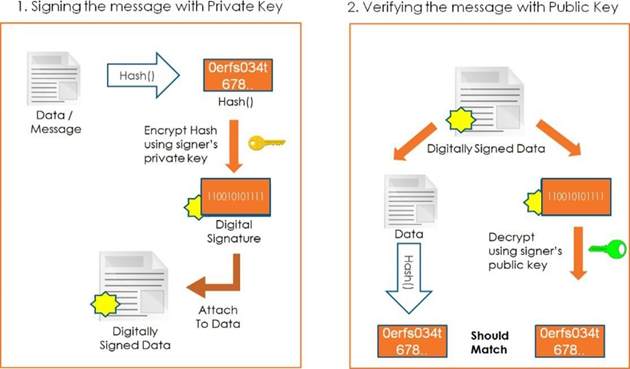
**Aim:** A digital signature is a mathematical scheme for presenting the authenticity of digital messages or documents. A valid digital signature gives a recipient reason to believe that

•The message was created by a claimed sender (authentication),

•The sender cannot deny having sent the message (non-repudiation),

•The message was not altered in transit (integrity).

Practical Lab Set-up:



**Theory:**

A digital signature is a mathematical approach for verifying the integrity and validity of a message, software, or digital document. It's the digital counterpart of a handwritten signature or a stamped seal, but it has a lot more security built in. The purpose of a digital signature is to prevent tampering and impersonation in digital communications.

Electronic papers, transactions, and digital messages can all benefit from digital signatures as proof of origin, identity, and status. They can also be used to affirm informed permission by signers.

Digital signatures are legally binding in many nations, including the United States, in the same way that traditional handwritten document signatures are.

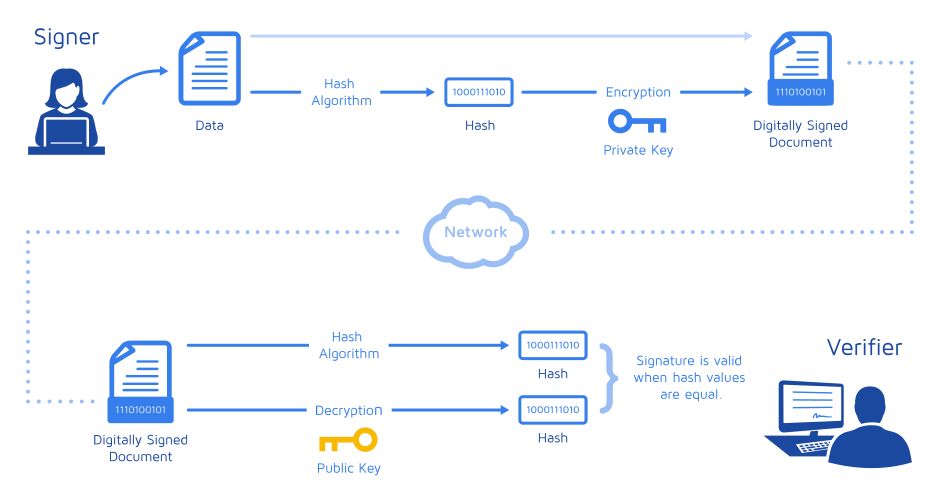
* **What are digital signatures and how do they work?**

Public key cryptography, often known as asymmetric cryptography, is used to create digital signatures. Two keys are produced using a public key algorithm like RSA (Rivest-Shamir-Adleman), resulting in a mathematically connected pair of keys, one private and one public.

The two mutually authenticating cryptographic keys of public key cryptography are used to create digital signatures. The person who makes the digital signature encrypts signature-related data with a private key, which can only be decrypted with the signer's public key.

If the recipient can't open the document using the signer's public key, there's a problem with the signature or the document. Digital signatures are verified in this way.

All parties must trust that the person who creates the signature has kept the private key secret in order for digital signature technology to work. If someone else has access to the private signing key, they could use it to make forged digital signatures in the owner's name.

