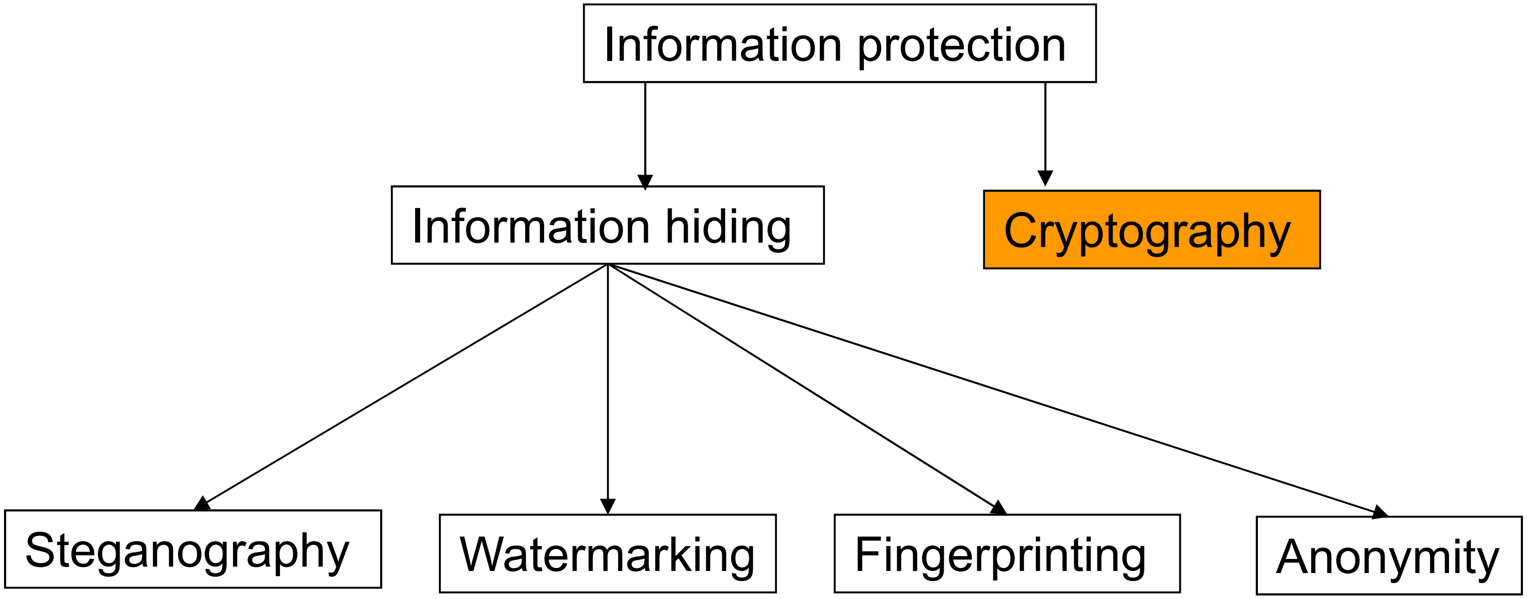
Network Security
Session 3

Hakim Sabzevari university
Dr.Malekzadeh

Security Solutions

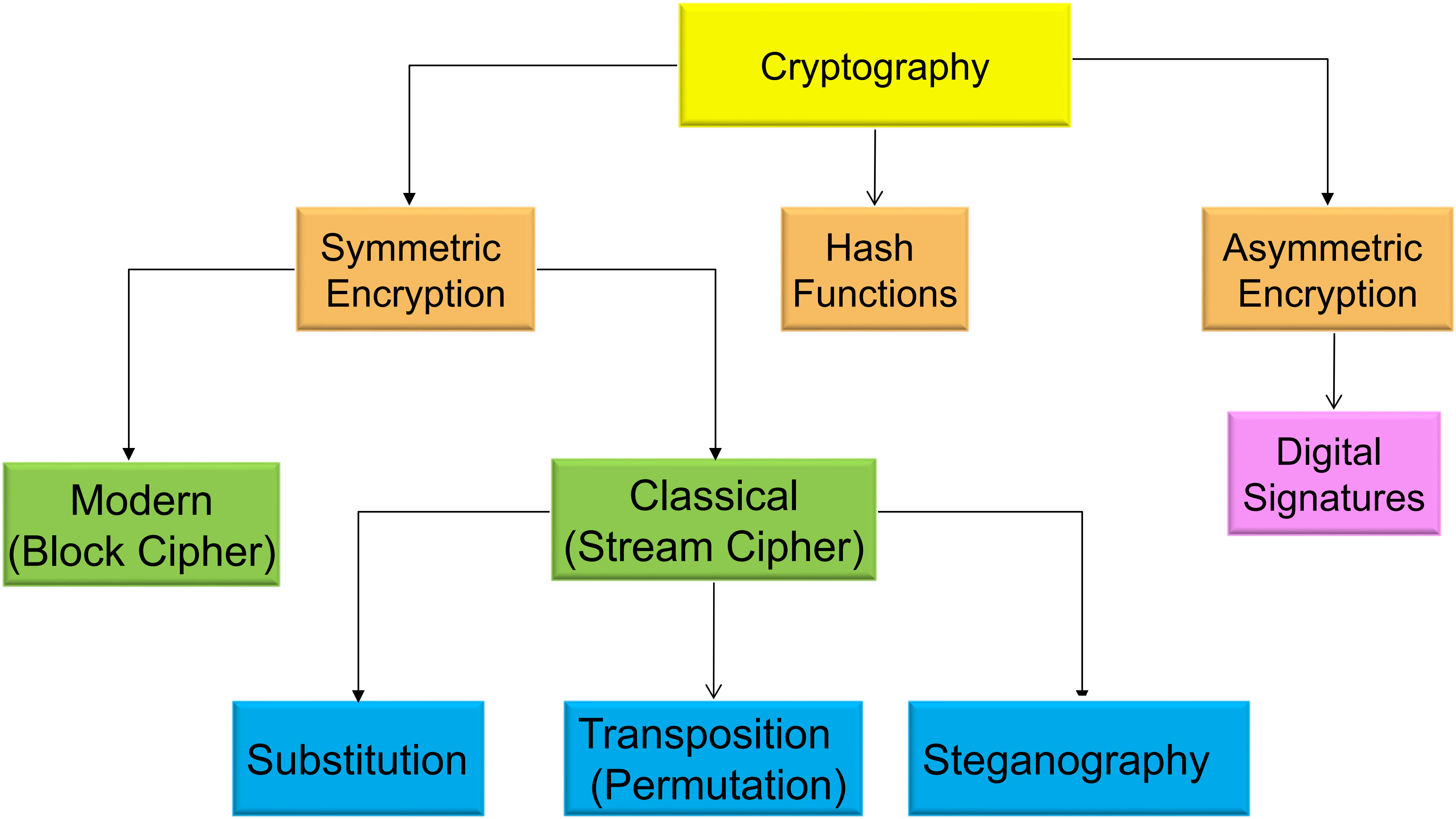
Information protection



Cryptography

Security mechanisms

To provide security services, there are different security mechanisms:



Hash functions

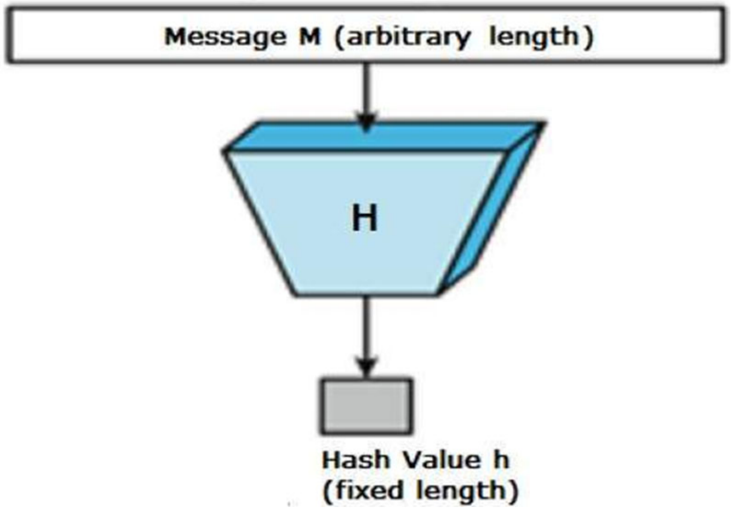
- Encryption algorithms are expensive and consume valuable system resources.

- Therefore, in the cases that we just want to investigate integrity of the data (make sure that the data has not been changed by any intruder) while the data does not have to be hidden, we use hash functions.

