Cryptography
Digital Signature

Anand Ballabh Joshi
Department of Mathematics
University of Lucknow, Lucknow, India

Digital signature

- We are familiar with the concept of the signature before.
- A person sign a document to show that it is originated from him or approved by him.
- The signature is the proof to the recipient that the document come from the right entity and nobody else.
- A sign of authentication: verified signature on documents
- A message can be signed electronically
- This type of signature is called digital signature.

Digital signature

- 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.
- An electronic signature can prove the authenticity of Alice as the sender of the message.
- This type of signature as a digital signature.

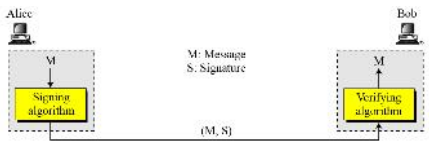
Conventional and digital signature: comparison

	Conventional Signature	Digital Signatures
(1) **Inclusion**	Included in the document as part of the document.	Send the signature as a separate document.
(2) **Verification Method**	Recipient compares the signature on the document with the signature on file.	• The recipient receives the message and the signature. • The recipient needs to apply a verification technique to the combination of the message and the signature to verify the authenticity.
(3) **Relationship**	Normally a *one-to-many* relationship between a signature and documents.	*One-to-one* relationship between a signature and a message.
(4) **Duplicity**	A copy of the signed document can be distinguished from the original one on file.	No such distinction unless there is a factor of time on the document

Digital signature

The sender uses a *signing algorithm* to sign the message
The message and the signature are sent to the receiver.

The receiver receives the message and the signature, and applies the *verifying algorithm* to the combination.
If the result is true, the message is accepted; otherwise, it is rejected.



Digital signature: need for key

In digital signature, the signer uses his private key, applied to a *signing algorithm*, to **sign** the document.

The verifier (recipient), uses the public key of the signer, applied to the *verifying algorithm*, to **verify** the document.

In a cryptosystem, we use the private and public keys of the receiver;
In digital signature, we use the private and public keys of the sender.

Hash function and digital signature

- Both encryption and digital signature can be combined, hence providing privacy and authentication.
- Symmetric key plays a major role in public key encryption implementations. This is because asymmetric key encryption algorithm are somewhat slower than symmetric key algorithms.

Hash function and digital signature

- For digital signature, another technique used is called hashing.
- Hashing produces a message digest that is small and unique representation of the complete message.
- Hashing algorithm is one way encryption ,i.e. impossible to derive the message from the digest.

Hash function and digital signature

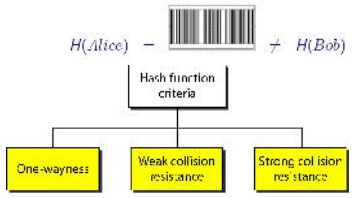
- The main reasons for producing a message digest are as follows:

1. The message integrity being sent is preserved; any message alteration will immediately be detected;
2. The digital signature will be applied to digest, which is usually considerably smaller than the message itself;
3. Hashing algorithm are much faster than any encryption algorithm (asymmetric or symmetric).

Hash Function

A hash function H takes as input a bit-string of any finite length and returns a corresponding 'digest' of fixed length.

$$H : \{0,1\}^* \rightarrow \{0,1\}^n$$

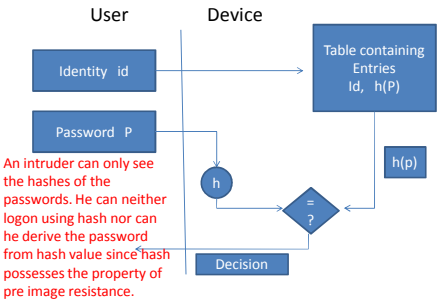


Hash function and its properties

1) One wayness (pre image resistance) : this property means it should be computationally hard to reverse a hash function. Or , if a hash function h and hash value z is given then it is difficult to find any input x such that h(x)=z.
2) Weak collision resistance (second pre image resistance): given and input M and its hash value it is hard to find a different M' such that h(M)=h(M')
3) Strong collision resistance: this property means it should be hard to find two different inputs of any length such that their hash values are same.

