CyberEdu

La sécurité par l'enseignement supérieur des NTIC

Sensibilisation et initiation à la cybersécurité

Module 3 : les aspects réseau et applicatifs

08/04/2021

1. Les bases de la cryptographie

a) Vocabulaire
b) Un peu d'histoire
c) Chiffrement symétrique
d) Chiffrement asymétrique
e) Chiffrement symétrique vs Chiffrement asymétrique
f) Signature électronique
g) Certificats électroniques
h) Jetons cryptographiques

1. Les bases de la cryptographie

a. Vocabulaire

La cryptographie est une discipline consistant à manipuler des données de telle façon que les services suivants puissent être fournis :

Intégrité

Objectif : s'assurer que les données n'ont pas été modifiées sans autorisation.
Remarque : dans les faits, la cryptographie ne s'attache pas vraiment à empêcher une modification de données, mais plutôt à fournir un moyen sûr de détecter une modification malveillante.

Confidentialité

Objectif : ne permettre l'accès aux données qu'aux seules personnes autorisées.

Preuve (authentification et non-répudiation)

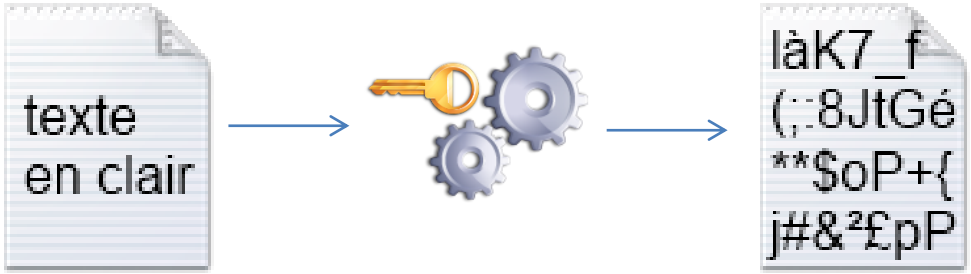
Objectif : fournir un moyen de preuve garantissant la véritable identité des entités ainsi que l'imputation de leurs actions.

1. Les bases de la cryptographie

a. Vocabulaire

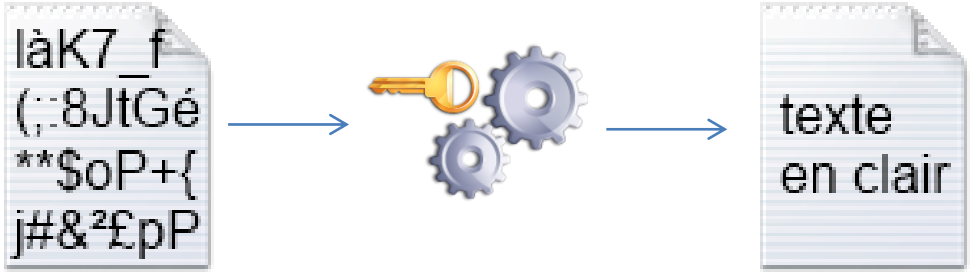
Chiffrer

Transformer une donnée de telle façon qu'elle devienne incompréhensible. Seules les entités autorisées pourront comprendre cette donnée chiffrée.



Déchiffrer

Transformer une donnée précédemment chiffrée pour reconstituer la donnée d'origine. Seules les entités autorisées ont la capacité de procéder à cette action.



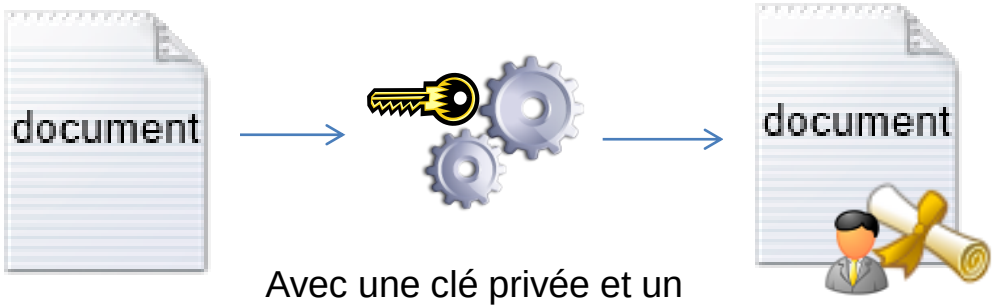
Recours à un algorithme et à une clé cryptographique.

1. Les bases de la cryptographie

a. Vocabulaire

Signer

Créer une signature électronique unique à la donnée et à son auteur. La signature lie donc la donnée d'origine et son auteur.



Avec une clé privée et un message en entrée, on obtient une signature en sortie

Vérifier la signature

S'assurer que la donnée d'origine n'a pas été modifiée et que son auteur est authentifié. Si la signature n'est pas valide, alors il ne faut pas faire confiance au document.

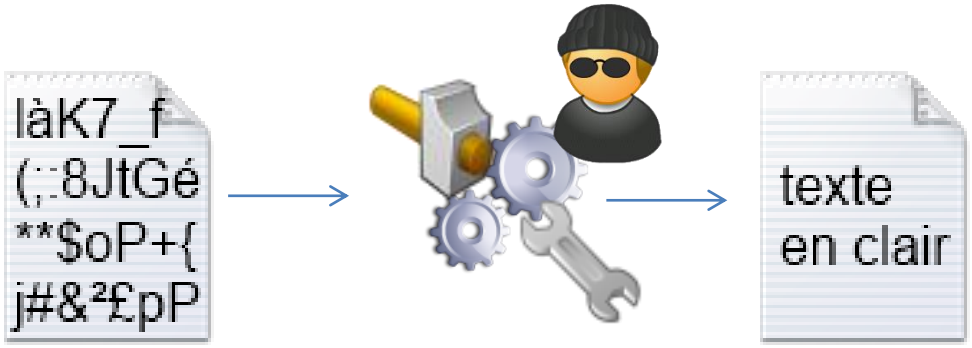
Avec la clé publique, la signature et le message en entrée,
on obtient un verdict OK/NOK en sortie

1. Les bases de la cryptographie

a. Vocabulaire

Décrypter

Reconstituer la donnée d'origine en tentant de « casser » la donnée chiffrée ou l'algorithme cryptographique.



Crypter

La notion de crypter n'existe pas. Il s'agit d'un abus de langage.

Le codage permet de passer d'une représentation des données vers une autre. Aucun secret n'est rattaché à cette notion. On parle de chiffrement lorsqu'on essaye de rendre l'information contenue illisible.

1. Les bases de la cryptographie

b. Un peu d'histoire : « Chiffrement de César »

Exemple d'algorithme cryptographiques historique. Les algorithmes sont maintenant basés sur des fonctions mathématiques.

Chiffrement de César

Méthode : il s'agit ici de « décaler » chaque caractère par un nombre déterminé.

Exemple : clé = 3

Exercice :

Donnée chiffrée : FBEHUHGX

Quelle est la donnée en clair ?

Décryptage en 26 essais !!!

1. Les bases de la cryptographie

b. Un peu d'histoire : « Chiffre de Vigenere »

- Chiffrement par substitution et par décalage. Utilisation d'une clé.

Exemple : clé : cyberedu
Texte à chiffrer : Bienvenu dans le cours cyberedu

Dgfrmiqo fyow ci fiwpt gpfhlgbv
dgfrmiqofyowcifiwptgpfhlgbv

Résiste à l'analyse de fréquence …

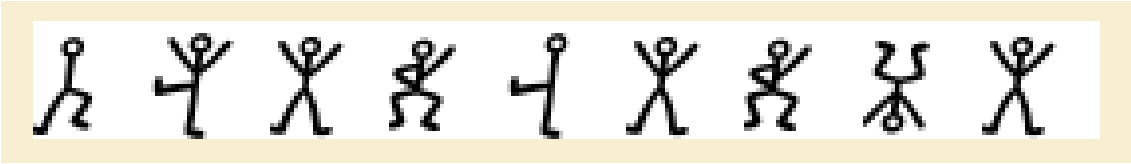
Cassé à partir de 1881….

Codage parfait : chiffre de Vernam

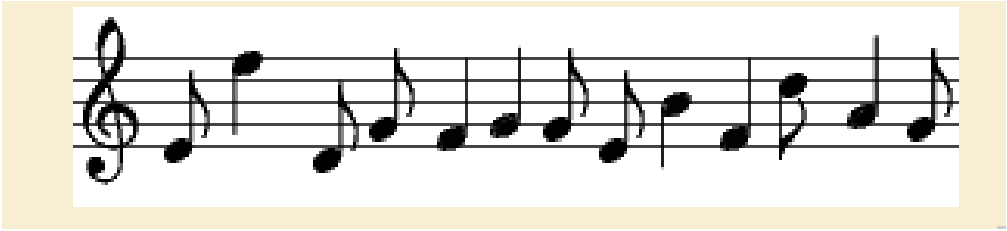
Clé Utilisée	26 lettres chiffrées																								
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	B	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

1. Les bases de la cryptographie

b. Un peu d'histoire : les codages



```
>++++++++++[<++++++++++>-]<.---.>++++[<++++>-]
<---.+++++.>+++++++++[<--------->-]<--.>+++++++++[<+++++++++>-]
<-----.-------.>++++++++[<-------->-]<-----.
```

