IAE LIMOGES
École Universitaire de Management

Master CCA 2nde année

«*Remember when, on the Internet, nobody knew who you were?*»

Sécurité et Cryptographie — P-F. Bonnefoi

Version du 9 janvier 2023

Table des matières

Introduction

Depuis l'Egypte ancienne, l'homme a voulu pouvoir échanger des informations de facon **confidentielle**.
En grec :
Cryptographie : (κρυπτο – γραφην) écriture cachée / brouillée.

Il existe de nombreux domaines où ce besoin est vital :

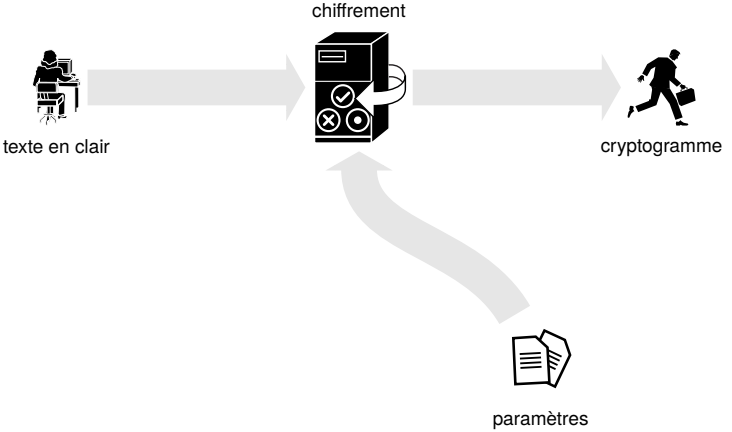
- ▷ **militaire** (sur un champ de bataille ou bien pour protéger l'accès à l'arme atomique) ;
- ▷ **commercial** (protection de secrets industriels) ;
- ▷ **bancaire** (protection des informations liées à une transaction financière) ;
- ▷ **vie privée** (protection des relations entre les personnes) ;
- ▷ **diplomatique** (le fameux «*téléphone rouge*» entre États-Unis et Union soviétique) ;
- ▷ ...

Définitions

Pour assurer la protection des accès à une information, on utilise des techniques de **chiffrement**.
Ces techniques s'appliquent à des **messages** lisibles appelés également «texte en clair».

Le fait de «*cacher*» un message de telle facon à le rendre secret s'appelle **chiffrement**.
La méthode inverse, consistant à retrouver le message original, est appelé **déchiffrement**.

Les messages à chiffrer, appelés «*texte en clair*», sont transformés grâce à une **méthode de chiffrement paramétrable**.
Si la méthode est connue de tous, ce sont les **paramètres** qui constituent la protection : ils servent à chiffrer/déchiffrer le message.



Ce **cryptogramme** est ensuite envoyé à son destinataire.

On appelle **cryptanalyse** les techniques employées pour déchiffrer un cryptogramme, **sans connaître** la méthode et/ou ses paramètres.

Le chiffrement est aussi appelé **cryptographie**.

L'ensemble des techniques de cryptographie et de cryptanalyse est appelé **cryptologie**.

3. 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)

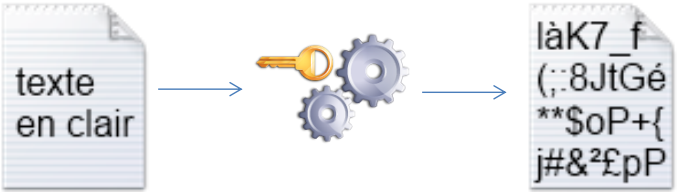
Objectif : fournir un moyen de preuve garantissant la véritable identité des entités ainsi que l'imputation de leurs actions.

3. Les bases de la cryptographie

a. Vocabulaire

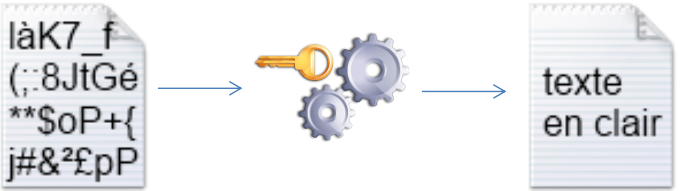
Chiffrer

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.

La stéganographie ou l'art de la dissimulation

En grec :
Stéganographie : (στεγανο – γραφην) écriture couverte/dissimulée.
Connaissance de l'existence de l'information $\Longrightarrow$ Connaissance de l'information
Cette méthode consiste à **dissimuler l'information à chiffrer** dans une autre information. On appelle cette méthode la «*stéganographie*».
Exemple : utiliser un bit tous les 8 bits dans une image (un bit de poids faible de préférence). L'image est faiblement modifiée et rien ne permet de savoir qu'elle contient un message caché.

Cette méthode peut être utilisé en plus de techniques de **cryptographie avancée** et permet d'en dissimuler l'usage.

Elles peut être utilisée de différentes manières :

- en **associant un groupe de lettres** à un caractère et en composant un texte qui ait un sens pour groupes de lettres, par exemple dans un compte rendu de partie d'échec où chaque coup joué correspond à une lettre du message secret et donne l'illusion d'une partie «*normale*» ;
- le **filigrane** ou «*watermarking*» pour dissimuler une information dans un document pour en permettre l'identification (protection des droits d'auteur) ;
- le **canal de communication caché** ou «*cover channel*» qui permet de diposer d'un véritable canal de communication en détournant l'usage de canaux de communications anodins. Cette technique permet de déjouer l'usage de firewall.
- ...

Exemple : ralentir artificiellement un transfert ftp ou au contraire l'accélérer pour coder un bit à 1 ou à 0, et pouvoir transmettre à un observateur le message qu'il construit.

La **cryptanalyse** reste **difficile** et doit s'appliquer à de **gros volumes** de données à **l'aveugle**.

Un peu d’Histoire...

Au début, il y eut les caractères et l'alphabet...

Historiquement, l'utilisation **d'alphabet** a permis de **coder** chaque mot du langage à partir de mêmes symboles à la différence des **idéogrammes chinois** par exemple.
L'ajout d'un **ordre** sur ces lettres à permis de définir les premières méthodes «*mathématiques*» de chiffrement d'un message constitué de lettres (code César, ROT13…).

Et des méthodes de chiffrement adaptées…

Ces chiffrements partent d'un message contenant des lettres vers un cryptogramme contenant également des lettres.
Ces méthodes se décomposent en deux grandes familles de chiffrement :

- par substitution ;
- par transposition.

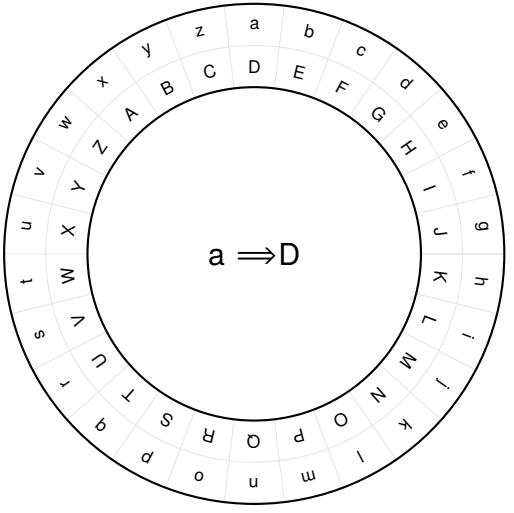
D'autres formes de chiffrement ?

Il existe également d'autres formes comme le **code morse** ou bien les **sémaphores** dans la Marine.
Ce sont des techniques de brouillage.

Chiffrement de César

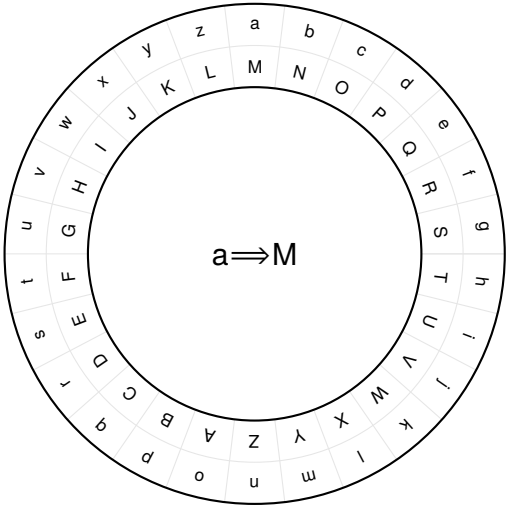
Le texte en clair : «*le petit chaperon se promenait dans la foret*»

chiffrement avec un décalage de 3 :



donne : «*OHSHW LWFKD SHURQ VHSUR PHQDL WGDQV ODIRU HW*»

chiffrement avec un décalage de 12 :



donne : «*XQBQF UFOTM BQDAZ EQBDA YQZMU FPMZE XMRAD QF*»

Et si on veut «*casser*» le chiffrement ?

Cryptanalyse du chiffrement par substitution

Dans le cas de l'utilisation d'un code par substitution, la cryptanalyse ou déchiffrement se fait par l'utilisation de données statistiques :

En anglais :

- les caractères les plus fréquemment utilisés sont : e, t, o, a, n, i…
- les combinaisons de deux lettres (digrammes) les plus fréquentes sont : th, in, er, re, et an.
- les combinaisons de trois lettres (trigrammes) : the, ing, and et ion.

Méthode empirique de cryptanalyse

Il suffit pour retrouver le texte en clair de :

- de rechercher les **caractères**, **digrammes** et **trigrammes** les plus fréquents du texte chiffré ;
- de faire des **suppositions** en les associants à ceux les plus fréquents d'un texte en clair (dans la langue choisi).