Applications of hash function: Password storing

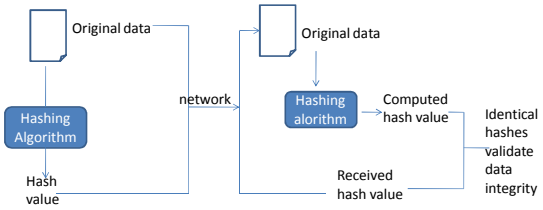
1. Password storing 2. Data integrity check



An intruder can only see the hashes of the passwords. He can neither logon using hash nor can he derive the password from hash value since hash possesses the property of pre image resistance.

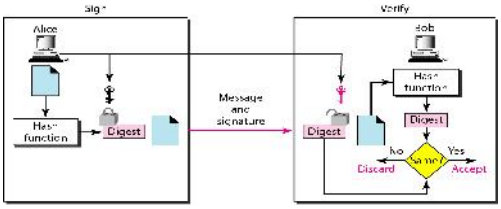
Instead of storing password in clear, mostly all login processes store the hash values of password in the file. Password file consists of a table of pairs which are in the form (user id, h(P))

Applications of hash function: message integrity



Digital signature and message integrity

- Digital signature provides message authentication.
- A digital signature provides message integrity using hash funciton.

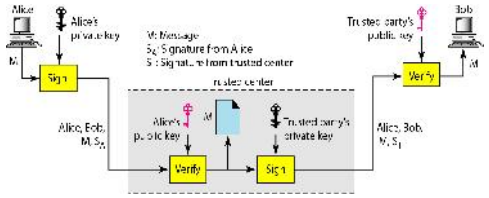


Digital signature and cryptographic goals

- The main cryptographic goals are
- Message confidentiality
- Message authenticity
- Message integrity
- Nonrepudiation
- A digital signature can directly provide the last three
- For message confidentiality we need encryption/decryption
- Nonrepudiation is shown in the next slide

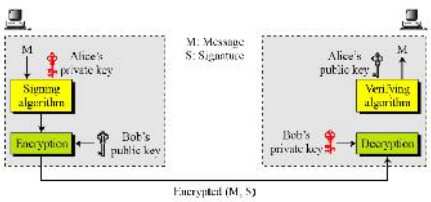
Digital signature and Nonrepudiation

- Nonrepudiation can be provided using a trusted party, using a trusted centre

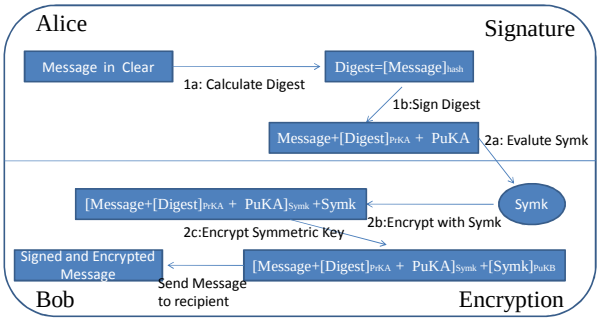


Message confidentiality

Digital signature does not provide privacy
If there is need of privacy another layer of encryption/decryption must be applied.



Overall digital signature process



Step for signing and encrypting a message

- 1) Message signature: Digital signature include two steps (see in figure 1a and 1b)

1a. Message digest evaluation: the main purpose of the message digest is to ensure that the message is kept unaltered; that is called message integrity.

1b. Digest signature :

Step for signing and encrypting a message

- 2) Message encryption: Encryption include the following three steps(in figure 2a 2b 2c)

2a. Creation of one time symmetric encryption/decryption key .

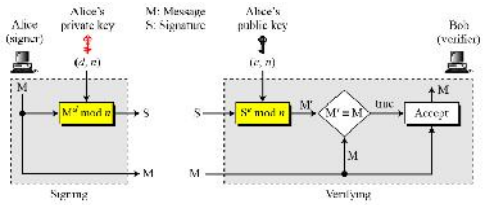
2b. Message encryption.

2c. Symmetric-key encryption.

Digital signature using RSA

- Key generation in RSA digital signature is same as in RSA cryptosystem to provide confidentiality.
- The digital signature scheme changes the role of the private and public keys:
  1. the private and public keys of sender are used
  2. the sender uses her private key to sign the message and receiver uses her public key to verify the signature
- In RSA digital signature scheme , d is private and e, n are public.

Signing and verifying: RSA scheme



RSA signature on message digest