Information System Security

Cryptography

Summary

- Definitions and principles
- Symmetric key algorithms
- Asymmetric key algorithms
- Hashing algorithms and uses
- Public key infrastructure (PKI) concepts and mechanisms

Definitions

- Cryptography : method of storing and transmitting data in a form that only those it is intended for, can read and process

- Effective way of protecting sensitive information stored on media or transmitted through untrusted network

Kerckhoffs' Principle

- **Auguste Kerckhoffs published a paper in 1883 stating that the only secrecy involved with a cryptography system should be the key**
- **The algorithm should be publicly known**
- **If security is based on too many secrets, there will be more vulnerabilities to possibly exploit**

- **Making an algorithm publicly available means that many more people can view the source code, test it, and uncover any type of flaws or weaknesses**
  - "Many heads are better than one"

Types of cipher

- **Symmetric encryption ciphers come in two basic types: substitution and transposition (permutation)**
- **The substitution cipher replaces bits, characters, or blocks of characters with different bits, characters, or blocks (*Caesar cipher*)**
- **The transposition cipher does not replace the original text with different text, but rather moves the original values around (*Scytale cipher*)**
  - It rearranges the bits, characters, or blocks of characters to hide the original meaning

Transposition cipher

Message

- Message to transpose

Broken into groups

- M e s s a g e t o t r a n s p o s e
- 1 2 3 4 5 1 2 3 4 5 1 2 3 4 5 1 2 3

Key

- 24153 31524 54312 213

Ciphertext

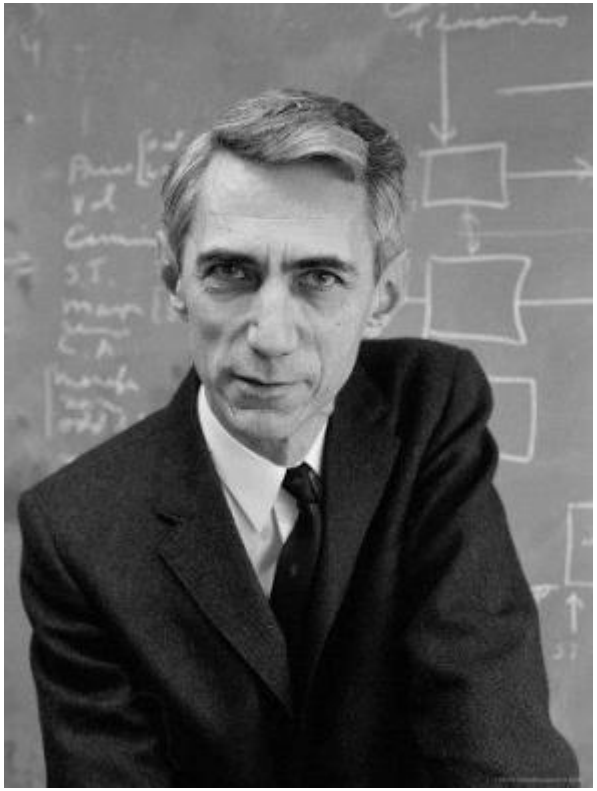
- Esmas tgteo psnra soe

Confusion and diffusion

- **Shannon defines two notions that any good cryptosystem should have :**

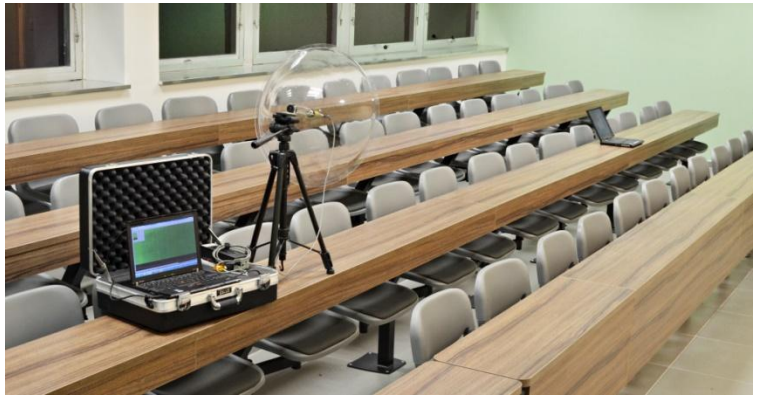
- **Principle of confusion: the calculation method from plaintext to ciphertext should be enough complex**
  - There must be no simple relationship between the bits of plaintext and the bits of ciphertext

- **Principle of diffusion: a single plaintext bit has influence over several of the ciphertext bits**
  - If one plaintext bit changes, then about half of the ciphertext bits will change



Cryptanalysis

- Cryptanalysis is the science of studying and breaking the secrecy of encryption processes, compromising authentication schemes, and reverse-engineering algorithms and keys
- It is an important piece of cryptology
- When carried out by the “good guys”, cryptanalysis is intended to identify flaws and weaknesses so developers can go back to the drawing board and improve the components

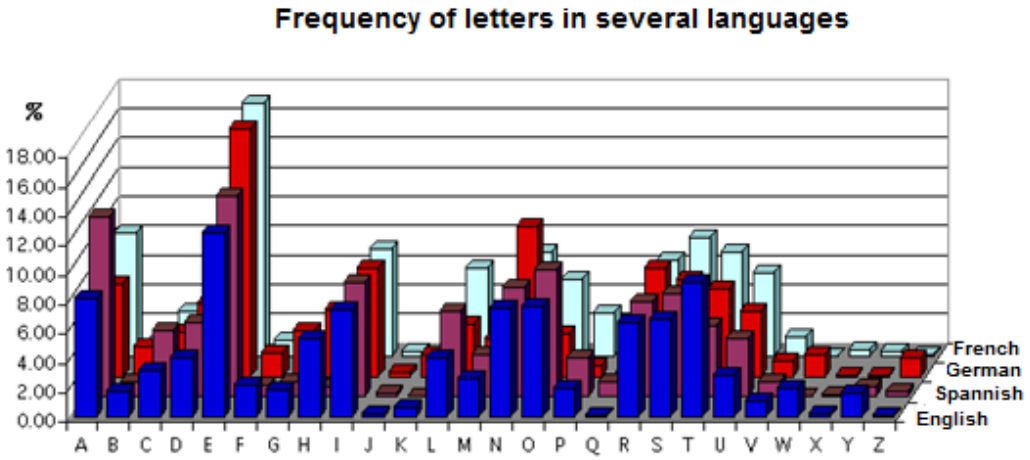


- Also performed by curious and motivated hackers, to identify the same types of flaws, but with the goal of obtaining the encryption key for unauthorized access to confidential information

