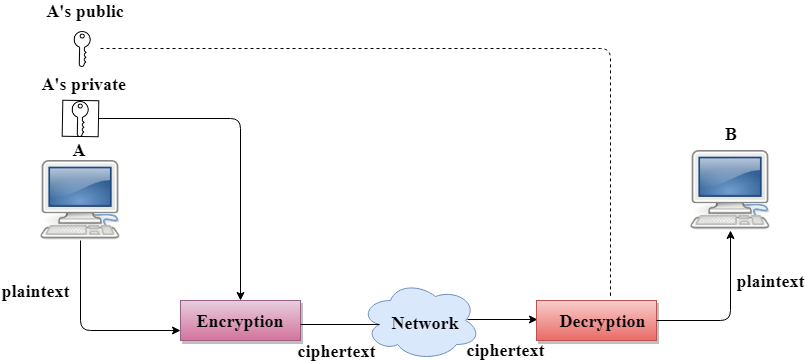
Digital Signature

The Digital Signature is a technique which is used to validate the authenticity and integrity of the message. We know that there are four aspects of security: privacy, authentication, integrity, and non-repudiation. We have already discussed the first aspect of security and other three aspects can be achieved by using a digital signature.

The basic idea behind the Digital Signature is to sign a document. When we send a document electronically, we can also sign it. We can sign a document in two ways: to sign a whole document and to sign a digest.

Signing the Whole Document

* In Digital Signature, a public key encryption technique is used to sign a document. However, the roles of a public key and private key are different here. The sender uses a private key to encrypt the message while the receiver uses the public key of the sender to decrypt the message.
* In Digital Signature, the private key is used for encryption while the public key is used for decryption.
* Digital Signature cannot be achieved by using secret key encryption.



Digital Signature is used to achieve the following three aspects:

* **Integrity:** The Digital Signature preserves the integrity of a message because, if any malicious attack intercepts a message and partially or totally changes it, then the decrypted message would be impossible.
* **Authentication:** We can use the following reasoning to show how the message is authenticated. If an intruder (user X) sends a message pretending that it is coming from someone else (user A), user X uses her own private key to encrypt the message. The message is decrypted by using the public key of user A. Therefore this makes the message unreadable. Encryption with X's private key and decryption with A's public key results in garbage value.
* **Non-Repudiation:** Digital Signature also provides non-repudiation. If the sender denies sending the message, then her private key corresponding to her public key is tested on the plaintext. If the decrypted message is the same as the original message, then we know that the sender has sent the message.

Note: Digital Signature does not provide privacy. If there is a need for privacy, then another layer of encryption/decryption is applied.

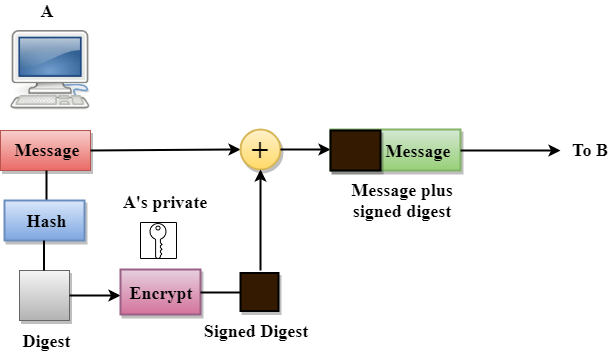
Signing the Digest

* Public key encryption is efficient if the message is short. If the message is long, a public key encryption is inefficient to use. The solution to this problem is to let the sender sign a digest of the document instead of the whole document.
* The sender creates a miniature version (digest) of the document and then signs it, the receiver checks the signature of the miniature version.
* The hash function is used to create a digest of the message. The hash function creates a fixed-size digest from the variable-length message.
* The two most common hash functions used: MD5 (Message Digest 5) and SHA-1 (Secure Hash Algorithm 1). The first one produces 120-bit digest while the second one produces a 160-bit digest.
* A hash function must have two properties to ensure the success:
  + First, the digest must be one way, i.e., the digest can only be created from the message but not vice versa.
  + Second, hashing is a one-to-one function, i.e., two messages should not create the same digest.

Following are the steps taken to ensure security:

* The miniature version (digest) of the message is created by using a hash function.
* The digest is encrypted by using the sender's private key.
* After the digest is encrypted, then the encrypted digest is attached to the original message and sent to the receiver.
* The receiver receives the original message and encrypted digest and separates the two. The receiver implements the hash function on the original message to create the second digest, and it also decrypts the received digest by using the public key of the sender. If both the digests are same, then all the aspects of security are preserved.

**At the Sender site**



**At the Receiver site**