****

* **What are the advantages of electronic signatures?**

The main advantage of digital signatures is security. Digital signatures have security features that ensure a document is not tampered with and signatures are genuine. The following are some of the security elements and approaches utilised in digital signatures:

* PINs, passwords, and codes are all examples of personal identification numbers (PINs). Used to identify and verify the identity of a signer, as well as to validate their signature. The most frequent methods are email, username, and password.
* Cryptography that is asymmetric. Employs a public key algorithm that encrypts and authenticates both private and public keys.
* Checksum. A long string of letters and numbers that reflects the total of a piece of digital data's accurate digits, which can be compared to detect faults or modifications. A checksum serves as a security measure.
* Check for redundancy on a cyclic basis (CRC). An error-detecting code and verification function that detects changes to raw data in digital networks and storage devices.
* Validation of the certificate authority (CA). By accepting, authenticating, issuing, and maintaining digital certificates, CAs function as trustworthy third parties and issue digital signatures. CAs are useful in preventing the creation of forged digital certificates.
* Validation of the trust service provider (TSP). A TSP is a person or legal organisation that performs digital signature validation on behalf of a corporation and provides signature validation results.
* **The following are some of the other advantages of employing digital signatures:**
* Timestamping. Timestamping is important where timing is critical, such as for stock trading, lottery ticket issuing, and legal procedures, because it provides the data and time of a digital signature.
* Internationally recognised and legally compliant. Vendor-generated keys are made and stored securely thanks to the public key infrastructure (PKI) standard. A rising number of countries are recognising digital signatures as legally binding due to the worldwide standard.
* Time is saved. Digital signatures make the time-consuming process of signing, storing, and exchanging physical documents much easier, allowing organisations to rapidly access and sign documents.
* Cost-cutting. Organizations can go paperless and save money on physical resources, as well as time, employees, and office space spent managing and transporting paper.
* Positive impact on the environment. Reducing paper consumption reduces both physical waste and the negative environmental impact of moving paper documents.
* Traceability. Digital signatures offer an audit trail, making it easier for businesses to maintain track of their internal records. There are fewer opportunities for a manual signee or record-keeper to make a mistake or misplace something now that everything is recorded and saved digitally.
* **What is the process for creating a digital signature?**
* Signing software, such as an email application, is used to produce a digital signature by providing a one-way hash of the electronic data to be signed.
* An algorithm generates a fixed-length string of letters and integers called a hash. The hash is then encrypted using the private key of the digital signature originator. The digital signature is comprised of the encrypted hash, as well as other information such as the hashing algorithm.
* Because a hash function can turn any input into a fixed-length result, which is usually significantly shorter, it is preferable to encrypt the hash rather than the full message or document. Hashing is much faster than signing, therefore this saves time.
* A hash's value is unique to the data it hashs. Any modification in the data, even a single character change, will result in a new value. This property allows others to decrypt the hash using the signer's public key to verify the data's integrity.
* It proves that the data hasn't changed since it was signed if the decrypted hash matches a second computed hash of the same data. If the two hashes don't match, the data has either been changed with and is now compromised, or the signature was made with a private key that doesn't match the public key supplied by the signer, resulting in an authentication problem.
* A digital signature can be used with any type of message, whether encrypted or not, to ensure that the sender's identity is verified and that the message was delivered intact. Because the digital signature is unique to both the document and the signer, it connects them together, it is difficult for the signer to deny having signed something. Nonrepudiation is the term for this characteristic.
* Digital signatures and digital certificates are not the same thing. A digital certificate is an electronic document that includes the issuing CA's digital signature. It connects a public key to a person or entity's identification and can be used to verify that a public key belongs to that person or entity.
* **Digital signature Working in Cryptography:**

Digital signature works in cryptography by utilizing these components:

* **Hash:** A hash is a fixed-length string of letter and numbers produced by a mathematical procedure and a large file. SHA-1 (Secure Hash Algorithm-1), SHA-2 and SHA-256 (Secure Hashing Algorithm-2 series, and MD5 (Message Digest 5) are some of the most prominent hashing algorithms in use today.
* **Asymmetric encryption:** Asymmetric encryption (also called public-key cryptography) happens to be a cryptographic approach that employs a key pair scheme. While the data can be encrypted using only one key, known as the public key, it can be decrypted using the other key, known as the private key.
* **Public key infrastructure (PKI):** It includes the standards, rules, systems, and people to facilitate the sharing of public keys and to validate the identity of entities or individuals.
* **Digital certificates:** Digital certificates are similar to driver’s licenses as they are used to identify the person who holds the certificate. A CA digitally signs digital certificates, which contain the individual’s or organization’s public key. The certificate might also include information about the organization, the individual, and the CA.
* **Certificate authority (CA):** The certificate authority is a third party that verifies a person’s identity. It does so by either generating a public/private key pair for them or correlates an existing key provided by that person. Once a person’s identification is verified, the CA issues a digital certificate. The digital certificate can be used to validate that person by public key.
* **PGP/OpenPGP:** PGP (Pretty Good Privacy), also known as OpenPGP, is used as a PKI alternative. PGP helps users “trust” other users by issuing signature certificates for people whose identities are verified.