Frequency analysis

- Simple substitution and transposition ciphers are vulnerable to attacks that perform frequency analysis

- In every language, some words and patterns are used more often than others



- Look for the most frequently repeated pattern of eight bits (which make up a character)

- Today, symmetric algorithms use substitution and transposition methods in their encryption processes, but the mathematics used are too complex to allow for simplistic frequency-analysis attacks to be successful

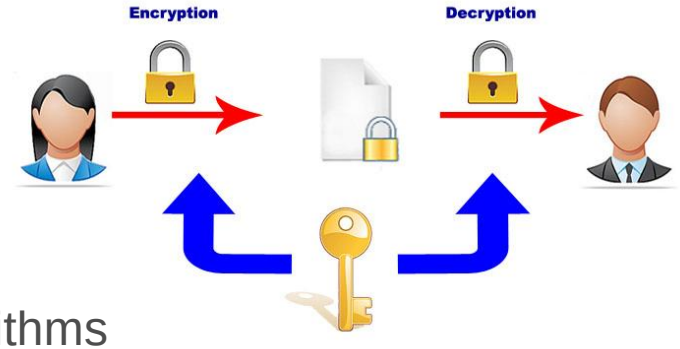
Governmental involvement

- **In France, before 1990, cryptology was mainly reserved for military and diplomatic domains, as well as sensitive sectors such as the banking sector**

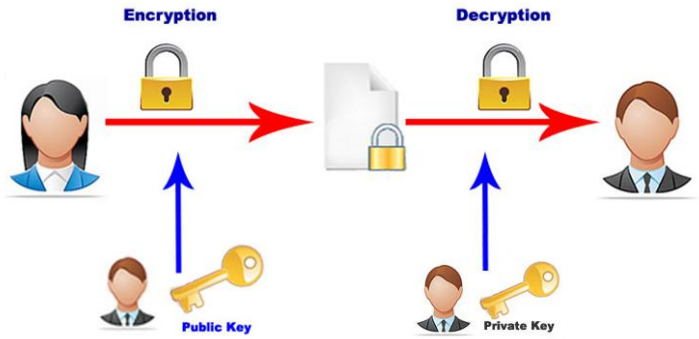
- **From the 90s, with the advent of Internet, the need to protect strongly increases**
  - Law No 96-659 of July 26th,1996 allows to use cryptography if the keys are stored in a **trusted third party** company
  - Decree No. 99-199 of March 17th, 1999 authorizes the use of "hardware or software offering a confidentiality service implemented by an algorithm whose **key is less than or equal to 128 bits** in length"
  - Law No 2004-575 of June 21st, 2004 abrogates the trusted thirds and indicates that **the use of cryptology is free**

Symmetric vs. Asymmetric Algorithms

- **Cryptography algorithms are either :**
  - Symmetric algorithms
    - ✓ Use symmetric keys (also called secret keys)

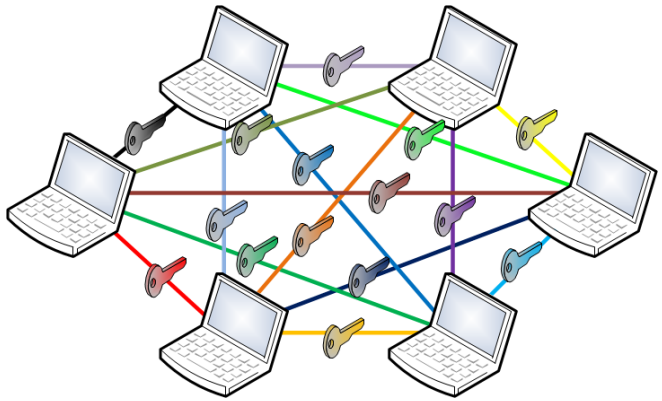


  - Asymmetric algorithms
    - ✓ Use asymmetric keys (also called public and private keys)



Symmetric Cryptography

- Each pair of users who want to exchange data using symmetric key encryption must have two instances of the same key
- The security of the symmetric encryption method is completely dependent on how well users protect the key
- If 6 people were going to communicate, then 15 keys would be involved
- $\left(\frac{n(n-1)}{2}\right)$ = number of keys



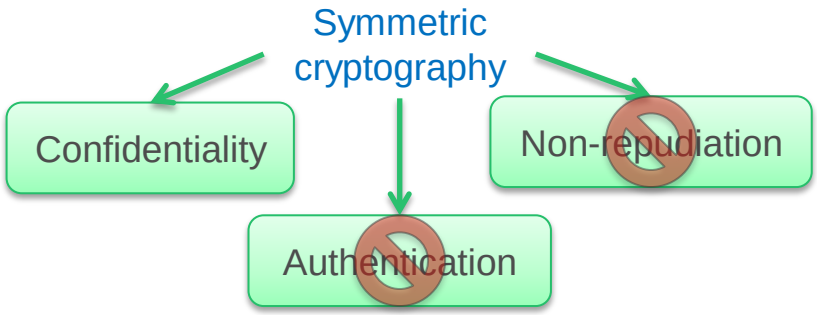
Strengths and weakness of symmetric algorithm

Strengths

- Much faster than asymmetric systems
- Hard to break if using a large key size

Weakness

- Requires a secure mechanism to deliver keys properly
- Each pair of users needs a unique key
  - ✓ As the number of individuals increases, so does the number of keys
- Provides confidentiality but not authentication or nonrepudiation



Symmetric algorithms

- **Examples of symmetric algorithms :**

Algorithm	Key size	Evaluation
Data Encryption Standard (DES)	56 bits	Too weak
International Data Encryption Algorithm (IDEA)	128 bits	Good but patented
RC4	1-2048 bits	Some keys are weak
RC5	128-256 bits	Good but patented
Rijndael (AES)	128-256 bits	Best choice
TripleDES (3DES)	112-168 bits	Deprecated
Twofish	128-256 bits	Very strong (finalist in the AES competition)

