Cybersecurity
420-950-VA

Vanier College
Tiago Bortoletto Vaz

Day plan

- Check-in
- Finish previous slides (HMACs, digital signatures and certificates)
- Cont. digital certificates
- Demo PicoCTF cryptography challenges
- Practical usage of asymmetric cryptography:
  - Lab4: data encryption, digital signatures (email and commits)

Disclaimer:

These slides are heavily base on the book:

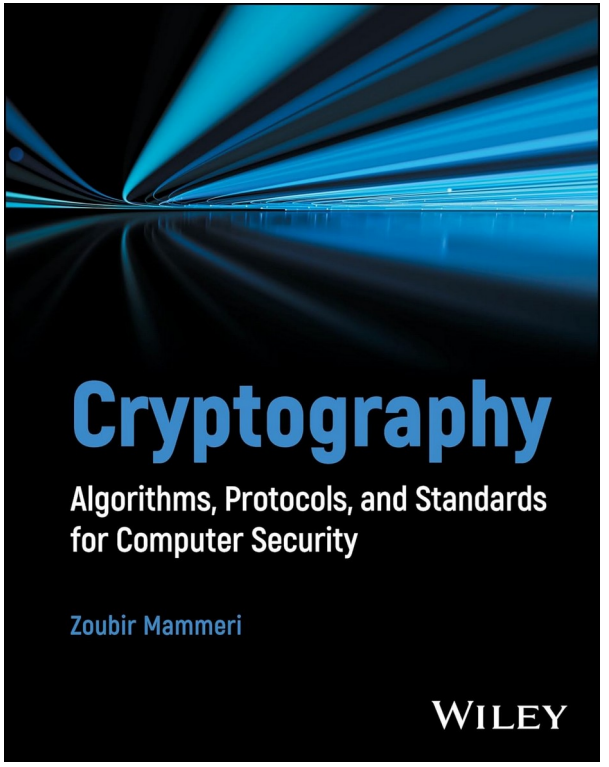
Cryptography: Algorithms, Protocols,
and Standards for Computer Security

by Zoubir Z. Mammeri

ISBN: 978-1-394-20750-3

February 2024

624 pages



Digital certificates (cont.)

- There exist two approaches to establish trust between communicating entities: trust based on **public keys** and trust based on **symmetric keys**.
- In the first category, to perform cryptographic operations (e.g. message decryption or signature verification), users of a public key require confidence that the associated private key (used to encrypt or sign) is owned by the legitimate remote entity (person, system, or organization).
- This confidence can be obtained through digital certificates, which are delivered by trusted third parties, called **Certificate authorities** (CAs).

Digital certificates (cont.)

- To better understand the notions relating to digital certificates in the computer-based society, let us take the following example: imagine someone who wants to sell a painting to somebody, who can afford it. The seller claims that the painting is made by a known painter and his/her signature is at the bottom of the painting.
- The painter’s signature is publicly known. The painting is (very) expensive. The question is: will the buyer take the seller at his/her word? Of course not. He/she requires a certificate (a document), which proves that the signature on the painting is that of the painter.
- The buyer will not trust any certificate; rather, he/she asks the seller to provide a certificate signed by a known authority in the art field, and whom the buyer trusts.

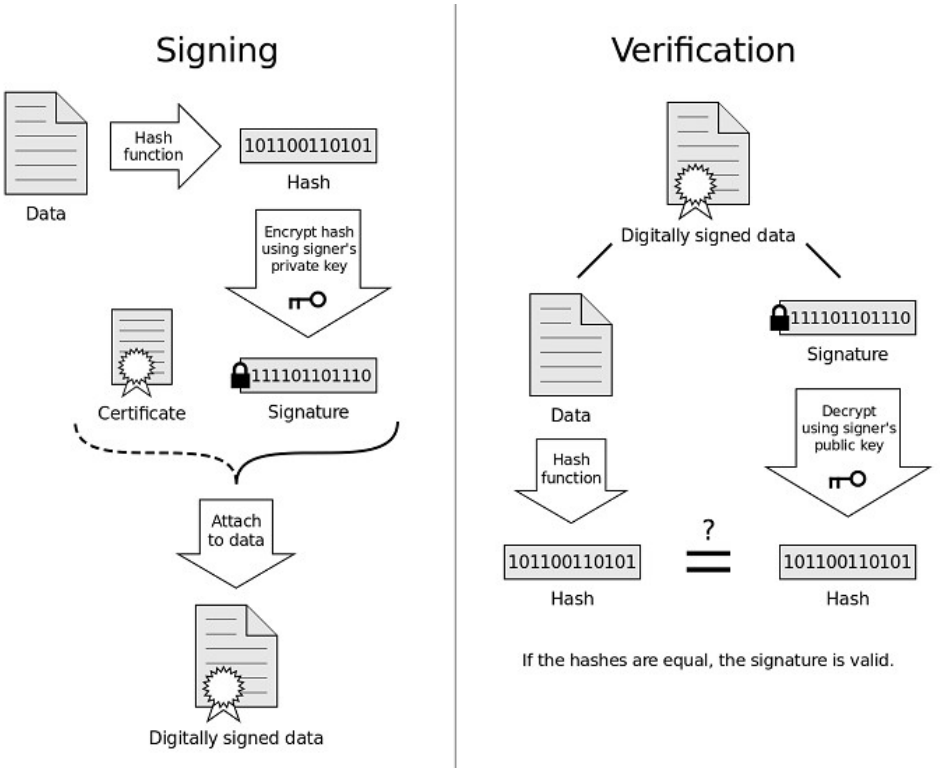
Digital certificates (cont.)