Par exemple dans un texte chiffré appartenant à une banque il est probable de trouver des mots tel que financier, montant, solde…

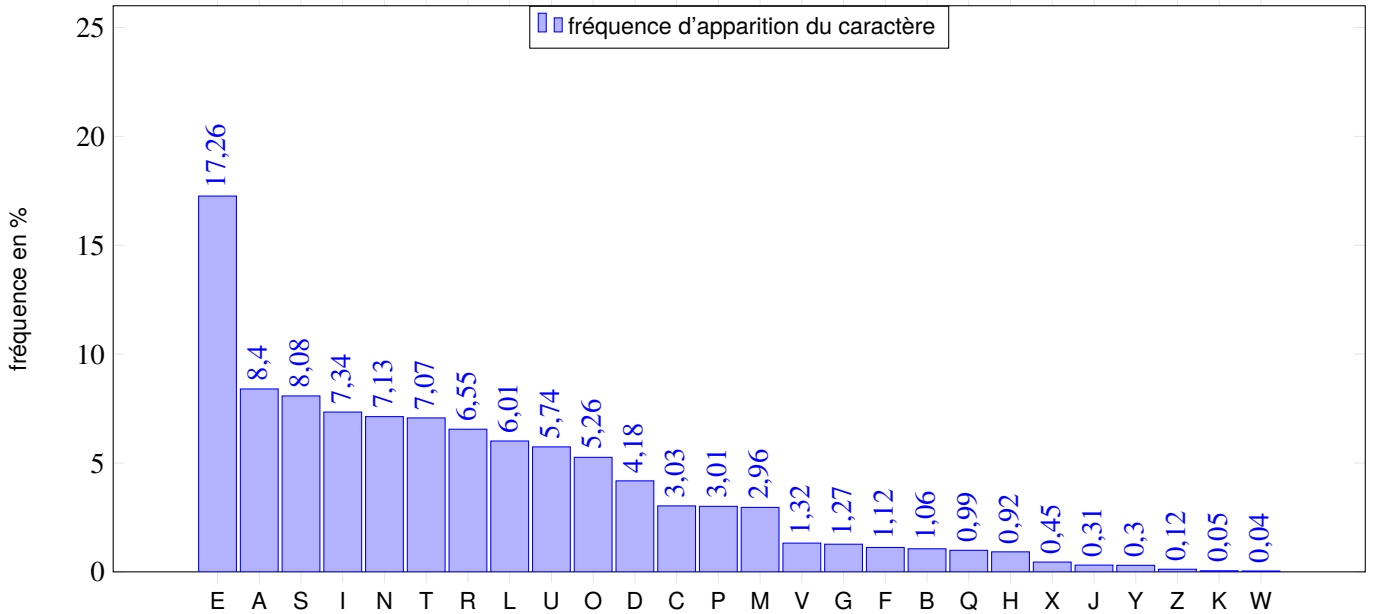
Comment finir la cryptanalyse ?

Si certains mots commencent à émerger du texte chiffré, alors il y a de **fortes probabilités** que le code de chiffrement soit découvert.

Un code par substitution **ne modifie pas** les **propriétés statistiques** des caractères, digrammes et trigrammes substitués.

Il conserve **l'ordre des caractères** du texte en clair, mais masque ces caractères.

Fréquence d'apparition des caractères, bigrammes et trigrammes en français



Les séquences de deux lettres triées suivant les plus fréquentes

Bigrammes	ES	DE	LE	EN	RE	NT	ON	ER	TE	EL	AN	SE	ET	LA	AI	IT	ME	OU	EM	IE
Nombres	3318	2409	2366	2121	1885	1694	1646	1514	1484	1382	1378	1377	1307	1270	1255	1243	1099	1086	1056	1030

Les séquences de trois lettres triées suivant les plus fréquentes

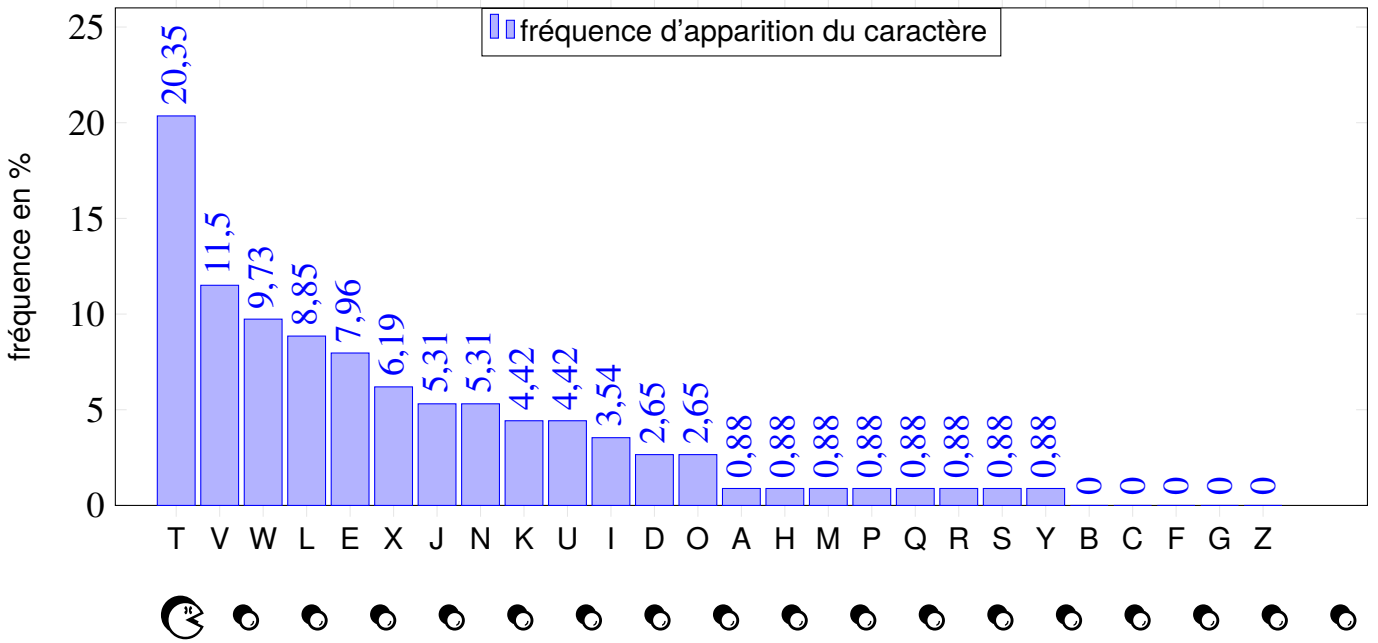
Trigrammes	ENT	LES	EDE	DES	QUE	AIT	LLE	SDE	ION	EME	ELA	RES	MEN	ESE	DEL	ANT	TIO	PAR	ESD	TDE
Nombres	900	801	630	609	607	542	509	508	477	472	437	432	425	416	404	397	383	360	351	350

Cryptanalyse de la substitution mono alphabétique

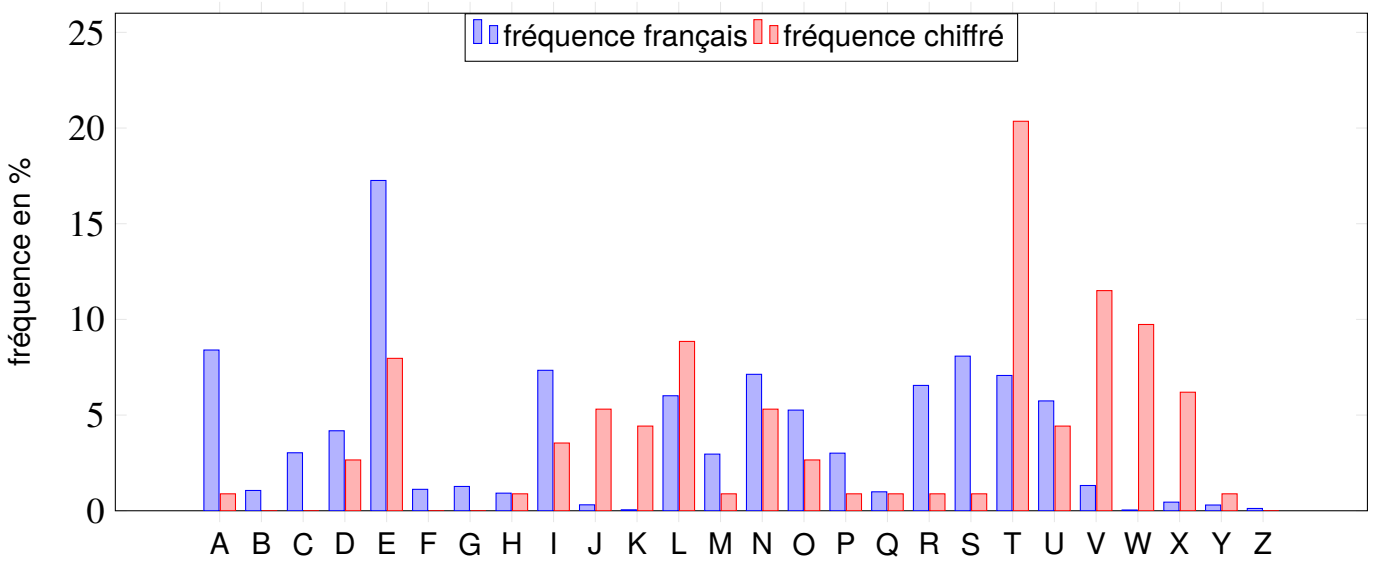
Teste chiffré

JTVMNKKTVLDEVVTLWTWITKTXUTLWJ
ERUTVTWTHDXATLIUNEWV.
JTVIEVWELOWENLVVNOEDJTVLTPTXYT
LWTWUTSNLITTVQXTVXUJXWEJEWTON
KKXLT.