Data Encryption Standard

- **DES (Data Encryption Standard) is the first modern commercial symmetrical algorithm**
  - It was developed in the 1970s by IBM with the help of the NSA
- **DES has been implemented in a majority of commercial products using cryptography functionality and in the applications of almost all government agencies**
- **In 1998, the Electronic Frontier Foundation built a computer system for $250,000 that broke DES in three days using a brute force attack against the keyspace**
  - In 1999, the key of DES was broken in 22 hours

Advanced Encryption Standard (AES)

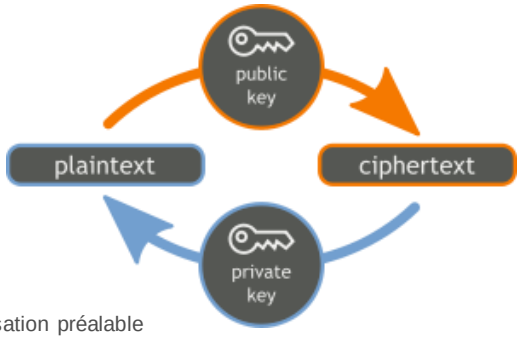
- Chosen in October 2000 by the NIST (National Institute of Standards and Technology) to replace the DES key size which became too small (56-bit)

Daemen and Rijmen

- The algorithm chosen to become the AES is Rijndael, condensed name of its designers : Rijmen and Daemen
- This is a symmetric block cipher (the block size is doubled compared with DES: from 64 to 128 bits)
- The size of the key is doubled or even quadrupled compared to DES (from 64-bit key to between 128 and 256 bits key) → if we could break DES in 1 second, it would take 149 trillion (10^{12}) years to break AES

Asymmetric Cryptography

- **In public key systems, each entity has different keys → asymmetric keys**
- **The two different asymmetric keys are mathematically related**
- **If a message is encrypted by one key, the other key is required in order to decrypt the message**
- **The pair of keys is made up of one public key and one private key**
  - The public key can be known to everyone
  - The private key must be known and used only by the owner



Asymmetric Cryptography

- **It is not possible to encrypt and decrypt using the same key**
  - Although mathematically related, the two keys are not the same key
- **If confidentiality is the most important security service to a sender, he encrypts the file with the receiver's public key**
  - This is called a secure message format because it can only be decrypted by the person who has the corresponding private key
- **If authentication is the most important security service to the sender, he encrypts the data with his private key**
  - This provides assurance to the receiver that the only person who could have encrypted the data is the individual who has possession of that private key
  - This is called an open message format because anyone with a copy of the corresponding public key can decrypt the message

Strengths and weaknesses of asymmetric algorithms

- **Strengths**
  - Better key distribution than symmetric systems
  - Can provide authentication and nonrepudiation
- **Weaknesses**
  - Works much more slowly than symmetric systems
  - Mathematically intensive tasks

Asymmetric algorithms

- **Examples of asymmetric key algorithms :**

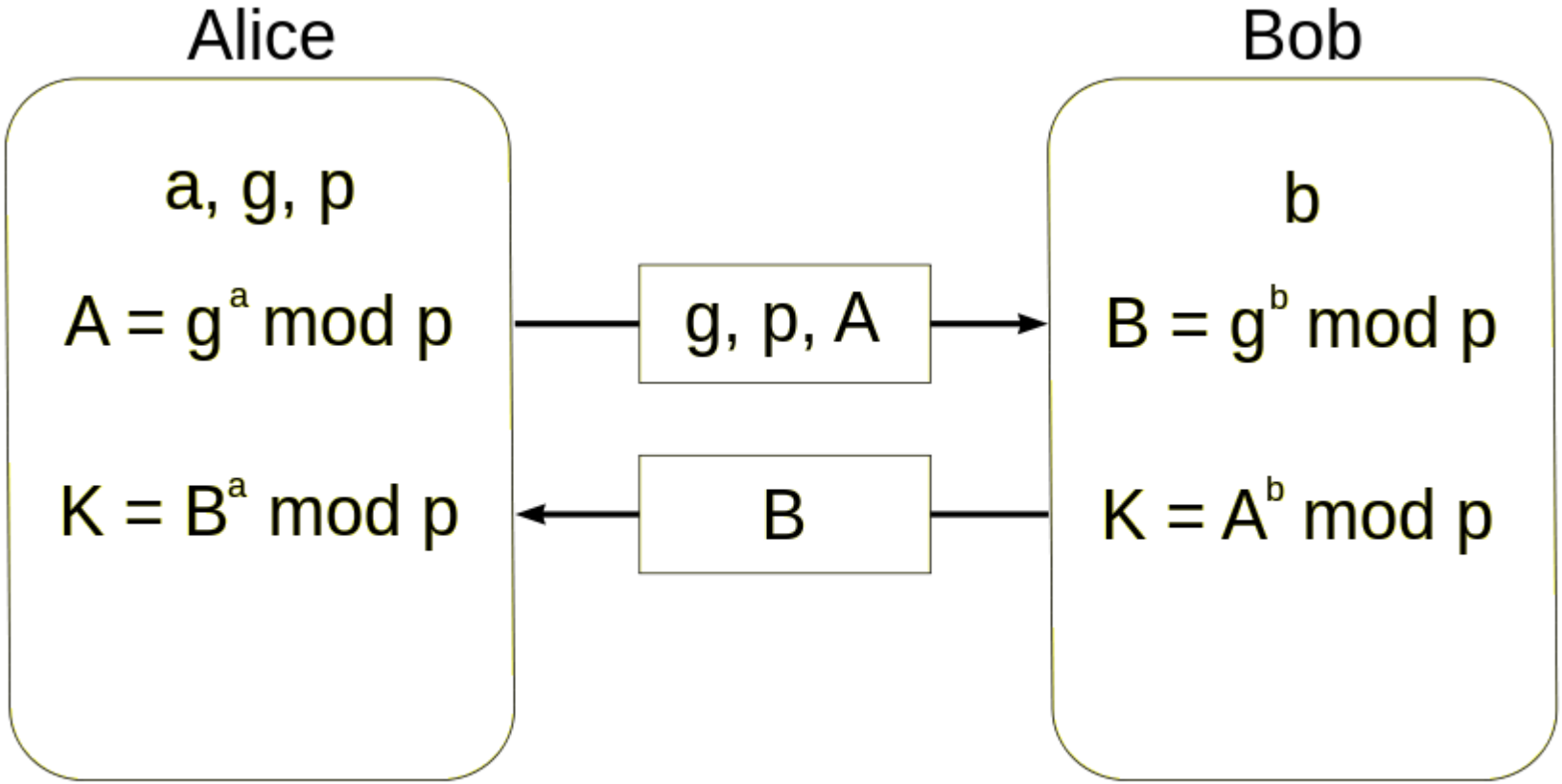
Algorithms	Usage
RSA	Encryption, key distribution and signature
Diffie-Hellman	Key agreement
Elliptic curve Diffie-Hellman (ECDH)	Key agreement protocol based on ECC (Elliptic Curve Cryptography) → reduction of group size from 2048 bits to 256 bits
Digital Signature Algorithm (DSA)	Digital signature

