Course: Cryptography and Network Security
Code: CS-34310
Branch: M.C.A - 4th Semester

Lecture – 13 : Message Authentication and Digital Signatures

Faculty & Coordinator : Dr. J Sathish Kumar (JSK)

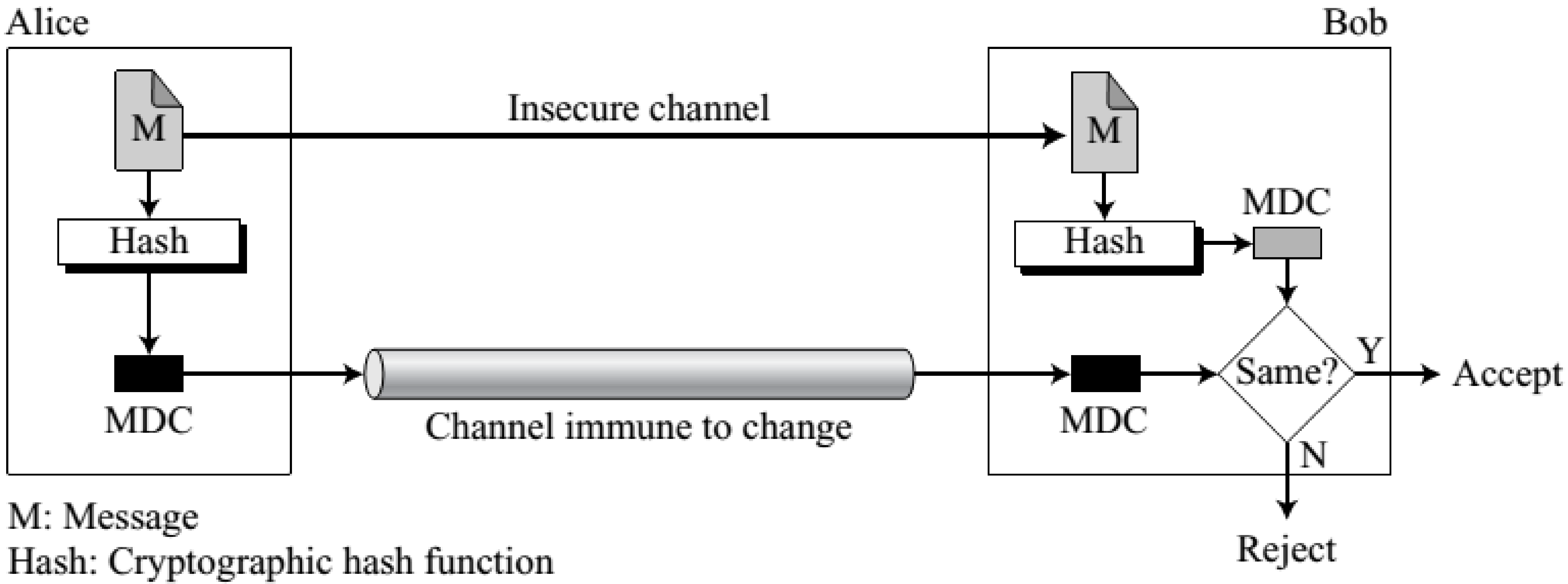
Department of Computer Science and Engineering