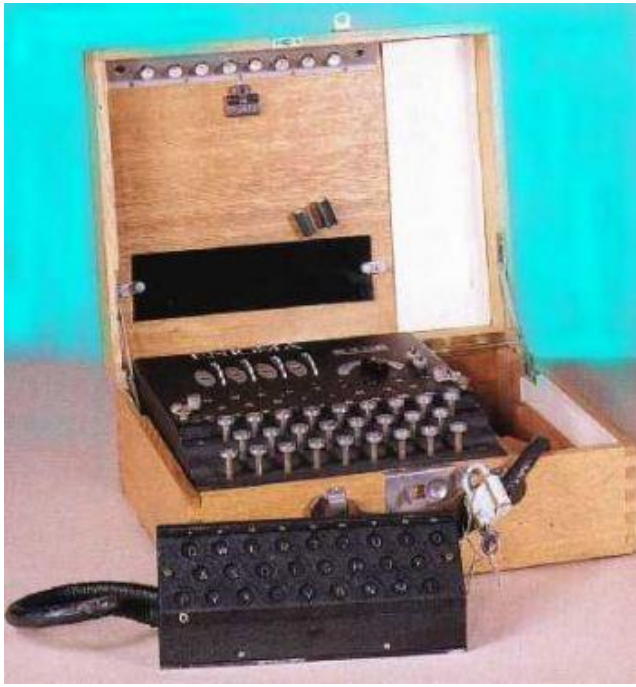


http://www.dcode.fr

1. Les bases de la cryptographie

b. Un peu d'histoire : « Machine Enigma »

Présentation des machines Enigma



- Machine initiale conçue au début du XXè siècle (1920). Elle a bénéficié de plusieurs évolutions et versions, et a été utilisée par les Allemands pendant la seconde guerre mondiale ;
- Les machines Enigma ressemblent à des machines à écrire, avec un clavier destiné à un opérateur, un tableau de sortie (panneau lumineux), plusieurs rotors, un réflecteur et un tableau de connexion ;
- La méthode de chiffrement est basée sur de la substitution :
  - L'opérateur tape le message en clair. Chaque lettre du message en clair est remplacée par une autre lettre dans le message chiffré (les lettres chiffrées s'allument sur le tableau de sortie au fur et à mesure de la frappe en clair de l'opérateur) ;
  - L'utilisation des rotors a pour conséquence qu'une lettre en clair sera être substituée par des lettres différentes tout au long du message chiffré.

source image : http://museeradiomili.com/cryptographie/

1. Les bases de la cryptographie

b. Un peu d'histoire : « Machine Enigma »

Les fonctions d'une machine Enigma

- Tableau de connexion
  - Se situe avant l'entrée sur le brouilleur ;
  - Effectue des permutations simples.

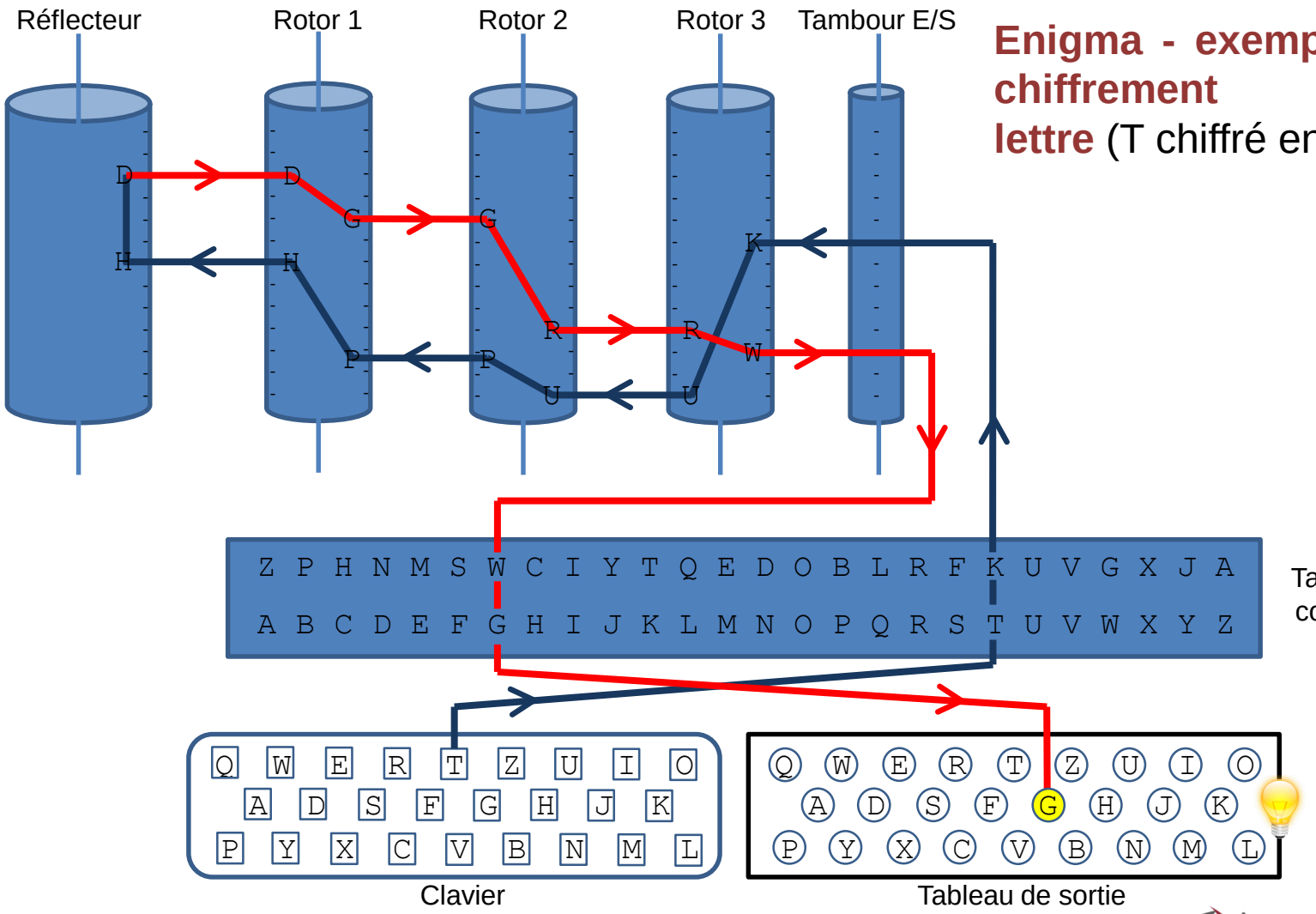
- De 3 à 6 rotors (selon le modèle)
  - Permutations aléatoires des lettres de l'alphabet ;
  - Le rotor tourne à chaque lettre tapée ;
  - Lorsque le premier rotor a fait un tour (26 positions), le second rotor tourne d'un cran, et ainsi de suite.

- Le réflecteur
  - Dernière permutation 2 à 2 des lettres avant de les faire retraverser les retors et le tableau de connexion.

source images : https://interstices.info/jcms/jalios_5127/accueil

1. Les bases de la cryptographie

b. Un peu d'histoire : « Machine Enigma »



Enigma - exemple de chiffrement d'une lettre (T chiffré en G)

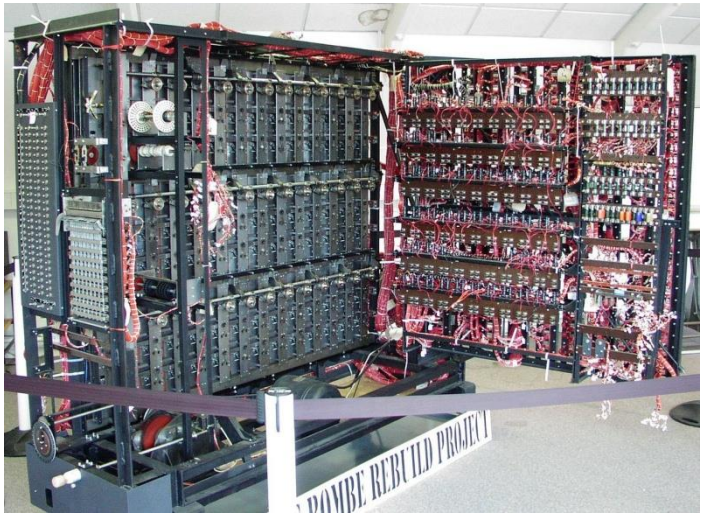
Tableau de connexion

1. Les bases de la cryptographie

b. Un peu d'histoire : « Machine Enigma »

- Chiffrage
  - Chaque jour l'ordre des rotors changent, tableau de connexion aussi

- Décryptage
  - Polonais : à l'aide d'une machine volée
    - Utilisation de 2*3 lettres identiques au début
    - *Marian Rejewski*
  - Anglais (après polonais) :
    - Par mot clé
    - Utilisation d'une bombe électromécanique
    - Bletchley Park, avec Alan turing