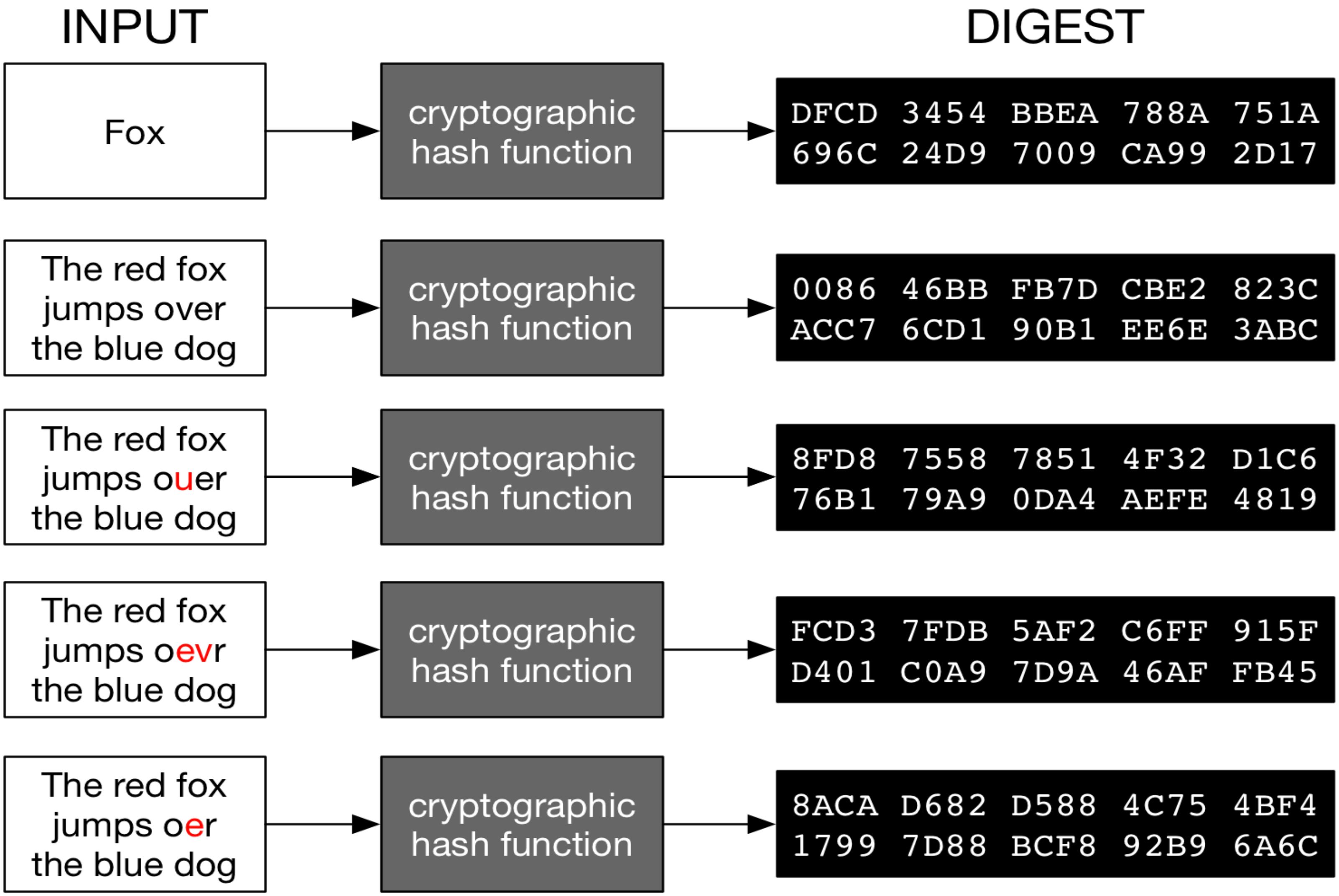
Hash functions cont…

- The hash functions create a fixed-length output from a variable-length data which is called hash value/message digest (MD)/hashed data.

- After making the MD, the plain-text message and its MD are sent to the receiver. The receiver applies the same hash function over the received plain-text message to produce a new MD. Then the receiver compares the received MD and the calculated MD and if the result matches, this means the received data was not altered and it is original.



Hash functions cont…



INPUT

DIGEST

Fox → cryptographic hash function → DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17

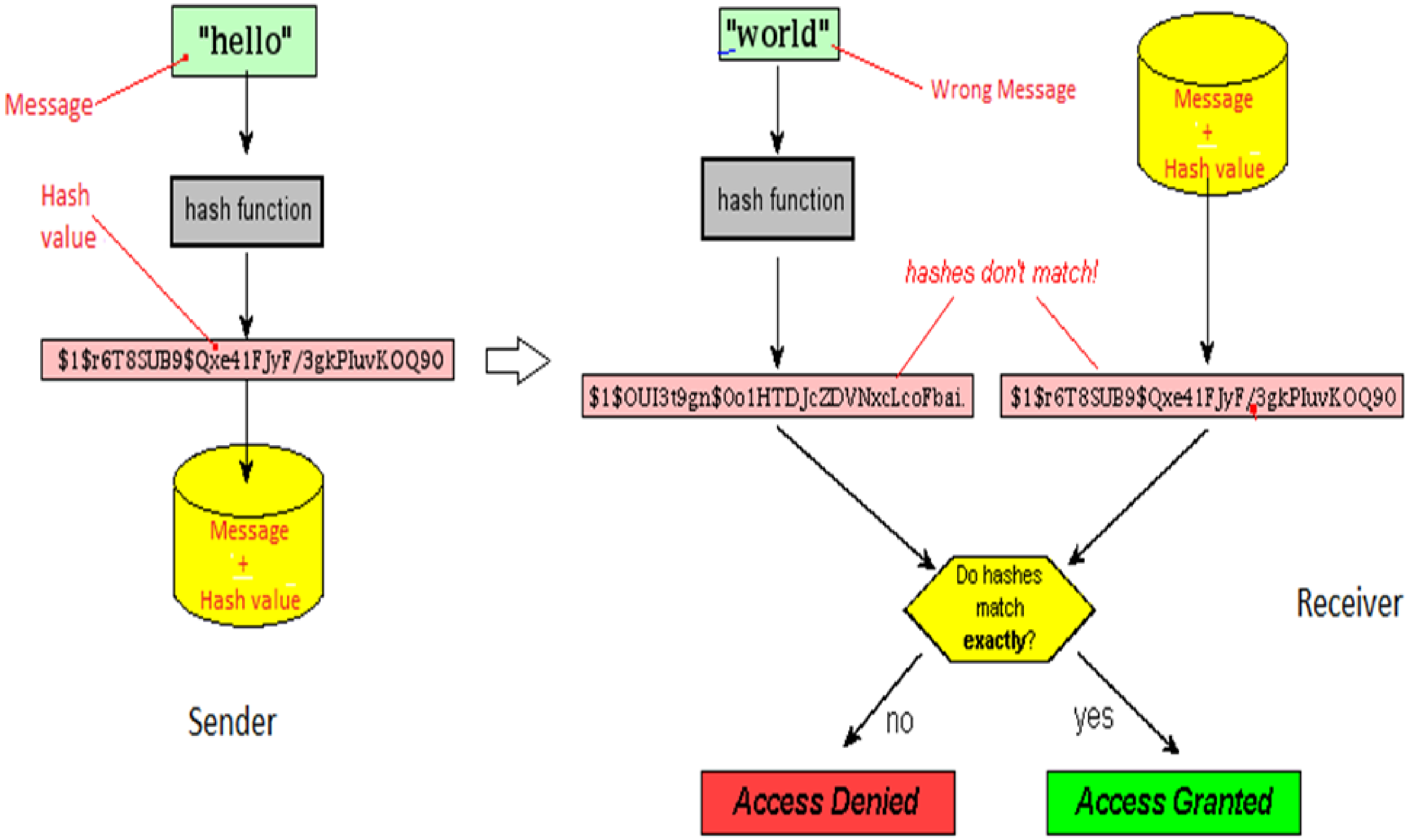
The red fox jumps over the blue dog → cryptographic hash function → 0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC

The red fox jumps ouer the blue dog → cryptographic hash function → 8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819

The red fox jumps oevr the blue dog → cryptographic hash function → FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45

The red fox jumps oer the blue dog → cryptographic hash function → 8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

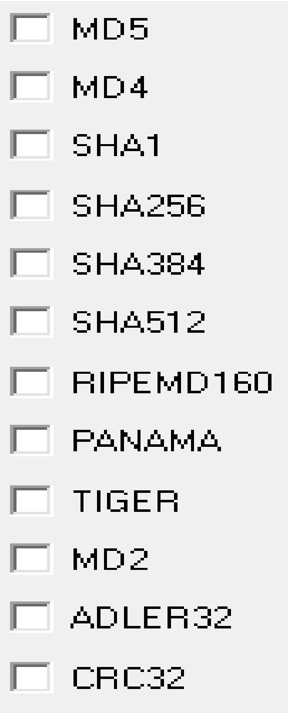
Hash functions process: checking integrity