Motilal Nehru National Institute of Technology Allahabad,
Prayagraj-211004

MESSAGE AUTHENTICATION

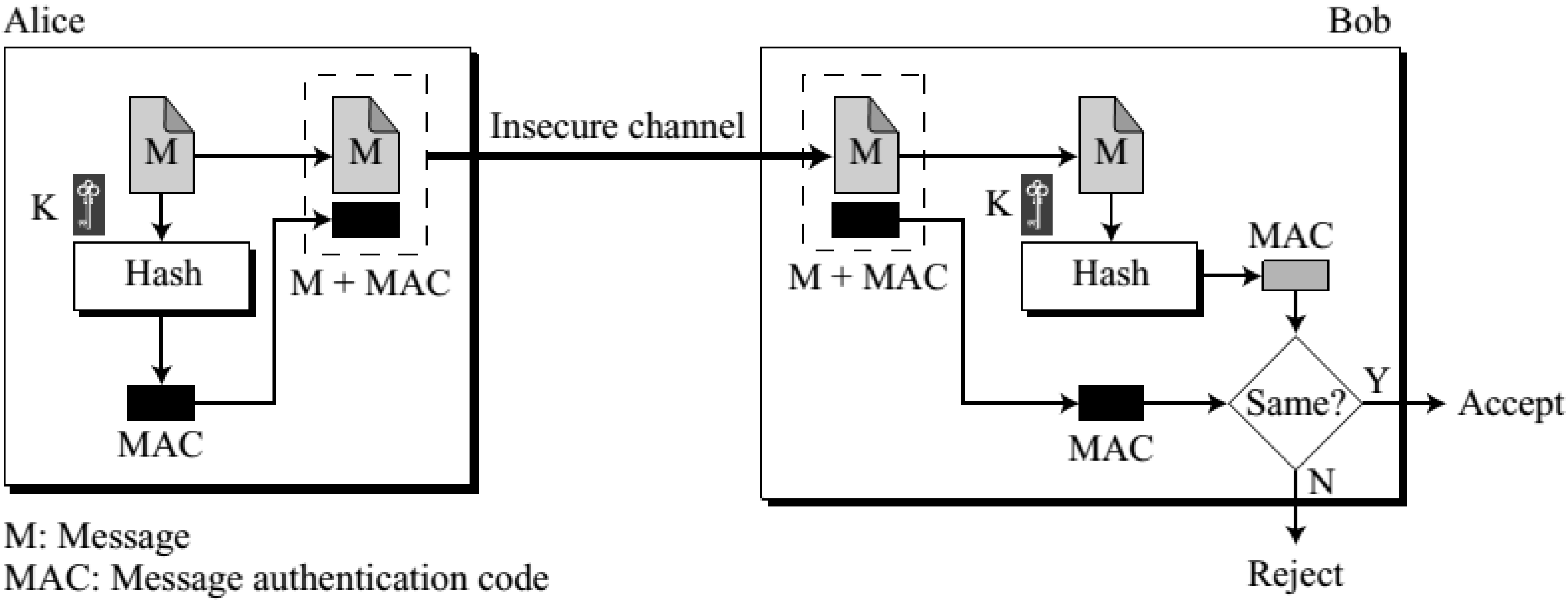
- A message digest guarantees the integrity of a message.
  - It guarantees that the message has not been changed.
- A message digest, however, does not authenticate the sender of the message.
  - When Alice sends a message to Bob, Bob needs to know if the message is coming from Alice.
- To provide message authentication, Alice needs to provide proof that it is Alice sending the message and not an impostor.
- A message digest per se cannot provide such a proof.
- The digest created by a cryptographic hash function is normally called a modification detection code (MDC).
  - The code can detect any modification in the message.
- What we need for message authentication (data origin authentication) is a message authentication code (MAC).

Modification detection code (MDC)



M: Message
Hash: Cryptographic hash function
MDC: Modification detection code

Message Authentication Code (MAC)



M: Message
MAC: Message authentication code
K: A shared secret key

Message Authentication Code (MAC)

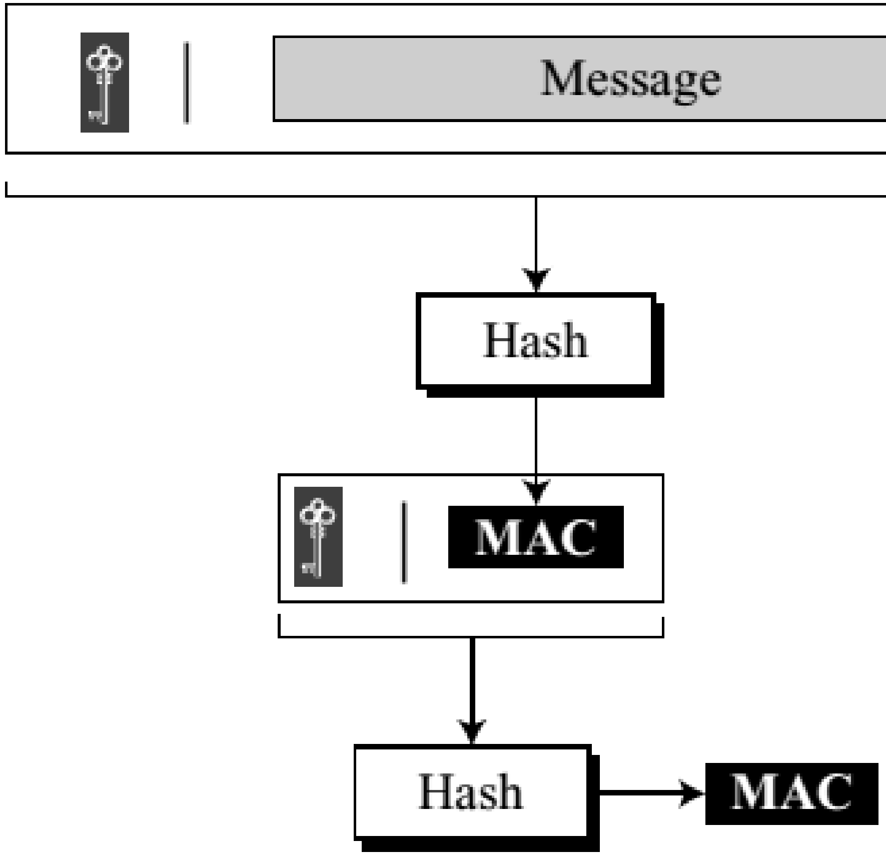
- Alice uses a hash function to create a MAC from the concatenation of the key and the message, h (K|M).
- She sends the message and the MAC to Bob over the insecure channel.
- Bob separates the message from the MAC.
- He then makes a new MAC from the concatenation of the message and the secret key.
- Bob then compares the newly created MAC with the one received.
- If the two MACs match, the message is authentic and has not been modified by an adversary.
- The MAC we have described is referred to as a prefix MAC because the secret key is appended to the beginning of the message.
- We can have a postfix MAC, in which the key is appended to the end of the message.
- We can combine the prefix and postfix MAC, with the same key or two different keys.