1. Les bases de la cryptographie

c. Chiffrement symétrique

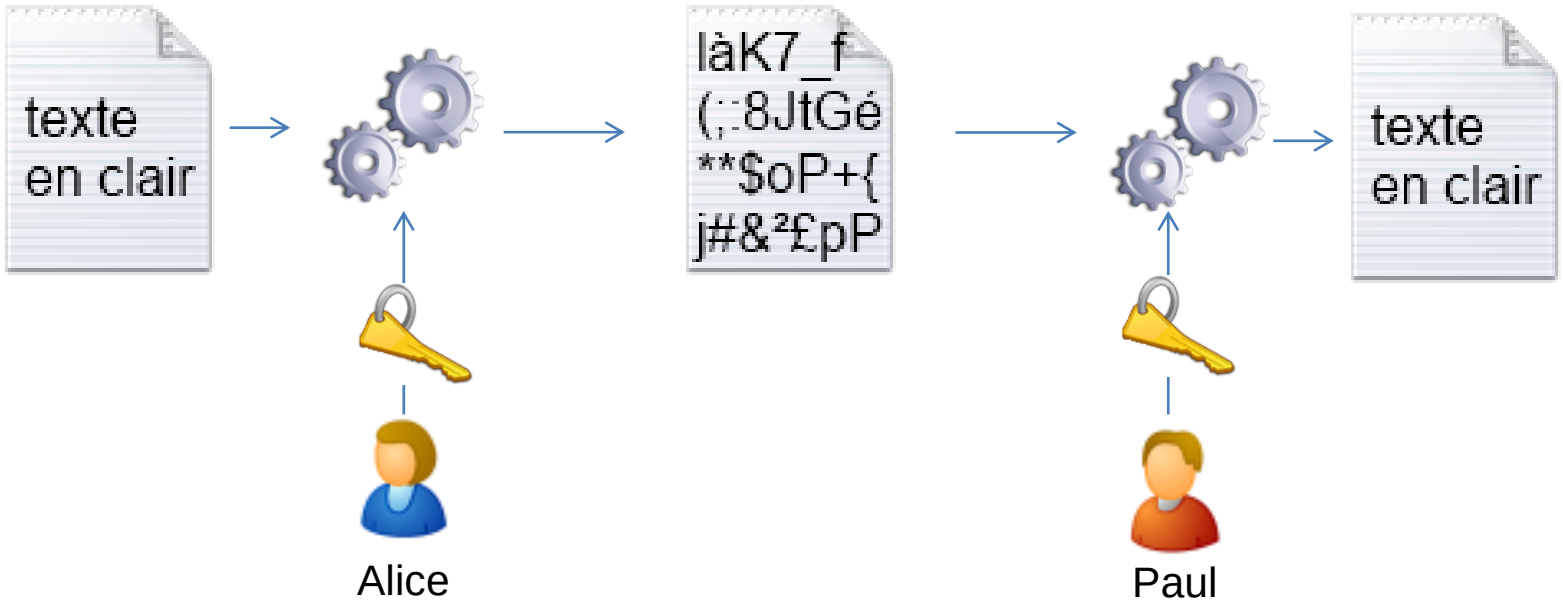
- La clé utilisée pour le chiffrement est la **même** que celle utilisée pour le déchiffrement ;

- Cette clé doit être **secrète :** seules les personnes habilitées doivent posséder cette clé, sinon la confidentialité du message n'est plus assurée !

1. Les bases de la cryptographie

c. Chiffrement symétrique

- Exemple : Alice souhaite envoyer un message confidentiel à Paul



Clé secrète partagée entre Alice et Paul

1. Les bases de la cryptographie

d. Chiffrement asymétrique

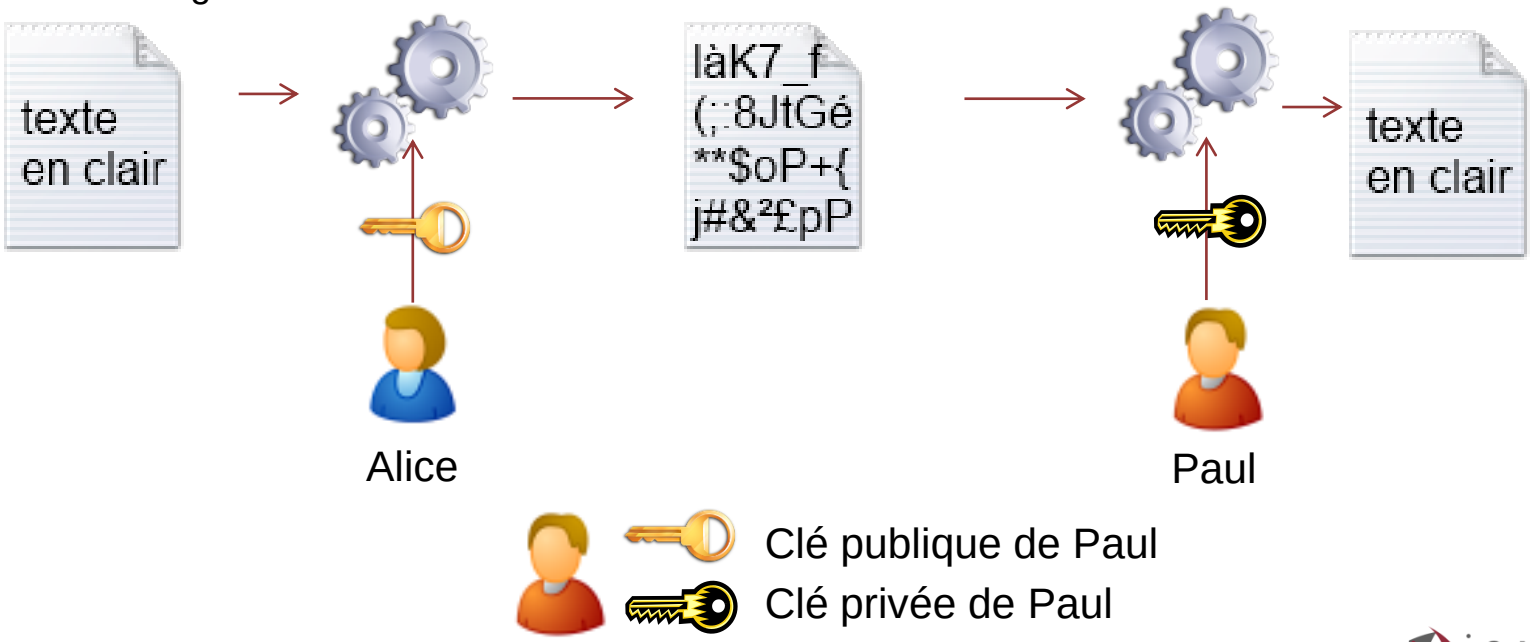
- La clé utilisée pour le chiffrement est **différente** de celle utilisée pour le déchiffrement. Il est nécessaire d'utiliser 2 clés :
  - **Clé publique** : comme son nom l'indique, cette clé est publique et peut être donnée à tout le monde ;
  - **Clé privée** : cette clé doit être personnelle et connue de son seul propriétaire. Elle ne doit jamais être divulguée !

- Ces deux clés sont mathématiquement liées
  - La connaissance de la clé publique ne permet pas de calculer de manière efficace la clé privée (attention à la taille de la clé, qui doit être suffisamment longue) ;
  - Chaque personne doit donc posséder 2 clés : une clé privée (confidentielle) et une clé publique qu'il peut divulguer à tout le monde.

1. Les bases de la cryptographie

d. Chiffrement asymétrique

- Exemple : Alice souhaite envoyer un message confidentiel à Paul
  - Alice chiffre le message avec la clé publique de Paul ;
  - Paul déchiffre le message grâce à sa privée ;
  - Notes :
    - Alice ne pourra jamais (et n'aura jamais besoin de) utiliser la clé privée de Paul puisque celle-ci est confidentielle à Paul !
    - Alice n'a pas besoin d'utiliser ses clés personnelles dans cet exemple de chiffrement sans signature.



1. Les bases de la cryptographie

e. Chiffrement symétrique vs Chiffrement asymétrique

Avantages

Chiffrement symétrique

- Rapidité des opérations (adapté à du trafic en temps réel) ;
- Clés courtes (256 bits suffisent actuellement) ;

Chiffrement asymétrique

- Facilité d'échange des clés : les seules clés qui ont besoin d'être échangées sont des clés publiques (dont il faut assurer la protection en intégrité) ;

Inconvénients

- Difficulté d'échange sécurisé des clés secrètes : comment le faire en protégeant ce secret ?

- Lenteur des opérations (peu adapté à du trafic en temps réel) ;
- Grande taille des clés (2048 bits minimum actuellement) ;

Exemples d'algorithmes sûrs (janvier 2017)

- AES.

- RSA.

1. Les bases de la cryptographie

f. Signature électronique

Rappel de l'objectif : **s'assurer de la non-modification d'une donnée**, et **s'assurer de l'identité de son auteur**. Si la signature n'est pas valide, cela indique que l'auteur « n'est pas le bon » ou que le donnée reçue n'est pas celle que son auteur avait signé.

Notes :

- **La signature électronique n'assure pas la confidentialité des données**, mais leur intégrité et la notion de preuve ;
- **Lorsque l'on chiffre un message, il est fortement recommandé de le signer également** afin d'assurer l'intégrité du message.

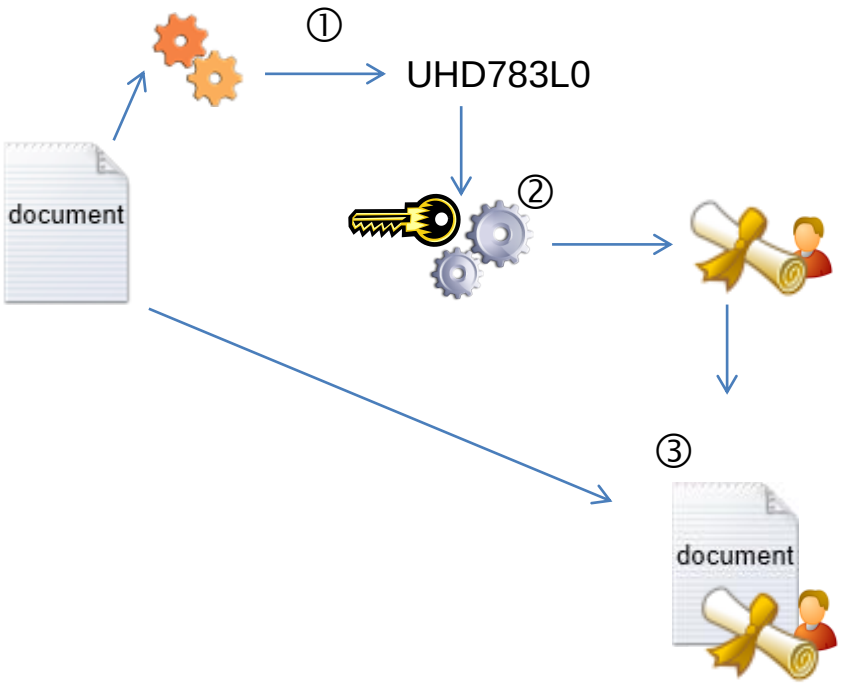
1. Les bases de la cryptographie

f. Signature électronique : principe

1. Le signataire d'un message génère – grâce à un algorithme cryptographique spécifique – une valeur unique calculée à partir du message que l'on souhaite signer : un condensat (un haché) ;
   - Les algorithmes de calcul de condensat sont publics et ne gèrent pas de secret, donc tout le monde peut les utiliser et calculer les mêmes condensats à partir d'un même message ;
   - Deux messages différents ne peuvent pas donner lieu au même condensat.
2. Le signataire utilise l'algorithme de signature, qui prend en entrée sa clé privée et le condensat précédent, pour produire une signature électronique ;
3. Le signataire envoie (ou stocke) le message et la signature électronique, permettant ainsi à un lecteur d'en prendre connaissance ;
4. Le lecteur calcule lui-même le condensat du message en clair ;
5. Le lecteur utilise l'algorithme de vérification de signature, qui prend en entrée la clé publique du signataire, le condensat et la signature, pour rendre un verdict. Si le verdict est négatif, alors il ne faut pas faire confiance au message reçu (celui-ci ne correspond pas — pour une raison que l'on ignore — au message du signataire).

