Message Digest & Digital Signature.

Presented By:

Hasibur Rahaman Khan

Concept of Hash (Message Digest)

The two most common hash functions are called MD5 (Message Digest 5) and SHA-I (Secure Hash Algorithm I). The first one produces a 120-bit digest. The second produces a 160-bit digest.

Note that a hash function must have two properties to guarantee its success.

First, hashing is one-way; the digest can only be created from the message, not vice versa.

Second, hashing is a one-to-one function; there is little probability that two messages will create the same digest. We will see the reason for this condition shortly.

After the digest has been created, it is encrypted (signed) using the sender's private key. The encrypted digest is attached to the original message and sent to the receiver.

Idea of a Message Digest

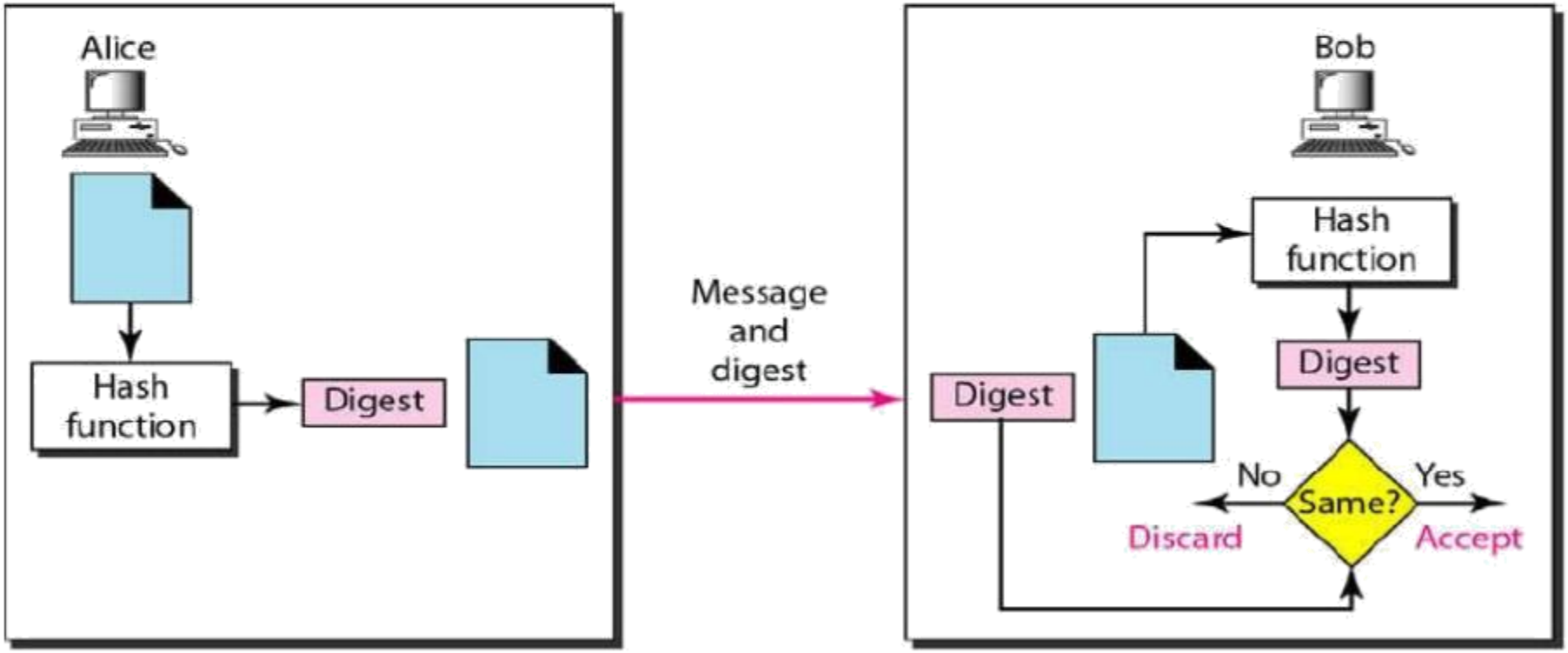
The concept of message digests is based on similar principles. However, it is slightly wider in scope. For instance, suppose that we have a number 4000 and we divide it by 4 to get 1000 Thus, 4 can become a fingerprint of the number 4000. Dividing 4000 by 4 will always yield 1000. If we change either 4000 or 4, the result will not be 1000.