Security of a MAC

- Suppose Eve has intercepted the message M and the digest h(K| M). How can Eve forge a message without knowing the secret key? There are three possible cases:
- If the size of the key allows exhaustive search, Eve may prepend all possible keys at the beginning of the message and make a digest of the (K| M) to find the digest equal to the one intercepted. She then knows the key and can successfully replace the message with a forged message of her choosing.
- The size of the key is normally very large in a MAC, but Eve can use another tool: the preimage attack. She uses the algorithm until she finds X such that h(X) is equal to the MAC she has intercepted. She now can find the key and successfully replace the message with a forged one. Because the size of the key is normally very large for exhaustive search, Eve can only attack the MAC using the preimage algorithm.
- Given some pairs of messages and their MACs, Eve can manipulate them to come up with a new message and its MAC.

The security of a MAC depends on the security of the underlying hash algorithm

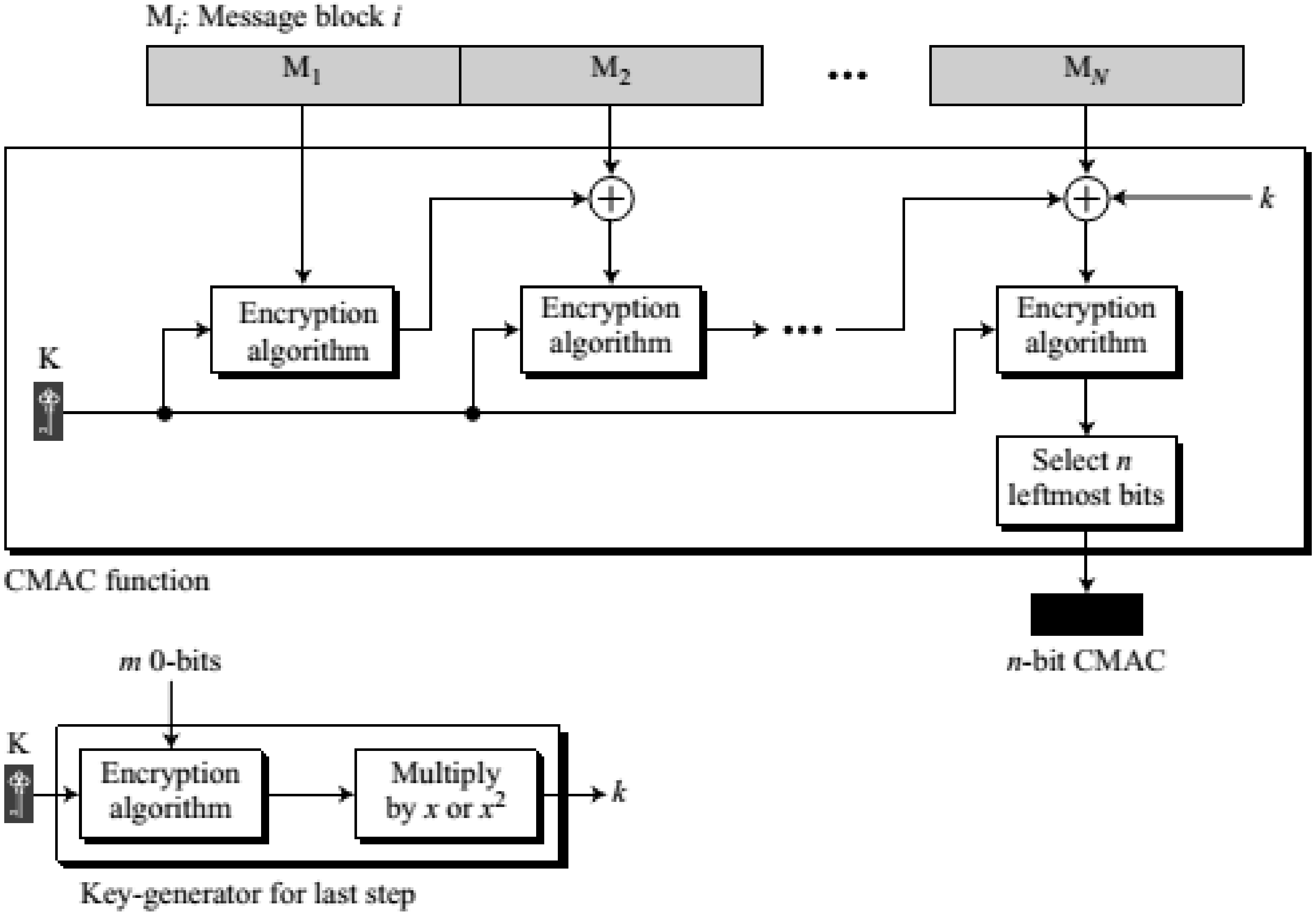
Nested MAC (OR) HMAC (Hashed MAC)