1. Les bases de la cryptographie

f. Signature électronique : illustration



Etapes de la signature :

① Le signataire génère le condensat unique associé au message ;

② Le signataire utilise l'algorithme de signature, qui prend en entrée sa clé privée et le condensat précédent, pour produire une signature électronique ;

③ Le signataire envoie (ou stocke) le message et la signature électronique, permettant ainsi à un lecteur d'en prendre connaissance ;

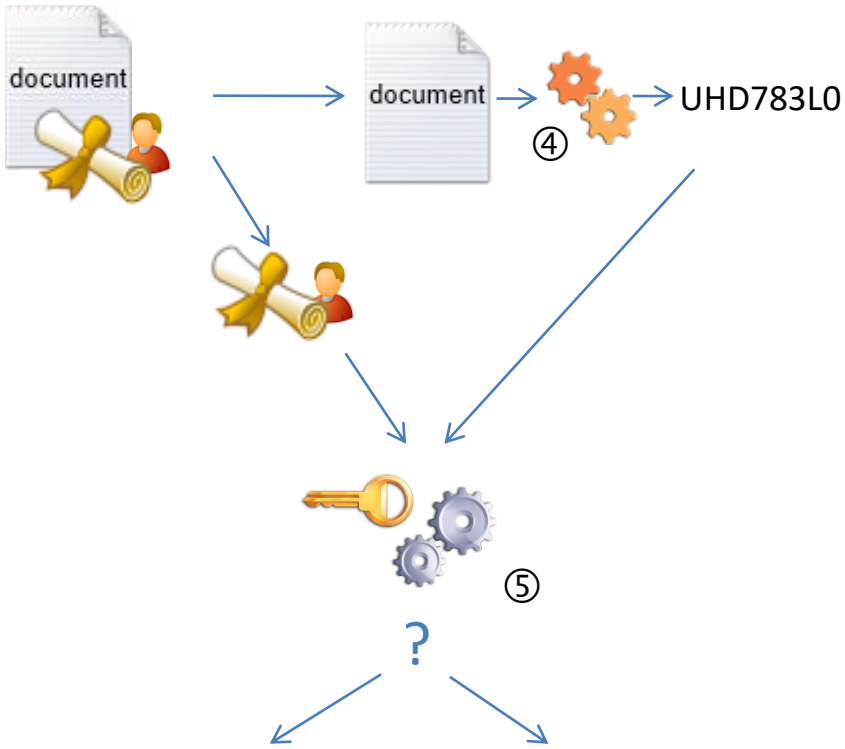
La vérification par le destinataire/lecteur est décrite sur la diapositive suivante.

Clé publique du signataire

Clé privée du signataire

1. Les bases de la cryptographie

f. Signature électronique : illustration



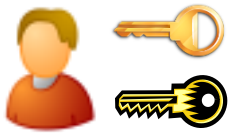
Etapes de la vérification de la signature par un lecteur/destinataire :

④ Le lecteur calcule le condensat du message en clair ;

⑤ Le lecteur utilise l'algorithme de vérification de signature, qui prend en entrée la clé publique du signataire, le condensat et la signature, pour rendre un verdict. Si le verdict est négatif, alors il ne faut pas faire confiance au message reçu (celui-ci ne correspond pas — pour une raison que l'on ignore — au message du signataire).

✓ La signature est valide. Le message est intègre.

✗ La signature est invalide. Le message n'est pas intègre.



Clé publique du signataire

Clé privée du signataire

1. Les bases de la cryptographie

g. Certificats électroniques

Un aspect important n'a pas été traité jusqu'à maintenant :

Les interlocuteurs de Paul ont besoin d'utiliser sa clé publique. Comment peuvent-ils **être certains que la « clé publique de Paul » appartient effectivement à Paul** et qu'elle n'a pas été générée frauduleusement en son nom ? Autre exemple, comment les visiteurs d'un site web bancaire peuvent **être certains que le site web est légitime** et qu'il ne s'agit pas d'un site frauduleux imitant celui d'une banque ?

- Solution : utilisation de certificats électroniques.

1. Les bases de la cryptographie

g. Certificats électroniques

Un certificat est un **fichier électronique** qui comprend notamment :

- La **clé publique** d'un individu (ou d'une entité ou d'un nom de domaine) ;
- Les détails de cet individu (ou de cette entité) : nom, prénom, nom de domaine, etc. ;
- La **signature par un tiers de confiance**, chargé de garantir que le propriétaire de la clé publique a été vérifié et – par conséquent – l'authenticité de la clé publique vis-à-vis de son propriétaire. La signature porte sur l'identité du détenteur et la clé publique afin d'assurer l'intégrité de l'ensemble ;
- D'autres informations telles que l'usage de la clé, *les dates de validité*, des informations concernant la révocation, etc.

Le tiers de confiance, une autorité de certification, en charge de :

- **Vérifier l'identité** de la personne demandant à créer le certificat ;
- **Créer le certificat** après vérification, **puis le signer** (avec la clé privée de l'autorité de certification) ;
- **Tenir à jour une liste des certificats qui ont été révoqués** (par exemple si la clé a été compromise).

1. Les bases de la cryptographie

g. Certificats électroniques

Comment connaitre les autorités de certification ?

- Elles sont directement intégrées par les éditeurs dans les systèmes d'exploitation et/ou les navigateurs ;
- L'utilisateur est également libre de rajouter l'autorité de certification de son choix si il choisit de faire confiance à des certificats signés par une autorité non-intégrée dans son navigateur.

