COMMUNICATION PROTECTION SYSTEMS THROUGH PUBLIC/PRIVATE KEY INFRASTRUCTURE, DIGITAL SIGNATURE, AUTHORIZATION CERTIFICATES AND TIME STAMPS.

Version 1.6

22/01/2022 – 13/02/2022

By Andrea Nicchi
www.volucer.it

TABLE OF CONTENTS

GENERAL PRINCIPLES

The use of networks and distributed processing paradigms have raised problems of confidentiality and communication protection. A distributed system is characterized by the use of :

- Loacal Network (LAN) / Wide Area Network (Internet);
- Distributed Database Systems;
- inter/intra-company exchange of data and documents;
- applications (e-commerce, e-mail, web systems);

GENERAL PRINCIPLES

Security problems arise from the fact that:

- networks are by their nature insecure;
- both basic and application SW may contain accidental or non-accidental errors;
- databases are distributed on the web and shared by many users;

GENERAL PRINCIPLES

For example, some types of attacks on networks are:

Spoofing of IP addresses: This is the falsification of the sender's address. The defense consists in applying authentication techniques not based on addresses.

Packet sniffing: This is the unauthorized reading of packets destined for another node on the network. The defense consists in adopting cryptographic techniques for the packets

Shadow server: this is a computer (host or user machine) that masquerades as a service provider. The main defense consists in applying server authentication techniques.

GENERAL PRINCIPLES

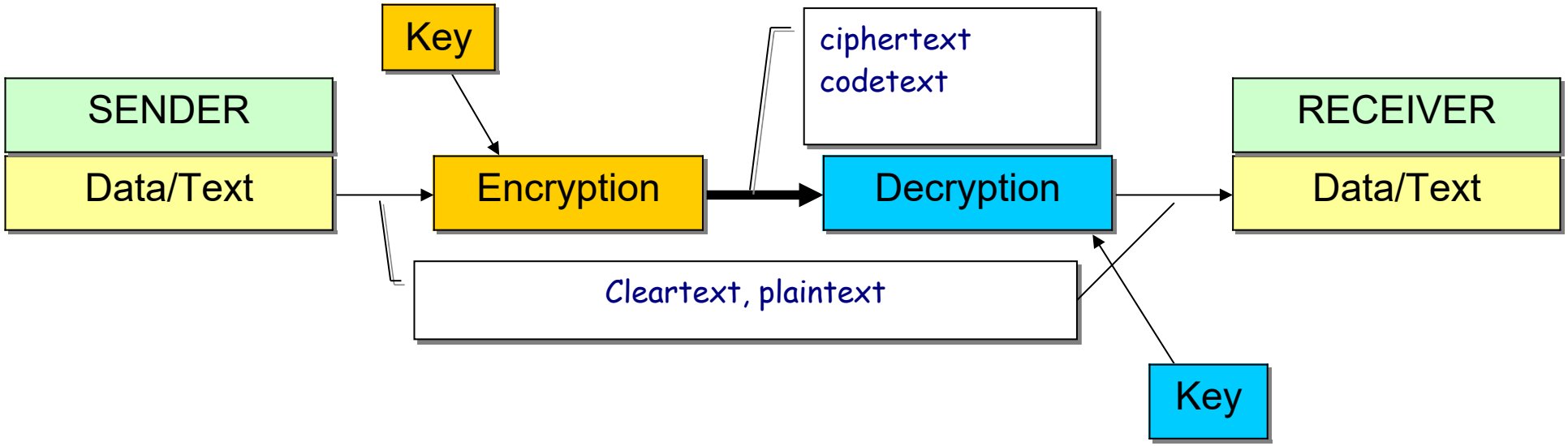
To increase the security in the exchange of information, it is necessary to guarantee the following characteristics for messages and data:

1. **CONFIDENTIALITY**: protection from unauthorized reading;
2. **INTEGRITY**: protection from unauthorized changes;
3. **AUTHENTICITY**: certainty of the source, destination and content of the message;
4. **NON-REPUDIATION**: certainty that the sender and the recipient cannot deny having respectively sent and received the message.

CRYPTOGRAPHY

Etymologically, encryption means "hidden writing" ("scrittura nascosta"). The term is derived from the Greek word **kryptos**, which means hidden. The encryption process always uses:

- **Keys;**
- **algorithm to encrypt** messages in order to make them unreadable to those who do not have the **key**;
- an appropriate **algorithm to decrypt** them.



CRYPTOGRAPHY IN EVERYDAY LIFE

Authentication/Digital Signatures: to verify the origin of a document, the identity of the sender, the time and date a document was sent and/or signed, the identity of a computer or user, and so on.

Time Stamping: Time stamping is a technique that can certify that a certain electronic document or communication existed or was delivered at a certain time.

Electronic Money: It includes transactions carried out electronically with a net transfer of funds from one party to another, which may be either debit or credit and can be either anonymous or identified.

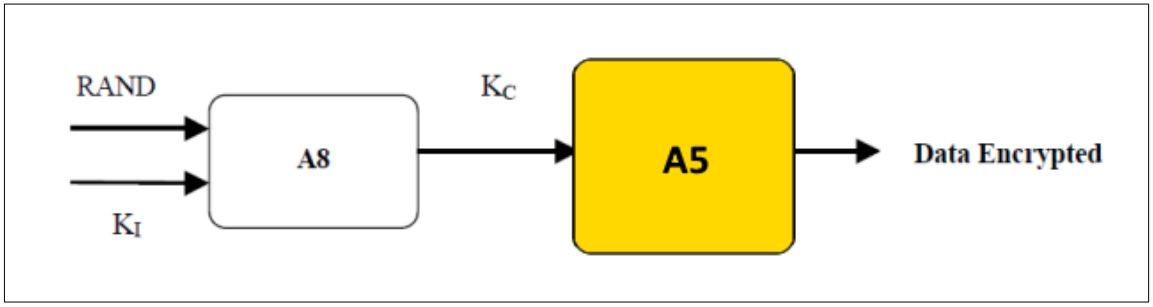
CRYPTOGRAPHY IN EVERYDAY LIFE

Encryption/Decryption in email: securing the content of emails from anyone outside of the email conversation looking to obtain a participant's information.

Encryption in WhatsApp: uses the 'signal' protocol for encryption, which uses a combination of asymmetric and symmetric key cryptographic algorithms. The symmetric key algorithms ensure confidentiality and integrity whereas the asymmetric key cryptographic algorithms help in achieving the other security goals namely authentication and non-repudiation.