Les fréquences calculées sur le texte chiffré



Comparaison des fréquences entre chiffré et clair



Début du déchiffrement

On associe les caractères qui ont la fréquence la plus élevées : T $\Longrightarrow$ e

```
JeVMNKKeVLDEVVeLWeWIeKeXUeLWJERUeVeWeHDXAeLIUNEWVJeVIEVWELOW
ENLVVNOEDJeVLePeXYeLWeWUeSNLIeeVQXeVXUJXWEJEWeONKKXLe
```

```
JeVMNKKeVLDEVVeLWeWIeKeXUeLWJERUeVeWeHDXAeLIUNEWVJeVIEVWELOW
 ENLVVNOEDJeVLePeXYeLWeWUeSNLIeeVQXeVXUJXWEJEWeONKKXLe
```

D'après la table étendue des fréquences de bigrammes, on trouve que les bigramme les plus fréquent, où les lettres sont les mêmes, sont :

- ▷ `ee` : la lettre «e» étant déjà affectée, on ne l'utilisera pas ;
- ▷ `ss` : on va associer V $\Longrightarrow$ s ;
- ▷ `ll` : on pourra tester cette association plus tard.

```
JesMNKKesLDEsseLWeWIeKeXUeLWJERUeseWeHDXAeLIUNEWsJesIEsWELOW
ENLssNOEDJesLePeXYeLWeWUeSNLIeesQXesXUJXWEJEWeONKKXLe
```

Puis avec l'association W $\Longrightarrow$ t :

```
JesMNKKesLDEsseLtetIeKeXUeLtJERUeseteHDXAeLIUNEtsJesIEstELOt
ENLssNOEDJesLePeXYeLtetUeSNLIeesQXesXUJXtEJEteONKKXLe
```

```
JesMNKKesLDEsseLtetIeKeXUeLtJERUeseteHDXAeLIUNEtsJesIEstELOt
 ENLssNOEDJesLePeXYeLtetUeSNLIeesQXesXUJXtEJEteONKKXLe
```

Le trigramme le plus fréquent commençant par «e» et finissant par «t» est «ent», d'où L $\Longrightarrow$ «n» :

```
JesMNKKesnDEssentetIeKeXUentJERUeseteHDXAenIUNEtsJesIEstEnOt
ENnssNOEDJesnePeXYentetUeSNnIeesQXesXUJXtEJEteONKKXne
```

Suite du déchiffrement

```
lesMNmmesnDEssentetIemeurentlERreseteHDuxenIrNEtslesIEstEnOt
ENnssNOEDlesnePeuventetreSNnIeesQuesurlutElEteONmmune
```

Les associations utilisées

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
x	y	z							l	m	n								e	r	s	t	u	v	w

Fin du déchiffrement

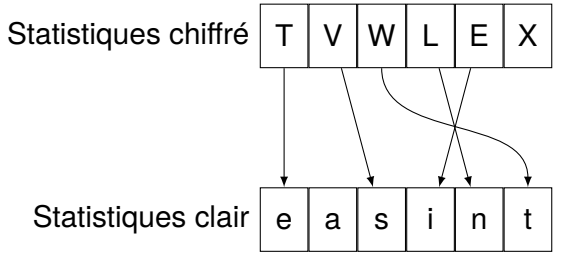
```
leshommesnaissentetdemeurentlibresetegauxendroitslesdistinct
ionssocialesnepeuventetrefondeesquesurlutilitecommune
```

Les associations utilisées

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
x	y	z	a	i	j		g	d	l	m	n	h	o	c	p	q	b	f	e	r	s	t	u	v	w

On remarquera que G⟹k même si ce caractère n'apparait pas dans le texte en clair.

Utilisation des fréquences les plus élevées pour le caractères, bigrammes et trigrammes



- VV ⟹ ss
- KK ⟹ mm
- TLW ⟹ ent

Utilisation d'un dictionnaire

Il est possible de tirer partie d'un **dictionnaire**, en regroupant les lettres en mots, puis en les recherchants dans le dictionnaire.

Dans tous les cas, la cryptanalyse reste un travail **exploratoire**, avec :

❶⇒la mise en place de nouvelles hypothèses ;

❷⇒la poursuite du processus de cryptanalyse ;

❸⇒le retour en arrière pour remettre en cause les dernières hypothèses ;

❹⇒le recommencement de cette méthode en ❶.

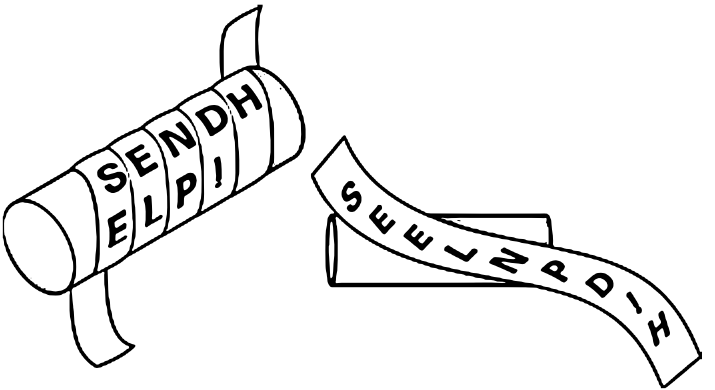
Autre forme de chiffrement

Toutes les lettres du message sont **présentes**, mais dans **un ordre différent**.

C'est un chiffrement de type **anagramme**.

Il utilise le principe mathématique des permutations (par colonne par exemple).

La scytale spartiate (5ème siècle avant notre ère) :



Texte en clair : `LA TRANSPOSITION PERMET EN THEORIE D'AVOIR UN HAUT DEGRE DE SECURITE`

L	R	S	S	I	P	M	E	H	R	D	O	U	A	D	R	E	C	I
A	A	P	I	O	E	E	N	E	I	A	I	N	U	E	E	S	U	T
T	N	O	T	N	R	T	T	O	E	V	R	H	T	G	D	E	R	E

Texte chiffré : `LRSSI PMEHR DOUAD RECIA APIOE ENEIA INUEE SUTTN OTNRT TOEVR HTGDE RE`

Les méthodes de chiffrement par transposition consistent à **réarranger** les données à chiffrer de telle façon à les rendre **incompréhensibles**.

En général : **réarranger géométriquement** les données pour les rendre **visuellement** inexploitables.

Par exemple : `Ceci est un texte à chiffrer de la plus haute importance`

Le texte est regroupé en tableau, suivant un nombre de colonnes donné.

C	e	c	i		e	s	t		u
n		t	e	x	t	e		à	
c	h	i	f	f	r	e	r		d
e		l	a		p	l	u	s	
h	a	u	t	e		i	m	p	o
r	t	a	n	c	e				

`Cncehre h atctiluaiefatn…`

Chaque colonne est ensuite copiée l'une après l'autre.

Cassable ?

Cryptanalyse

- Déterminer si une substitution n'a pas été utilisée : une analyse statistique des caractères suffit à déterminer si les caractères ont été substitués (statistiques fréquentielles du texte identiques à celle d'un texte en clair).
- Si ce n'est pas le cas, il y a une **forte probabilité** pour qu'un chiffrement par transposition ait été employé.
- Ensuite, il faut faire une **hypothèse** sur le **nombre de colonnes** utilisées pour réaliser la transposition.

*Les codes de transposition contrairement aux codes par substitution **ne cachent pas** les caractères, mais modifient l'ordre des caractères.*

Et l'ordinateur fut…

L'arrivée des ordinateurs a totalement démodé ces méthodes de chiffrement (*on ne parle plus d'ailleurs de chiffrement car ces méthodes ne résiste pas au traitement informatique*).

La machine **Enigma** utilisée par les nazis a été «*cassée*» par trois cryptographes polonais : Marian Rejewski, Jerzy Różycki et Henryk Zygalski, puis cette méthode a été améliorée par Alan Turing, pionnier de l'informatique.

Il faut attendre les annés 60 pour voir les méthodes de **chiffrement moderne** basées sur l'usage de **clés**.

Combiner Substitution et Transposition

il est possible de faire subir aux caractères du «texte en clair» :

- une substitution ;
- plusieurs opérations de transposition.

Changer les paramètres de ces combinaisons très souvent

l'utilisation des paramètres de chaque opération doit être réduite au chiffrement de quelques messages avant d'être changés pour de nouveaux paramètres.

Combiner les paramètres

Les opérations sont connues, la séquence d'application des opérations est définie par la séquence des paramètres de chaque opération.

La combinaison des différents paramètres des différentes opérations permet de définir un **secret**.

Ce secret permet de réaliser le déchiffrement et assure la sécurité du cryptogramme.
Il est appelé **clé de chiffrement**.

Le but

rendre l'apparence du cryptogramme la plus « aléatoire » possible, c-à-d **éliminer les relations statistiques** des caractères du cryptogramme pour éviter la cryptanalyse :
Transposition + Substitution = Diffusion

L'actualité ?

les chiffrements tels que DES «*Data Encryption System*» et AES «*Advanced Encryption System*» sont utilisés à l'heure actuelle.

Utilisation de la cryptographie moderne pour la sécurité

Ce type de chiffrement repose sur l'utilisation :

- d'un **algorithme public**, connu de tous ;
- d'une **clé**.

