Digital Signature:

A digital signature is a mathematical technique which validates the authenticity and integrity of a message, software or digital documents. It allows us to verify the author name, date and time of signatures and authenticate the message contents.

For example, when Alice sends a message to Bob, Bob needs to check the authenticity of the sender. Bob needs to be sure that the message comes from Alice and not Eve. Bob can ask Alice to sign the message electronically. In other words, an electronic signature can ~~provide~~ prove the authenticity of Alice as the sender of the message. We refer to this type of signature as a digital signature.

Process of digital signature:

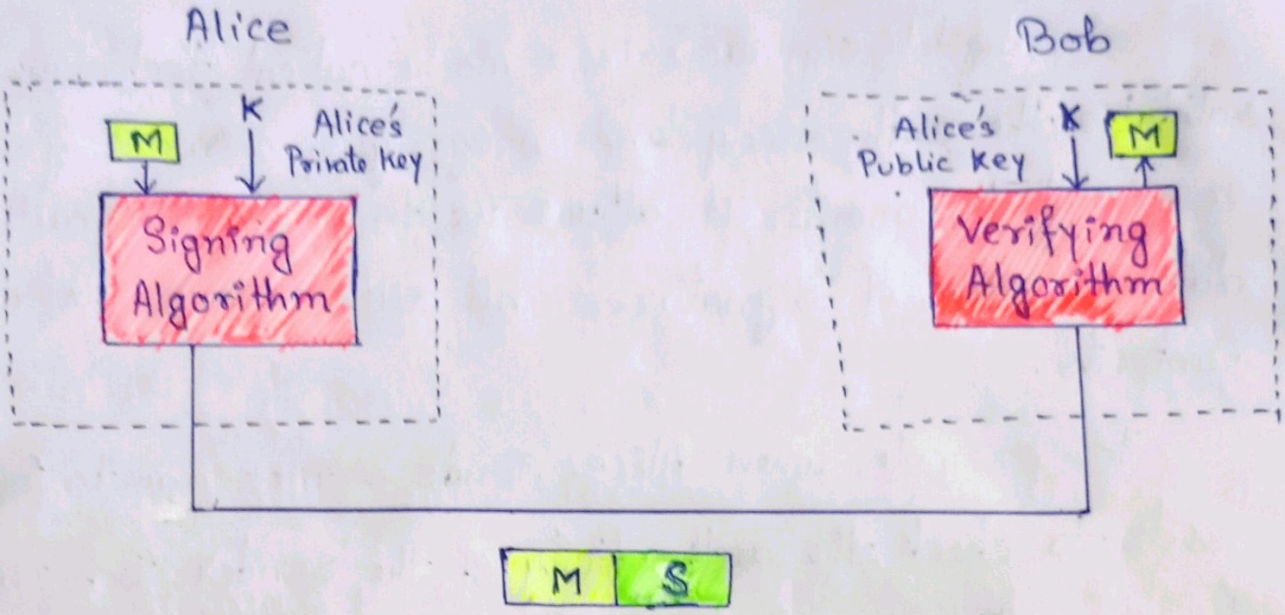
The basic process of digital signature is as follows,

i) The sender uses a signing algorithm to sign the message.

ii) The message and signature are sent to the receiver.

iii) The receiver receives the message and the signature and applies the verifying algorithm

iv) If the result is true, the message is accepted; otherwise it is rejected.



M: Message

S: Signature

Services Provided by digital signature:

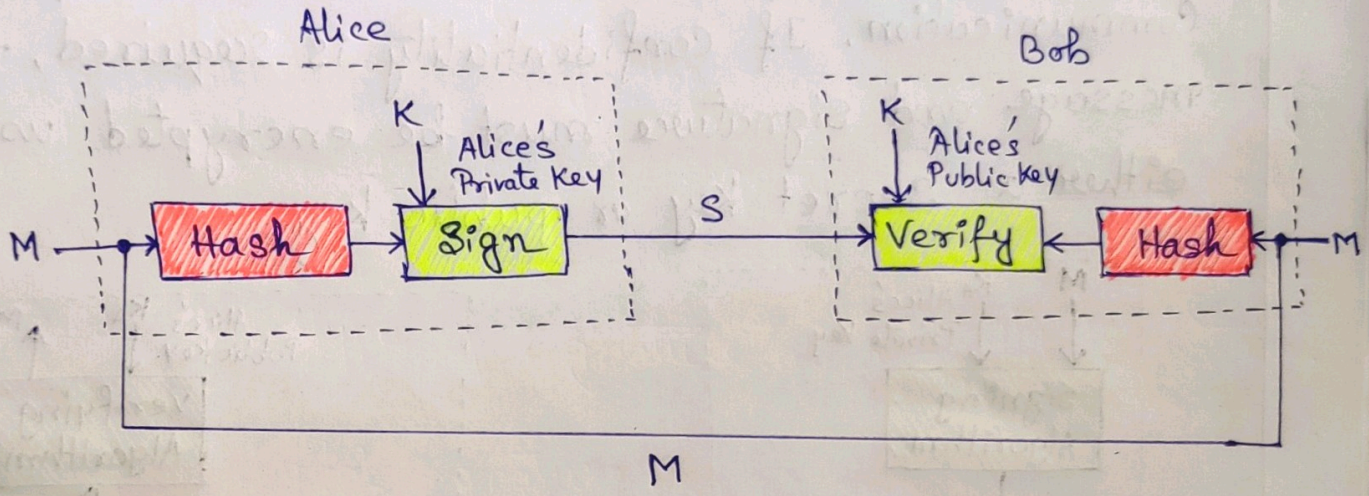
A digital signature can directly provide services such as, message authentication, message integrity and nonrepudiation.