CRYPTOGRAPHY IN EVERYDAY LIFE

Sim card Authentication: Authentication To decide whether or not the SIM may access the network, the SIM needs to be authenticated. A random number is generated by the operator, and is sent to the mobile device.



This session KC is used, in combination with the A5 algorithm to encrypt/decrypt the data.

Disk encryption: programs can encrypt your entire hard disk so that that it cannot be deciphered easily by unauthorized people.

SYMMETRIC KEY CRYPTOGRAPHY

1. **M** to denote PLAINTEXT;
2. **C** to denote CIPHERTEXT;
3. **F** mathematical function for ENCRYPTION;
4. $\mathbf{F^{-1}}$ mathematical function for DECRYPTION;
5. **K** to denote KEY.

$$\mathbf{F(M,K) = C \quad - \quad F^{-1}(C,K) = M}$$

A symmetric cipher is an encryption and decryption function for which:

$$\mathbf{F^{-1}(F(M,K),K) \quad = M}$$

The cipher is said to be symmetric because **the same key is used for both encryption and decryption**.

SYMMETRIC KEY CRYPTOGRAPHY

BLOCK CIPHERS

A cryptographic PRIMITIVE is an algorithm that can be used to encode or decode a message.

LOW LEVEL PRIMITIVE: e.g. cryptographic algorithms, …
HIGH LEVEL PRIMITIVE: e.g. digital signature,...

Cryptographic primitives for encryption:

- ✔DES
- ✔Triple DES
- ✔AES

SYMMETRIC KEY CRYPTOGRAPHY

BLOCK CIPHERS: DES

DES – Data Encryption Standard

- algorithm adopted in 1977 by NIST;
- 64-bit block cipher;
- takes as input 64 bits of plaintext and a 64 bits key;
- key size is 56 bit;
- in 1998 Electronic Foundation Frontier (www.eff.org) demostrates that it was not secure.
- It is susceptible to brute-force attack. It was broken in 56 hours.

SYMMETRIC KEY CRYPTOGRAPHY

BLOCK CIPHERS: Triple DES

Triple DES – Data Encryption Standard

it is an algorithm based on DES that can be used to achieve higher level of security than DES alone.

Triple DES encryption consist of:

- taking an input message M;
- encrypting with the first key K1;
- descrypting the resulting message with the second key K2;
- encrypting that message with the third key K3.

Triple DES more secure than DES but it can be up to THREE TIME SLOWER. - TOO MUCH PERFORMACE DEGRADATION

SYMMETRIC KEY CRYPTOGRAPHY

BLOCK CIPHERS: AES

AES – Advanced Encryption Standard

- algorithm by two Belgian cryptographers in August 1999;
- support key and block sizes of 128, 192, and 256 bits;
- three different key lengths: 128, 192, or 256 bits;
- was adopted by NIST in October 2000.

It provides security with larger keys and faster execution time.

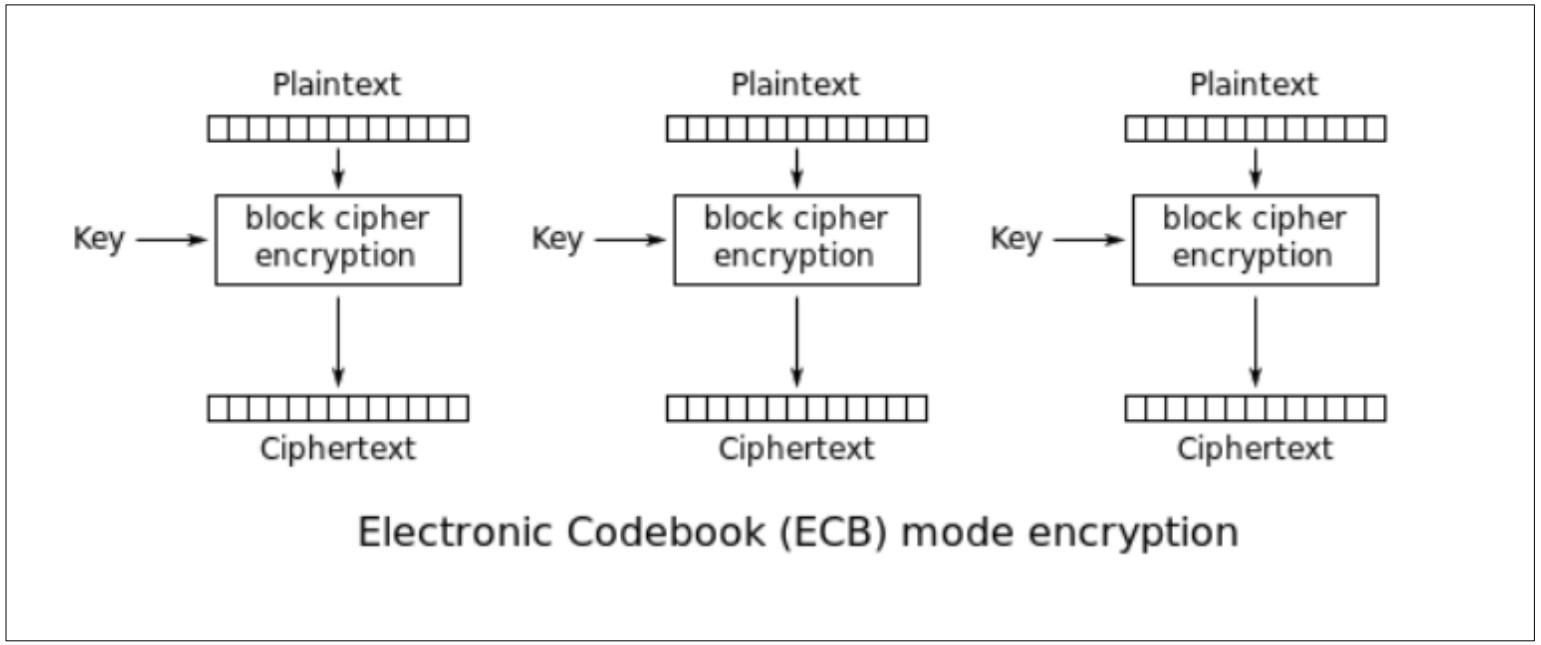
It works well on mobile devices that have slower processors and less memory than desktop computers.