Il correspond à la cryptographie moderne, par rapport aux codes par substitution et transposition.

Auparavant, les algorithmes étaient simples mais utilisaient des **clés longues**.
Exemple : un XOR entre le message à transmettre et une clé de même taille suffit à le rendre indéchiffrable...technique du masque jetable
Maintenant, le but est d'utiliser des algorithmes sophistiqués et complexes associés à des **clés courtes**.

Ces algorithmes représente des **investissements à long terme**, c-à-d qu'ils sont employés pendant de nombreuses années jusqu'à ce qu'ils ne puissent plus assurer le même niveau de sécurité.

Il existe **deux sortes** de chiffrement :

- à **clé symétrique** ;
- à **clé asymétrique**.

Rappel de l'hypothèse de base de la cryptographie :
Principe de Kerckhoff – Auguste Kerckhoff, «La cryptographie militaire», février 1883

- *L'opposant connaît le système cryptographique*
- *Toute la sécurité d'un système cryptographique doit reposer sur la clé, et pas sur le système lui-même*

Chiffrement à clé symétrique

Principe

La même clé doit être employée pour chiffrer ou déchiffrer le message : on parle de clé symétrique ou secrète.

Le chiffrement consiste alors à appliquer un algorithme avec la clé secrète sur les données à chiffrer. Le déchiffrement se fait à l'aide de cette **même clé secrète**.

Remarques

La qualité d'un crypto système symétrique se mesure par rapport :

- à des propriétés statistiques des textes chiffrés ;
- à la résistance aux classes d'attaques connues.

En pratique

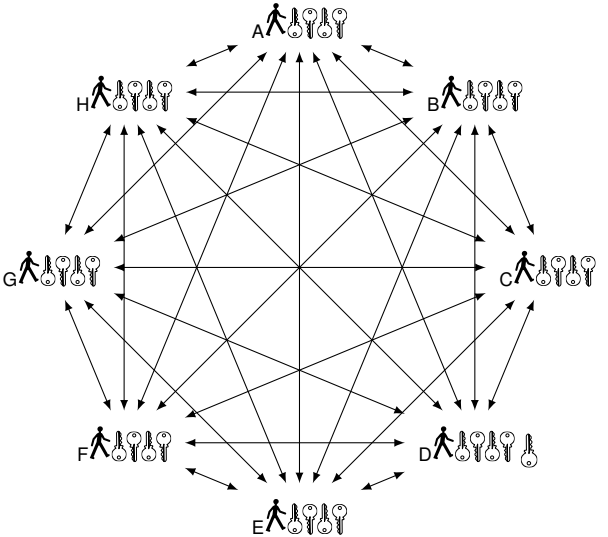
Tant qu'un crypto système symétrique n'a pas été cassé, il est bon, après il est mauvais !

Les limites du chiffrement symétrique

La multiplication des clés

Pour établir un canal de communication entre deux individus :

- Il faut qu'il soit chiffré avec une clé partagée entre les deux individus ;
- Il est ainsi confidentiel pour ceux qui ne possède pas la clé de chiffrement.



Pour que deux canaux de communications soient indépendants l'un de l'autre, c-à-d qu'une personne accède à l'un mais pas à l'autre, il faut que ces deux canaux utilisent des **clés différentes**.

Il est possible qu'un des interlocuteurs connaissent plusieurs clés utilisées dans différents canaux le reliant à des utilisateurs différents.

Exemple l'utilisateur D possède une clé pour chaque lien (avec H, G, F, E et C).

Problème comment échanger toutes ces clés ?

Pas d'intégrité et d'identification de l'auteur

Si Alice, Bob et Cédric partage le même lien de communication alors ils partagent la même clé de chiffrement symétrique.

Bob

clé secrète

Message

clé secrète

Cédric

Alice

clé secrète

Message
(modifié par Cédric)

❶ Bob chiffre le message à destination d'Alice

❷ Cédric intercepte le message, le modifie, et le chiffre à nouveau avec la clé secrète

Problème

Chacun peut intercepter et modifier les messages qui s'échangent.

Et l’asymétrique alors ?

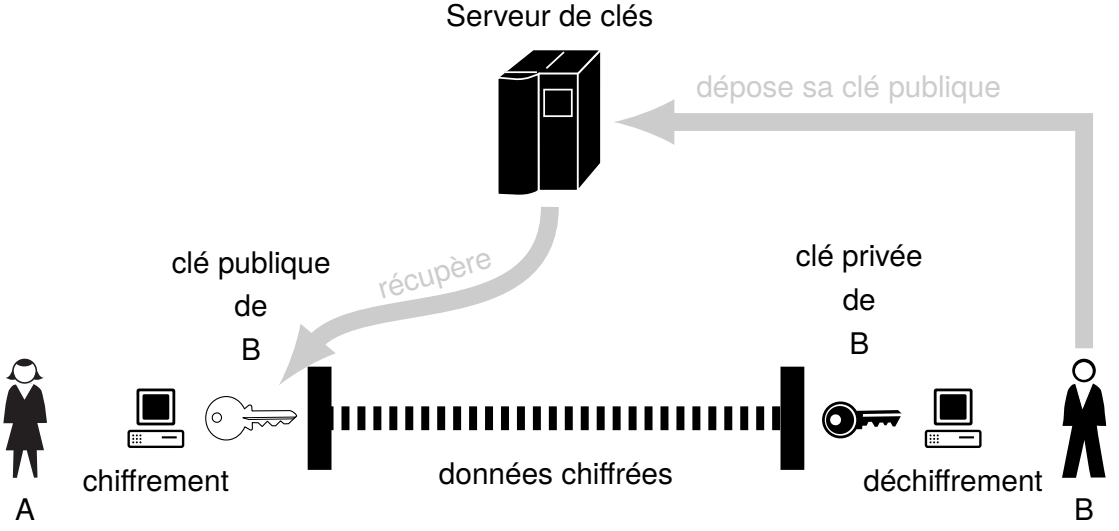
Chiffrement à clé asymétrique

Principe

Il utilise :

- une **clé publique** connue de tous ;
- une **clé privée** connue seulement du destinataire du cryptogramme.

*Ces chiffrements à «*clé publique*» ont été découverts par James Ellis (Angleterre) en 1969 et par Whitfield Diffie (Etats unis) en 1975.*



L'idée de la conception de tels algorithmes revient à Diffie et Hellman en 1976.

Échange par réseau

Un objectif de la cryptographie est de permettre à deux personnes, **Alice** et **Bob**, de communiquer au travers d'un canal peu sûr (téléphone, réseau informatique ou autre), sans qu'un opposant **Cédric**, puisse comprendre ce qui est échangé.

Scénario type

- Alice souhaite transmettre à Bob un ensemble de données (texte, nombres, …).
- Alice transforme ces informations par un **procédé de chiffrement** en utilisant la **clé publique** de Bob ;
- Alice envoi le texte chiffré au travers du canal de communication ;
- Cédric, *qui espionne peut-être le canal*, ne peut **reconstituer l'information**, contrairement à Bob qui dispose de la **clé privée** pour déchiffrer le cryptogramme.

Construction des clés

Les utilisateurs (A et B) choisissent une **clé aléatoire** dont ils sont seuls connaisseurs (il s'agit de la clé privée).

A partir de cette clé, ils **déduisent** chacun automatiquement par un algorithme la **clé publique**.

Les utilisateurs **s'échangent** cette clé publique au travers d'un canal **non sécurisé**.

Chiffrement d'un message

Lorsqu'un utilisateur désire **envoyer un message** à un autre utilisateur, il lui suffit de **chiffrer** le message à envoyer au moyen de la **clé publique** du destinataire (*qu'il trouvera par exemple dans un serveur de clés tel qu'un annuaire ou bien en signature d'un courrier électronique*).

Le destinataire sera en mesure de **déchiffrer** le message à l'aide de sa clé privée (**qu'il est seul à connaître**).

Rapports entre les clés

La recherche de la clé privée à partir de la clé publique revient à résoudre un **problème mathématique notoirement très compliqué**, c-à-d demandant un **grand nombre d'opérations** et beaucoup de mémoire pour effectuer les calculs $\Longrightarrow$ infaisable !

Par exemple dans RSA, l'algorithme le plus utilisé actuellement, la déduction de la clé privée à partir de la clé publique revient à résoudre un problème de factorisation de grand nombre que lequel travaille les mathématiciens depuis plus de 2000 ans !

Le choix des clés doit être fait de la manière la plus **imprédictible possible** : éviter les mots du dictionnaire, nombres **pseudo-aléatoires** à germe de génération difficile à deviner, *etc.*

Des clé et des cadenas

Alice :

▷ crée une **clé aléatoire** (la clé privée) ;

▷ puis fabrique un **grand nombre de cadenas** (clé publique) qu'elle met à disposition dans un casier accessible par tous (le casier joue le rôle de canal de communication non sécurisé).

Bob :

▷ prend un cadenas (ouvert) ;

▷ ferme une valise contenant le document qu'il souhaite envoyer à Alice ;

▷ envoi la valise à Alice, propriétaire de la clé publique (le cadenas).

Cette dernière pourra ouvrir le cadenas et la valise avec sa clé privée.

