2.

* The signature can only be created by someone who knows the secret information.
* Once a signature is created, anyone can validate that the signature is associated with the individual and the document, without needing to know the secret information used to create the digital signature.
* Since the signature depends on the document, it cannot be used to validate a different document.
* It is impossible to produce a document that differs from the original document by even a single bit but for which the signature is still valid.

3.

The signature must be a bit pattern that depends on the message being signed. • The signature must use some information unique to the sender to prevent both forgery and denial. • It must be relatively easy to produce the digital signature. • It must be relatively easy to recognize and verify the digital signature. • It must be computationally infeasible to forge a digital signature, either by constructing a new message for an existing digital signature or by constructing a fraudulent digital signature for a given message. • It must be practical to retain a copy of the digital signature in storage.

4. A **direct digital signature**involves only the communicating parties (source, destination). It is assumedthat the destination knows the public key of the source. A digital signature may be formed by encryptingthe entire message with the sender's private key or by encrypting a hash code of the message with thesender's private key.

An **arbitrated digital signature**operates as follows. Every signed message from a sender X to a receiverY goes first to an arbiter A, who subjects the message and its signature to a number of tests to check itsorigin and content. The message is then dated and sent to Y with an indication that it has been verified tothe satisfaction of the arbiter.