SYMMETRIC KEY CRYPTOGRAPHY

ENCRYPTING MORE DATA

ECB – Electronic Code Block

divide large plaintext in block and encrypt each block at time

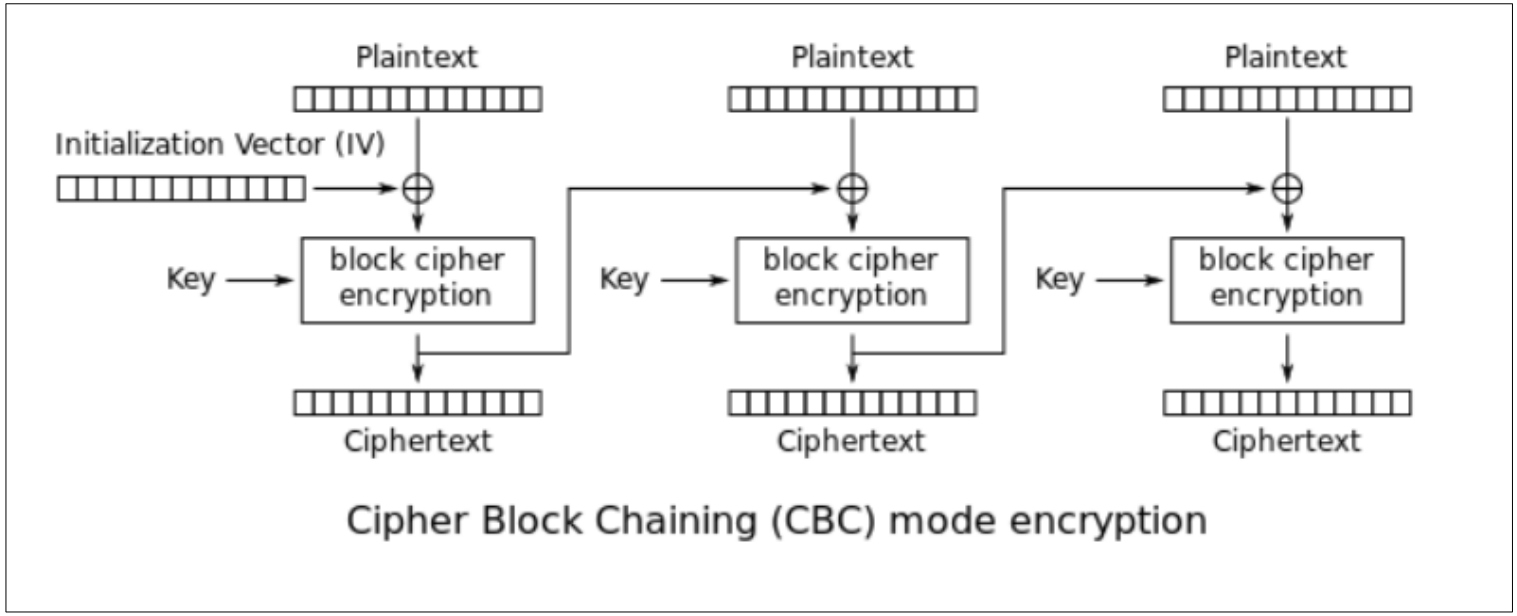


SYMMETRIC KEY CRYPTOGRAPHY

ENCRYPTING MORE DATA

CBC – Cipher Block Chaining

To encrypt the plain text in more secure fashion we use the output of previous block of ciphertext with the current plaintext block before encrypting to produce the next ciphertext block.



Cipher Block Chaining (CBC) mode encryption

SYMMETRIC KEY CRYPTOGRAPHY

SECURITY BY OBSCURITY ?

- The algorithms are completely public.
- The security doesn't depend on the secrecy of algorithm, it depends on the keys provided as an imput to the algorithm.
- An attacker should defeat the mathematical properties of the algorithm.

SYMMETRIC KEY CRYPTOGRAPHY

STREAM CIPHERS

- another class of symmetric encryption;
- one byte of plaintext is encrypted at time rather than 64, 128, or more bits at time;
- it is much faster tha block ciphers;
- an infinite sequence of random bits is generated for use as the key so the key bits are never reused.

Theoretical motivation: ONE-TIME PAD

A one-time pad is a cipher in which plaintext is XORed with a random stream of bits of the same length as the plaintext. Claude SHANNON (1949) proved that one-time pad offer a property called "perfect secrecy" (it means under brute-force attack, every possible decription is equally likely), because ciphertext is indipendent from plaintext.

SYMMETRIC KEY CRYPTOGRAPHY

STREAM CIPHERS: RC4

- very popular stream cipher that approximate a one-time pad.
- Since it is impratical to have a key that is long as the plaintext itself, RC4 uses a fixed-size key as a SEED that is used to generate an infinite stream of key bits.
- It is approximately ten times faster than DES.
- You need only to make sure not to use the same key more than ONCE.

RC4 in the real word:

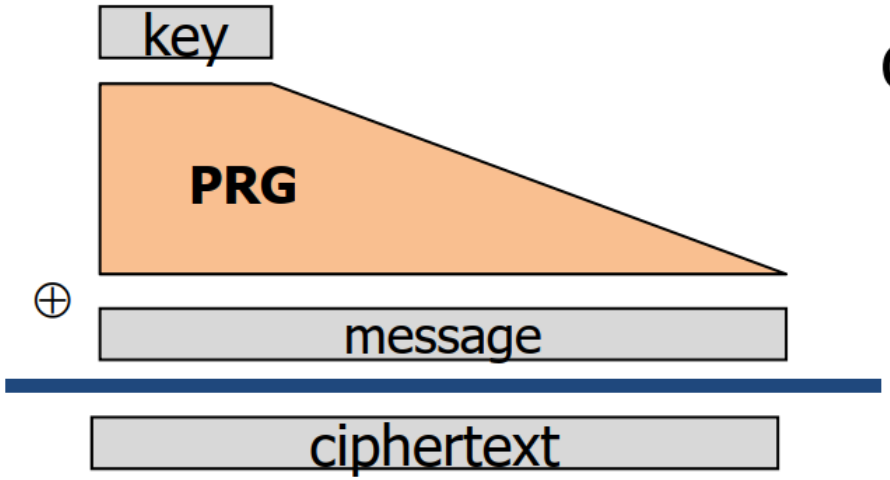
- ✔SSL (Secure Socket Layer)
- ✔Wired Equivalent Privacy (WEP)

SYMMETRIC KEY CRYPTOGRAPHY

STREAM CIPHERS (single use key)