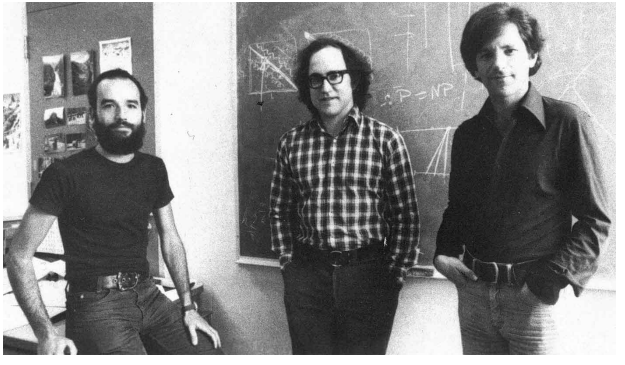
Les contraintes pour un tel algorithme

Il faut trouver un couple de fonctions f (fonction unidirectionnelle) et g (fonction de «*backdoor*») :
C'est un problème mathématique difficile !
Au départ, le système à clé publique n'a d'abord été qu'une idée dont la faisabilité restait à démontrer.

Des algorithmes ont été proposés par des mathématiciens

Un des premiers algorithmes proposé repose sur la **factorisation du produit de deux grands nombres entiers**.
Suivant la taille des nombres, cette factorisation peut demander un temps de calcul de plusieurs années : le problème est résolu !

Cet algorithme a été proposé par Rivest, Shamir et Adleman en 1977, ce qui a donné naissance à RSA.



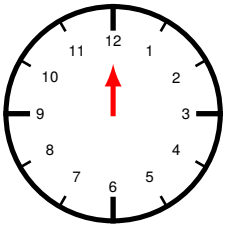
L'idée générale est la suivante :

- la fonction f est l'**exponentiation modulaire** ;
- la **clé publique** est la valeur c utilisée en combinaison avec le produit n de deux grands nombres entiers ;
- la **clé privée** est la valeur z ;
- g consiste en la **factorisation** de n.

Seul Bob, qui connaît z et g peut déchiffrer le message chiffré.

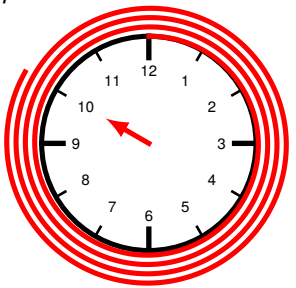
Les nombres modulaires : $x \bmod p$

Il est 0h ou 12h :



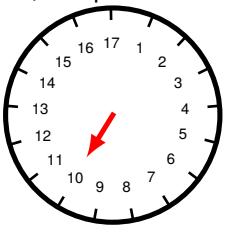
Et si on avance de 46h ?

on tourne de 46h autour du cadran...
On fait 3 tours : $3 * 12 = 36$
plus $46 - 36 = 10$ *h*



Ce qui fait $46 \bmod 12$? *10h !*

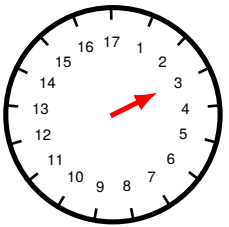
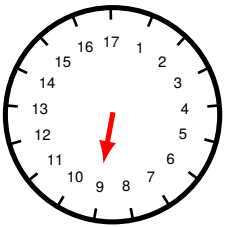
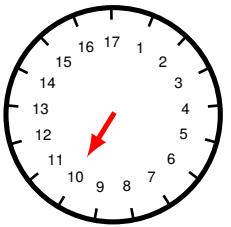
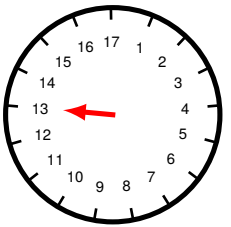
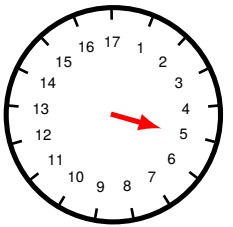
Et si on utilise un **nombre premier**, comme 17, à la place de 12 ?



et 3, la «*racine primitive*» modulo 17, c-à-d n'ayant pas de facteur en commun...

Les résultats de l'exponentiation modulaire :

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	...
$3^n \bmod 17$	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1	...

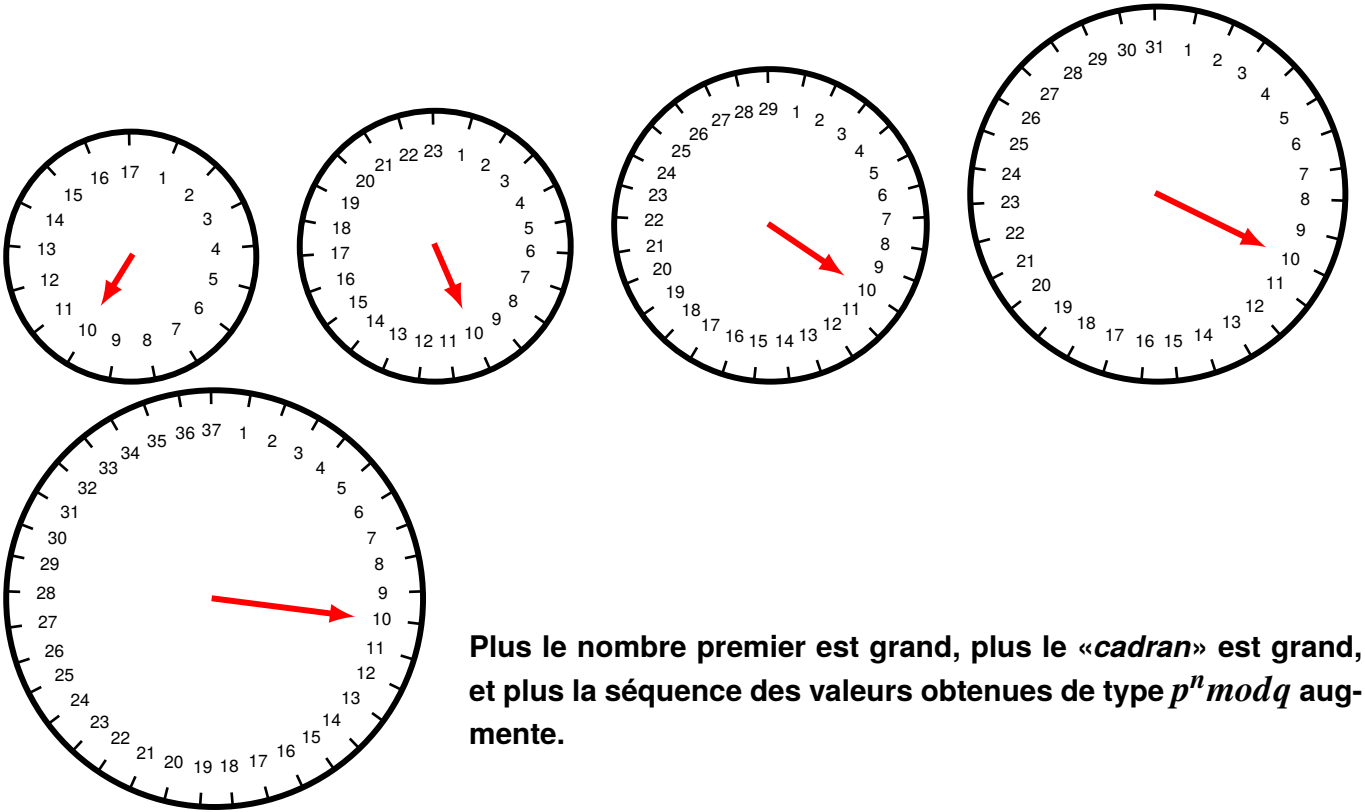






...

Les valeurs sont **également distribuées** autour du cadran...ce qui donne l'impression qu'elles sont **aléatoires**.
La **procédure inverse** qui permet de passer de 12, par exemple, à la valeur de x telle que : $3^x \bmod 17 = 12$ est **dure** !

$\Longrightarrow$ ***pourquoi ne pas s'en inspirer pour définir un crypto-système ?***

Pour différents nombres premiers : 17, 23, 29, 31, 37, ...

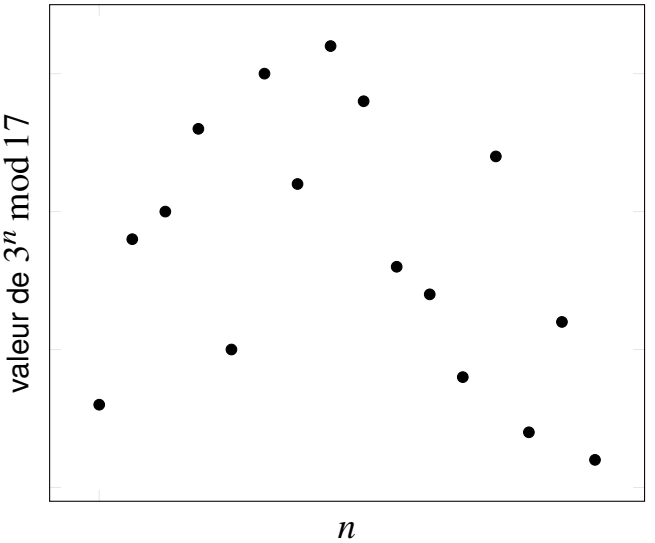


Plus le nombre premier est grand, plus le «*cadran*» est grand, et plus la séquence des valeurs obtenues de type $p^n \bmod q$ augmente.

On vérifie le «*caractère aléatoire*» des résultats de l'exponentiation modulaire :

On recommence

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	...
$3^n \bmod 17$	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1	3	9	10	...



▷ Pourquoi la **procédure inverse** qui permet de passer de 12, par exemple, à la valeur de x telle que : $3^x \bmod 17 = 12$ est-elle **dure** ?

⟹ parce-qu'il faut **essayer toutes les valeurs possibles** avant de trouver la bonne, ce qui peut prendre beaucoup de temps !