CMAC, or CBCMAC

CMAC, or CBCMAC is also called Data Authentication Algorithm.

The method is similar to the cipher block chaining (CBC) mode



Digital Signature

Digital Signature

- A person signs a document to show that it originated from her or was approved by her.
- The signature is proof to the recipient that the document comes from the correct entity.
- When Alice sends a message to Bob, Bob needs to check the authenticity of the sender; he 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 prove the authenticity of Alice as the sender of the message.
- We refer to this type of signature as a digital signature.

Digital Signature: Inclusion

- A conventional signature is included in the document; it is part of the document.
- When we write a check, the signature is on the check; it is not a separate document.
- But when we sign a document digitally, we send the signature as a separate document.
- The sender sends two documents: the message and the signature.
- The recipient receives both documents and verifies that the signature belongs to the supposed sender.
- If this is proven, the message is kept; otherwise, it is rejected.

Digital Signature: Verification Method

- For a conventional signature, when the recipient receives a document, she compares the signature on the document with the signature on file.
- If they are the same, the document is authentic.
- The recipient needs to have a copy of this signature on file for comparison.
- For a digital signature, the recipient receives the message and the signature.
- A copy of the signature is not stored anywhere.
- The recipient needs to apply a verification technique to the combination of the message and the signature to verify the authenticity.