Problem: OTP key is as long the message

Solution: Use a **pseudo**-random key ⟶ stream ciphers



$$c \leftarrow PRG(k) \oplus m$$

Real-world stream ciphers: (e.g. in Crypto++)

RC4 (126MB/sec) , **SALSA 20/12** (643MB/sec) , **Sosemanuk** (727MB/sec)

eStream ciphers

SYMMETRIC KEY CRYPTOGRAPHY

STREAM CIPHERS: RC4

NOT USE THE SAME KEY MORE THAN ONCE

P = Plaintext, C = ciphertext, K = key

Client encrypts: C1 = P1 XOR K
Server responds: C2 = P2 XOR K
a passive **eavesdropper** can compute:

C1 XOR **C2** =P1 XOR K XOR P2 XOR K = **P1** XOR **P2**

which reveals the client and server's plaintext

No integrity ciphertext can be modified in a meaningful ways

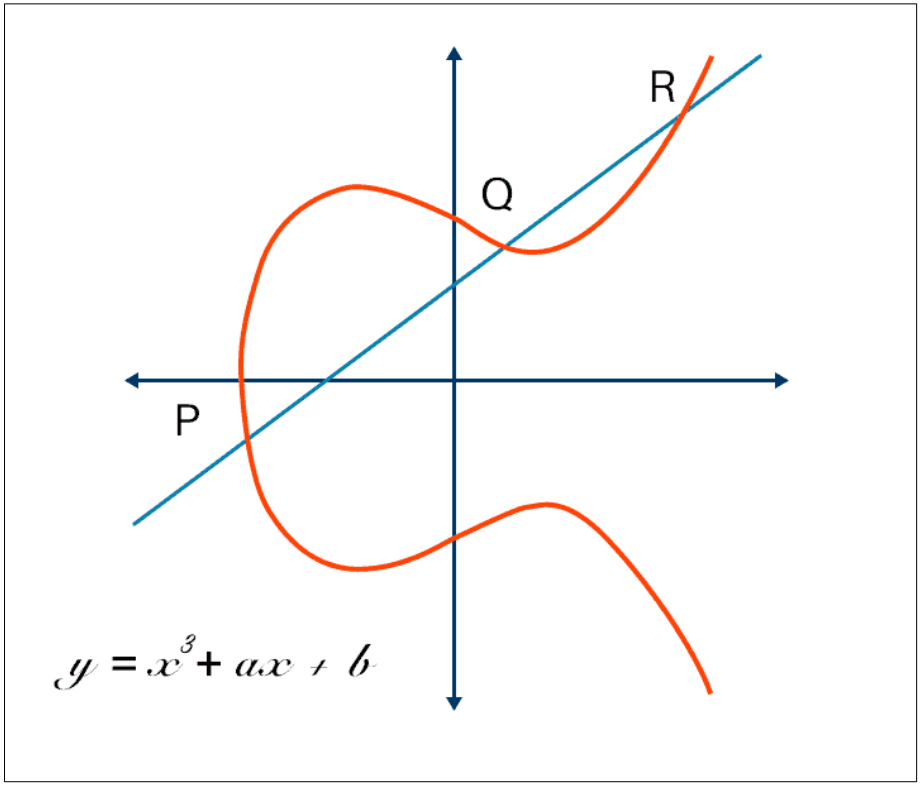
ASYMMETRIC KEY CRYPTOGRAPHY - RSA

It was introduced in 1976 by Diffie and Hellmann and independently by Merkle.

- there is no key exchange as is the case with secret or symmetric key cryptography;
- the public key cryptographic algorithms used are: **RSA** (River, Shamir, Adlemann) 1978 and Diffie Helmann 1977;
- These algorithms are made so that what is signed with the public key can only be decrypted with the respective private key and,
- at the same time, what is signed with the private key can only be decrypted with the respective public key.

ASYMMETRIC KEY CRYPTOGRAPHY - ECC

Elliptic Curve Cryptography (ECC) is a key-based technique for encrypting data. ECC focuses on pairs of public and private keys for decryption and encryption of web traffic.



ASYMMETRIC KEY CRYPTOGRAPHY - ECC

- ✔ an elliptic curve cryptography key of 384 bit achieves the same level of security as an RSA of 7680 bit. However, to remain secure, RSA needs keys that are 2048 bits or longer. This makes the process slow, and it also means that key size is important.
- ✔ Key size is a serious advantage of elliptic curve cryptography, because it translates into more power for smaller, mobile devices.
- ✔ ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers.

The ECC cryptography is considered a natural modern successor of the RSA cryptosystem, because ECC uses smaller keys and signatures than RSA for the same level of security and provides very fast key generation, fast key agreement and fast signatures.

THE DIGITAL SIGNATURE: DEFINITION

- It is a particular type of electronic signature;
- based on a system of cryptographic keys, one public and one private, related to each other,
- which allows the holder through the public key, respectively, to disclose and verify the origin and integrity of an electronic document or a set of electronic documents.

THE DIGITAL SIGNATURE: PROPERTIES

- ✓ It can be considered the same as the handwritten signature;
- ✓ It is based on the asymmetric cryptographic key system;
- ✓ It uses a Digital Certificate issued by a subject with specific guaranteed and professional skills called the Key Certification Authority.
- ✓ It is created using a device with high security features (Smart Card or USB Token).

PUBLIC KEY CRYPTOGRAPHIC SYSTEM

- The encryption and decryption keys are completely different from each other
- They are chosen by the recipient Dest who makes public the encryption key K [pub] which is therefore known to everyone;
- he keeps secret the decryption key K [priv] which is therefore known only to him.
- Basically there is a pair **(K [pub], K [priv])** for each user on the system.

PUBLIC KEY CRYPTOGRAPHIC SYSTEM

- Encryption of a message **m** to be sent to Dest is performed by any sender such as:

$$c = \textbf{Encrypt}(m, k[pub])$$

  where both k [pub] and the cipher function **Encrypt** are known to all.

- Decryption of a message is performed by Dest as:

$$m = \textbf{Decrypt}(c, k[priv])$$

where the decryption function **Decrypt** is known to all but k [priv] is not available to others who cannot therefore reconstruct m.

PUBLIC KEY CRYPTOGRAPHIC SYSTEM
USE SCENARIOS

1) The sender encrypts the message with their private key;

2) The recipient who knows the identity of whoever sent him the message decrypts it using the sender's public key;

- The AUTHENTICATION of the message and the INTEGRITY of the message are guaranteed.
- CONFIDENTIALITY is not guaranteed since the sender's public key is available to everyone.