i) Message Authentication:

A secure conventional signature can provide message authentication. Bob can verify that the message ~~auth~~ is sent by Alice because Alice's public key is used in verification. Alice's public key cannot verify the signature signed by Eve's private key.

ii) Message Integrity :

The integrity of the message is preserved even if we sign the whole message because we cannot get the same signature if the message is changed. The digital signature schema today use a hash function in the signing and verifying algorithm that preserve the integrity of the message.



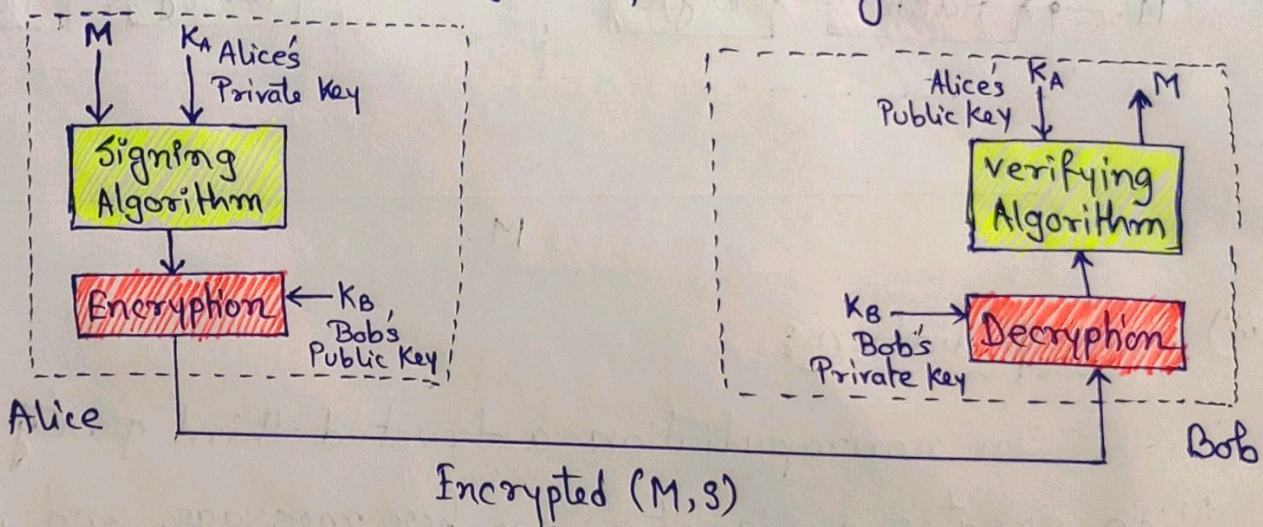
iii) Nonrepudiation :

In nonrepudiation a trusted third party is used. Alice creates a signature for her message and sends the message, her identity, Bob's identity and the signature to the center. The center, after checking that the Alice's public key is valid verifies that the message came from Alice. The center then saves a copy of the message with the sender's identity, receiver identity and a

timestamp in its archive. The center uses its private key to create another signature from the message. The ~~Sender~~ Center then sends the message, the new signature Alice's identity and Bob's identity to Bob. Bob verifies the message using the public key of the trusted center.

iii) Confidentiality:

A digital signature does not provide confidential communication. If confidentiality is required, the message and signature must be encrypted using either a secret key or public key.



Types of Attack:

There are three kinds of attacks on digital signature,

i) Key-only attack:

In the key-only attack, Eve has access only to

the public information released by Alice. To forge a message, Eve needs to create Alice's signature to convince Bob that the message is coming from Alice.

ii) Known-Message Attack:

In the known-message attack, Eve has access to more or one message signed by Alice. Eve tries to create another message and forge Alice's signature on it. This is similar to known-plaintext attack.

iii) Chosen-Message Attack:

In the chosen-Message attack, Eve somehow makes Alice one or more message for her. Eve now has a chosen message-signature pair. Eve later create another message, with the content she wants and forge Alice's signature.

*Note: Can we use a secret (Symmetric) key to both sign and verify a signature?

→

No, we cannot use a secret (Symmetric) key to both sign and verify a signature.

First, a secret key is known by only two participants. So if Alice needs to sign another document she needs to use another secret key.

Second creating a secret key involves authentication, which uses digital signature. we have a vicious cycle.

Third Bob could use the secret key between himself and Alice sign a document send it to Ted and pretend that it came from Alice.