Encrypting Msg with Sender's Private Key

CRYPTOGRAPHY DIGITAL SIGNATURES

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.

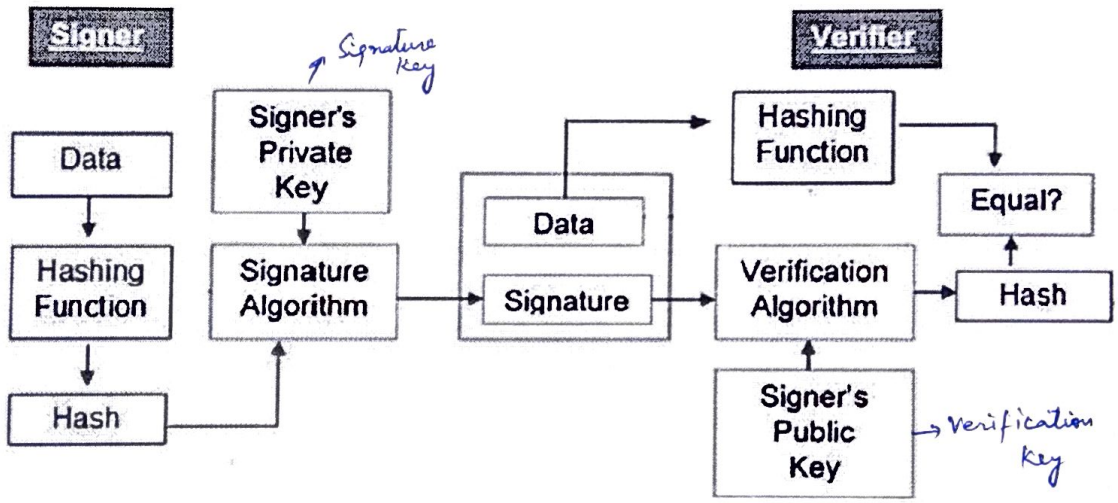
Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.

A *digital signature* uniquely identifies the originator of digitally signed data and also ensures the integrity of the signed data against tampering or corruption.

One possible method for creating a digital signature is for the originator of data to create the signature by encrypting all of the data with the originator's private key and enclosing the signature with the original data. Anyone with the originator's public key can decrypt the signature and compare the decrypted message to the original message. Because only someone with the private key can create the signature, the integrity of the message is verified when the decrypted message matches the original. If an intruder alters the original message during transit, the intruder cannot also create a new valid signature. If an intruder alters the signature during transit, the signature does not verify properly and is invalid.

Model of Digital Signature

As mentioned earlier, the digital signature scheme is based on public key cryptography. The model of digital signature scheme is depicted in the following illustration –



The following points explain the entire process in detail –

- Each person adopting this scheme has a public-private key pair.
- Generally, the key pairs used for encryption/decryption and signing/verifying are different.
  The private key used for signing is referred to as the signature key and the public key as the verification key.
- Signer feeds data to the hash function and generates hash of data.

- Hash value and signature key are then fed to the signature algorithm which produces the digital signature on given hash. Signature is appended to the data and then both are sent to the verifier.
- Verifier feeds the digital signature and the verification key into the verification algorithm. The verification algorithm gives some value as output.
- Verifier also runs same hash function on received data to generate hash value.
- For verification, this hash value and output of verification algorithm are compared. Based on the comparison result, verifier decides whether the digital signature is valid.
- Since digital signature is created by 'private' key of signer and no one else can have this key; the signer cannot repudiate signing the data in future.

Importance of Digital Signature

Out of all cryptographic primitives, the digital signature using public key cryptography is Considered as very important and useful tool to achieve information security.

Apart from ability to provide non-repudiation of message, the digital signature also provides Message authentication and data integrity. Let us briefly see how this is achieved by the digital signature –

a) **Message authentication** – When the verifier validates the digital signature using public key of a sender, he is assured that signature has been created only by sender who possess the corresponding secret private key and no one else.

b) **Data Integrity** – In case an attacker has access to the data and modifies it, the digital signature verification at receiver end fails. The hash of modified data and the output provided by the verification algorithm will not match. Hence, receiver can safely deny the message assuming that data integrity has been breached.

c) **Non-repudiation** – Since it is assumed that only the signer has the knowledge of the signature key, he can only create unique signature on a given data. Thus the receiver can present data and the digital signature to a third party as evidence if any dispute arises in the future.

By adding public-key encryption to digital signature scheme, we can create a cryptosystem that can provide the four essential elements of security namely – Privacy, Authentication, Integrity, and Non-repudiation.