PUBLIC KEY CRYPTOGRAPHIC SYSTEM
USE SCENARIOS

1) The sender encrypts the message with the recipient's public key known to all;

2) The recipient recognizes that the message is for him and decrypts it with his own private key known only to him.

- Only the recipient will be able to read the message in this way CONFIDENTIALITY is guaranteed if it is successful.

PUBLIC KEY CRYPTOGRAPHIC SYSTEM

In a communication, then as we will see:

- The encryption of the message guarantees CONFIDENTIALITY;
- The Electronic Signature INTEGRITY, AUTHENTICITY and NON-REPUDIATION.

Let's now analyze in detail the signature process of any "file" (text document, image, ...):

PUBLIC KEY CRYPTOGRAPHIC SYSTEM

SENDER

A. Apply to the message to be sent an algorithm for generating the electronic signature, i.e. with ONE WAY HASH functions it generates a **SUMMARY** (fingerprint, fingerprint or cryptogram) of the message content in a string of relatively limited length (128 bits or multiples of 128 bit). These functions are structured in such a way that any change in the original message is reflected in the string value.

B. This fingerprint is **encrypted** using a public key algorithm with the sender's private key, thus obtaining the **ELECTRONIC SIGNATURE**.

C. The electronic signature is **attached** at the bottom of the message, obtaining the **SIGNED MESSAGE**.

PUBLIC KEY CRYPTOGRAPHIC SYSTEM

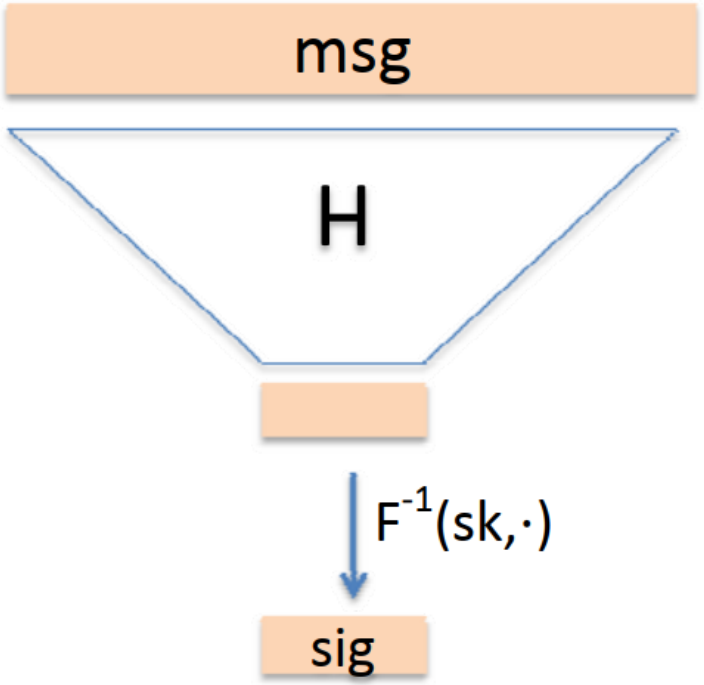
RECEIVER

A. Calculates the summary of the message with the same ONE WAY HASH function and autonomously
B. The ELECTRONIC SIGNATURE is decrypted with the public key, thus obtaining AUTHENTICATION of the message, as only the sender knows the private key.
C. If the fingerprint is the same as the one sent, the message is INTACT.
D. The sender is the only person who can have signed the message, therefore he will not be able to repudiate what is signed (NON-REPUDIATION of the message)

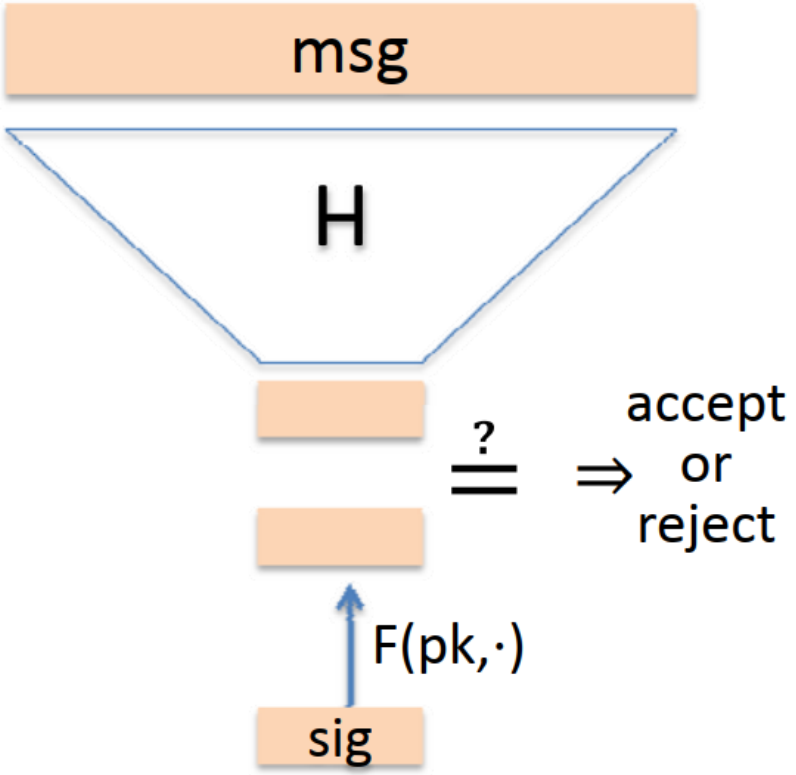
PUBLIC KEY CRYPTOGRAPHIC SYSTEM

DIGITAL SIGNATURE

sign(sk, msg):



verify(pk, msg, sig):



PUBLIC KEY CRYPTOGRAPHIC SYSTEM

To ensure:

1. CONFIDENTIALITY: protection from unauthorized reading;
2. INTEGRITY: protection from unauthorized changes;
3. AUTHENTICITY: certainty of the source, destination and content of the message;
4. NON-REPUDIATION: certainty that the sender and the recipient cannot deny having respectively sent and received the message.

YOU MUST:

Sign the message with your private key

Encrypt the signed message with the Recipient's public key

KEY CERTIFICATION

Checking the correspondence between signature and message only guarantees that it was generated using the private key corresponding to the public key.

Correspondence between the keys and the author of the message must be ensured.

The key certification serves to establish that the key belongs to the rightful owner.