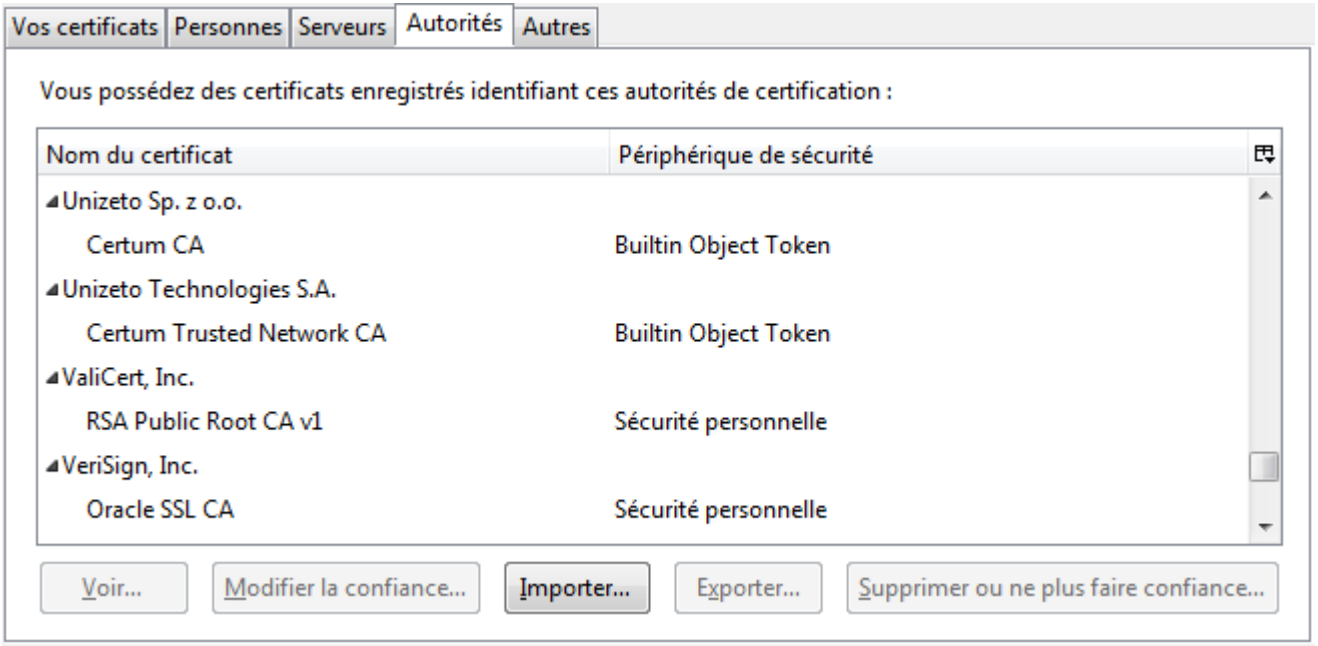


Image : magasin de certificats de Firefox

1. Les bases de la cryptographie

g. Certificats électroniques

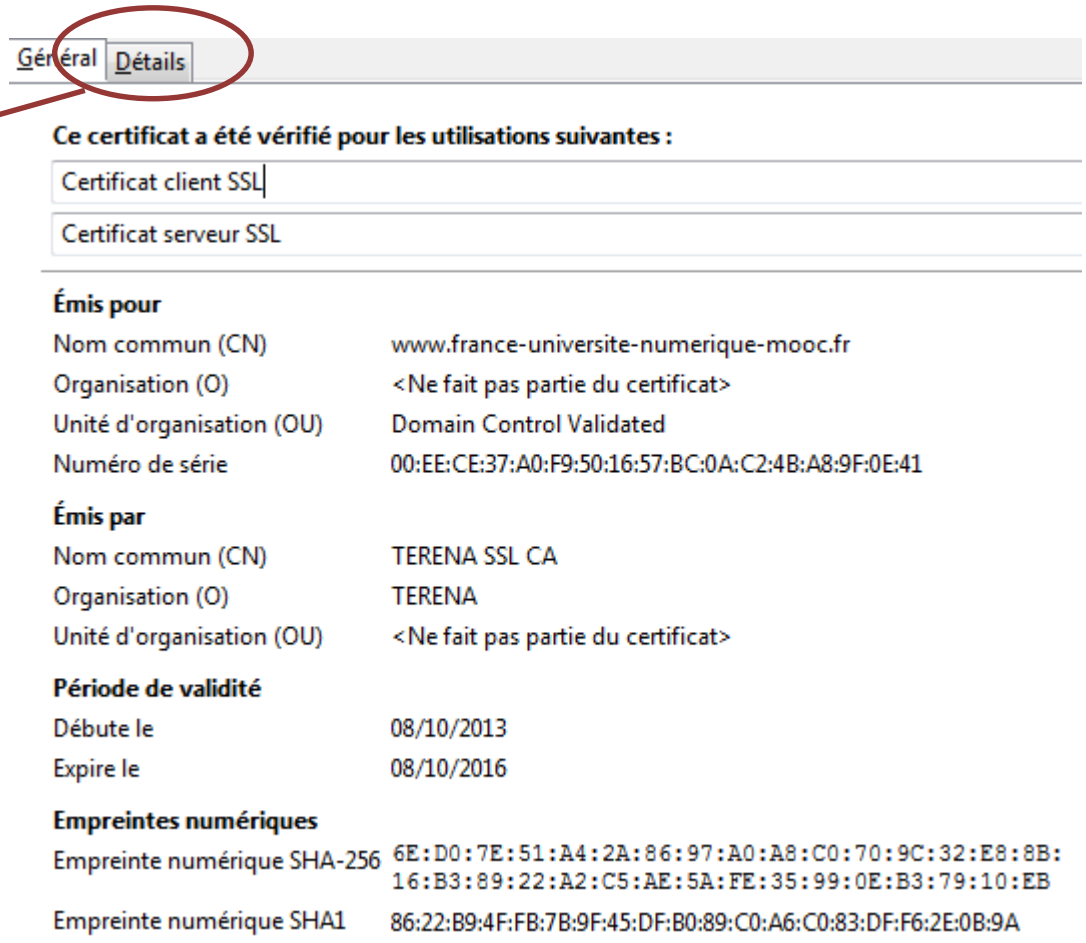
Exemple d'un certificat pour le site web www.france-universite-numerique-mooc.fr

Les détails techniques du certificat, la clé et la signature se trouvent dans **Détails**

Détenteur de la clé publique

Autorité de certification

Dates de validité du certificat



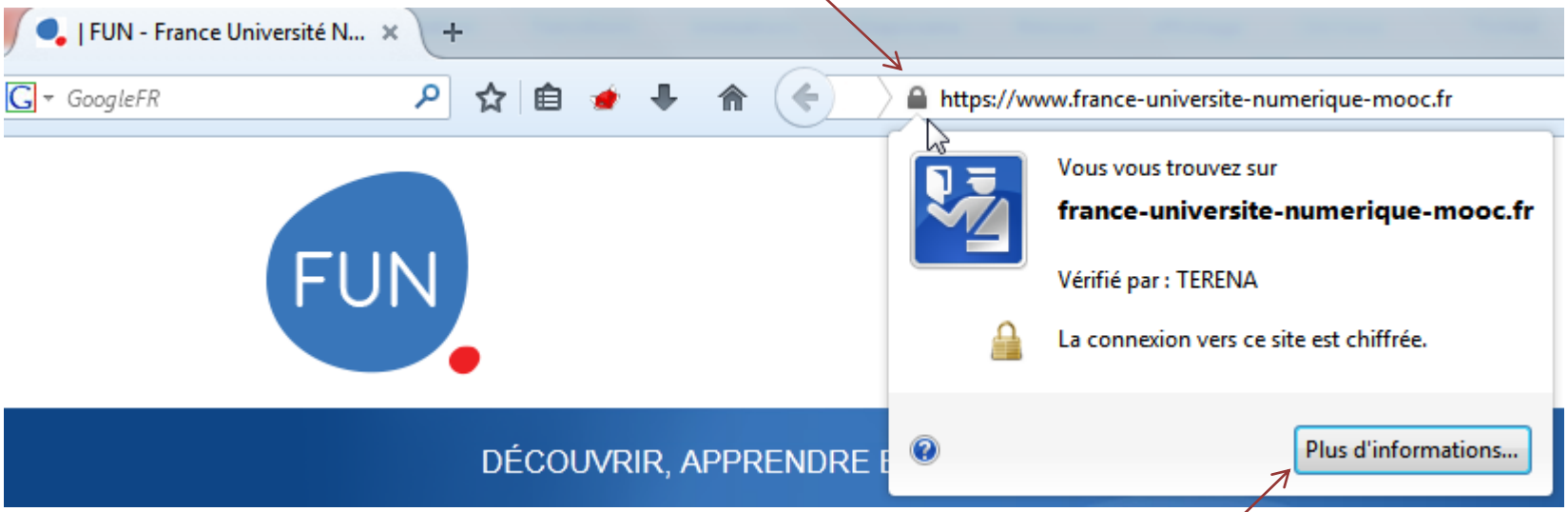
1. Les bases de la cryptographie

g. Certificats électroniques

Où trouver les certificats dans un navigateur ?

Exemple avec Firefox pour ouvrir le certificat d'un site WEB

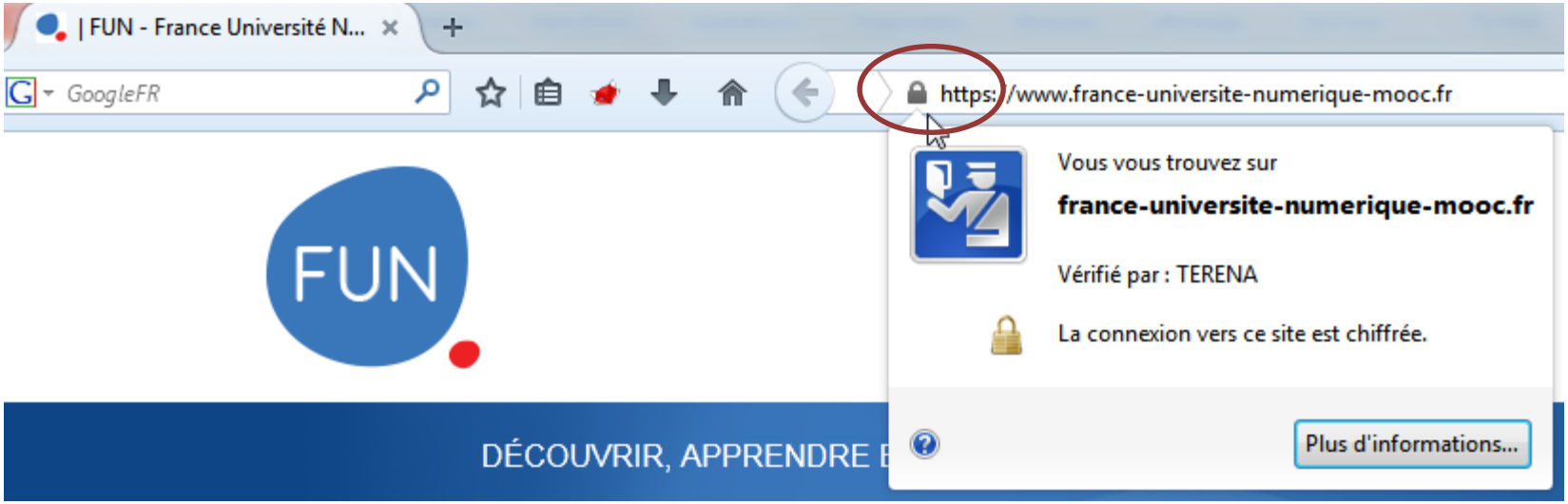
Cliquer sur le cadenas à côté de l'URL



Cliquer ici pour afficher le certificat

1. Les bases de la cryptographie

g. Certificats électroniques



Puisque le certificat du site WEB est disponible et valide, cela amène donc deux avantages à l'utilisateur, caractéristiques du HTTPS

- Nous sommes confiants que **le site WEB est légitime** (i.e. le certificat a été vérifié et signé par une autorité de certification de confiance) ;
- Puisque le certificat contient la clé publique du site WEB, nous pouvons donc **chiffrer nos connexions vers ce site** (méthode : chiffrement avec la clé publique du destinataire comme nous l'avons vu au préalable dans ce cours).