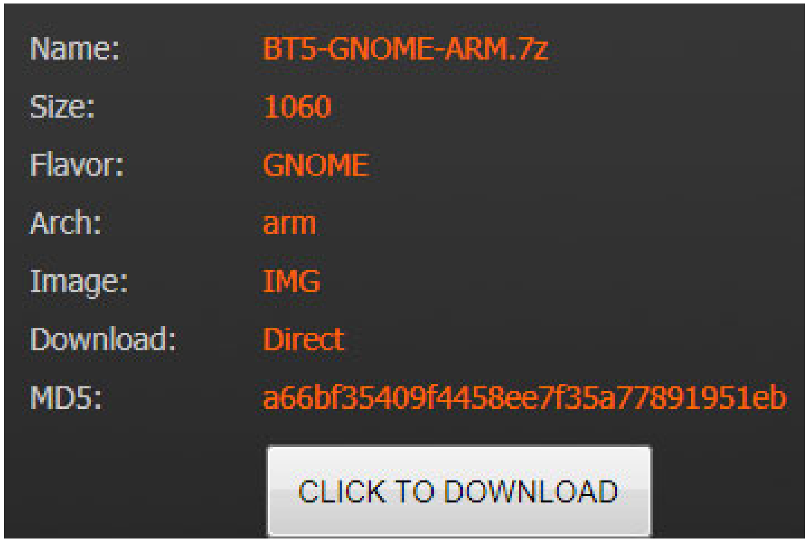
Hash functions cont…

- The MD is used to identify the data integrity and would not be reversed. A hash function compresses the bits of a message to a fixed-size hash value in a way that makes it difficult to come up with a message that would hash to a particular hash value.

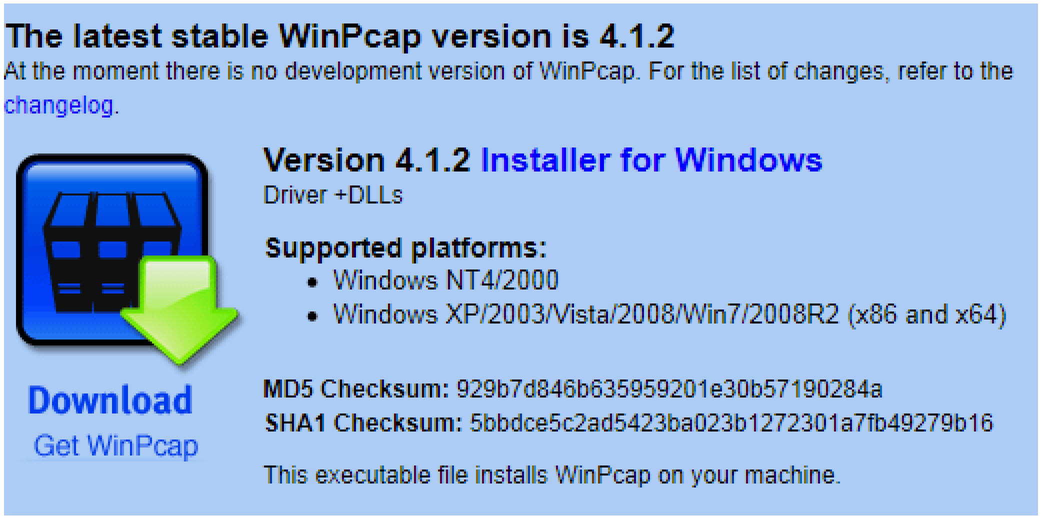
- The most common hash functions are MD5, SHA1 (secure hash algorithm), and SHA2.



Hash functions cont…



Name:	BT5-GNOME-ARM.7z
Size:	1060
Flavor:	GNOME
Arch:	arm
Image:	IMG
Download:	Direct
MD5:	a66bf35409f4458ee7f35a77891951eb



The latest stable WinPcap version is 4.1.2

At the moment there is no development version of WinPcap. For the list of changes, refer to the changelog.

Version 4.1.2 Installer for Windows

Driver +DLLs

Supported platforms:

- Windows NT4/2000
- Windows XP/2003/Vista/2008/Win7/2008R2 (x86 and x64)

MD5 Checksum: 929b7d846b635959201e30b57190284a

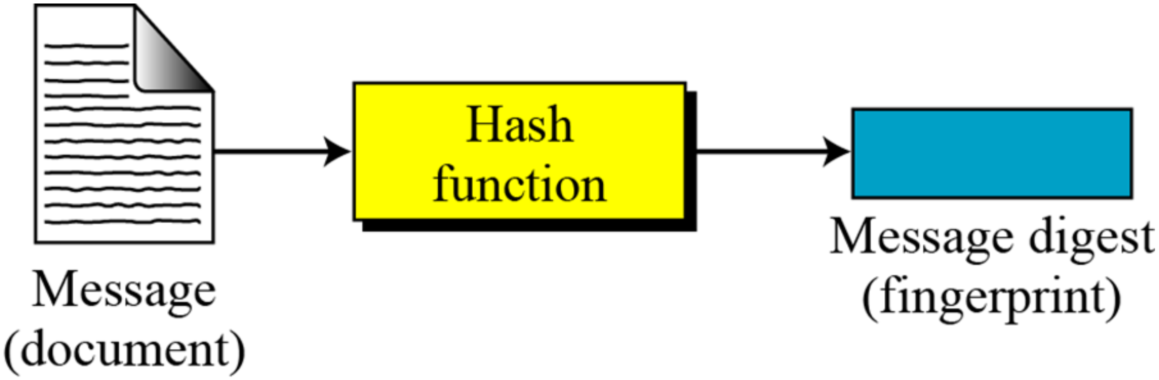
SHA1 Checksum: 5bbdce5c2ad5423ba023b1272301a7fb49279b16

This executable file installs WinPcap on your machine.

Hash functions cont…

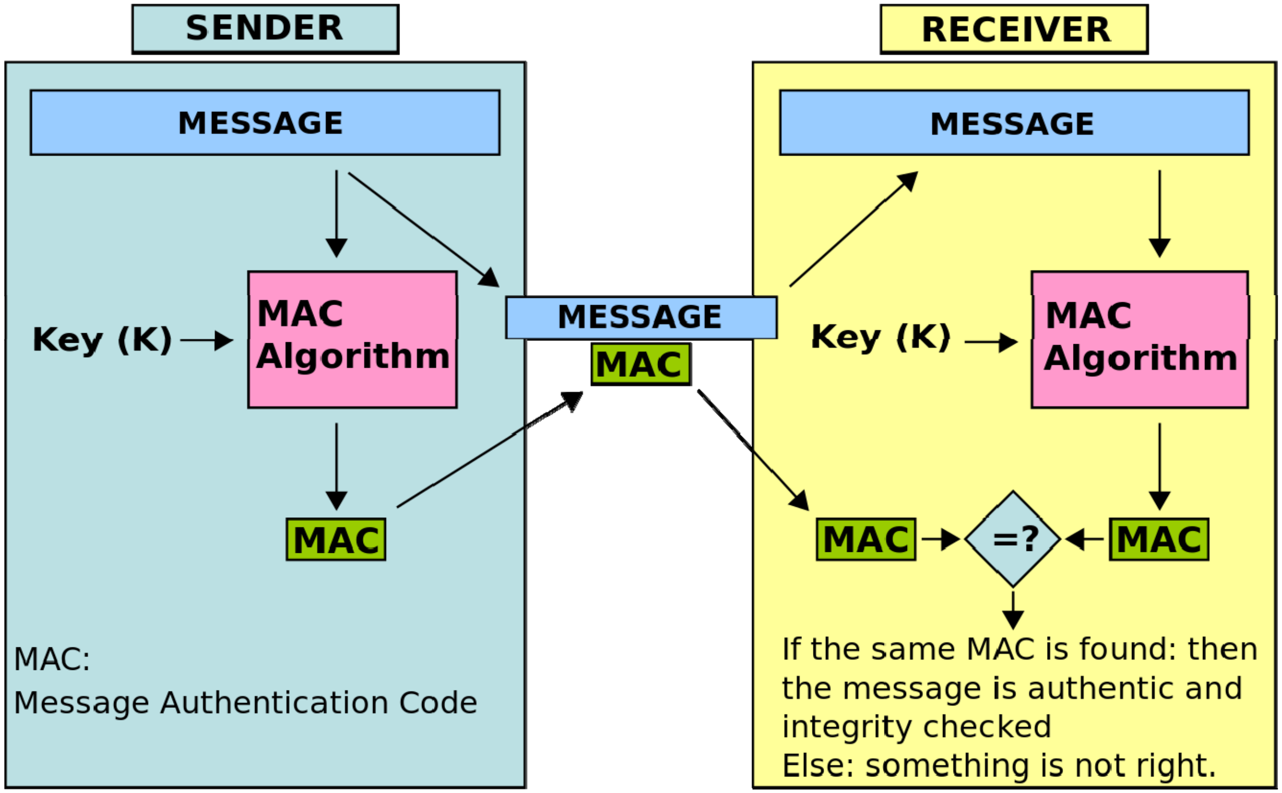
- However, hash functions are keyless and just provide integrity not authentication.