Diffie-Hellman

- **Deals with the issue of secure distribution of the symmetric key**
- **Exchanges information that don't need to be protected over an untrusted network, and generated the exact same symmetric key on each system**
- **Enables two systems to receive a symmetric key securely without requiring a previous relationship or prior arrangements**
- **It is a key agreement, which is different from key exchange**
  - With key exchange functionality, the sender encrypts the symmetric key with the receiver's public key before transmission (hybrid cryptography)

Diffie-Hellman

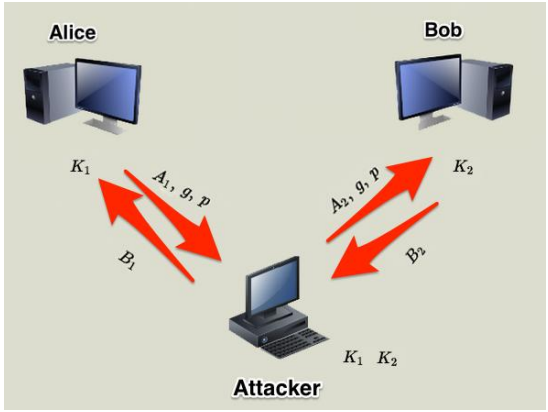
- The algorithm is based on the difficulty of calculating discrete logarithms in a finite field



$$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$$

- Alice and Bob share the same secret key : K

Diffie-Hellman



- **The Diffie-Hellman algorithm is vulnerable to a man-in-the-middle attack, because no authentication occurs before public keys are exchanged**
- **The countermeasure to this type of attack is to have authentication of the exchanges**
  - Use of digital signatures and digital certificates
- **Although the Diffie-Hellman algorithm is vulnerable to a man-in-the-middle attack, it does not mean this type of compromise can take place anywhere this algorithm is deployed**
  - Implementations include another piece of software or a protocol that compensates for this vulnerability

RSA

- **RSA, named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman, is the most popular public key algorithm**
  - RSA is a worldwide de facto standard and can be used for digital signatures, key exchange, and encryption
  - It was developed in 1978 at MIT and provides authentication as well as key encryption
- **The security of this algorithm comes from the difficulty of factoring large numbers**
- **The algorithm creates a public key and a private key from a function of large prime numbers**
  - The key size must be at least 2048 bits