KEY CERTIFICATION

Two mechanisms are used:

- there is a mechanism of mutual trust, whereby a network of trust is formed: there is no single certifying body (mechanism used by PGP by Phil Zimmermann in 1991);

- there is a hierarchical certification infrastructure or Public Key Infrastructure (PKI) (1970 → 1990);

KEY CERTIFICATION AUTHORITY (CA)

Bodies responsible for certifying the validity of public keys.
The CA authenticates the association:

< user, public key >

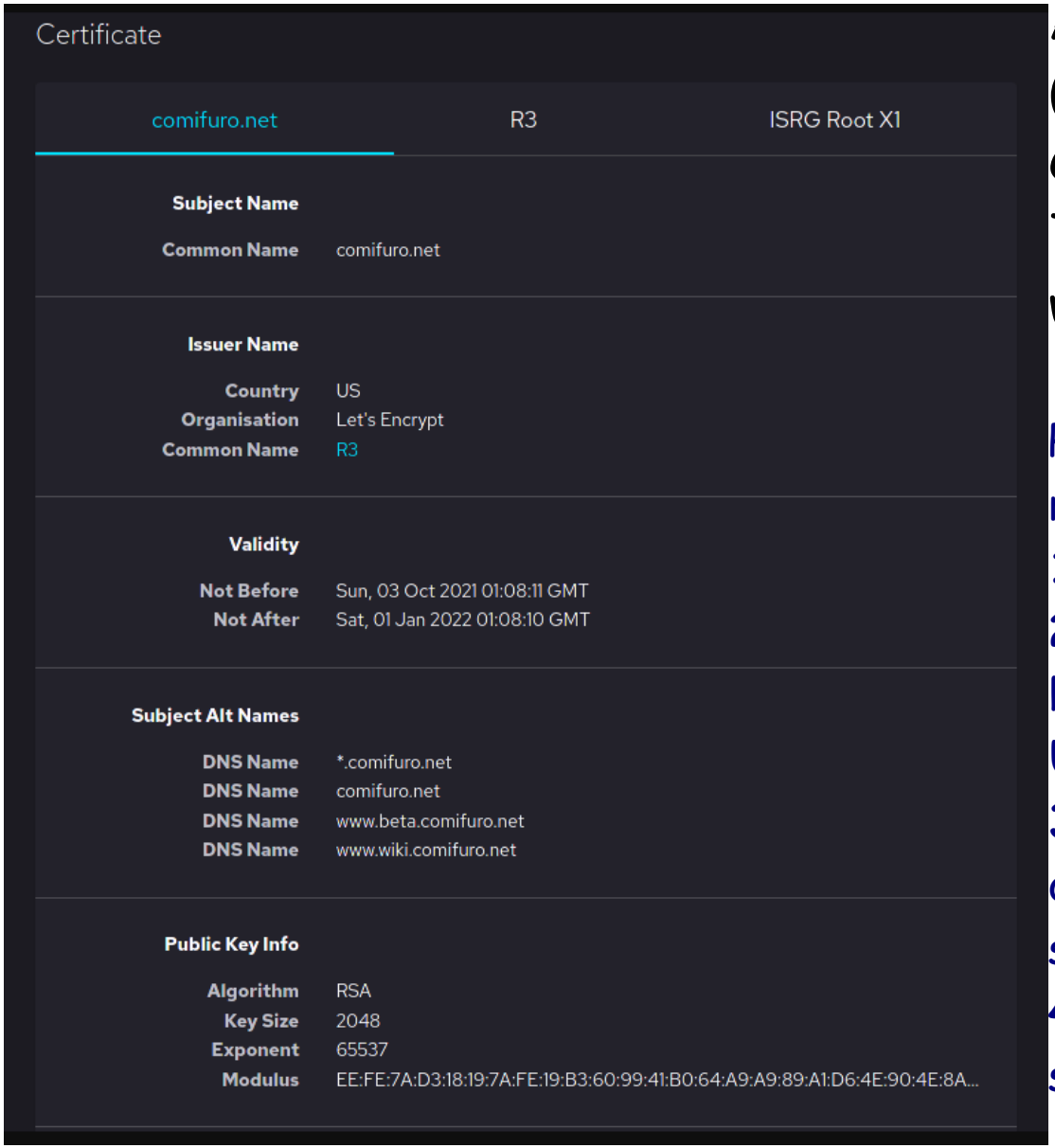
by issuing a digital certificate, as well as the registry office of a municipality authenticates the association <personal data, photograph> by issuing the identity card.

The **Digital Certificate** consists of the public key and a list of information relating to its owner, appropriately signed by the CA.

Digital Certificate

1. An indication of its format (version number);
2. The name of the CA that issued it;
3. A serial number that uniquely identifies this certificate within the issuing CA;
4. The specification of the algorithm used by the CA to create the electronic signature, combined with a description of the parameters it needs;
5. The validity period of the certificate;
6. The name of the user to whom this certificate refers and a series of information related to him;
7. An indication of the public key protocol adopted by this user for encryption and signature (name of the algorithm, its parameters and the user's public key;
8. CA signature performed on all previous information.

Digital Certificate



A New CA Let's encrypt (letsencrypt.org). A nonprofit Certificate Authority providing TLS certificates to 260 million websites till 2021.

Provinding via an automated agent running on web server.