Another important point is, if we are simply given the number 4, but are not given any further information, we would not be able to trace back the equation 4 x 1000 = 4000. Thus, we have one more important concept here. The fingerprint of a message (in this case, the number 4) does not tell anything about the original message (in this case, the number 4000). This is because there are infinite other possible equations, which can produce the result 4.

Another simple example of message digest is shown in fig. Let us assume that we want to calculate the message digest of a number 7391753. Then, we multiply each digit in the number with the next digit (excluding it if it is 0), and disregarding the first digits of the multiplication operation, if the result is a two-digit number.

Message Digest

Different algorithms are used to convert original message into its message digest. The popularly used ones are MD5 or Message Digest 5 (developed by Rivest) a modified version of earlier MD4, MD3 and MD2, while the first one was simply MD, and the SHA (Secure Hash Algorithm) developed by National Institute of Standards and Technology (NISI) in 1993. SHA-I is promoted & prominently used than the MD5 algorithm.



Digital Signatures

In earlier discussion of Asymmetric key cryptography, we had considered the only situation, in which if X is sender & Y receiver, then X encrypts the message with Y's public key and on receiving, Y decrypts with his own private key. This method only ensures secure communication between the two. Now consider another situation. If X is sender and Y is receiver, X encrypts the message using his own private key! On receiving, Y decrypts it using X's public key. The purpose behind this move is 'authentication'. It is clear that, only X knows his private key.

So, when Y receives this message (encrypted with X's private key), it is an indication or proof that it has originated only from X and none else! Remember that in earlier scheme, the purpose was only 'confidentiality' and the origin of message was not the concern.

Now, one may say that if someone else wants to intercept this communication it should be easy. i.e. anyone can decrypt the message who knows X's public key. This is true, but then it will not be possible for anyone to again encrypt this message as only X knows his private key. Thus receiver here will not be fooled that message came from X This scheme confirms the origin of the message. So, in this case X cannot deny that he has sent the message to Y, because it was encrypted with X's private key, known only to X

Steps for the process

Sender's Side:

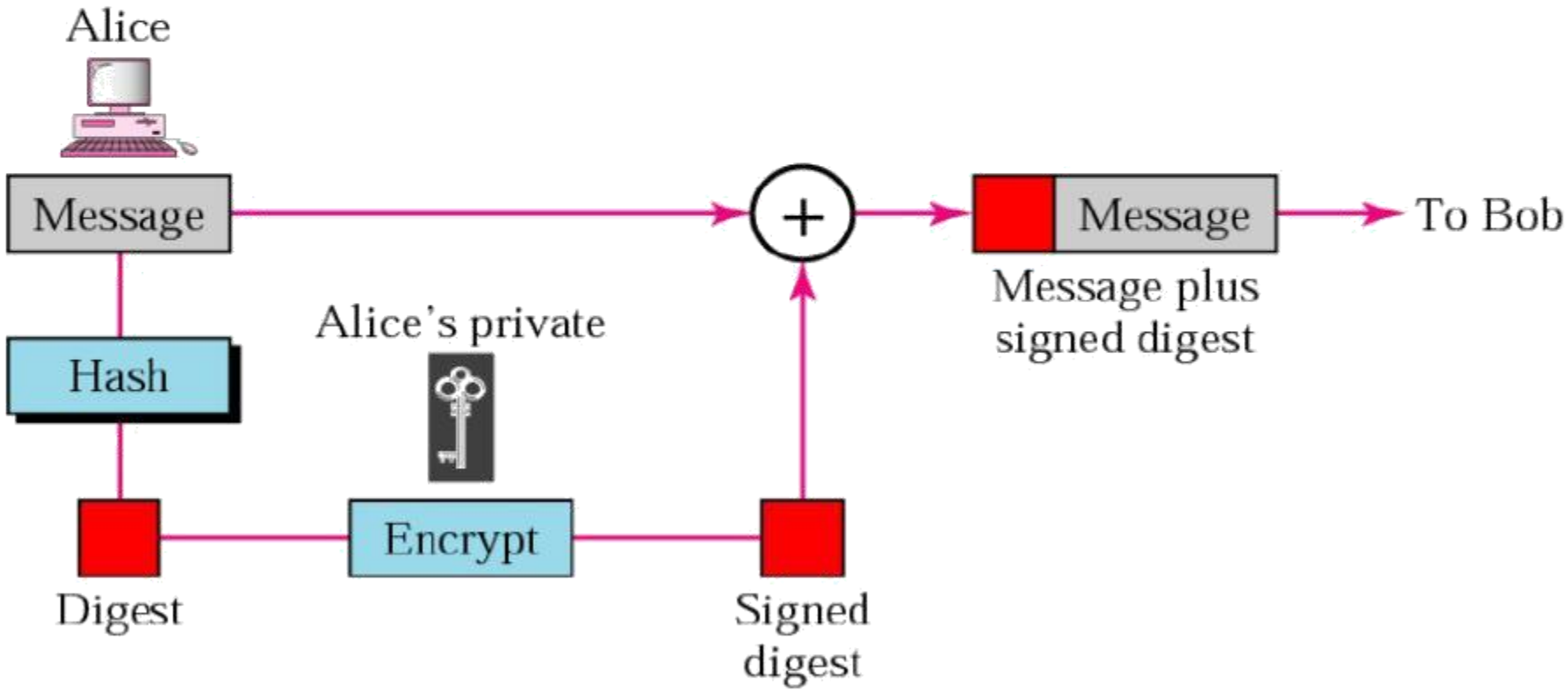
1. If X is the sender, the SHA-1 algorithm is used to first calculate the message digest (MD 1) of original message.
2. This MD1 is further encrypted using RSA with X's private key. This output is called the Digital Signature (DS) of X.
3. Further, the original message (M) along with the Digital signature (DS) is sent to receiver.