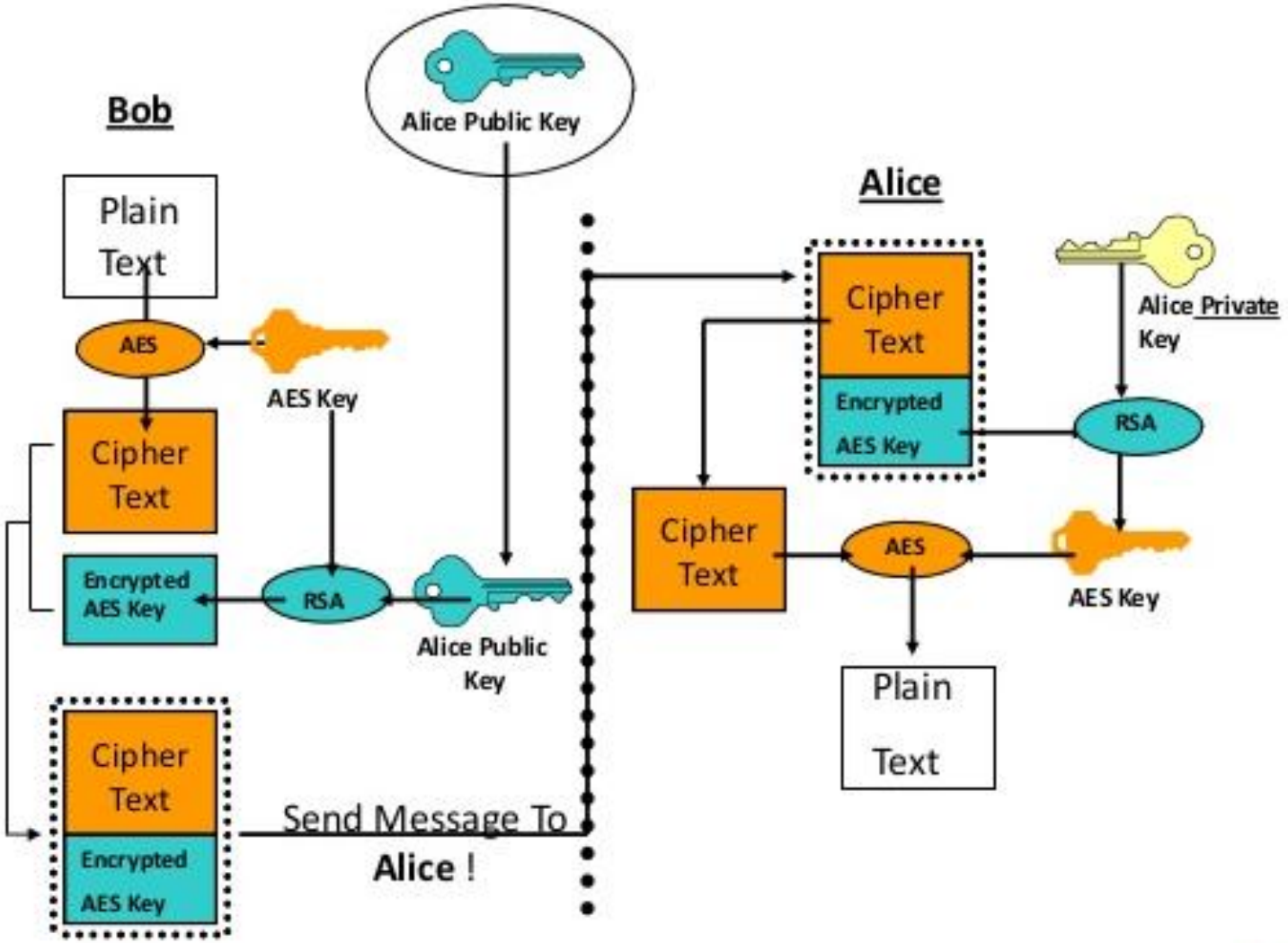
Hybrid cryptography

- **Hybrid system uses symmetric and asymmetric encryption methods together**

- **The two technologies are used in a complementary manner, with each performing a different function**
  - Symmetric algorithm creates keys used for encrypting bulk data
  - Asymmetric algorithm creates keys used for automated key distribution

- **Because your message is most likely going to be longer than the length of the key, we use the faster algorithm on the message (symmetric) and the slower algorithm on the key (asymmetric)**

Hybrid cryptography



Message integrity

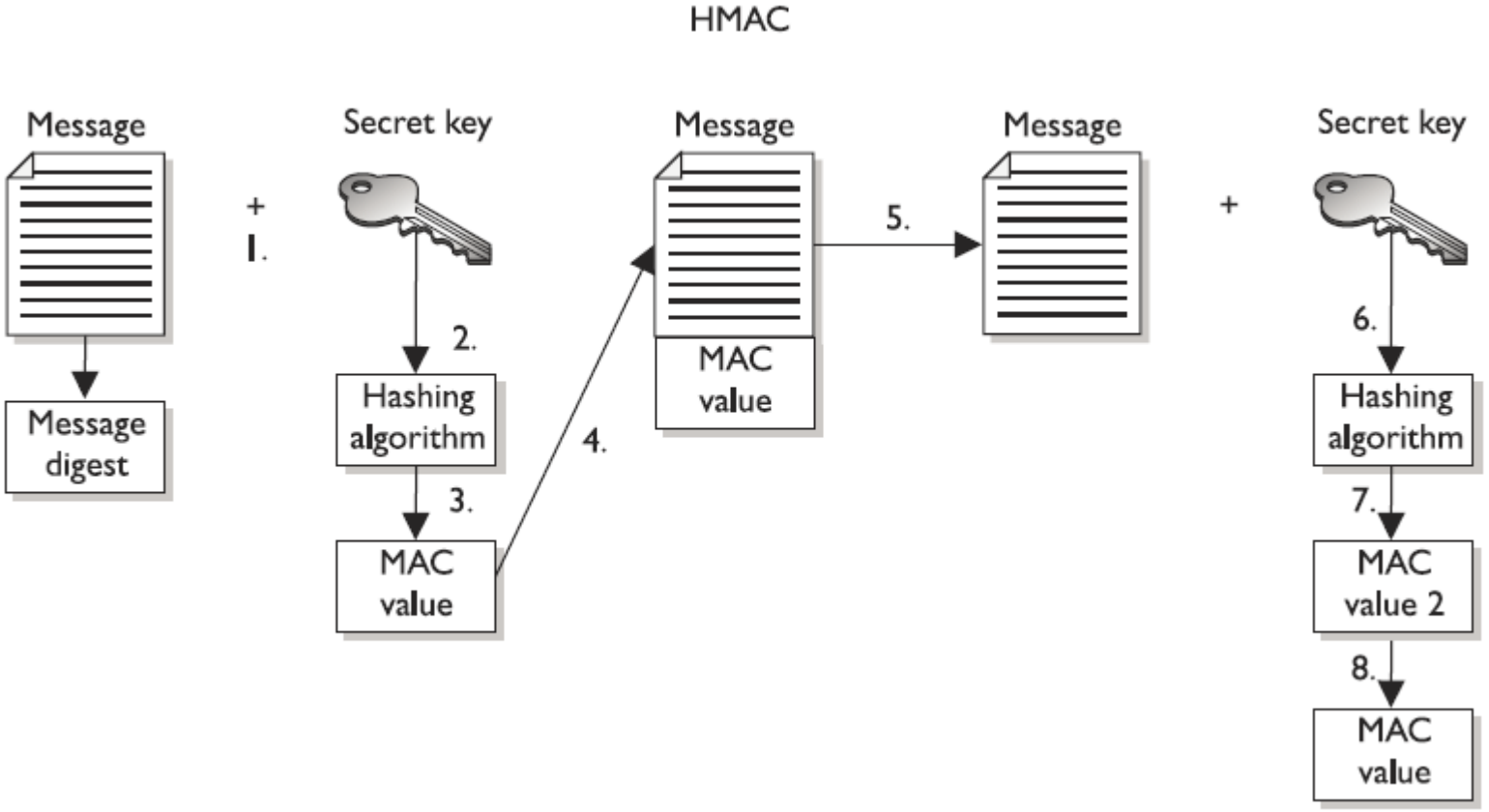
- **A one-way hash is a function that takes a variable-length string and a message and produces a fixed-length value called a hash value**

- **To be ensure a message does not get altered, calculate a hash value for the message and append it to the message itself**
  - The receiver performs the same hashing function the sender used and then compare his result with the hash value sent with the message
  - If the two values are the same, the receiver can be sure the message was not altered during transmission
  - If the two values are different, the receiver knows the message was altered, either intentionally or unintentionally, and discards the message

- **One-way hash functions are never used in reverse**

Hash Message Authentication Code (HMAC)