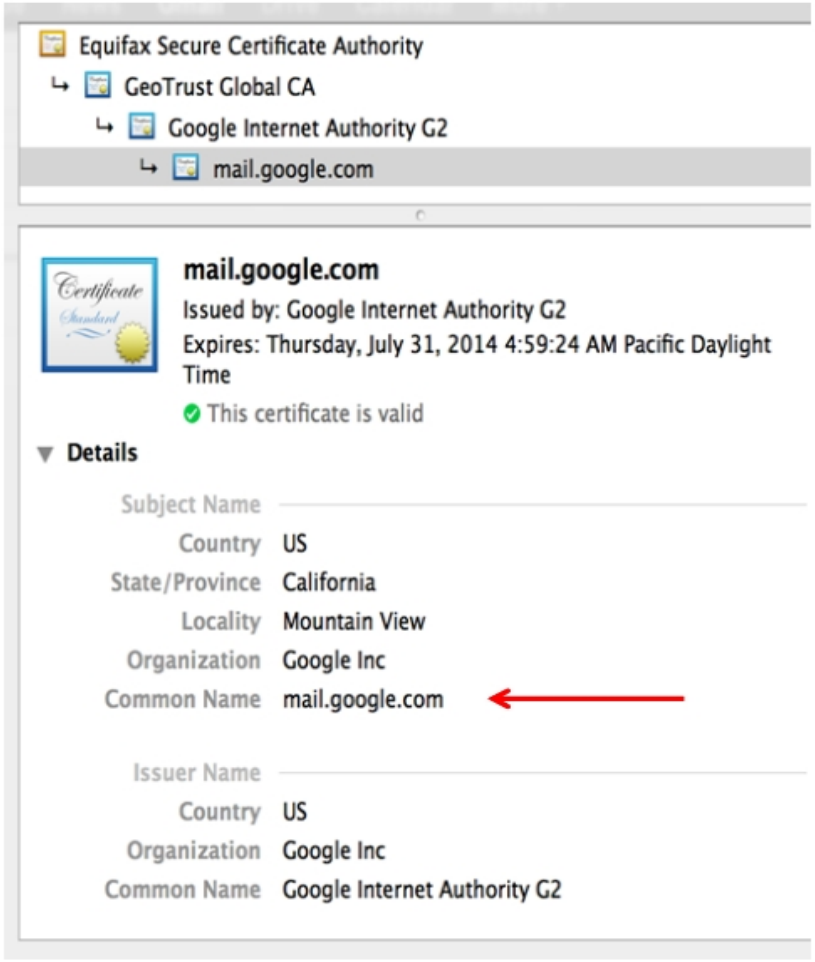
1. install agent on web server;
2. agent proves domain ownership by DNS record or page at fixed URI;
3. let's encrypt CA checks domain ownership. If valid, issue cert and sends to agent;
4. agent installs cert on web server.

Digital Certificate

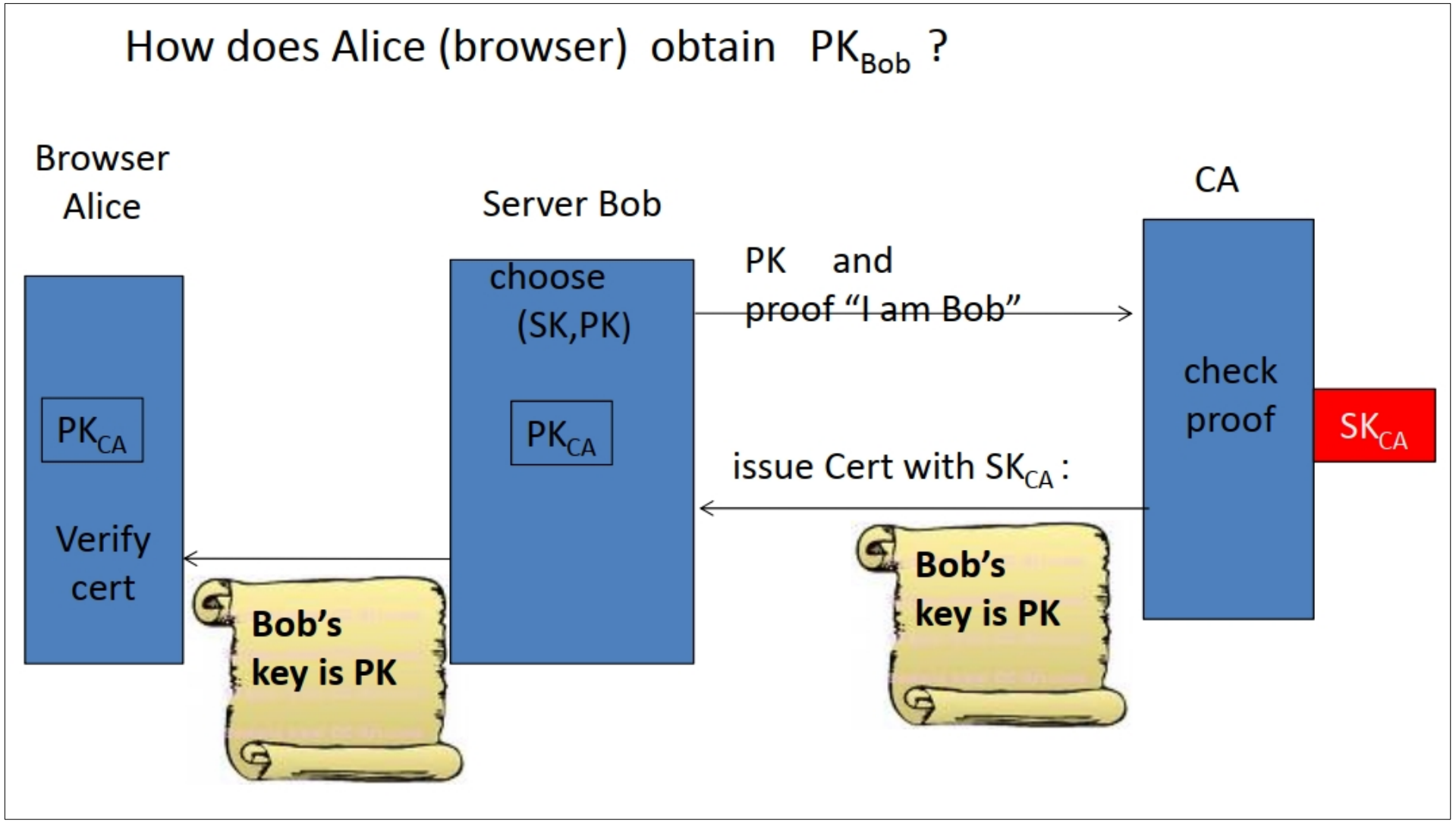
Certificates: example

Important fields:

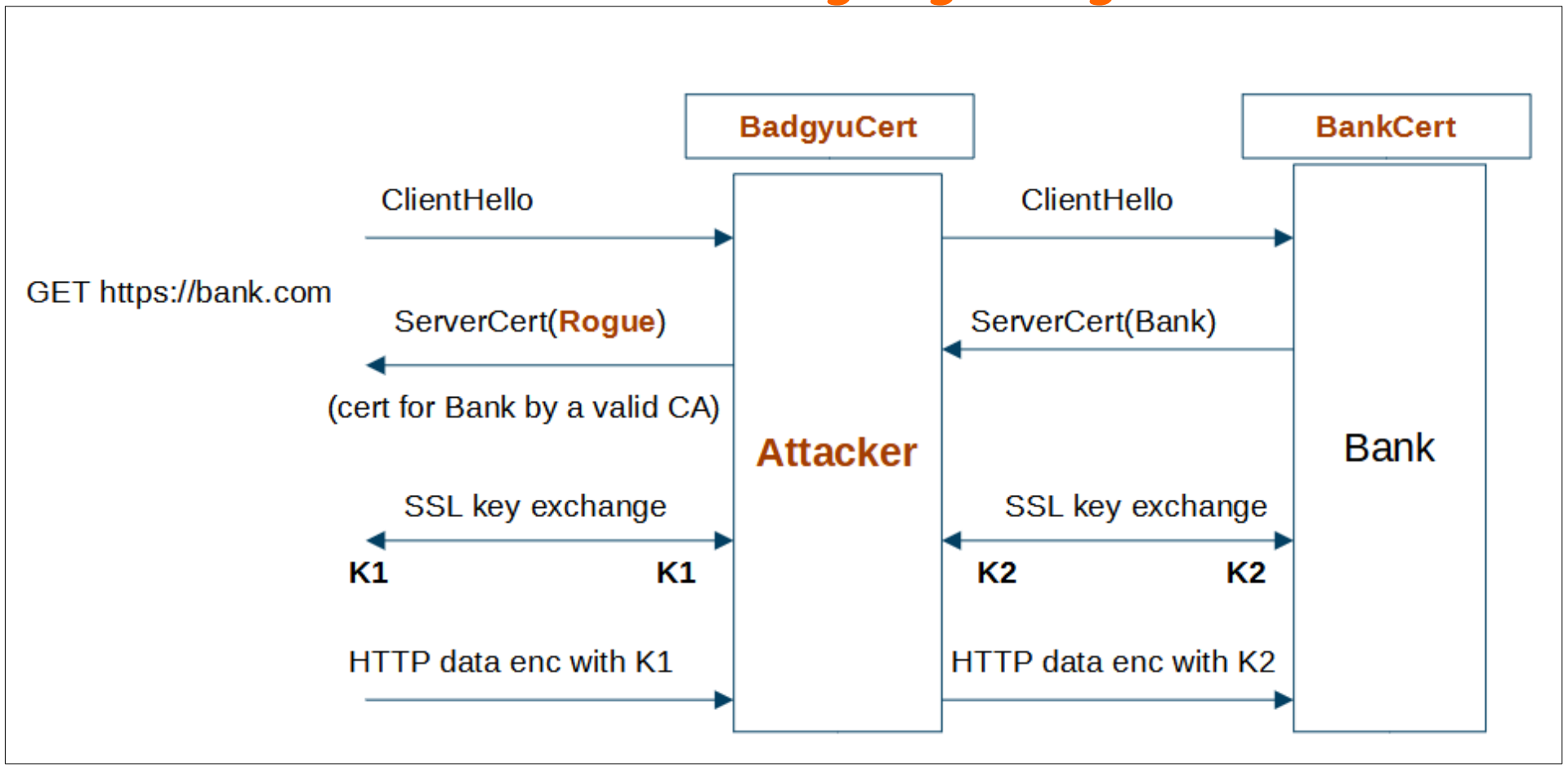
Serial Number	5814744488373890497
Version	3
Signature Algorithm	SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
Parameters	none
Not Valid Before	Wednesday, July 31, 2013 4:59:24 AM Pacific Daylight Time
Not Valid After	Thursday, July 31, 2014 4:59:24 AM Pacific Daylight Time
Public Key Info	
Algorithm	Elliptic Curve Public Key (1.2.840.10045.2.1)
Parameters	Elliptic Curve secp256r1 (1.2.840.10045.3.1.7)
Public Key	65 bytes : 04 71 6C DD E0 0A C9 76 ...
Key Size	256 bits
Key Usage	Encrypt, Verify, Derive
Signature	256 bytes : 8A 38 FE D6 F5 E7 F6 59 ...



Digital Certificate



Man in the middle attack using rogue Digital Certificate



Attacker proxies data between user and bank and use to eavesdropp traffic, that is see all traffic and can modify data at will


Sistema di Crittografia a Chiave Pubblica
SCENARIO OPERATIVO: CERTIFICAZIONE DELLE CHIAVI
CA1
Certification Authority
Public Key Infrastructure o struttura gerarchica di certificazione
CAk
CAn
Dominio della CA
Insieme dei certificati firmati con la chiave pubblica della CA
Garantisce tramite i certificati la corrispondenza chiave-possessore usando la propria chiave pubblica
Chiavi Private
Cittadini Imprese Enti
Chiavi Pubbliche

Public Key Infrastructure (PKI): software PKI-enabled

The software that wants to interact with PKI must be enabled to manage the aspects listed below:

Public key certificates: The SW must be able to verify the CA's signature on the certificate and ensure that this certificate has not expired.

Backup and recovery: To prevent any damage caused by the loss of your certificate, it must be possible to safely duplicate the keys, thus allowing their eventual recovery.

Public Key Infrastructure (PKI): software PKI-enabled

Certificate Repository: To minimize certificate verification times, it is necessary that the software contains a small list of the most used certificates so as not to have to go through the PKI each time in search of the competent CA.

Certificate revocation: Upon revocation of a certificate, the SW must be able to invalidate any copy present in its repository.

Support for cross-certification: allows you to accept certificates that have not been issued by a CA to which the domain to which you belong belongs

TIMESTAMP

The time stamping of electronic documents is one of the operations envisaged by the legislation on digital signature

The time stamp of an electronic document is an operation carried out:

1. to certify the existence of an electronic document at a certain date and time;
2. avoid documents being drawn up using revoked or expired signature certificates.

TIMESTAMP

Time stamp operation:

A) The fingerprint of the message is sent to the CA;

B) The CA sends the fingerprint that becomes MARKED FINGERPRINT to the TIME Stamping Authority (TSA - Time Stamping Authority);

C) The marked fingerprint is encrypted with the CA's private key: ENCRYPED MARKED FINGERPRINT;

D) The encrypted marked fingerprint is associated with the message and sent. With the public key of the CA it is possible to recover the imprint of the document and the date and time of its generation.

CONSIDERATIONS

Weak Point: it is represented by the revoked certificates. The CAs make a public archive available to users. The frequency of checking these certificates and the manner in which they are communicated to users are crucial points for the safety and efficiency of the system. We try to compensate for this with the Local Archive of Certificates of both other users and their CAs.

The use of the fingerprint allows you not to apply the INEFFICIENT encryption algorithm to the entire text, which can be very long.

The fingerprint allows the authentication of a trusted third party without this being aware of the content of the message.

Назарыңызға рахмет!

Спасибо за внимание!

Thank you for your attention!