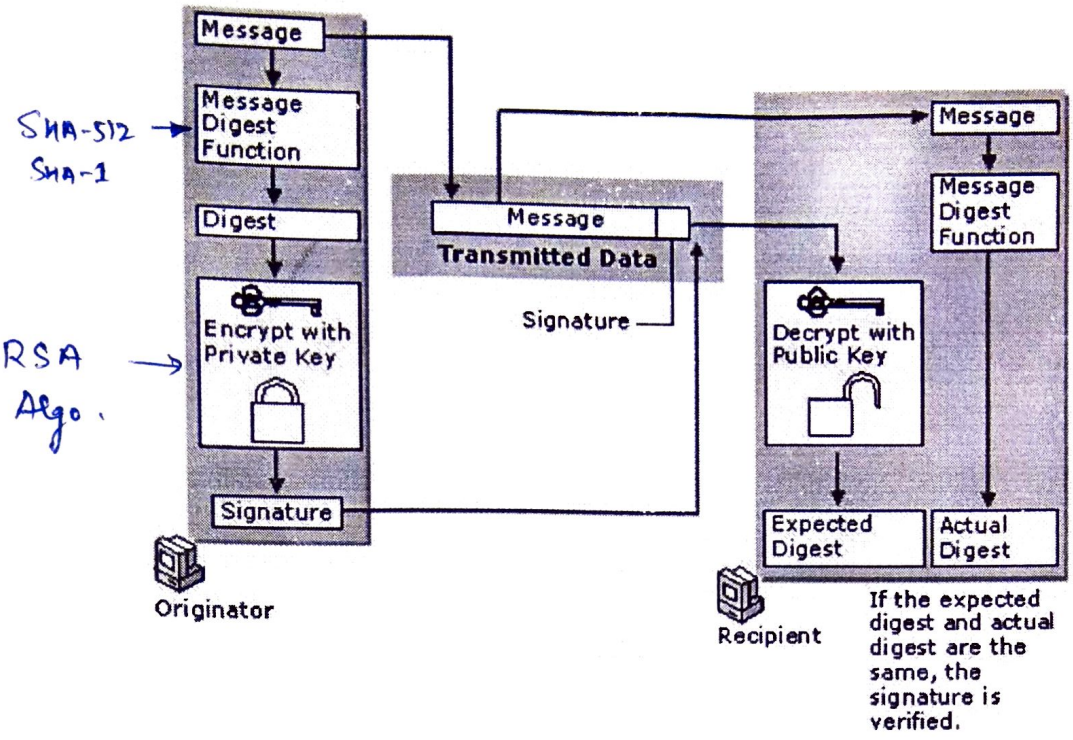
Two Approaches :→

(i) DS using RSA

(ii) DS using DSS/DSA.

RSA Data Security Digital Signature Process

In the RSA digital signature process, the private key is used to encrypt only the message digest. The encrypted message digest becomes the digital signature and is attached to the original data. Figure illustrates the basic RSA Data Security digital signature process.



To verify the contents of digitally signed data, the recipient generates a new message digest from the data that was received, decrypts the original message digest with the originator's public key, and compares the decrypted digest with the newly generated digest. If the two digests match, the integrity of the message is verified. The identity of the originator also is confirmed because the public key can decrypt only data that has been encrypted with the corresponding private key.

Digital Signature Security Standard

Another widely used technology for creating digital signatures is the Digital Signature Security Standard (DSS) that was developed by the National Security Agency and adopted by the United States government as its digital-signature standard. DSS defines the Digital Signature Algorithm (DSA), which functions in a manner similar to RSA. Although similar to RSA, DSA does not encrypt message digests with the private key or decrypt the message digest with the public key. Instead, DSA uses special mathematical functions to generate a digital signature composed of two 160-bit numbers that are derived from the message digest and the private key. DSA uses the public key to verify the signature, but the verification process is more complex than RSA.

The digital signature processes for DSA and RSA are generally considered to be of equal strength. However, DSA requires the use of the SHA-1 message digest function to ensure strong digital signatures. RSA can be used with other message digest functions (besides SHA-1) that might produce weaker digital signatures. Because the DSA signature verification process increases computer processor load significantly, relative to the verification process for RSA (all other conditions being equal), the RSA digital signature process generally provides better overall performance.

Because DSA is used only for digital signatures and makes no provisions for data encryption (for example, to provide secure secret key exchange), DSA is usually not subject to the export or import restrictions commonly imposed on RSA cryptography technology. Therefore, DSS digital signature technology can often be used when RSA digital signature technology cannot be used because of government-imposed export or import restrictions.

Uses for Digital Signatures

Anyone with the public key can use it to perform a validity check of digital signatures created by the private key. Only a digital signature created by the appropriate private key decrypts and validates properly with the public key. If a different private key was used to sign the data, the validity check fails. If the contents of digitally signed data or the digital signature have been tampered with or are corrupted, the validity check also fails. Valid digital signatures can be used to perform the following functions:

- Authenticate online entities.
- Verify the authorship or origin of digital data.
- Ensure the integrity of digital data against tampering.

Many security technologies use digital signatures. For example, Microsoft® Authenticode® can be used to digitally sign software programs, safeguarding them when they are distributed on the intranet or Internet to help counter the threat of software tampering and the spread of viruses and other malicious code. Likewise, the S/MIME protocol can be used to digitally sign e-mail messages to ensure the integrity of mail communications.