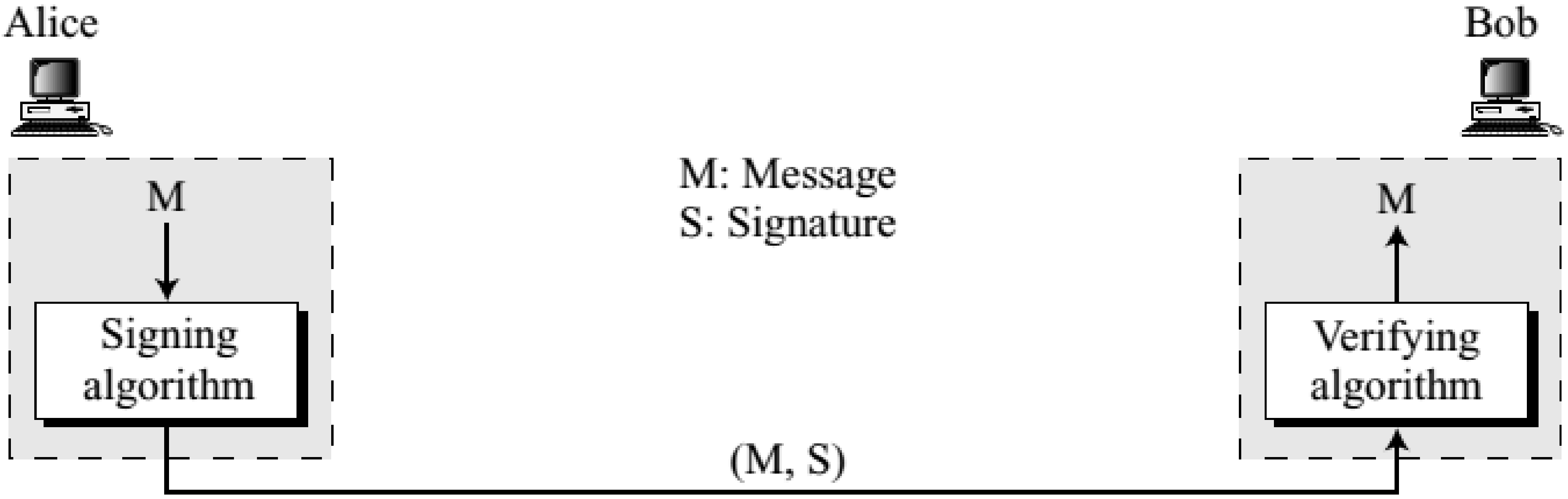
Digital Signature: Relationship

- For a conventional signature, there is normally a one-to-many relationship between a signature and documents.
- A person uses the same signature to sign many documents.
- For a digital signature, there is a one-to-one relationship between a signature and a message.
- Each message has its own signature. The signature of one message cannot be used in another message.
- If Bob receives two messages, one after another, from Alice, he cannot use the signature of the first message to verify the second.
- Each message needs a new signature.

Digital Signature: Duplicity

- In conventional signature, a copy of the signed document can be distinguished from the original one on file.
- In digital signature, there is no such distinction unless there is a factor of time (such as a timestamp) on the document.
- For example,
  - Suppose Alice sends a document instructing Bob to pay Eve.
  - If Eve intercepts the document and the signature, she can replay it later to get money again from Bob.

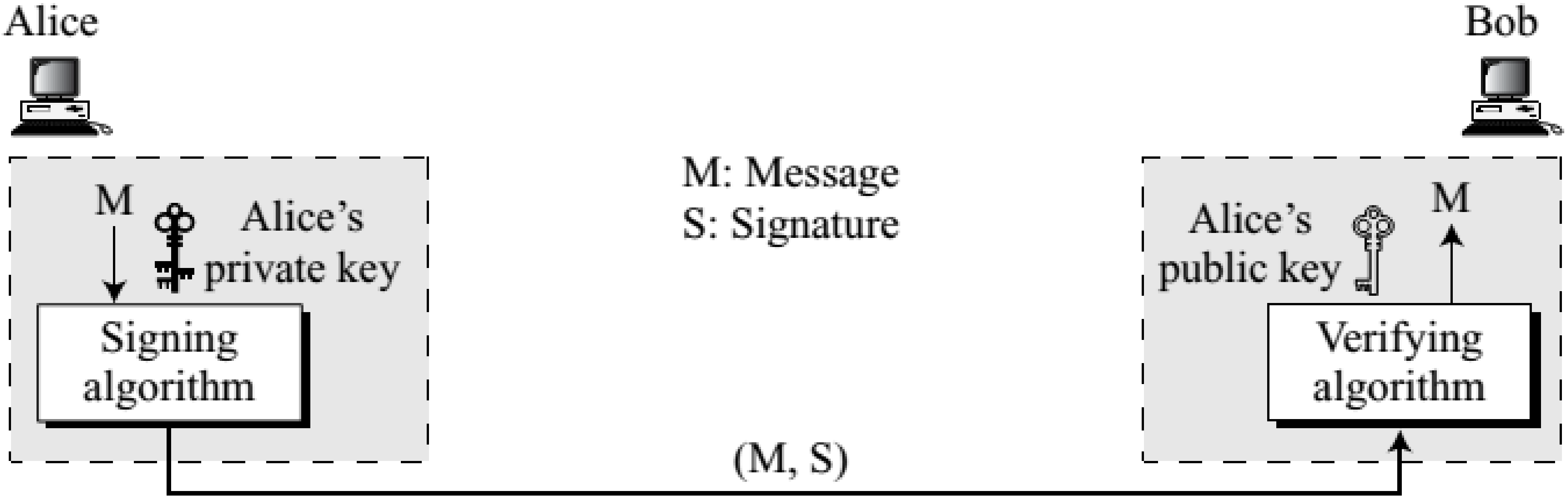
Digital Signature Process



Need for Keys

- A conventional signature is like a private “key” belonging to the signer of the document. The signer uses it to sign documents; no one else has this signature.
- The copy of the signature is on file like a public key; anyone can use it to verify a document, to compare it to the original signature.
- In a digital signature, the signer uses her private key, applied to a signing algorithm, to sign the document.
- The verifier, on the other hand, uses the public key of the signer, applied to the verifying algorithm, to verify the document.
- Note that when a document is signed, anyone, including Bob, can verify it because everyone has access to Alice’s public key.
- Alice must not use her public key to sign the document because then anyone could forge her signature.