- What if a hacker intercepts message, alters it, generates a new hash value, and sends the message and its new hash value to the recipient claiming to be the original sender.



Message authentication code (MAC)

- Thus, in addition of ensuring the integrity of the message, sometimes we need to ensure the data origin authentication as well.
- It is where Message authentication code (MAC) comes to play.
- MAC is a function of the message and a secret key that by an algorithm produces a fixed-length value that serves as the authenticator: MAC = C(K,M).



MAC:
Message Authentication Code

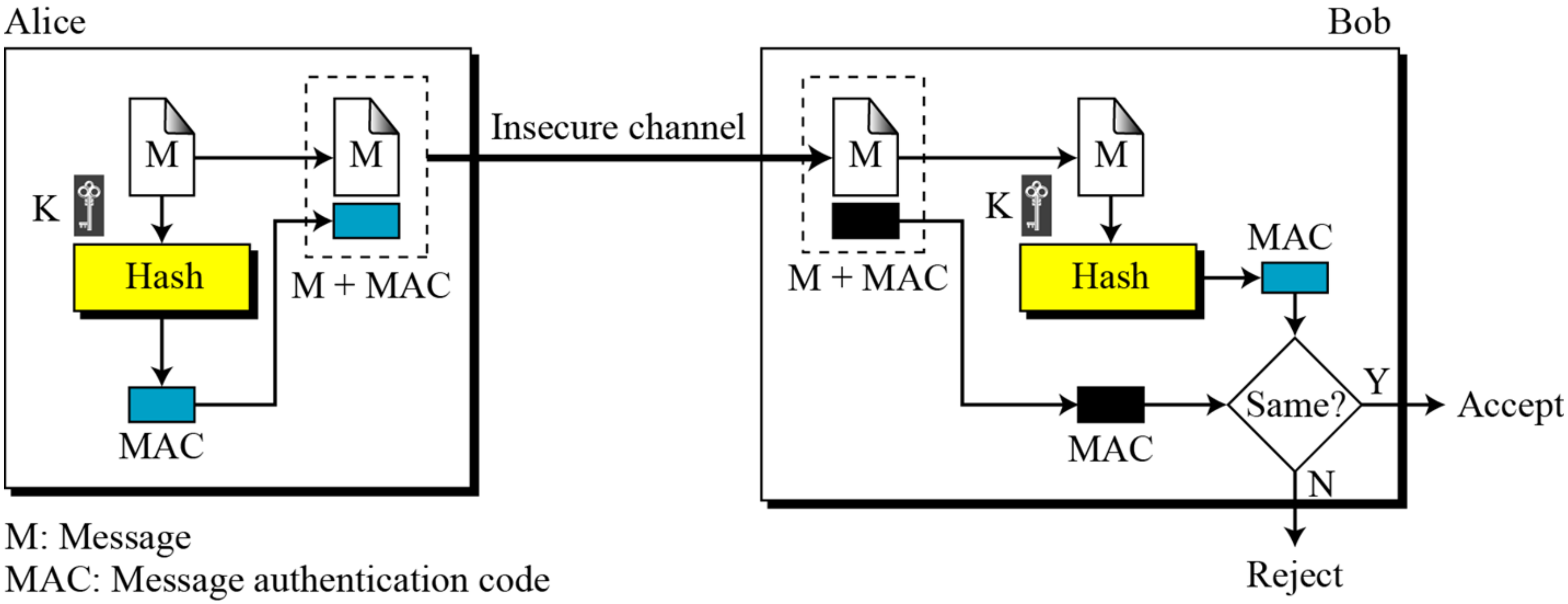
If the same MAC is found: then the message is authentic and integrity checked
Else: something is not right.

MAC cont…

- There are two types of MAC:
  - Hash-based MAC (HMAC): it uses an hash function to generate MAC.
  - Cipher-based MAC (CMAC): is hash-less MAC. It uses an encryption algorithm (DES, AES, etc.) to generate MAC.

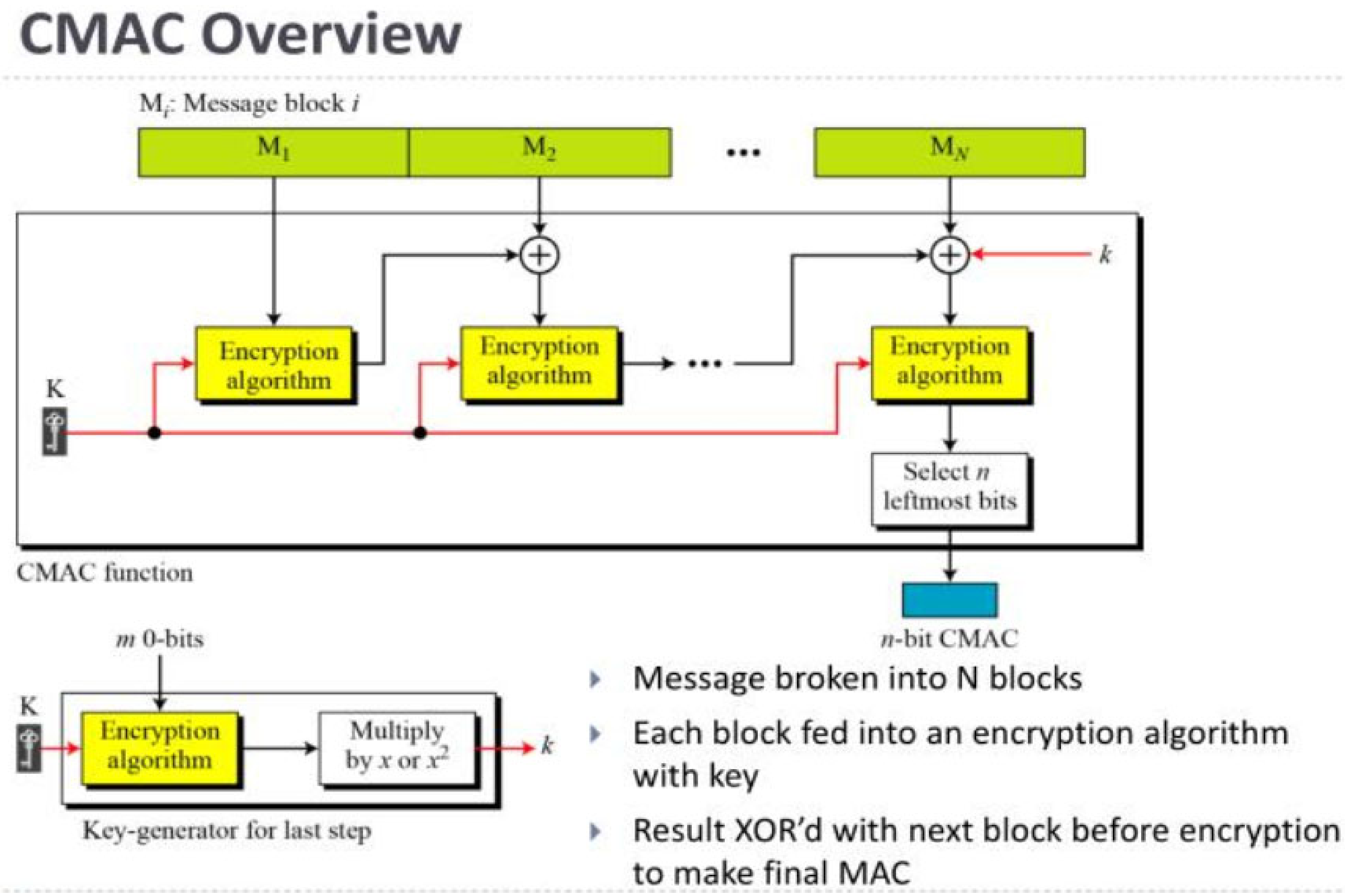
HMAC

- Hashed-based message authentication code (HMAC) is the process of combining existing cryptographic hashing functions with a key.
- HMAC is the combination of encryption and hashing:
  - The sender calculates the hash value, encrypts it with his symmetric key, transmit the data and encrypted hash value together.
  - The recipient uses his copy of the symmetric key to decrypt the original hash value.