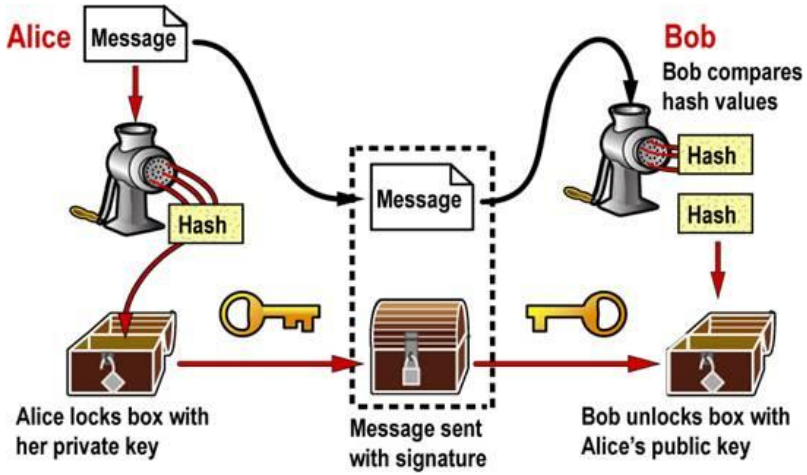
- HMAC function encrypts the hash with a symmetric key before concatenating the hash with the message



- This type of technology requires the sender and receiver to have the same symmetric key

Digital signature

- A digital signature is a hash value that has been encrypted with the sender's private key
- The act of signing means encrypting the message's hash value with a private key
- The hashing function ensures the integrity of the message, and the signing of the hash value provides authentication and nonrepudiation

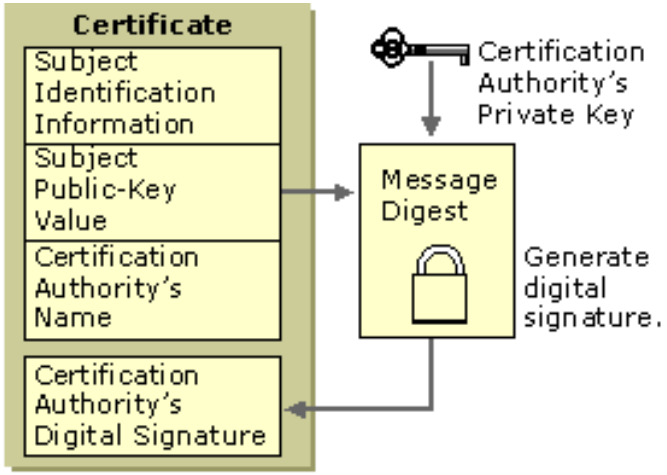


Type of security services

Algorithm type	Encryption	Digital signature	Hashing function	Key distribution
RSA (asymmetric)	X	X		X
Diffie-Hellman (asymmetric)				X
Digital Signature Algorithm – DSA (asymmetric)		X		
DES (symmetric)	X			
AES (symmetric)	X			
MD5 (Hash)			X	
SHA (Hash)			X	

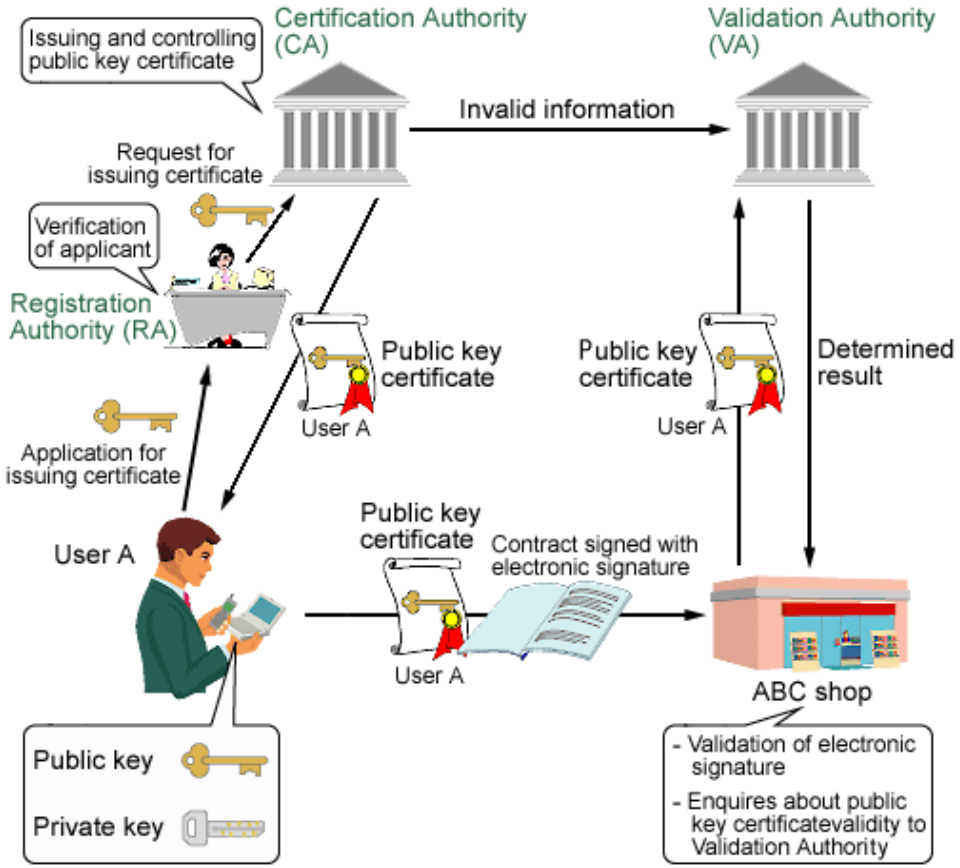
Digital certificate

- **The digital certificate is an electronic document that matches a public key with an entity (person, company, computer ...)**
- **The standard for how the CA creates the certificate is X.509**
  - Many cryptographic protocols use this type of certificate, including TLS
- **The certificate includes**
  - identity information,
  - public-key value,
  - algorithm information,
  - lifetime dates
  - name of the certification authority
  - the signature of the certification authority



Public Key Infrastructure (PKI)

- **PKI consists of**
  - programs,
  - data formats,
  - procedures,
  - communication protocols,
  - security policies,
  - and public key cryptographic mechanisms