Crypto-système : recherche d'un problème difficile à résoudre

$3^{29} \bmod 17$ --- facile ---> 12

$3^{?} \bmod 17$ <--- difficile --- 12

Problème du «*logarithme discret*» :
$\Longrightarrow$ pour trouver l'exposant, il faut **essayer les différentes valeurs possibles** !

Est-ce trouvable en cherchant ?

Pour des valeurs petites, comme 17 oui... mais si on utlise des nombre plus grands comme :

```
41 699 392 957 415 060 122 123 251 743 926 118 047 280 755 942 727 859 562 221 144 422 770 879 634
528 234 687 327 545 978 537 253 643 190 435 384 223 451 790 600 743 186 710 706 948 084 596 275 495
353 648 241 532 947 688 879 507 515 517 193 627 711 579 879 475 350 089 816 821 087 217 733 022 854
019 999 144 696 637 566 134 923 661 835 848 181 145 153 671 156 026 923 341 312 533 527 164 598 580
084 075 991
```

ce nombre premier a été choisi sur 1024bits.

Il faut **beaucoup, beaucoup de temps** pour y arriver ! *Suivant la taille, plusieurs années avec des ordinateurs puissants !*

Et si on essaye d'aller plus loin ?

La fonction $\Phi(n)$ calcule le nombre d'entiers inférieur à n qui ne partagent pas de diviseur supérieur à 1 avec n.
Exemple : $\Phi(8) = 4$, *car* $\boxed{1}, 2, \boxed{3}, 4, \boxed{5}, 6, \boxed{7}$, *il y en a 4 ayant cette propriété.*

On peut arriver à :

- ▷ $\Phi(n) = n - 1$ si n est premier, sinon Φ(n) est **long à calculer** (il faut **énumérer** les différents entiers) ;
- ▷ $\Phi(a * b) = \Phi(a) * \Phi(b)$;
- ▷ si on choisit **deux nombres premiers** p_1 et p_2 et on calcule $n = p_1 * p_2$,
  on a $\Phi(n) = \Phi(p_1) * \Phi(p_2) = (p_1 - 1) * (p_2 - 1)$
- ▷ Théorème d'Euler : $m^{k*\Phi(n)+1} = m \bmod n$
  On essaye de trouver $e * d = k * \Phi(n) + 1$, soit $d = \frac{k*\Phi(n)+1}{e}$,
  $\Longrightarrow$ d'où notre **cryptosystème** : $\boxed{\text{message}^e \bmod n = \text{chiffré}}$ et $\boxed{\text{chiffré}^d \bmod n = \text{message}}$

Chiffrement

Alice prépare ses valeurs :

$p_1 = 53$

$p_2 = 59$

$n = 53 * 59 = 3127$ (le module)

$\Phi(n) = 52 * 58 = 3016$

$e = 3$

$d = \frac{2*(3016)+1}{3} = 2011$

Alice **partage** avec Bob :

$n = 3127$

$e = 3$ *clé publique*

et conserve **secrétement** :

$n = 3127$

$d = 2011$ *clé privée*

Bob **veut envoyer un message** à Alice :

$m = 89$ où 89 correspond à une lettre de l'alphabet par exemple ;

Il calcule :

$m^e \bmod n \Longrightarrow 89^3 \bmod 3127 = 1394$

et transmets à Alice la valeur $m' = 1394$

Déchiffrement

Alice reçoit $m' = 1394$.

Elle calcule :

$1394^{2011} \bmod 3127 = 89$

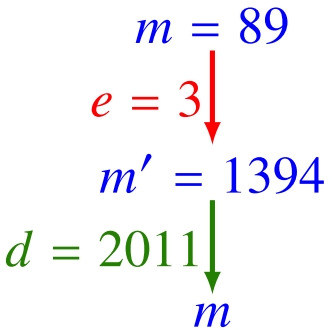
et retrouve le message m de Bob !

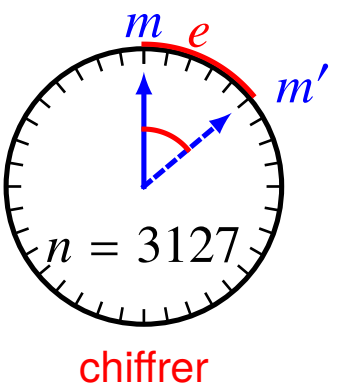
Un attaquant obtenant les valeurs

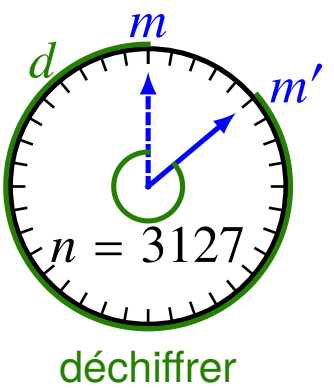
$n = 3127, 1394$ *et* $e = 3$

doit calculer $\Phi(3127)$ *pour trouver* d

Ce qui lui prendrait trop de temps pour n *très grand !*



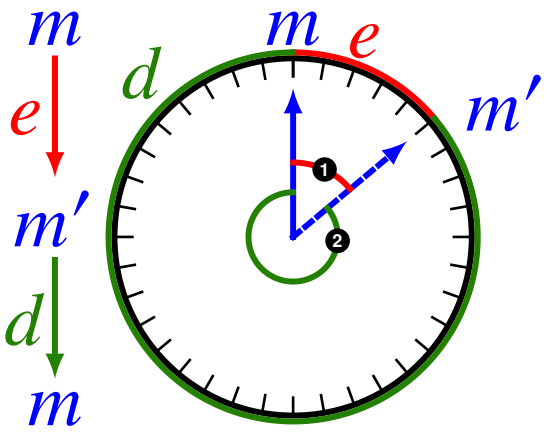


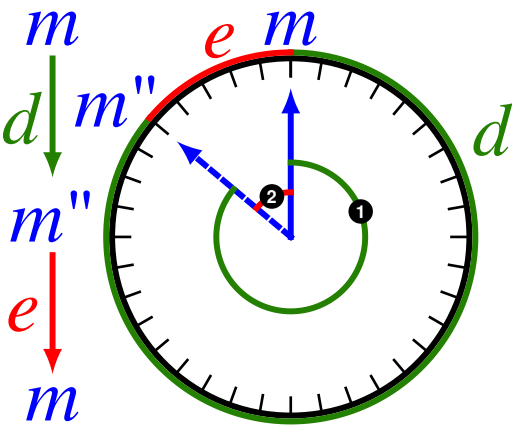


Chiffrement ? Déchiffrement ? Ce ne serait pas la même chose ?

On peut **permuter** l'usage de e et d...

$$(m^e)^d \bmod n = m^{e*d} \bmod n = m^{d*e} \bmod n = (m^d)^e = m$$





On peut créer un message m'' qui **peut être «(dé)chiffrer» avec la clé publique** (e et n) en le message original m mais qui ne peut être **créer qu'avec la clé privée** (d et n) !

$\Longrightarrow$ Seule la personne **ayant la clé privée** peut chiffrer un message choisi **déchiffrable par la clé publique** associée...

$\Longrightarrow$ On peut **authentifier** la personne ! C-à-d **garantir son identité**, car elle est la **seule à posséder** cette clé privée !

3. Les bases de la cryptographie

e. Chiffrement symétrique vs Chiffrement asymétrique

Chiffrement symétrique	Chiffrement asymétrique
Avantages	
• Rapidité des opérations (adapté à du trafic en temps réel) ; • Clés courtes (256 bits suffisent actuellement) ;	• 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 2015)	
• AES.	• RSA.

Un dernier problème pour la route…

Le système de chiffrement à clé publique est universel si **chacun publie sa clé publique** dans un annuaire.
Pour envoyer un message chiffré à Bob, il suffit de trouver **sa clé publique** dans l'annuaire et de s'en servir pour **chiffrer le message** avant de le lui envoyer (seul Bob pourra déchiffrer le message).
Il faut bien sûr que **l'annuaire** soit **sûr**.

Oscar peut avoir substitué sa propre clé publique à celle de Bob afin de pouvoir lire les messages destinés à Bob.

Il peut même les renvoyer à Bob une fois lu !

Ce qui empêche Bob de s'en rendre compte et de changer sa bi-clé, et d'en informer Alice.

Propriété unique de RSA

L'algorithme a la propriété spéciale suivante :

$$\text{chiffrement}(\text{déchiffrement}(M)) = \text{déchiffrement}(\text{chiffrement}(M))$$

C'est-à-dire que l'utilisation de sa **clé privée** pour chiffrer un message M permet de construire un message M' qui peut être déchiffré par sa **clé publique**...ainsi il est **possible de prouver** que l'on dispose de la **clé privée associée à la clé publique** !

Application à l'authentification

En effet, la clé privée est **connue uniquement de son propriétaire**. Avec cette clé je peux chiffrer n'importe quel message que l'on me propose...

...et le message chiffré peut être **déchiffré par tout le monde** grâce à la clé publique ! Si je possède la clé privée **associée** à la clé publique $\Longrightarrow$ je suis la personne **associée** à cette clé publique !

Notion de «*Challenge*/*Response*»

Si Alice veut authentifier Bob (s'assurer que Bob est bien Bob) :

a. elle demande à Bob de lui chiffrer un message (n'importe lequel, si possible un **nouveau à chaque fois**) ;

b. Bob utilise sa **clé privée** pour le faire et renvoie le message chiffré à Alice ;

c. Alice vérifie qu'elle retrouve bien son message en déchiffrant le message chiffré reçu avec la **clé publique de Bob** : si c'est le même message, c'est Bob !