1. Les bases de la cryptographie

h. Jetons cryptographiques (tokens)

- Les jetons sont utilisés pour **stocker des clés privées** (cryptographie asymétrique) ou **secrètes** (cryptographie symétrique) ;
- Puisqu'un jeton contient une information sensible (une clé privée ou secrète), il faut donc **protéger ce jeton** pour que seules les personnes habilitées puissent l'utiliser ;
- Exemples de jetons et leurs moyens de protection (ainsi que leur niveau de sécurité) :

  - **Fichier sur disque**, associé à un mot de passe connu de l'utilisateur seulement (exemple avec l'application libre GPG) ;

  - **Jeton USB**, associé à un mot de passe (exemple de nombreux produits commerciaux qui utilisent un jeton physique pour authentifier un utilisateur sur un poste de travail) ;

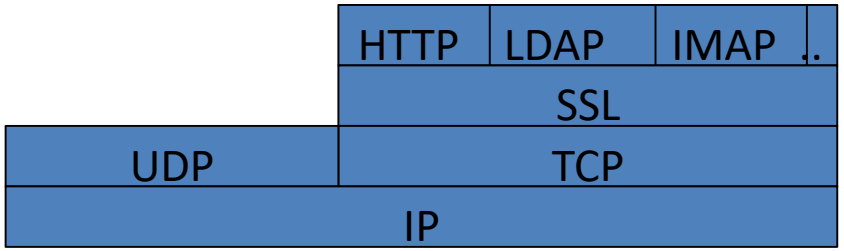
  - **Carte à puce**, associée à un mot de passe simple (exemple des cartes bancaires avec un code PIN permettant d'authentifier le propriétaire de la carte avant d'autoriser la transaction).
    - Afin d'éviter qu'une personne malveillante ne découvre facilement le mot de passe simple, on impose un verrouillage de la carte à puce après 3 tentatives infructueuses.

1. Le protocole SSL / TLS

i. Secure Sockets Layer / Transport Layer Security

- SSL ou TLS assure :
  - l'authentification du serveur
  - la confidentialité des données
  - l'intégrité des données
  - (optionnel) l'authentification du client

- Transparent pour l'utilisateur
  - Chiffrement seulement des données
  - Se situe entre la couche TCP et la couche applicative



1. Le protocole SSL

i. Evolution SSL /TLS

- SSLv1 -> juillet 1994 par Netscape (jamais utilisé)

- SSLv2 -> fin 1994, intégré à Netscape Navigator
  en mars 1995 → apparition du **https**

- SSLv3 -> novembre 1995

- **TLS (Transport Layer Security)**
  -> normalisé par l'IETF
  -> RFC 2246, en 1999
  -> basé sur SSLv3, mais avec de petits changements, donc incompatibilité

  actuellement TLS v1.3 possible

1. Le protocole SSL

i. Fonctionnement SSL

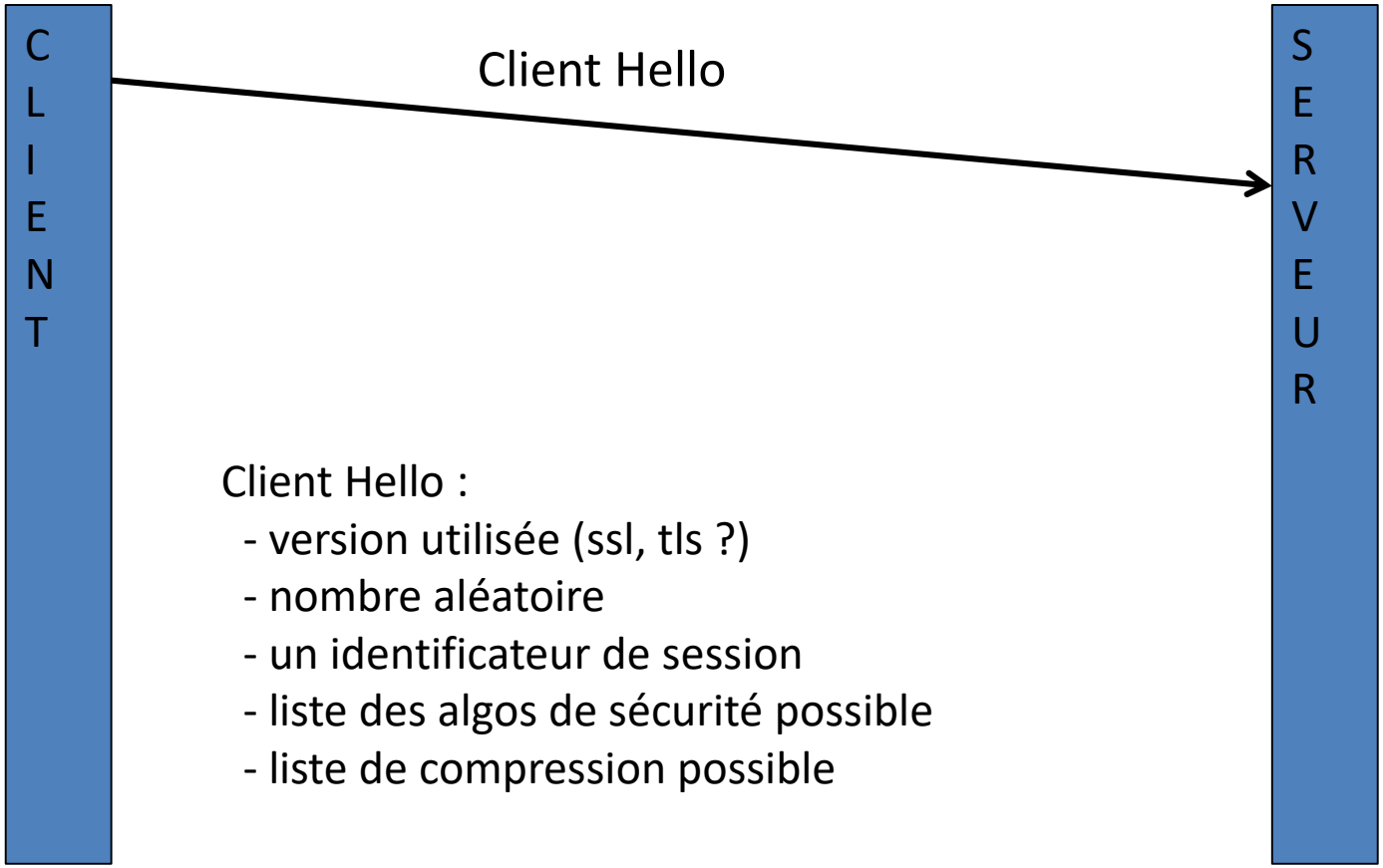
- SSL est composé de deux étapes
  - SSL Handshake
    - Échange des informations pour le chiffrement (longueur de clé, protocoles utilisés, etc..)
    - Utilisation de certificats et de clés publiques pour échanger une clé de session symétrique

    Pré-requis serveur : Certificat + clé publique/privée
  - SSL Record
    - Échange des données chiffrées par la clé de session
    - Impossible à décrypter même si les échanges précédents ont été récupérés