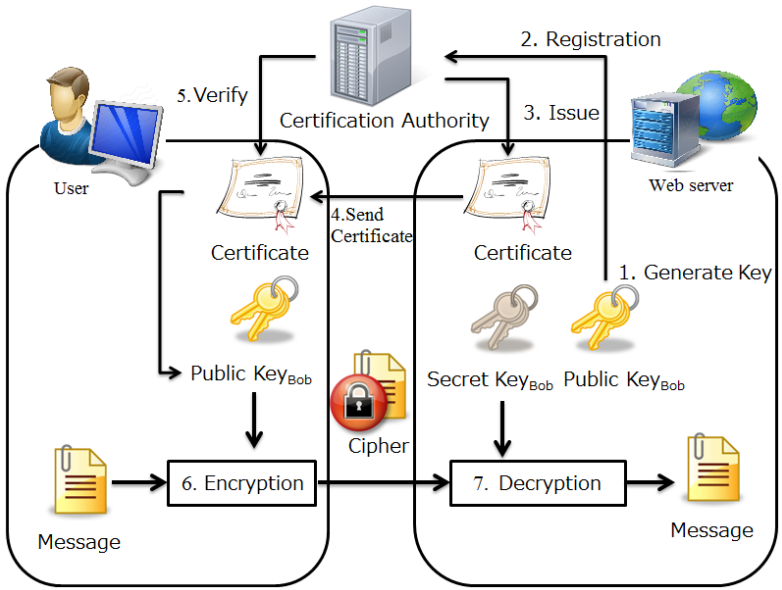


- **PKI establishes a level of trust within an environment**

ECE PARIS ÉCOLE D'INGÉNIEURS

Public Key Infrastructure (PKI)

- PKI provides authentication, confidentiality, nonrepudiation, and integrity of the exchanged messages
- The infrastructure assumes that the receiver's identity can be positively ensured through certificates
- The infrastructure contains the pieces that will :
  - identify users,
  - create and distribute certificates,
  - maintain and revoke certificates,
  - distribute and maintain encryption keys



ECE PARIS ÉCOLE D'INGÉNIEURS

Public Key Infrastructure (PKI)

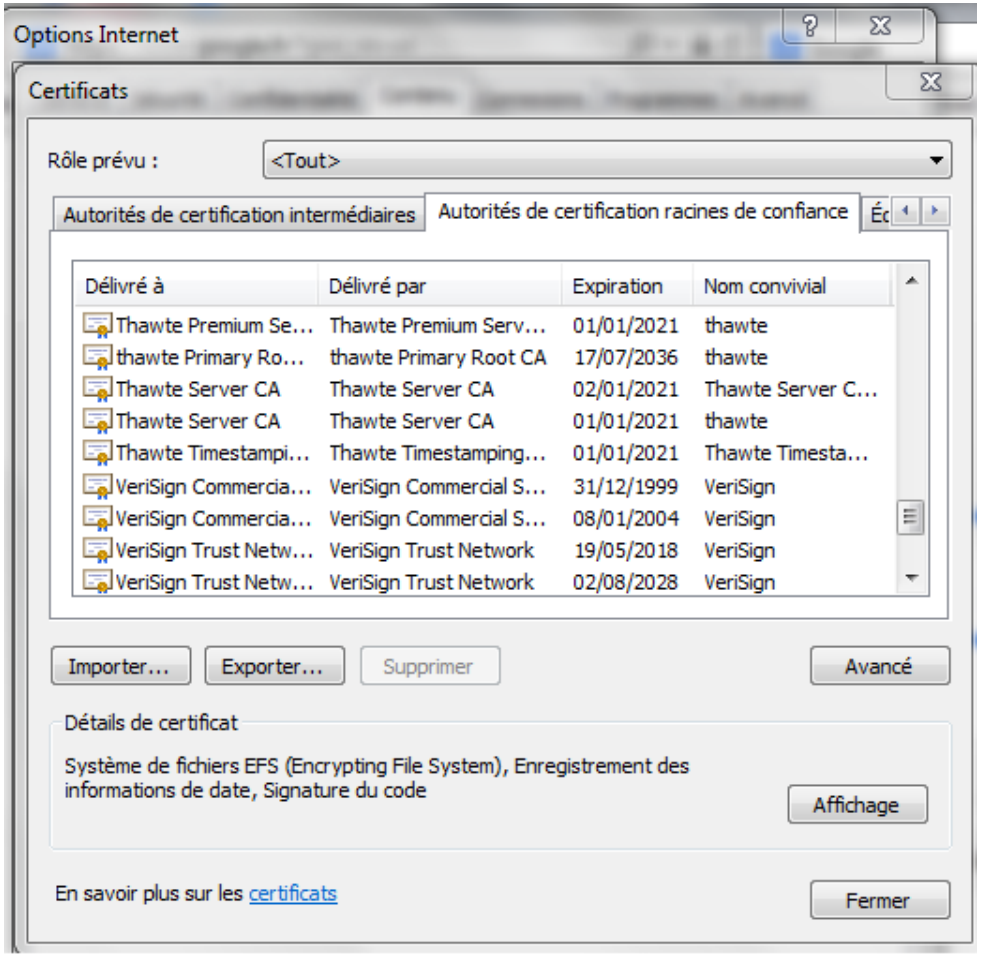
- Each person who wants to participate in a PKI requires a digital certificate, which is a credential that contains the public key for that individual along with other identifying information
- The certificate is created and signed (digital signature) by a trusted third party, which is a certification authority (CA)
- When the CA signs the certificate, it binds the individual's identity to the public key, and the CA takes responsibility for the authenticity of that individual

Certification Authorities (CA)

- A CA is a trusted organization (or server) that maintains and issues digital certificates
- When a person requests a certificate, the registration authority (RA) verifies individual's identity and passes the certificate request off to the CA
- The CA constructs the certificate, signs it, sends it to the requester, and maintains the certificate over its lifetime
- People who trust a certificate authority trust each other indirectly

Certification Authorities (CA)