Adding key to the digital signature process

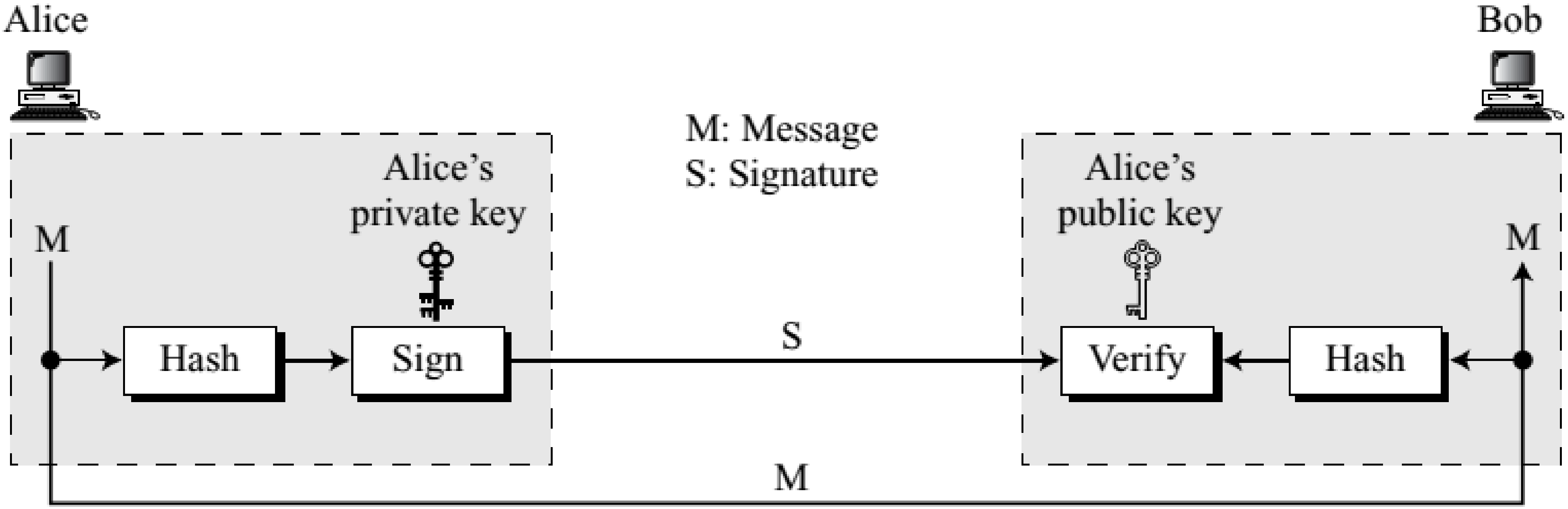


Digital Signature

- A digital signature needs a public-key system. The signer signs with her private key; the verifier verifies with the signer’s public key.

- A cryptosystem uses the private and public keys of the receiver: a digital signature uses the private and public keys of the sender.

Signing the Digest



Digital Signature SERVICES

- Several security services were discussed including
  - message confidentiality,
  - message authentication,
  - message integrity, and
  - nonrepudiation.

- A digital signature can directly provide the last three;

- For message confidentiality we still need encryption/decryption.

Digital Signature : Message Authentication

- A secure digital signature scheme, like a secure conventional signature (one that cannot be easily copied) can provide message authentication (also referred to as data-origin authentication).
- Bob can verify that the message 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.
- A digital signature provides message authentication

Digital Signature : 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.