C'est de «**l'authentification vivante**» !

Chiffrement symétrique ou asymétrique ?

Comparaisons entre RSA et DES

RSA

- ⋆ clé de 1024 bits
- ⋆ chiffrement matériel : 300 Kbits/sec
- ⋆ chiffrement logiciel : 21,6 Kbits/sec
- ⋆ *Inconvénient majeur* : un pirate substitue sa propre clé publique à celle du destinataire, il peut alors intercepter et décrypter le message pour le recoder ensuite avec la vraie clé publique et le renvoyer sur le réseau.
  «L'attaque» ne sera pas décelée.
- ⋆ *Usage* : chiffrer des données courtes (de quelques octets) telles que les clés secrètes et les signatures électroniques.

facteur 1000 !

DES

- ◦ clé de 56 bits
- ◦ chiffrement matériel : 300 Mbits/sec
- ◦ chiffrement logiciel : 2,1 Mbits/sec
- ◦ *Inconvénient majeur* : attaque «*brute force*» rendue possible par la puissance des machines.
- ◦ *Usage* : chiffrement rapide, adapté aux échanges de données de tous les protocoles de communication sécurisés.

Vitesse de chiffrement

- □ il existe un **décalage de puissance de calcul** nécessaire pour le chiffrement/déchiffrement à clé secrète par rapport à celui à clé publique ;
- □ le chiffrement à clé secrète est utilisable pour un débit de données supérieur («réaliste» pour sécuriser une transaction entre deux utilisateurs sur Internet).

Résolution du problème de l'échange des clés secrètes

- ▷ utilisation d'une méthode **hybride** combinant à la fois chiffrement symétrique et asymétrique.

Le chiffrement symétrique

est

beaucoup plus rapide

que

le chiffrement asymétrique...

Combinaison symétrique/asymétrique

L'utilisation d'algorithme de chiffrement à clé **asymétrique** : il est coûteux en puissance de calcul nécessaire à le mettre en œuvre.

La **puissance de calcul** des ordinateurs augmente ?

$\Longrightarrow$ il est nécessaire d'améliorer la sécurité des algorithmes symétriques et asymétriques pour résister à la cryptanalyse ;

– Comment ? **augmenter la taille** des clé par exemple ;

Conséquence :

▷ le **décalage** entre besoin de calcul entre symétrique et asymétrique **reste** !

Une solution : la combinaison

Il faut trouver un moyen de **partager secrètement** une même clé secrète :
l'échange de la clé secrète d'un algorithme de chiffrement symétrique est «protégé» par un algorithme de chiffrement asymétrique.

Cette clé partagée sera appelée **clé de session**.

C'est un **compromis** entre le chiffrement symétrique et asymétrique permettant de combiner les deux techniques.

Il existe deux méthodes pour construire et partager une clé de session :

▷ **Première** possibilité :
- ◇ construire une **clé de session** à l'aide de la méthode d'échange de clé de **Diffie-Hellman**.
- ◇ les interlocuteurs n'ont **pas besoin de partager une clé** avant de commencer leur communication chiffrée ! *Cette méthode est extrémement employée pour initier un canal de transmission sécurisée avant tout échange.*

▷ **Seconde** possibilité :

a. générer **aléatoirement** une clé de **taille raisonnable** utilisée pour un algorithme de chiffrement symétrique ;

b. **chiffrer** cette clé à l'aide d'un algorithme de **chiffrement à clé publique**, à l'aide de la clé publique du destinataire ;

c. envoyer cette clé chiffrée au destinataire ;

d. le destinataire déchiffre la clé symétrique à l'aide de sa clé privée.

Les deux interlocuteurs disposent ensuite :

□ d'une **clé symétrique commune** qu'ils sont seuls à connaître ;

□ et donc, de la possibilité de **communiquer en chiffrant** leur données à l'aide d'un algorithme de chiffrement symétrique rapide.

*Cela impose que l'un des interlocuteurs **possède la clé publique** de l'autre (pas toujours facile de s'assurer que la clé publique appartient bien à la bonne personne).*

Avantages

- la clé secrète est chiffrée et échangée : pas d'interception possible ;
- elle est changée à chaque communication : sécurité plus robuste dans le temps ;
- après l'échange on bascule le chiffrement en utilisant un **algorithme symétrique** plus rapide ;
- on démarre l'échange avec l'utilisation d'un algorithme asymétrique qui possède l'avantage d'offrir un moyen **d'authentifier** les interlocuteurs.

Remarque

Cela **impose** que l'un des interlocuteurs possède la **clé publique de l'autre** (pas toujours facile de s'assurer que la clé publique appartient bien à la bonne personne).

Attention

La PFS, «*Perfect Forward Secrecy*», correspond à la protection des échanges futurs en cas de **compromission** de la **clé privée du serveur** :

- ▷ si la clé de session est échangée **chiffrée par la clé publique du serveur**
  ⟹les transactions antérieures sont déchiffrables ;
- ▷ si la clé de session est déterminée par DH : la compromission de la clé publique **ne permet pas de déchiffrer** les transactions !

Seule la première possibilité avec Difie-Hellman garantie la PFS...

Et Comment Améliorer la Sécurité
si la puissance des ordinateurs
augmente constamment ?

La sécurité offerte par le chiffrement à clé

La sécurité d'un code à clé est **proportionnelle** à la taille de la clé employée, c-à-d **plus la clé est longue plus il faut de calcul et donc de temps pour arriver à le casser**.

Attaque «*brute force*» :

▷ **essayer toutes les clés possibles** pour déchiffrer le message chiffré ;

⟹ plus la clé est **longue** (nombre de bits), **plus il y a de clés à essayer** (2 fois plus de clé à essayer pour chaque bit ajouté !).

Remarque : *pour un **niveau de sécurité équivalent**, la taille des clés est souvent **plus petite** en chiffrement symétrique qu'en chiffrement asymétrique.*
128bits en AES contre 2048bits par exemple en RSA.

Mais, le **niveau de sécurité** est à mettre en **rapport** avec le type de données à sécuriser :

▷ une **transaction bancaire** doit être sécurisée pendant quelques minutes ;

▷ un **document secret d'état** doit pouvoir être protégé plus de 50 ans par exemple.

Le chiffrement d'une communication

ne

permet pas l'authentification...

L'authentification est suivie par l'autorisation

L'autorisation définit les ressources, services et informations que la personne identifiée peut utiliser, consulter ou mettre à jour, exemple : son courrier électronique, des fichiers sur un serveur FTP…

L'approche traditionnelle

Combinaison d'une identification et d'un mot de passe (code secret personnel).
Le mot de passe doit posséder certaines caractéristiques : non trivial, difficile à deviner, régulièrement modifié, secret…
Des outils logiciel ou hardware de génération de mots de passe existent, mais les mots de passe générés sont difficiles à retenir !

L'approche évoluée, la notion de challenge/réponse

Authentification avec du chiffrement asymétrique :

- ▷ Alice envoie à Bob un **message aléatoire** «*challenge*» :
- ▷ Bob renvoie à Alice le **message chiffré à l'aide de sa clé privée** «*réponse*» ;
  exploitation de la propriété chiffrement(*déchiffrement*(M)) = *déchiffrement*(*chiffrement*(M)) ;
- ▷ Alice peut **déchiffrer** ce message chiffré à l'aide de la **clé publique de Bob**… $\Longrightarrow$ c'est Bob !

Si on utilise du chiffrement asymétrique
peut-on faire à la fois de
l'authentification et de l'échange sécurisé ?

Authentification à l'aide du chiffrement à clé publique et échange de clé de session

On suppose que chaque interlocuteur possède **la clé publique** de l'autre. *Ce qui n'est pas évident…*
On désire échanger une clé de session tout en s'assurant de l'identité de chacun.

Scénario : Alice veut échanger avec Bob

1. Alice chiffre avec la **clé publique de Bob** son **identité** et un **nombre aléatoire** N ;
   L'identité permet de sélectionner la clé publique d'«Alice»
2. Alice envoie ce message à Bob qui peut le déchiffrer et retrouver N
   Bob qui reçoit ce message ne sait pas s'il vient d'Alice ou bien d'Oscar (l'intrus)
3. Bob répond par un message chiffré avec la **clé publique d'Alice**, contenant : N, un nombre aléatoire P et S une clé de session ;
4. Alice reçoit le message et le déchiffre à l'aide de sa clé privée
   Si Alice trouve N alors c'est bien Bob qui lui a envoyé le message puisqu'il était le seul à pouvoir déchiffrer N, pas d'intrus qui peut s'insérer dans la communication.
   Ce n'est pas possible non plus que cette réponse soit un message déja échangé puisque N vient juste d'être choisi par Alice (protection contre le rejeu).
5. Alice valide la session en renvoyant à Bob le nombre P chiffré maintenant avec la clé de session S

L'échange est maintenant basculé en chiffrement à clé secrète avec la clé S…

Problème

Comment être sûr de disposer de la bonne clé publique ?
Il faut disposer d'un intermédiaire de confiance qui détient et distribue les clés publiques.

Ok pour les échanges sécurisés.

Mais pour un document, comment faire de l'authentification ?

L'authentification d'un document

L'authentification d'un document correspond à **identifier son propriétaire/créateur**.

Quelle sorte de chiffrement utiliser pour chiffrer le document ?