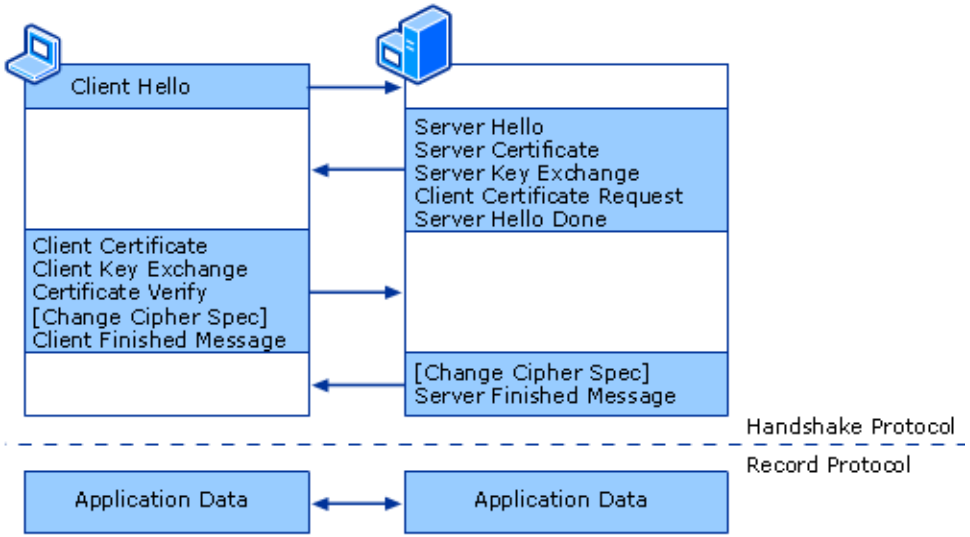
- The CA can be internal to an organization
- Other CAs are organizations dedicated to this type of service, and other individuals and companies pay them to supply it
- Browsers have several well-known CAs configured by default



ECE PARIS ÉCOLE D'INGÉNIEURS

HTTPS

- HTTP Secure (HTTPS) is HTTP running over TLS
- Transport Layer Security (TLS) uses public key encryption and provides data encryption, server authentication, message integrity, and optional client authentication
- Communication begins with a negotiation between the client and the server

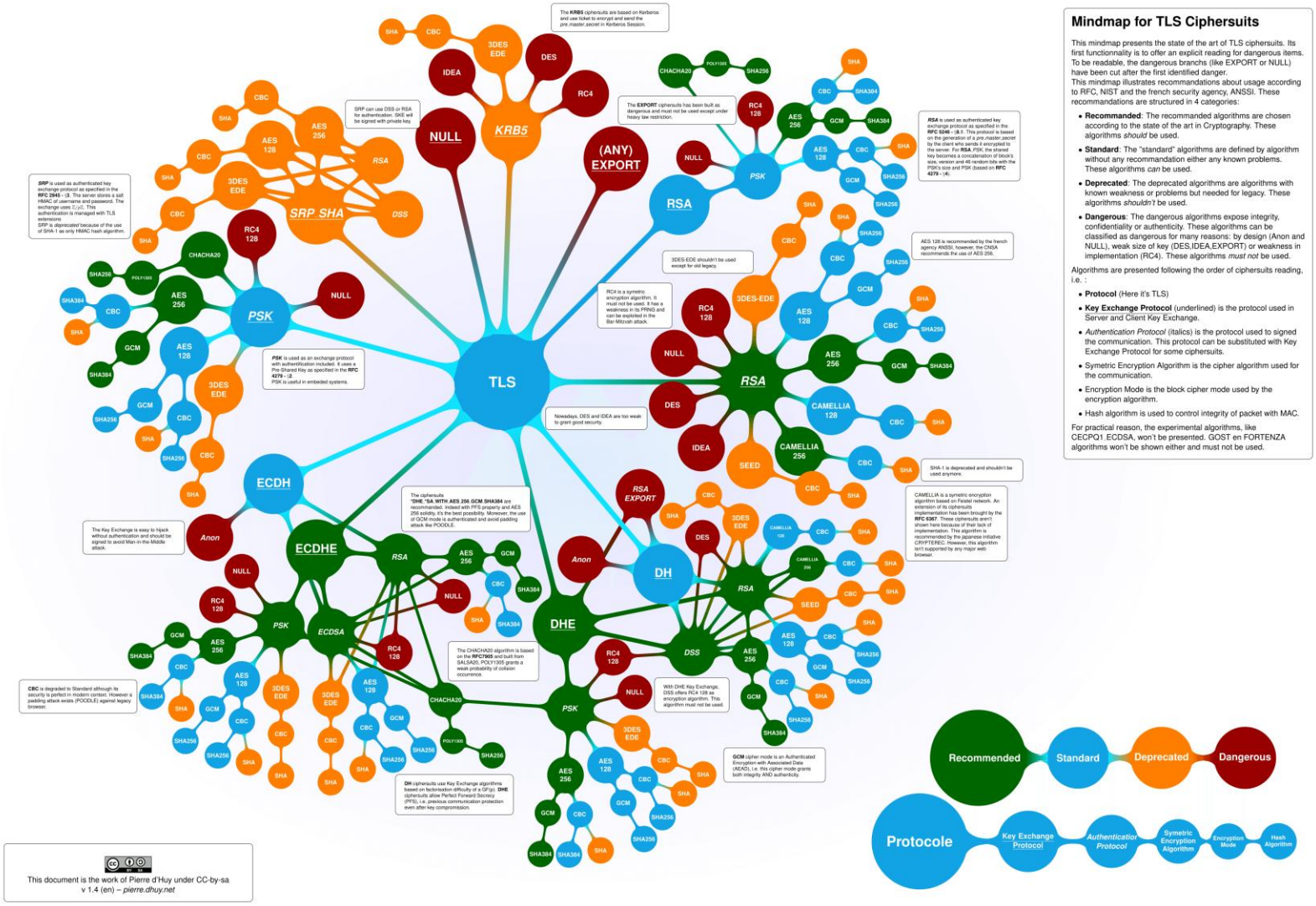


HTTPS

- **Client and server try to use the most powerful encryption protocol and decrease until finding a protocol common to both**

- **Remote site authentication is performed using the digital certificate issued by a certification authority**
  - The browser checks the validity of the certificate of the website against the certificates existing on the computer

HTTPS algorithms



ECE PARIS ÉCOLE D'INGÉNIEURS