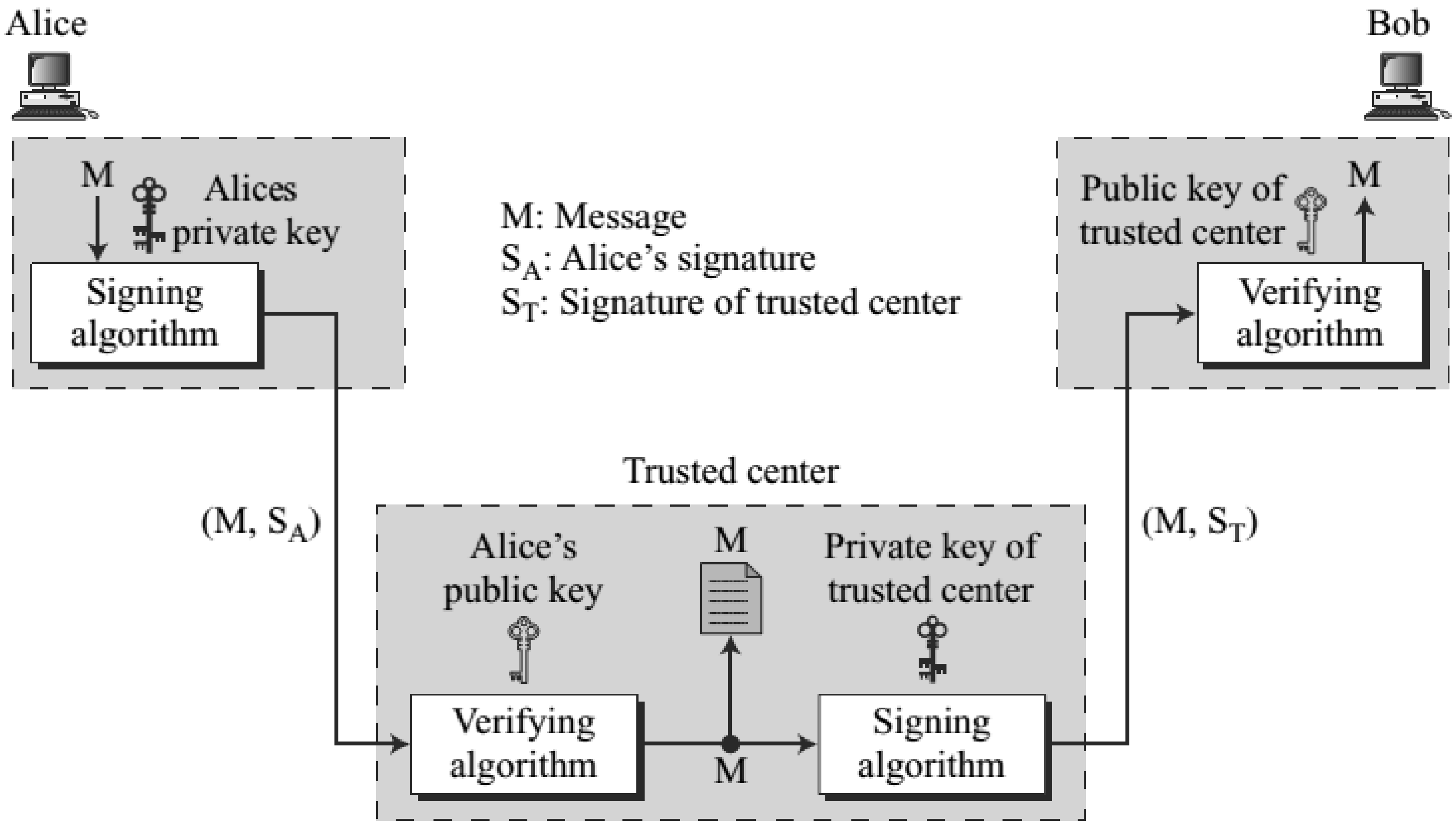
- The digital signature schemes today use a hash function in the signing and verifying algorithms that preserve the integrity of the message.

- A digital signature provides message integrity

Digital Signature : Nonrepudiation

- If Alice signs a message and then denies it, can Bob later prove that Alice actually signed it?
- For example, if Alice sends a message to a bank (Bob) and asks to transfer $10,000 from her account to Ted’s account, can Alice later deny that she sent this message?
- With the scheme we have presented so far, Bob might have a problem.
- Bob must keep the signature on file and later use Alice’s public key to create the original message to prove the message in the file and the newly created message are the same.
- This is not feasible because Alice may have changed her private or public key during this time; she may also claim that the file containing the signature is not authentic.
- One solution is a trusted third party.