Receiver's Side:

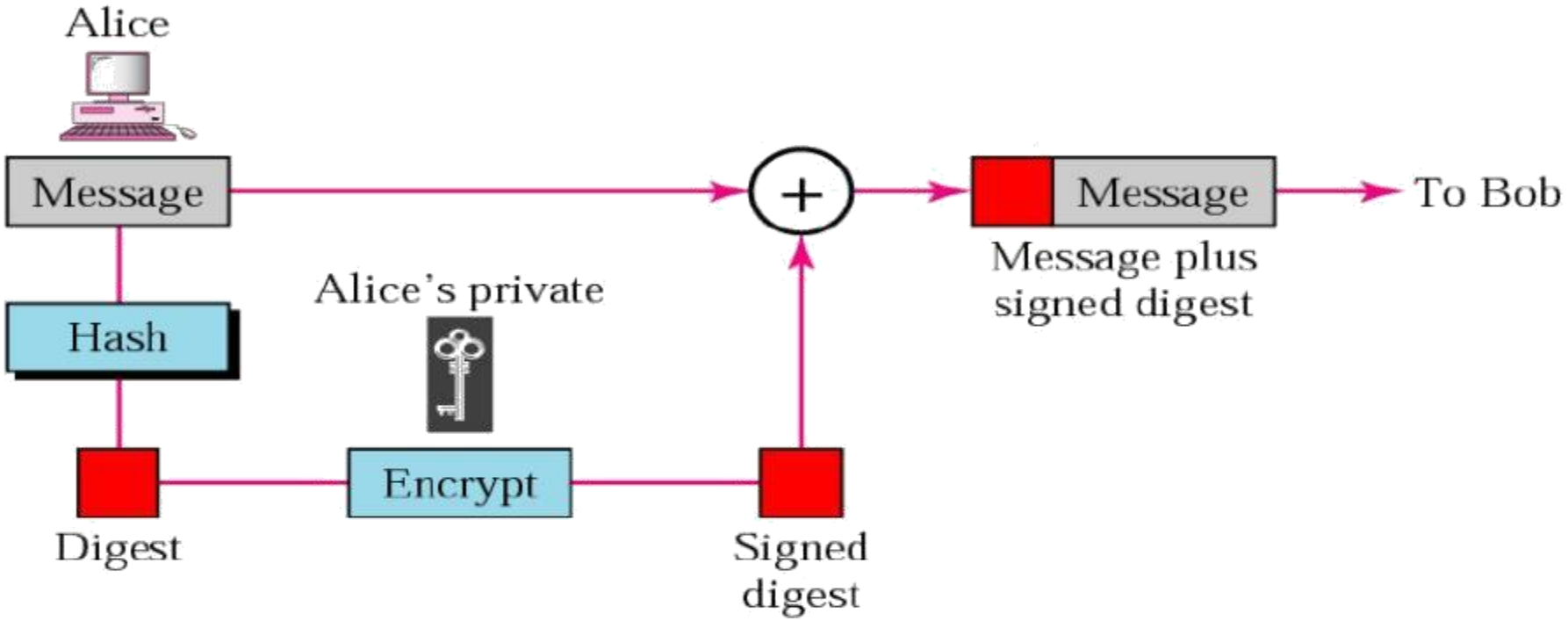
4. Y thus receives the original message (M) and X's digital signature. Y uses the same message digest algorithm used by X to calculate the message digest (MD2) of received message (M).
5. Also, Y uses X's public key to decrypt the digital signature. The outcome of this decryption is nothing but original message digest (MD1) calculated by X.
6. Y, then compares this digest MD1 with the digest MD2 he has just calculated in step 4. If both of them are matching, i.e. MDI = MD2, Y can accept the original message (M) as correctly authenticated and assured to have originated from X. whereas, if they are different, the message shall be rejected.