1. Le protocole SSL

i. Mise en place

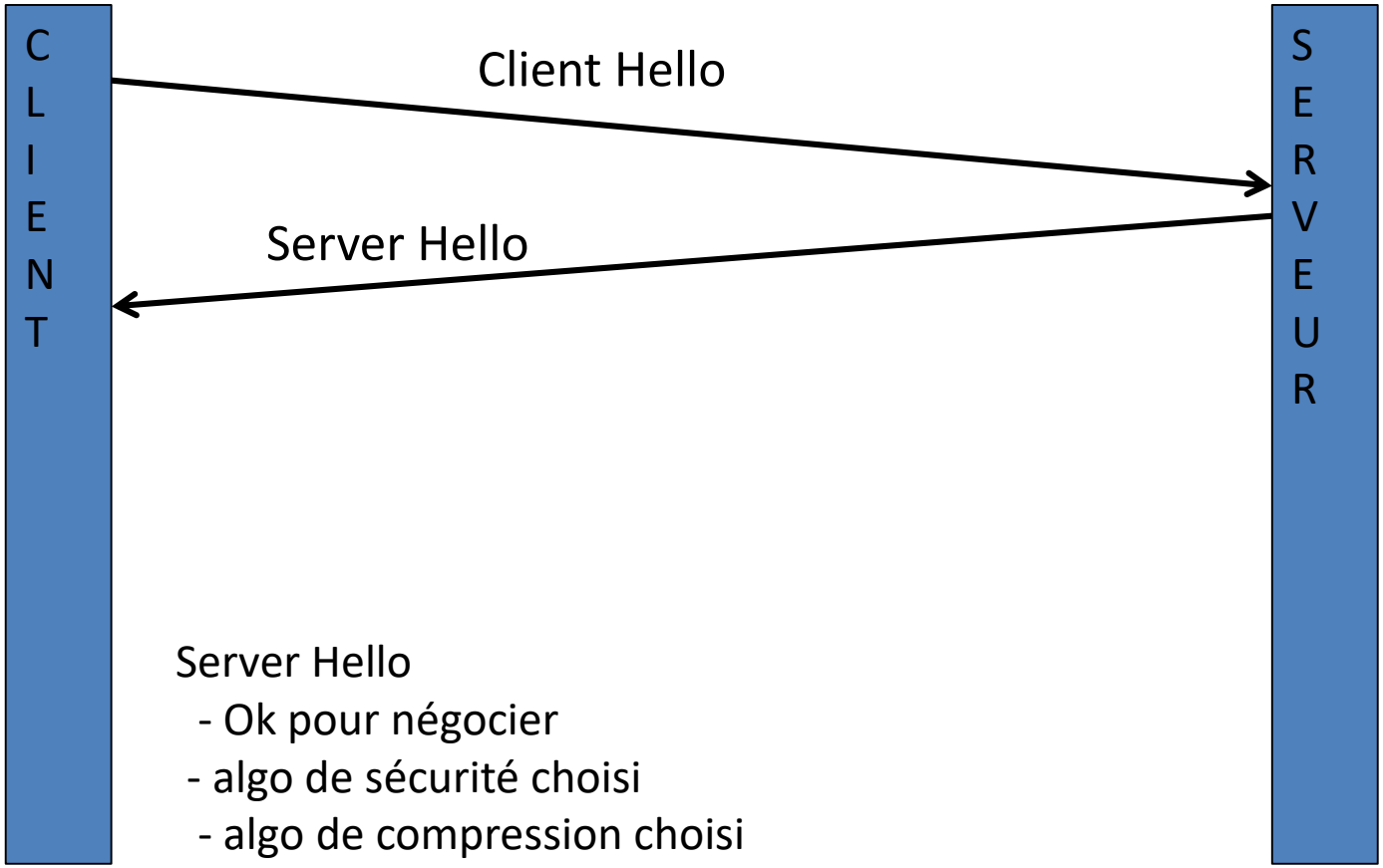
- Handshake



1. Le protocole SSL

i. Mise en place

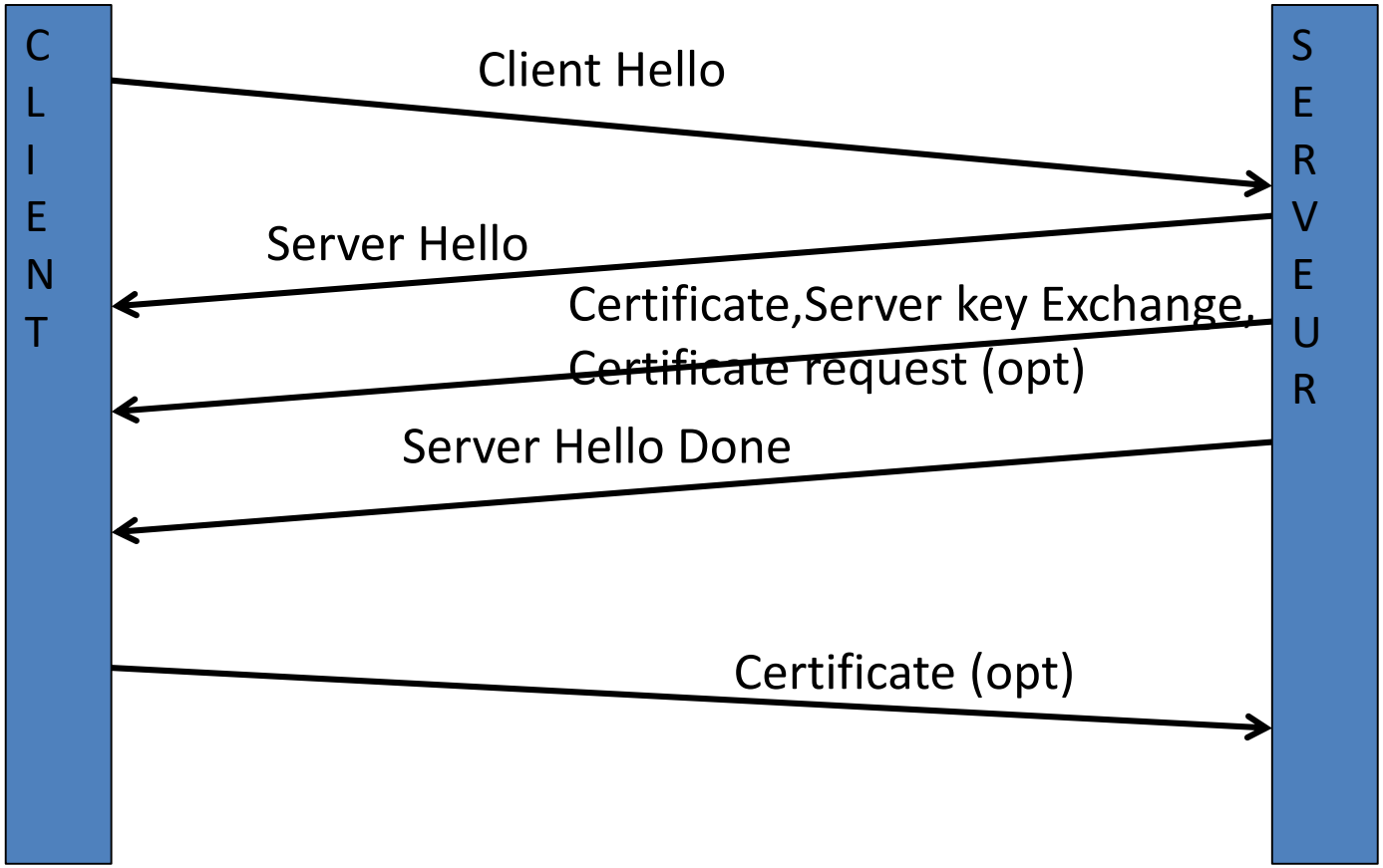
- Handshake



1. Le protocole SSL

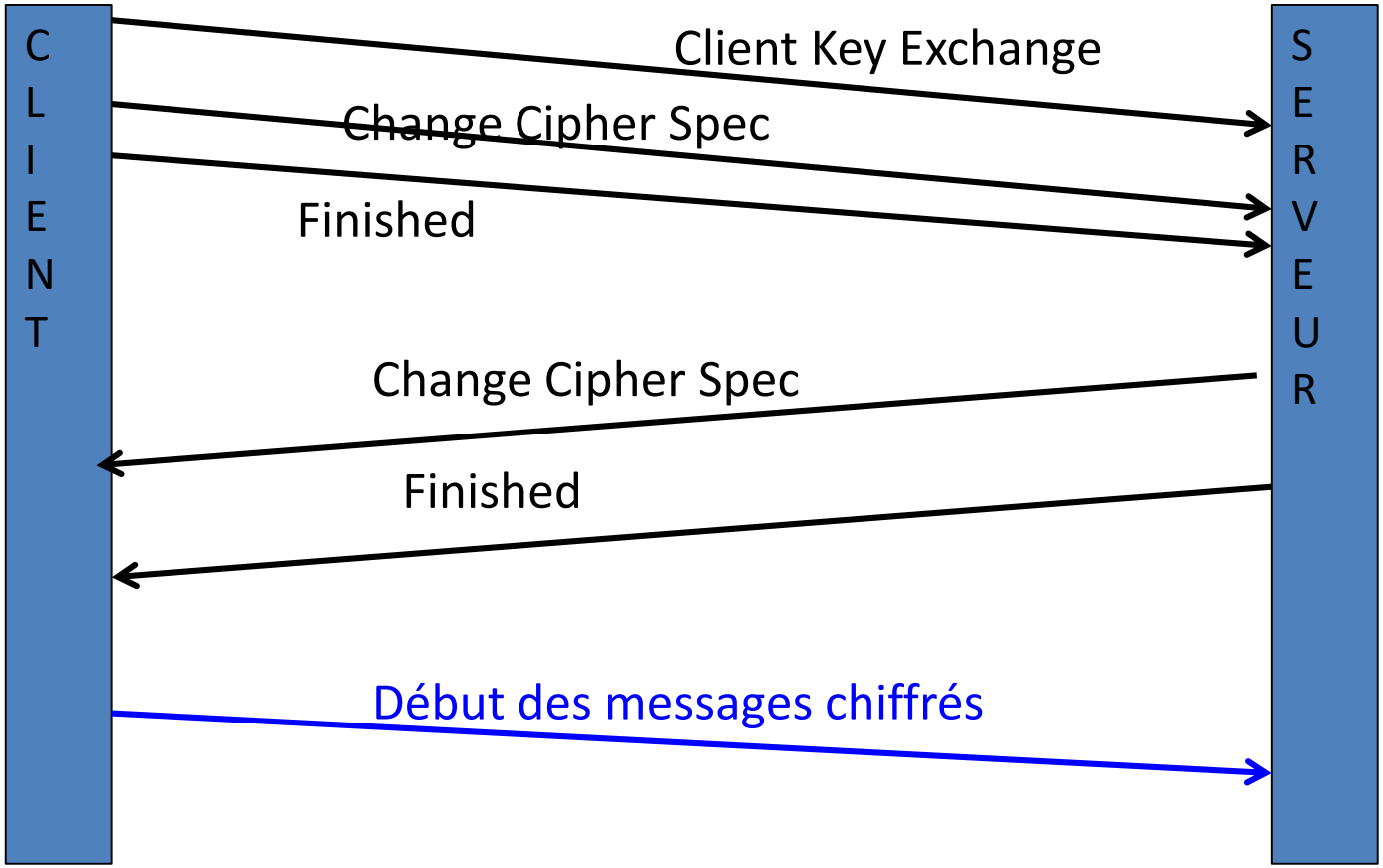
i. Mise en place

- Handshake



1. Le protocole SSL

- Handshake (suite et fin)



2. La sécurité des applications web

a) Usurpation d'identité via les cookies
b) Injection SQL

2. La sécurité des applications web

a. Usurpation d'identité via les cookies

Comme toutes les applications, les applications web sont sujettes à des vulnérabilités. Nous allons en voir deux d'entre elles :

- une faiblesse basée sur les cookies ;
  - Ce qui permet – par exemple – à un attaquant de contourner un mécanisme d'authentification.

- une faiblesse basée sur un code source mal développé.
  - Ce qui permet – par exemple – à un attaquant de contourner un mécanisme d'authentification, d'accéder à des données pour les divulguer ou les corrompre.

2. La sécurité des applications web

a. Usurpation d'identité via les cookies

Les cookies sont des fichiers gérés par les navigateurs web afin de stocker (et réutiliser) des informations concernant l'utilisateur, par exemple :

- son identifiant ;
- ses préférences d'affichage et de disposition de la page web.