- Public-key infrastructures are the frameworks, which provide certification management functions (creation, granting, revocation, renew, cancellation, and storage of digital signatures).
- They are of paramount importance to establish trust between partners that do not a priori trust each other in the open digital world. Today, digital certificates are used by billions of end-entities, including web servers and their clients, in many applications, such as calls and conferences via VPNs, cloud servers, and Internet-of-things devices.
- The main protocol to secure communications over the internet is with no doubt TLS (Transport Layer Security), which is the underlying security layer of the well-known HTTPS.

Digital certificates (cont.)

- Definitions:
  - **Digital certificate** (or public-key certificate): it is an electronic document used to prove the ownership of a public key.
  - **X.509 certificate**: it is a digital signature compliant with the ISO/ITU-T X.509 standard.
  - **Owner (of a certificate)**: it is an entity that is identified as the subject in a public-key certificate; it may be an individual, a device, a computer, an organization, a company, or something else.
  - **Certificate authority (CA)**: it is a trusted third party, which signs and issues digital certificates used to prove the ownership of public keys.

Digital certificates (cont.)



https://cheapsslsecurity.com/blog/digital-signature-vs-digital-certificate-the-difference-explained/

Digital certificates (cont.)

X.509 Standard Format:

- A digital certificate is a data structure that contains an entity identity, a public key (including the associated set of domain parameters and the algorithm that can use the public key), the identifier, and the signature of the trusted authority that issued the certificate to bind an entity ID to a public key, and possibly other information.
- The standard format of certificates in Internet domains is the X.509 format, which is defined by the following fields

Digital certificates (cont.)

- The standard format of certificates in Internet domains is the X.509 format, which is defined by the following fields:

Version number	V3
Serial number:	00:EE:90:29:A6:43:6D:7A:8A:09:27:16:8C:23:70:A4:30
Signature algorithm ID:	Hash function = sha256 Encryption algorithm = RSA
Issuer name	Country = US Organization = Google Trust Services
Validity period	Not before = Mon, 30 May 2022 09:54:30 GMT Not after = Mon, 22 Aug 2022 09:54:29 GMT
Subject name	www.google.com
Subject public key	Algorithm = Elliptic Curve, Key size = 256Curve = P-256Public key value = 04:95:7F:89:52:E9:A9:DE:D9:5B:D3:3D:23:54:FF:03:FF:F1:70:BB:A2:59:04:B5:D8:75:5D:A2:1B:D4:46:FD:C3:AF:E3:E3:05:8B:69:7C:D6:B8:DE:CA:99:C7:15:BD:BA:4F:8A:72:A7:AE:B9:48:F8:9E:60:98:C1:E9:06:F7:D8
Extensions	Key usages = Digital signature, server authentication CRL Endpoints = Distribution point http://crls.pki.google/gts1c3/zdATt0Ex_Fk.crl
Signature	Hash = SHA-2560A:F0:03:67:5E:AE:A4:74:0D:05:1C:48:08:2D:D5:BA:D4:7F:60:37:22:04:BA:3C:1B:4C:0E:01:B3:B3:38:F7

Digital certificates (cont.)

Signature of the CA (last field in the previous image):

- To sign a certificate, the CA computes the hash of the fields of the certificate and then encrypts it with its private key.
- Thus, the authenticity of the certificate can be verified using the public key of the CA.
- Any entity, which trusts a CA, knows the public key of that CA.
- Certificate verifier first decrypts the signature using the CA public-key, then it hashes the fields of the certificate, using the same hash function than that used by the CA, and then compares the hashes.

Digital certificates (cont.)

Public key infrastructure (PKI): it is framework that is used to issue, maintain, and revoke digital certificates.

There exist two categories of PKIs: **private** and **public** PKIs.

1) **Private PKI:** it involves the security of exchanges between entities within an organization or a company. Private certificates are issued by internal CAs and are trusted only inside the organization/company.

2) **Public PKI:** it issues certificates for public servers and users to perform e-banking, e-commerce, and many other types of transactions.

Digital certificates (cont.)