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

CMAC



CMAC Overview

- Message broken into N blocks
- Each block fed into an encryption algorithm with key
- Result XOR'd with next block before encryption to make final MAC

Symmetric-key cryptography

- The symmetric-key/shared secret/secret-key/private-key cryptography is a mechanism by which the same key is used for both encrypting and decrypting.
- Analogy: locking and unlocking a door with the same key.
- This characteristic requires sophisticated mechanisms to securely distribute the secret-key to both parties.

Public-key cryptography/asymmetric

- Public-key/asymmetric cryptography is any cryptographic system that uses two keys:
  - a public key known to everyone
  - a private or secret key known only to the recipient of the data.

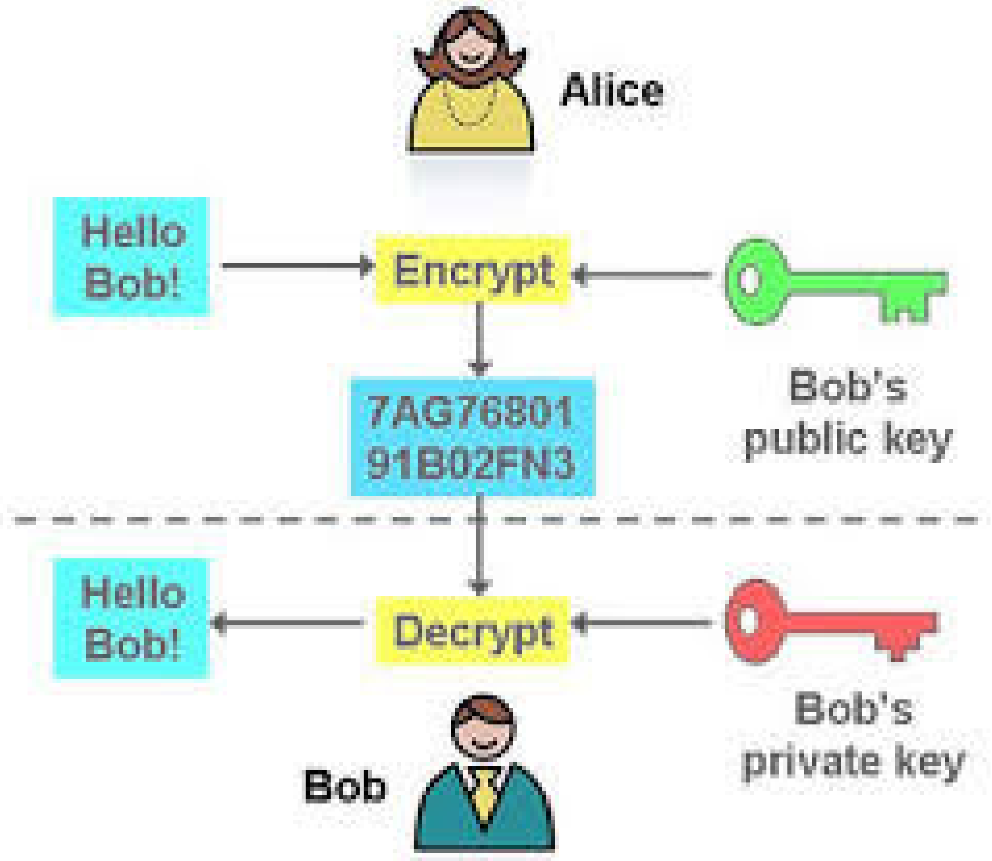
- To generate two keys, algorithms such as RSA, DSA, or ElGamal, Diffie-Hellman are used.

Public-key applications

- Asymmetric key algorithms are important as they are used in many areas:
  - Encryption
  - Authentication
  - Digital signatures
  - Digital certificates
  - Key distribution

Public-key encryption

- In public-key encryption, a message is encrypted with a recipient's public key. The message cannot be decrypted by anyone who does not possess the matching private key, who is thus presumed to be the owner of that key and the person associated with the public key.



Public-key encryption cont…

- Encrypting data and messages offers the following security benefits.
  - Confidentiality: because the content is encrypted with an individual's public key, it can only be decrypted with the individual's private key, ensuring only the intended recipient can decrypt and view the contents
  - Integrity: part of the decryption process involves verifying that the contents of the original encrypted message and the new decrypted match, so even the slightest change to the original content would cause the decryption process to fail

Digital signature

- The digital signature of an electronic document is the equivalent to a handwritten signature on a document in paper.

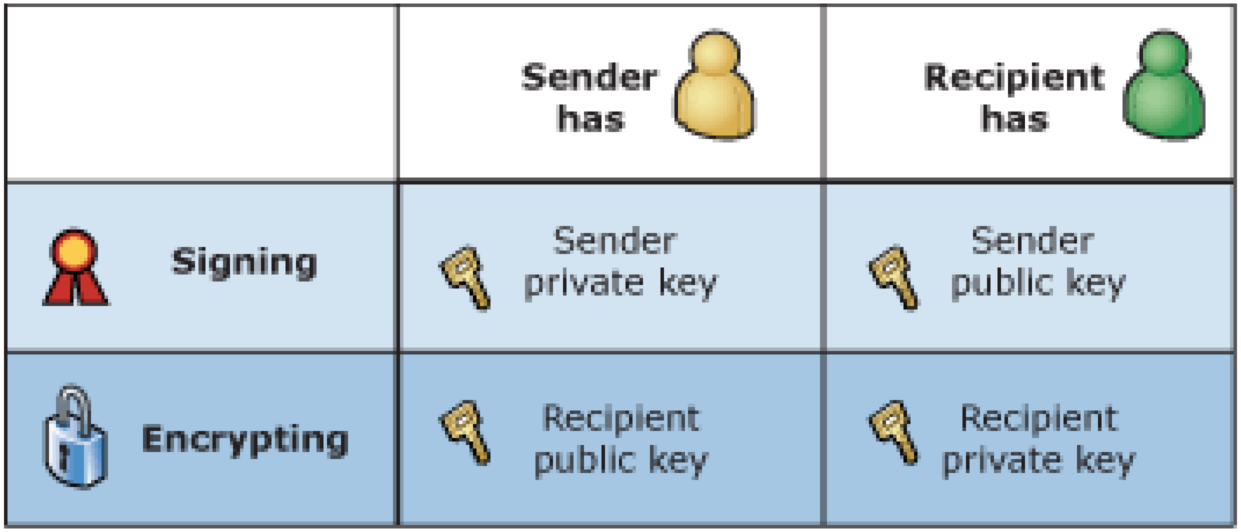
- Digital signatures ensures that a message wasn't altered and that the sender is the one who 'signed' the message, the owner of the key pair.

- Digital signatures use asymmetric cryptography: the signing process uses the private key and the verification process uses the public key from the same key pair.

Digital signature vs. Encryption

- For the Encryption, the content is encrypted using public key of receiver and can only be decrypted with the private key of receiver.

- However, for the Digital signatures, the content is signed with private key of sender and is verified by the public key of sender.



	Sender has	Recipient has
Signing	Sender private key	Sender public key
Encrypting	Recipient public key	Recipient private key