Digital Signatures

This method turns out to be foolproof. Even if an attacker intercepts anywhere in between, it is not likely for him to again sign the modified/read message, as only X in this case will know the private key! Hence, even if intercepted, this method remains very much secure and reliable!

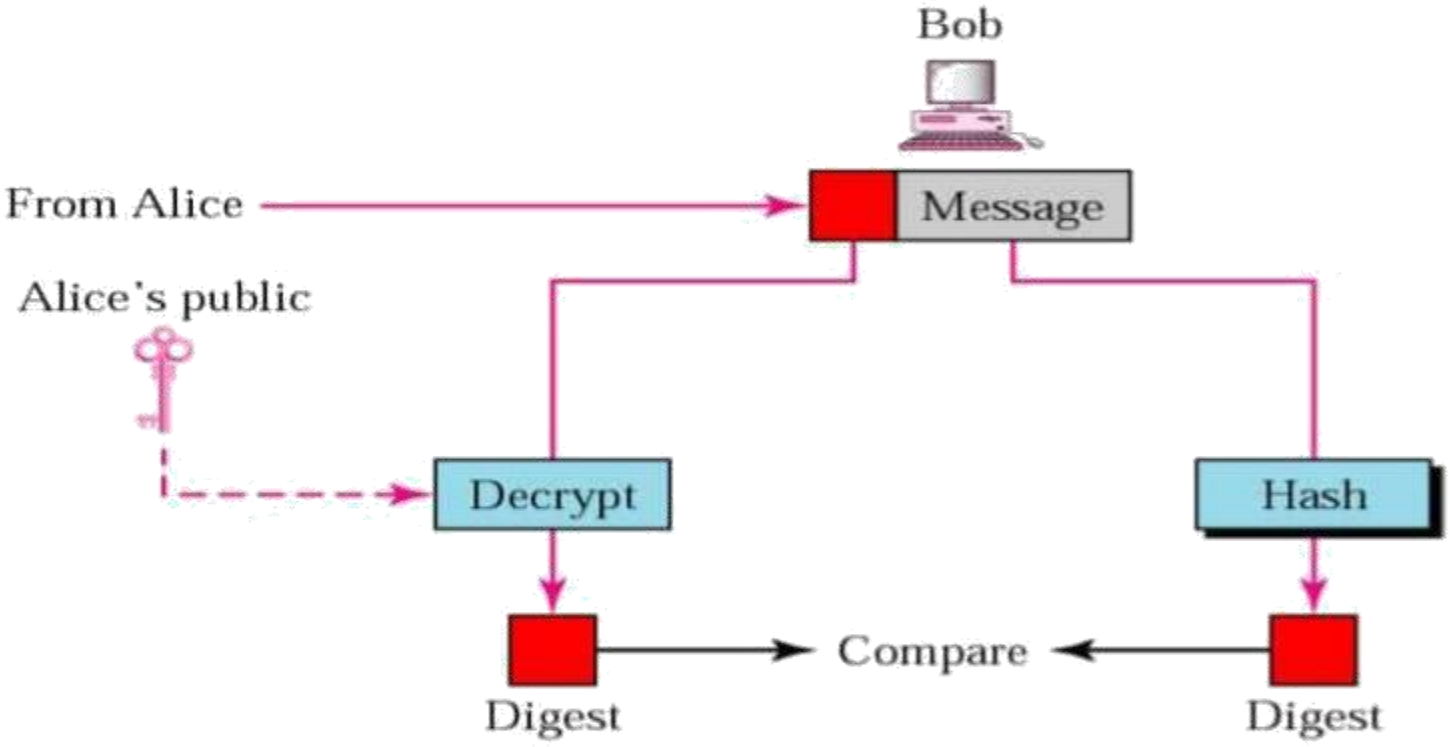


The Sender's Side



After the digest has been created, it is encrypted (signed) using the sender's private key. The encrypted digest is attached to the original message and sent to the receiver.