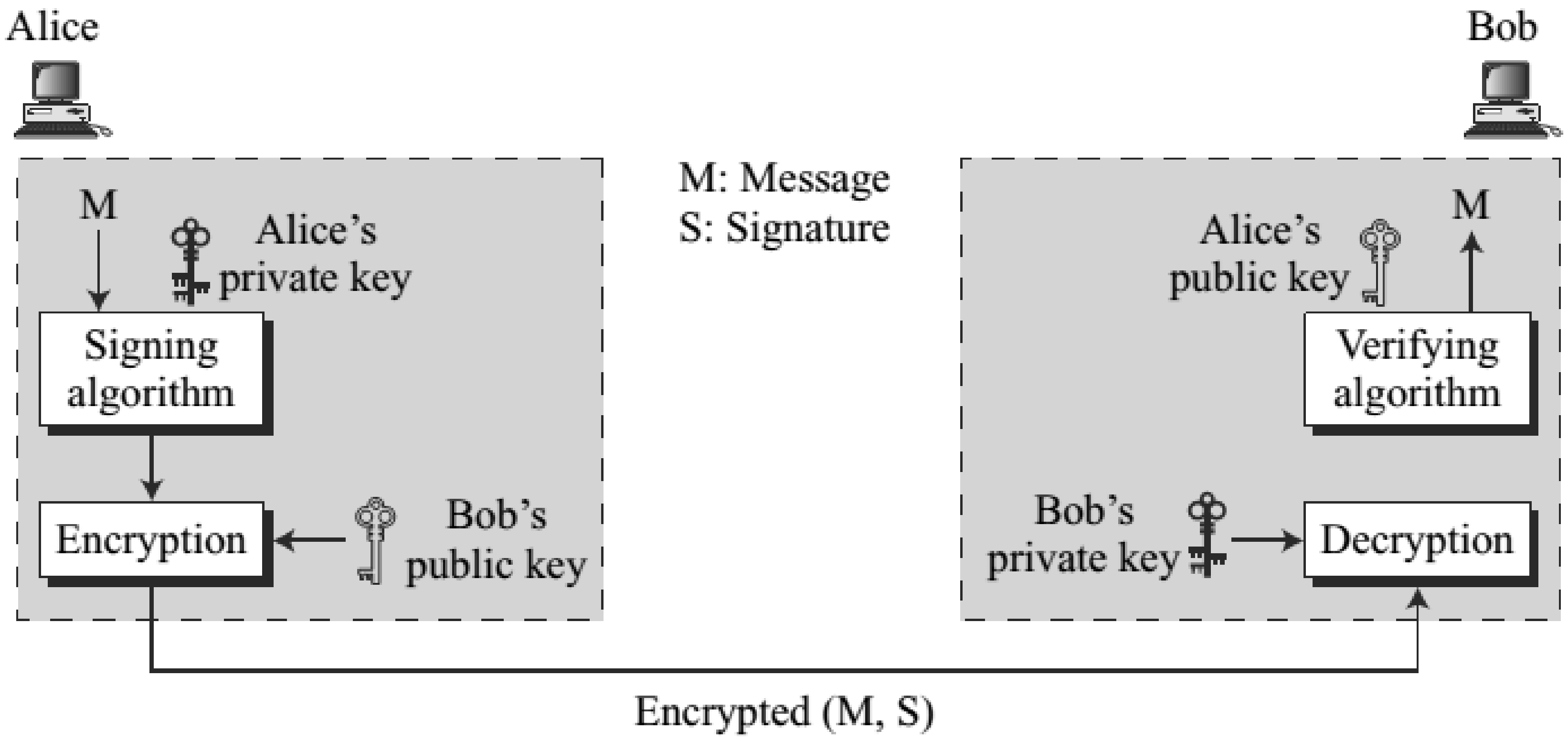
Digital Signature : Nonrepudiation



Digital Signature : Nonrepudiation

- Alice creates a signature from her message (S_A) and sends the message, her identity, Bob’s identity, and the signature to the center.
- The center, after checking that Alice’s public key is valid, verifies through Alice’s public key that the message came from Alice.
- The center then saves a copy of the message with the sender identity, recipient identity, and a timestamp in its archive.
- The center uses its private key to create another signature (S_T) from the message.
- The 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.
- **Nonrepudiation can be provided using a trusted party.**

Digital Signature : Confidentiality



A digital signature does not provide confidential communication.

If confidentiality is required, the message and the signature must be encrypted using either a secret-key or public-key cryptosystem.

A digital signature does not provide privacy.
If there is a need for privacy, another layer of encryption/ decryption must be applied.

ATTACKS ON DIGITAL SIGNATURE

- 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.
  - This is the same as the ciphertext-only attack we discussed for encipherment.
- Known-Message Attack
  - In the known-message attack, Eve has access to one or more message-signature pairs.
  - In other words, she has access to some documents previously signed by Alice.
  - Eve tries to create another message and forge Alice’s signature on it.
  - This is similar to the known-plaintext attack we discussed for encipherment.

ATTACKS ON DIGITAL SIGNATURE

- Chosen-Message Attack
  - In the chosen-message attack, Eve somehow makes Alice sign one or more messages for her.
  - Eve now has a chosen-message/signature pair.
  - Eve later creates another message, with the content she wants, and forges Alice's signature on it.
  - This is similar to the chosen-plaintext attack we discussed for encipherment.
- If the attack is successful, the result is a forgery.
- We can have two types of forgery:
  - existential and
  - selective.

Forgery Types

- Existential Forgery
  - In an existential forgery, Eve may be able to create a valid message-signature pair, but not one that she can really use.
  - In other words, a document has been forged, but the content is randomly calculated.
  - This type of forgery is probable, but fortunately Eve cannot benefit from it very much.
  - Her message could be syntactically or semantically unintelligible.
- Selective Forgery
  - In selective forgery, Eve may be able to forge Alice’s signature on a message with the content selectively chosen by Eve.
  - Although this is beneficial to Eve, and may be very detrimental to Alice, the probability of such forgery is low, but not negligible.