Les cookies sont nécessaires pour toutes les pages web dynamiques qui nécessitent d'identifier ou d'authentifier l'utilisateur, en permettant notamment la mise en œuvre de sessions :

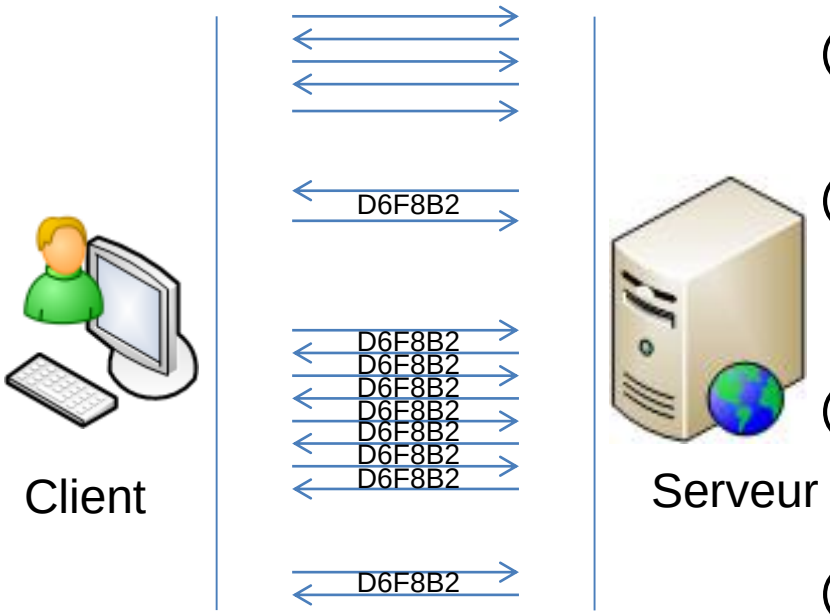
- les sites marchand (afin d'afficher le panier de l'utilisateur connecté) ;
- les sites bancaires (afin d'afficher le solde du compte de l'utilisateur connecté et non pas celui d'un autre client) ;
- les sites « en général » (afin d'afficher des publicités ciblées sur notre navigation).

Il est possible – sous certaines conditions – d'usurper l'identité d'un utilisateur sur un site web si on arrive à récupérer son cookie d'identification.

2. La sécurité des applications web

a. Usurpation d'identité via les cookies

Fonctionnement habituel d'une connexion sur un site web nécessitant une authentification (site marchand, site bancaire, etc.) :



① Phase d'authentification (via un mot de passe en général) ;

② Phase de génération du cookie d'identification*. L'utilisateur est maintenant connecté « à son compte »

③ Phase de « navigation » : le cookie est inclus dans tous les échanges afin que le serveur puisse identifier la connexion de l'utilisateur ;

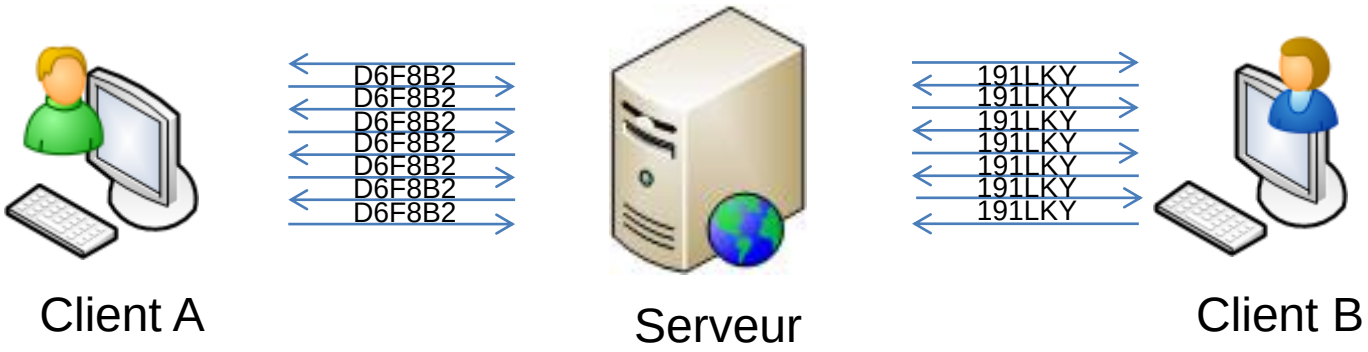
④ Phase de déconnexion : la session de l'utilisateur est maintenant clôturée. Le cookie est invalidé.

- Un cookie d'identification est en fait une chaine de caractères aléatoire et **unique**, suffisamment longue pour qu'elle ne puisse pas être générée deux fois par erreur. Exemple d'un cookie d'identification : D6F8B2BE3ED3040D9A3C10-D6F8B2A305D048B9

2. La sécurité des applications web

a. Usurpation d'identité via les cookies

A tout moment d'une connexion, chaque utilisateur du site web possède donc son propre cookie, unique à lui. Le serveur est donc en mesure d'identifier à qui appartient chaque connexion, et donc d'afficher les pages web qui lui sont propre.

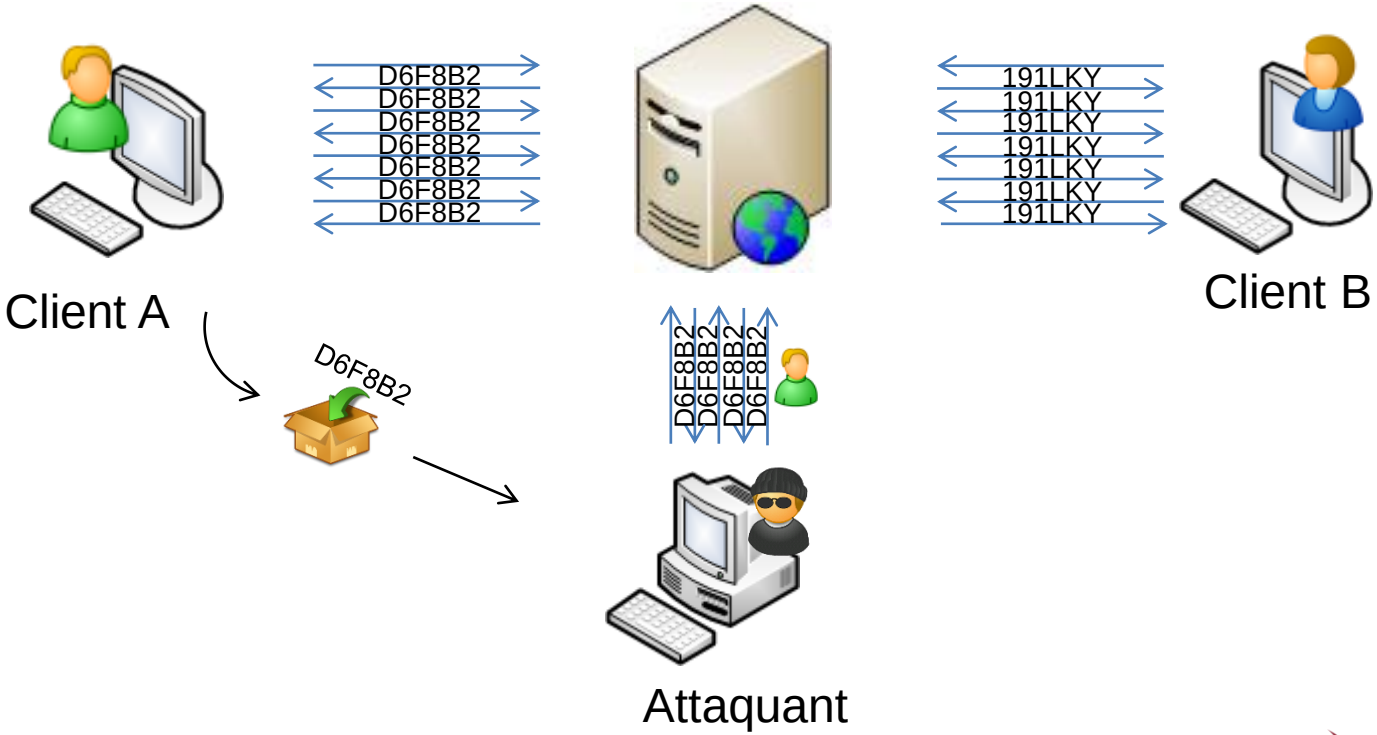


2. La sécurité des applications web

a. Usurpation d'identité via les cookies

Mais que se passe-t-il si un attaquant arrive à dérober le cookie d'un utilisateur et se connecte au même serveur ?

- Il se fait passer pour l'utilisateur dont il a dérobé le cookie au près du serveur applicatif ! Il usurpe donc l'identité de la victime et accède à son compte.



2. La sécurité des applications web

a. Usurpation d'identité via les cookies

L'attaquant peut dérober un cookie d'identification par différents moyens :

– soit en écoutant le trafic **réseau HTTP** et en interceptant les données applicatives, dont le cookie ;
  - Moyen de protection : l'utilisateur doit **s'assurer que le site auquel il est connecté utilise du HTTPS** (le cookie est donc chiffré pendant le transport).

– soit en dérobant le cookie sur le poste de travail en utilisant une vulnérabilité du système ;
  - Moyen de protection : l'utilisateur doit **sécuriser son système d'exploitation et ses logiciels** correctement (services inutiles désactivés, installation des mises à jours de sécurité, anti-virus, etc. voir le module 2 pour plus d'informations).

– soit en dérobant le cookie sur le poste de travail via des méthodes d'ingénierie sociale ciblées sur l'utilisateur ;
  - Moyen de protection : l'utilisateur doit **être sensibilisé aux méthodes d'ingénierie sociale** (phishing, spam, etc.) afin de « ne pas tomber dans le panneau »

– soit en dérobant le cookie via une faille sur le serveur ;
  - Moyen de protection : l'exploitant du serveur doit **suivre les bonnes pratiques de sécurisation et du maintien en condition de sécurité** du serveur, ainsi que les **bonnes pratiques de développement applicatif**.