The Receiver's Side



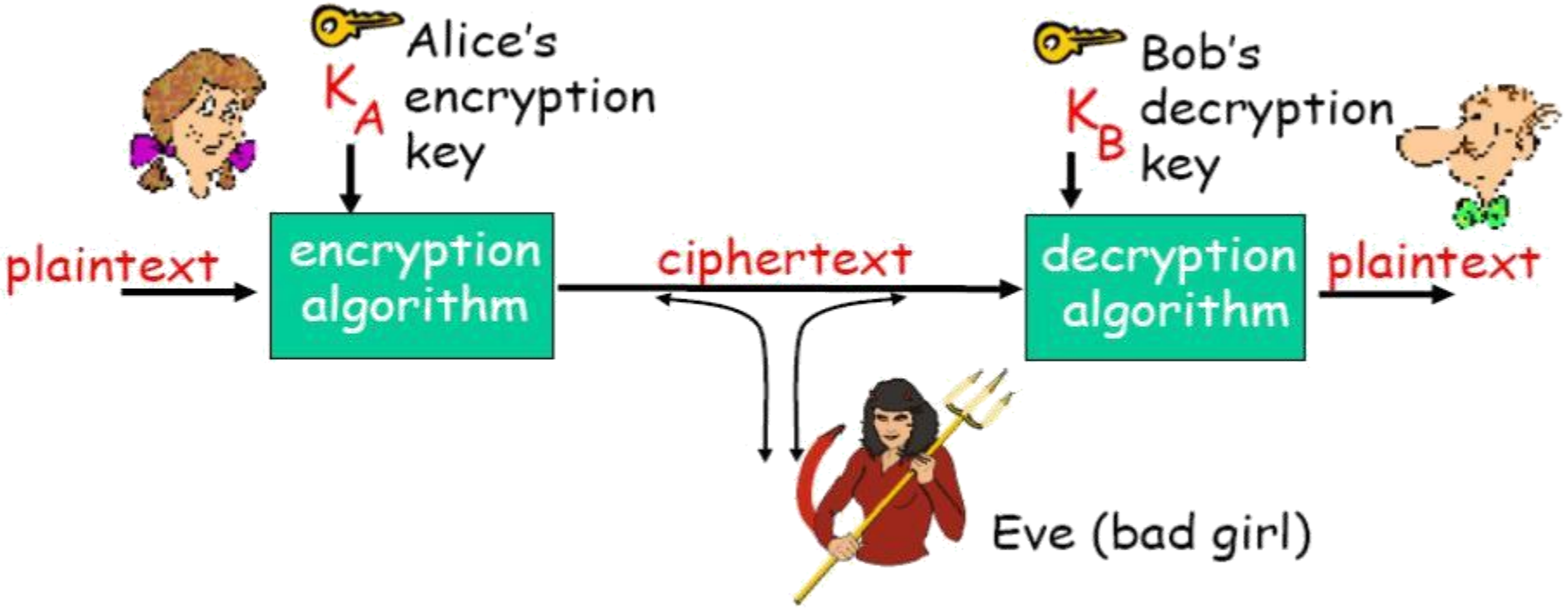
The receiver receives the original message and the encrypted digest. He separates the two. He applies the same hash function to the message to create a second digest. He also decrypts the received digest, using the public key of the sender. If the two digests are the same, all three security measures are preserved.

Properties of Digital Signatures

- Digital signature does not provide privacy. If there is a need for privacy, another layer of encryption/decryption must be applied.
- **Digital signatures can provide**

1. Integrity,
2. Authentication, and
3. Nonrepudiation.

Properties of Digital Signatures



K_A Alice's key

K_B Bob's key

Alice, Bob are two entities (person, process, client, server) that like to communicate. Eve is another entity which for eg. intercepts the communication.

THANK YOU