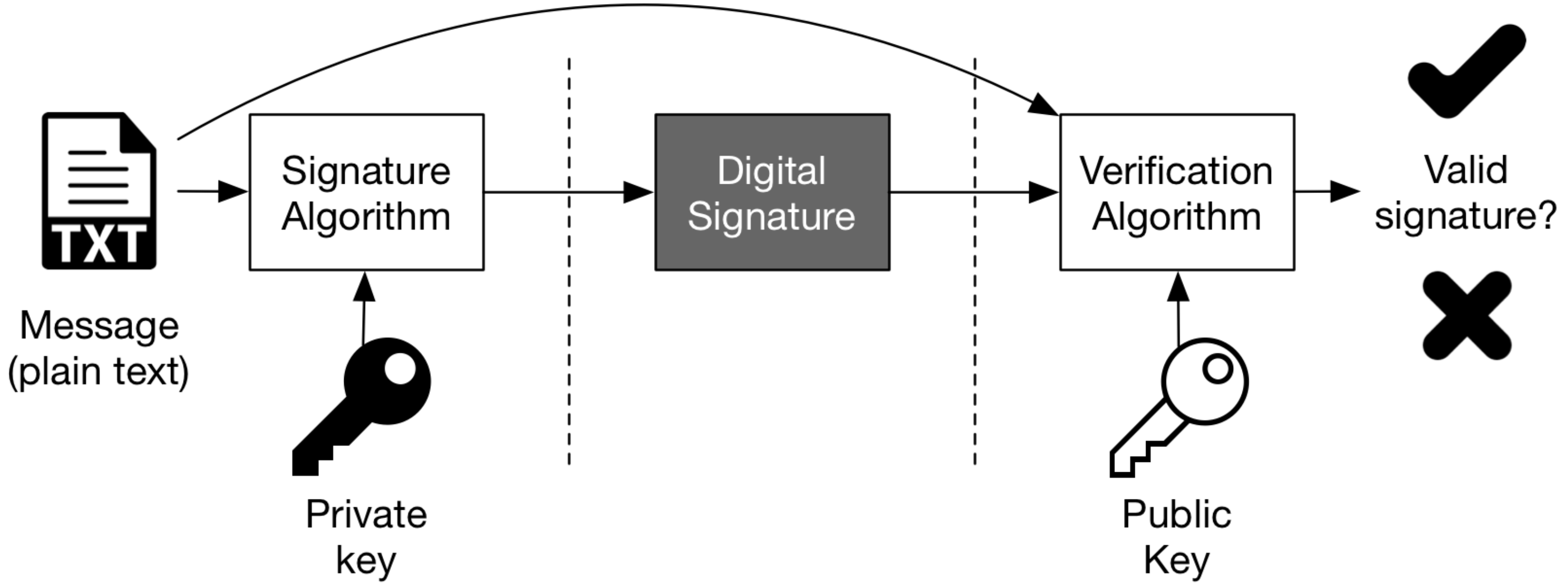
Digital signature functions

- The digitally signing documents and emails offers the following benefits:
  - Authentication of originator: since the sender's unique private key was used to apply the signature, recipients can be confident that the sender was the one to actually apply the signature
  - Non-repudiation of origin: since the sender is the only one with access to the private key used to apply the signature, he/she cannot later claim that it wasn't him/her who applied the signature
  - Integrity of a message: when the signature is verified, it checks that the contents of the document match what was in there when the signature was applied. Even the slightest change to the original document would cause this check to fail. Once a document is signed, its data can not be altered without invalidating the signature.

Digital signature generation

- A digital signature can be created in two methods:
  - Without hashing
  - With hashing

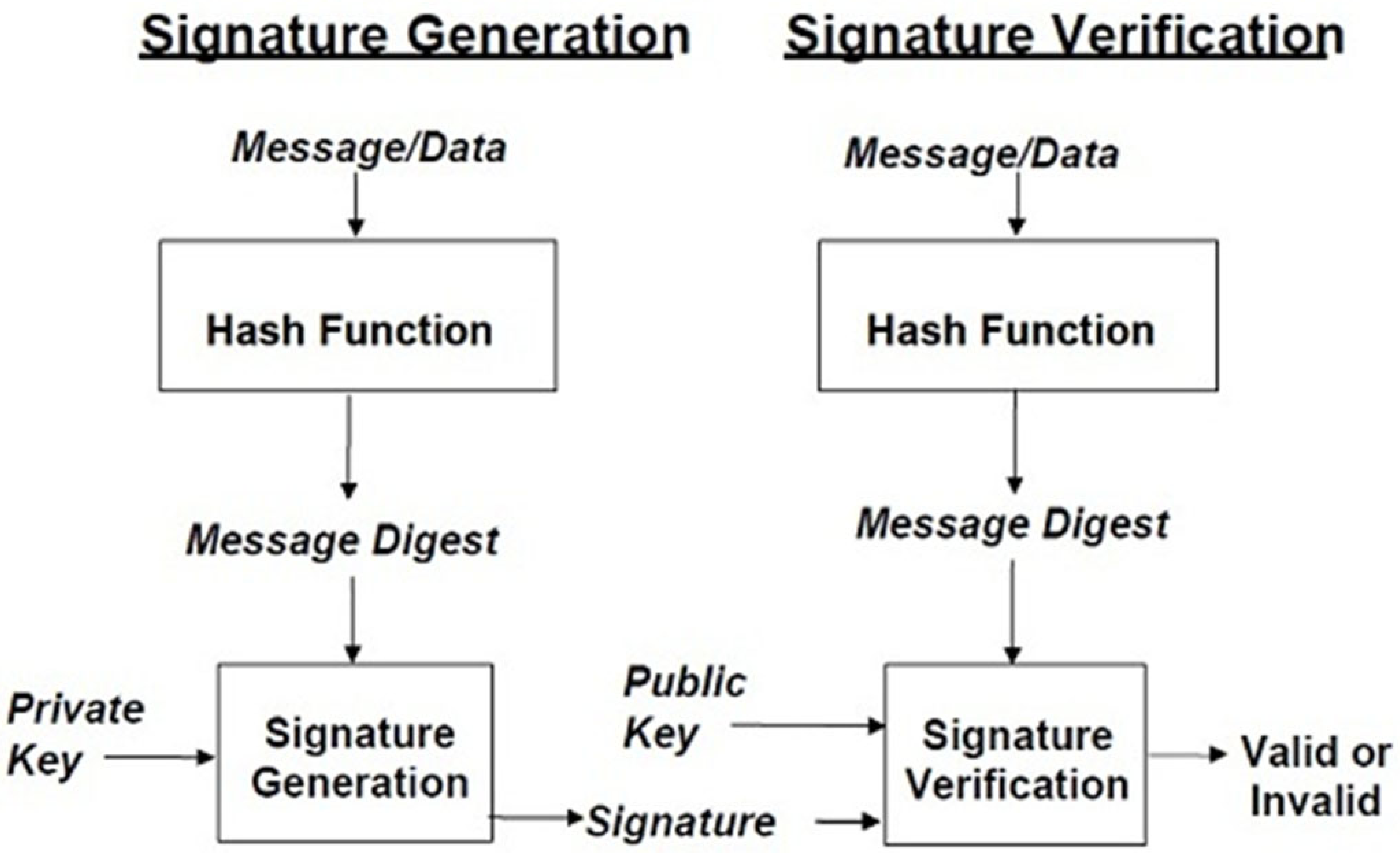
Digital signature without hashing



Digital signature with hashing

- For Digital signature, another technique used is hashing.
- The digital signature will be applied to the digest because a hash function can convert an arbitrary input into a fixed length value, which is usually much shorter.

Digital signature with hashing cont…



Digital certificate

- As we can see, public key plays an important role:
- Notice:
  - In public key cryptography, the sender relies receiver’s public key to encrypt the massage.
  - In digital signature, the receiver relies on the sender’s public key to verify the signature.
- But, how can both of them be sure of each other's public key? That is where digital certificates come to play.

Digital certificate cont…

- A digital certificate is used to bind a person with a specific public key.
- If there were no certificates, the signature could be easily be forged.
- Someone could pretend to be Alice and sign documents with a key pair he claims is Alice's.
- This way, the recipient could not check if the public key belongs to the sender.

Digital certificate analogy

- Digital certificates function similarly to identification cards such as passports and drivers' licenses.
- ID cards are issued by recognized (government) authorities. When someone requests an ID card, the authority verifies the identity of the requester, certifies that the requester meets all requirements to receive the ID card , and then issues it.
- When an ID card is presented to others, they can verify the identity of its owner.

- The ID card provides the following security benefits:
  - It contains personal information to help identify and trace the owner.
  - It contains the information that is required to identify and contact the issuing authority.
  - It is designed to be tamper-resistant and difficult to counterfeit.
  - It is issued by an authority that can revoke the identification card at any time (for example, if the card is misused or stolen).
  - It can be checked for revocation (ابطال) by contacting the issuing authority.

PKI

- Managing keys and digital certificates is complex, so the public key infrastructure (PKI) framework was created.

- A PKI system is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.

PKI services

- **PKI is a framework.** It can provide 4 services:
  - Authentication using digital certificate: to identify a user who claim who he is, in order to access the resource.
  - Non-repudiation using digital signature: to make the user becomes unable to deny that he has sent the message, signed the document or participated in a transaction.
  - Confidentiality using encryption: to make the transaction secure, no one else is able to read/retrieve the ongoing transaction unless the communicating parties.
  - Integrity: to ensure the information has not been tampered during transmission.

PKI digital certificate: X.509

- Among the existing formats for PKI digital certificates, the X.509 PKI is the most common (compared to PGP and SKIP certification methods).

- X.509 is a standard that is used to design and create different types of digital certificates.

- X.509 certificates are generic and highly flexible format. They are used in many protocols such as TLS/SSL, IPSEC, SET, S/MIME (Email), and eBusiness applications.

- For example, SSL uses X.509 certificates. We say, SSL makes use of what is known as asymmetric cryptography, commonly referred to as public key cryptography (PKI).

X.509

- An X.509 digital certificate proves the identity of the certificate holder. Certificate-Based Authentication.

- Digital certificates are issued by a trusted third party, called certification authority (CA).

- Digital Certificate are data issued by trusted CA and signed by CA's private key.

- CA say that "Alice's public key is ABC“ and Bob's public key is DEF“.

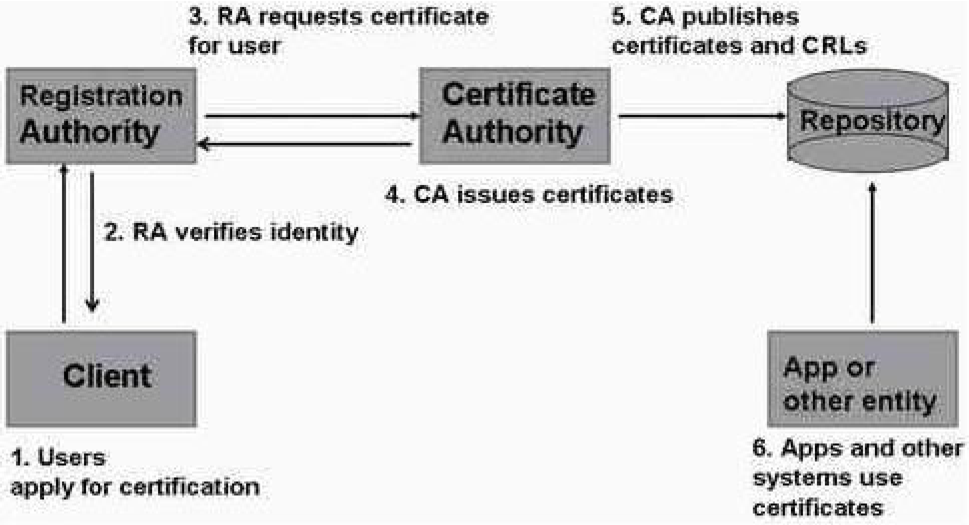
- The owner of the certificate does not need to share public key. Whenever the recipient needs, it goes to CA to search for Public key that's related with that certificate.

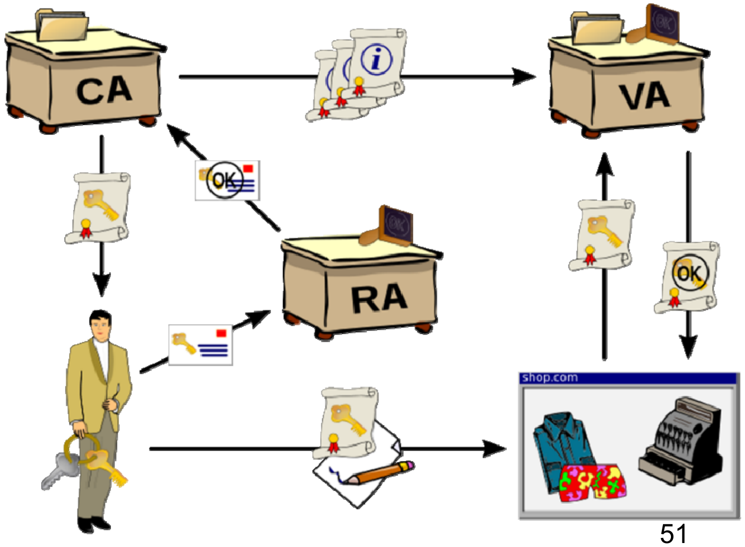
X.509 elements

- A typical X.509 PKI system consists of the following components:
  - A registration authority (RA) that verifies subject's identity.
  - A certificate authority (CA) that issues the digital certificate binding subject's identity with subject's public key.
  - A validation authority (VA) that verifies the digital certificate of a subject.
  - A certificate revocation list (CRL) that contains certificates revoked (لغو) by the CA.
  - Subjects (users, organizations, or systems) who wants to use the public and private key technology to exchange information securely.
  - A public and private key encryption technology that can be used to encrypt and decrypt information.
  - Policies that govern the operation of the PKI.
  - The digital certificates themselves.
  - Applications that are written to use the PKI.

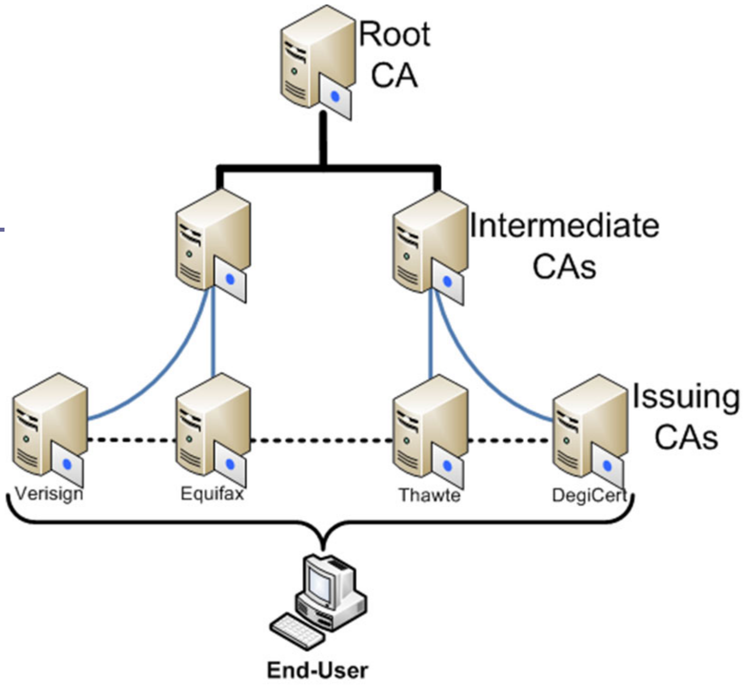
How X.509 works

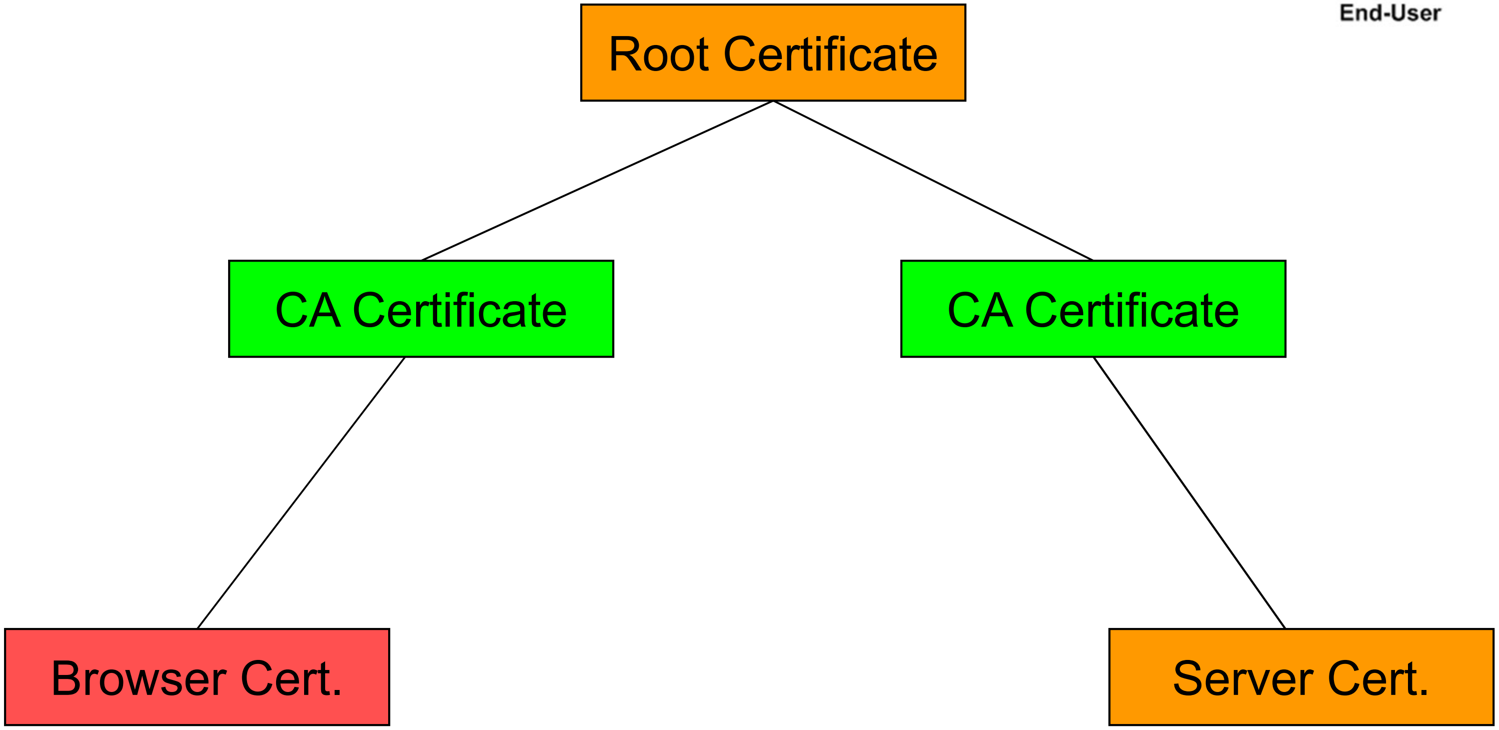
- A user sends his requests for a digital certificate to registration authority (RA). The RA is responsible for accepting requests for digital certificates and authenticating the entity making the request.
- The RA verifies user requests for a digital certificate and tells the certificate authority (CA) to issue it. Then, the CA, a trusted agent such as Corporation or Bank, issues the certificate and saves the CRLs on certificate store.
- After that, the user can digitally sign a contract using his new certificate. His identity is then checked by the contracting party with a validation authority (VA) which again receives information about issued certificates by the certification authority.


3. RA requests certificate for user
5. CA publishes certificates and CRLs
Registration Authority
Certificate Authority
Repository
4. CA issues certificates
2. RA verifies identity
Client
App or other entity
1. Users apply for certification
6. Apps and other systems use certificates



CAs trust model





Root Certificate

CA Certificate

CA Certificate

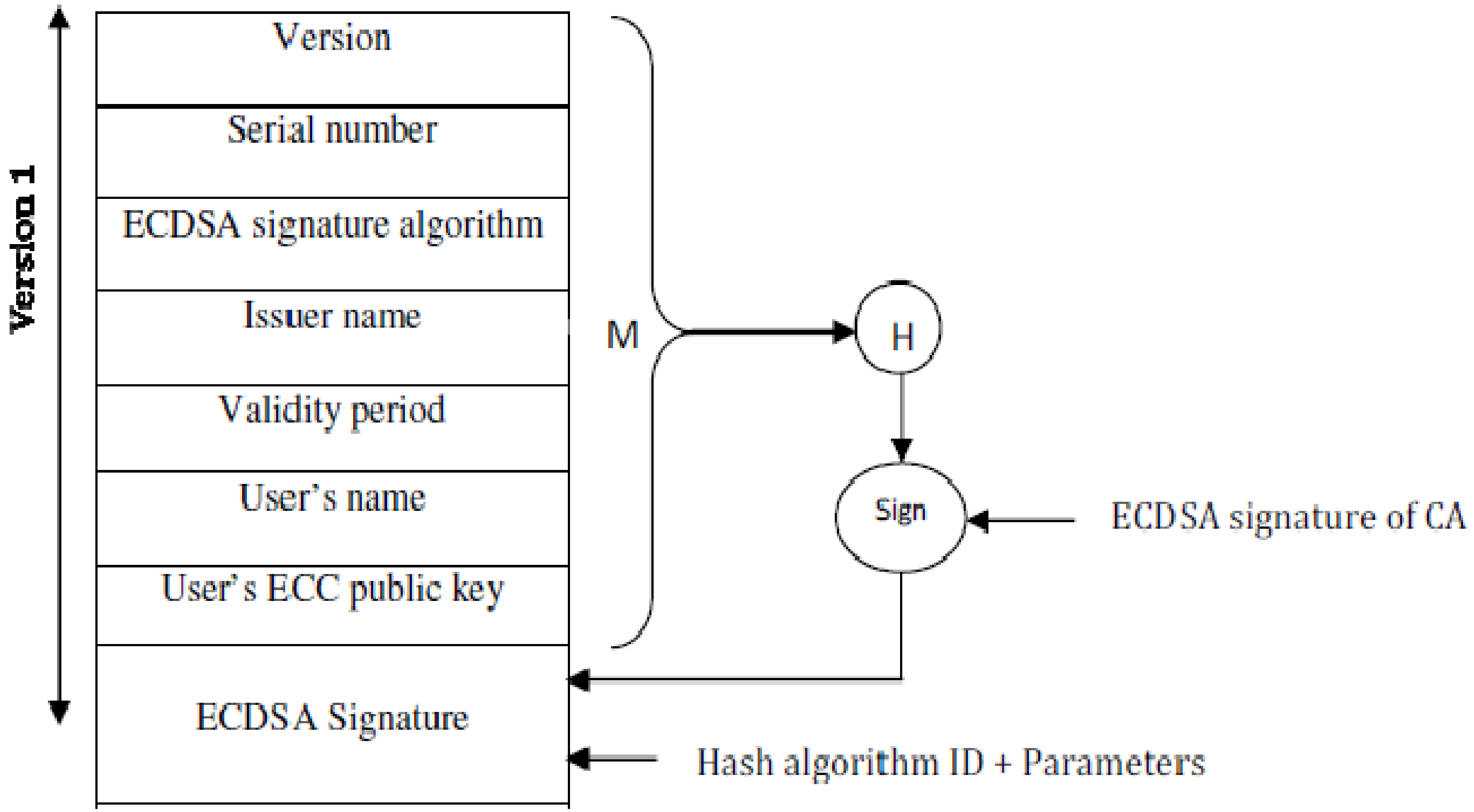
Browser Cert.

Server Cert.

X.509 information

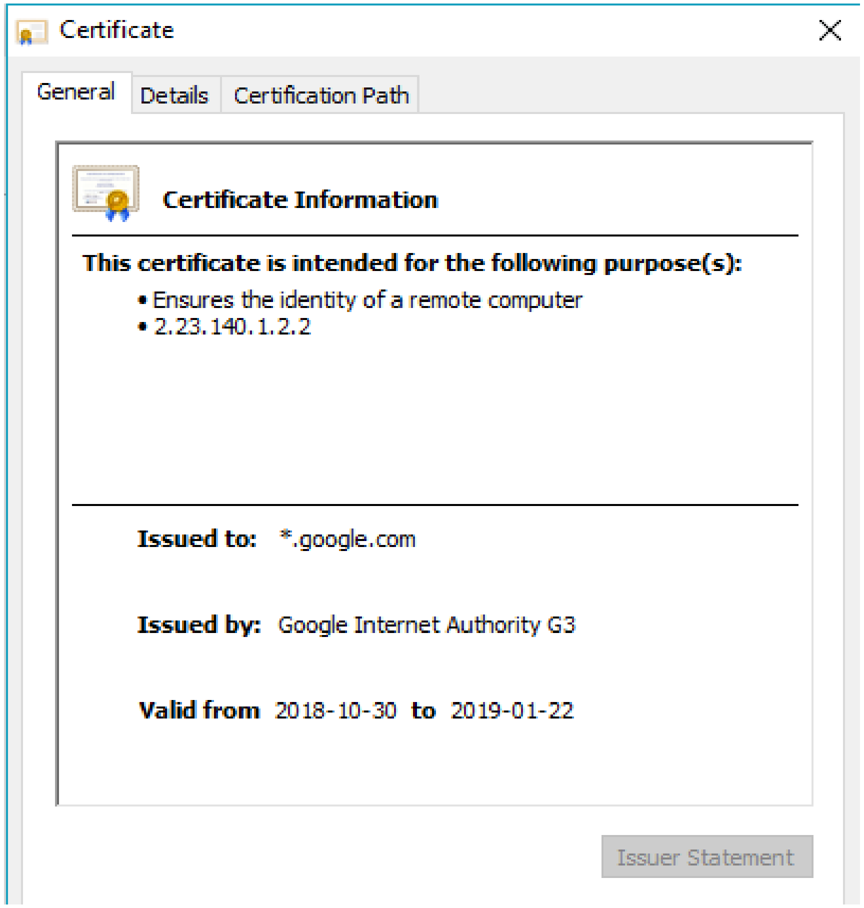
- An X.509 certificate contains information about the identity to which a certificate is issued and the identity that issued it. Standard information in an X.509 certificate includes:
  - Version – which X.509 version applies to the certificate (which indicates what data the certificate must include)
  - Serial number – the identity creating the certificate must assign it a serial number that distinguishes it from other certificates
  - Algorithm information – the algorithm used by the issuer to sign the certificate
  - Issuer distinguished name – the name of the entity issuing the certificate (usually a certificate authority)
  - Validity period of the certificate – start/end date and time
  - Subject distinguished name – the name of the identity the certificate is issued to
  - Subject public key information – the public key associated with the identity
  - Extensions (optional)

X.509 information cont…



Example of SSL X.509 digital certificate

- The data included in the digital certificate contains:
  - Owner of certificate
  - Name of the CA (who issued the certificate)
  - The expired date
  - other types of metadata



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- 2.23.140.1.2.2

Issued to: *.google.com

Issued by: Google Internet Authority G3

Valid from 2018-10-30 **to** 2019-01-22

Key distribution

- One of the biggest problems in cryptography is the distribution of keys. Suppose you live in the city A and want to pass information secretly to your friend in city B. In order to transmit data securely, you two need to agree on keys to encode/decode messages. But you must give keys to your friend in a safe way:
  - If you mail them, they might be stolen.
  - If you send them cryptographically, and someone has broken your code, that person will also have the next key.
  - If you have to go to city B regularly to hand-deliver the next key, that is also expensive.
  - If you hire some courier to deliver the new key, you have to trust the courier.

- The solution to address this problem is public key cryptography.