- **Chiffrement symétrique ?** Impossible. On peut vérifier la provenance d'un document que par la seule vérification que le document a été chiffré par une clé secrète que l'on connait.
  S'il faut connaître la clé secrète pour vérifier, il est impossible de démontrer la provenance d'un document sans donner cette clé secrète.
  Tous ceux qui veulent vérifier la doit posséder la clé secrète et tout le monde peut modifier le document !
  Le document est toujours chiffré, il ne peut être consulté librement !

- **Chiffrement asymétrique ?** Possible. On chiffre le document avec la clé privée de son propriétaire.
  Tout le monde peut vérifier avec la clé publique du propriétaire du document que ce document a été chiffré avec sa clé privée.
  Sa clé privée est...privée : c'est bien son document !
  *Si la clé privée a été utilisée, cela n'a pu être fait qu'avec l'accord du propriétaire : **non répudiation** !*
  Le document est chiffré mais peut être déchiffré par tous (en se procurant librement la bonne clé publique du propriétaire).
  *Cela revient à de la **signature** !*

Oui, mais le chiffrement asymétrique est lent !

Solution : il faut «compresser» le document avant de le signer (résumé ou «*digest*» en anglais)...
...et s'assurer que la «compression» du document est **bien associée** au bon document ;
...et qu'il n'est **pas facile** de trouver **un autre document** qui a la même «compression» qu'un autre (pour faire accepter un document et le remplacer par un autre).

Une **fonction de hachage** est une fonction permettant d'obtenir un **résumé** d'un texte, c-à-d une suite de caractères assez courte représentant le texte qu'il résume.

La fonction de hachage doit être :

- telle qu'elle associe **un et un seul résumé** à un texte en clair (cela signifie que la moindre modification du document entraine la modification de son résumé), c-à-d «sans collision».
- une fonction **à sens unique**, «*one-way function*», afin qu'il soit **impossible** de retrouver le message original à partir du résumé.

$y = H(x)$, mais il est impossible de retrouver x à partir de y !

Propriétés

une fonction de hachage H transforme une entrée de données d'une dimension variable m etdonne comme résultat une sortie de données inférieure et fixe h ($h = H(m)$).

- l'entrée peut être de dimension variable ;
- la sortie doit être de dimension fixe ;
- $H(m)$ doit être relativement facile à calculer ;
- $H(m)$ doit être une fonction à sens unique ;
- $H(m)$ doit être «sans collision».

Utilisation - Authentification et intégrité

Les algorithmes de hachage sont utilisés :

- pour la vérification si un document a été modifié (le changement d'une partie du document change son empreinte), on parle **d'intégrité** ;
- dans la génération des **signatures numériques**, dans ce cas, le résultat h est appelé «empreinte» en le combinant avec les propriétés des chiffrements asymétriques.

Qu'est-ce qu'une fonction de hachage ?

Une **fonction de hachage** est une fonction qui fait correspondre **à toute information** une valeur appelée «***hash***».

Exemple : pour accéder rapidement à un livre dans une base de données, on utilise une fonction de hachage pour accéder directement au livre recherché :

f : {*ensemble des titres de livres*} $\mapsto$ {*ensemble des hashs*}

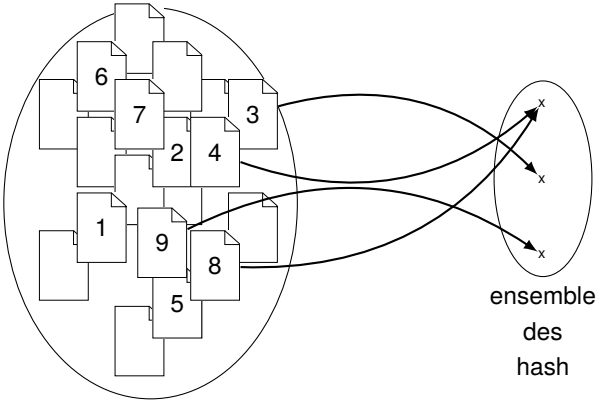
f(*20 000 Lieues sous les mers*) $\rightarrow 598$

f(*Les androïdes rêvent-ils de moutons électriques ?*) $\rightarrow 698593$

*Ainsi, on ne parcours pas tous les titres, mais on va **directement** à la valeur indiquée par la fonction de hachage.*

*Si deux livres possèdent le même hash, on parle de «**collision**». Une bonne fonction de hachage limite les collisions.*

Fonction de hachage cryptographique

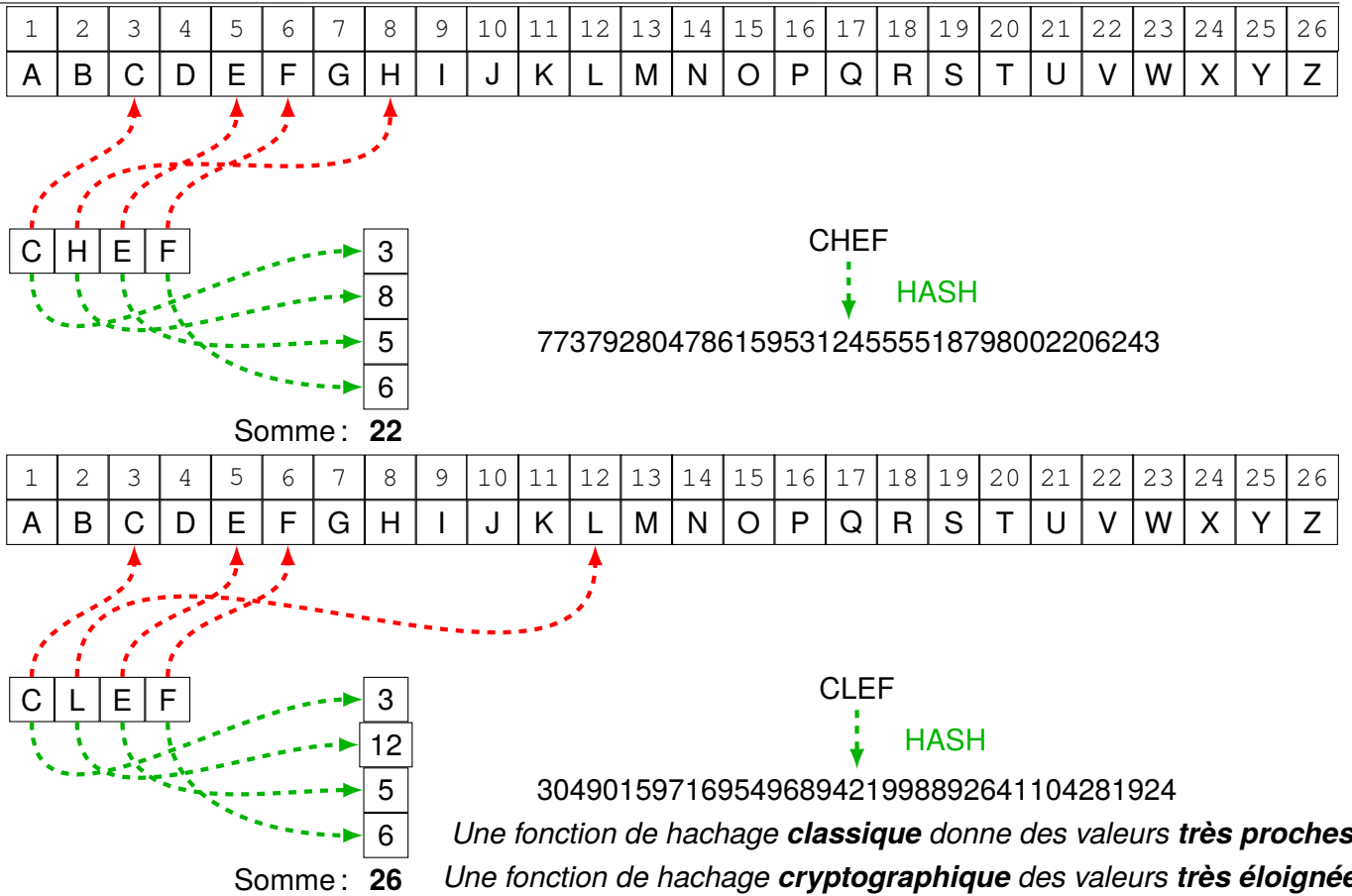


Une **fonction de hachage cryptographique** possède les propriétés suivantes :

- **pour tout document électronique** elle calcule un hash ;
- depuis le hash il est **impossible** de retrouver le document ;
- deux documents **proches** possédent des hashs **très différents** ;
- pour un **hash connu**, il est difficile, voire **impossible** de trouver le document permettant de l'obtenir ;
- il est très difficile, voire **impossible**, de trouver deux documents différents ayant le **même hash** (collision).
- le hash est de taille **fixe** et **limitée** (le document peut être de taille quelconque).

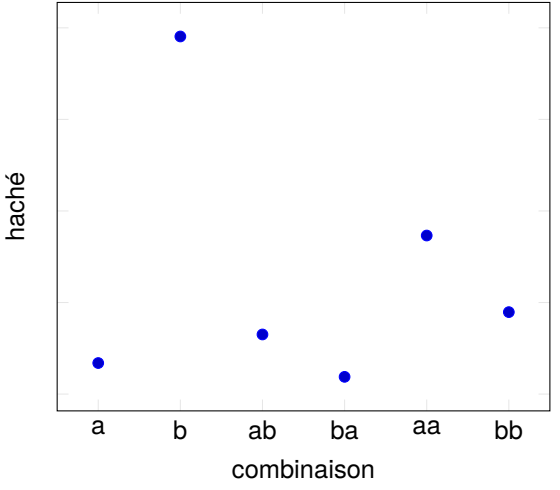
*On parle aussi **d'empreinte** de documents.*

Fonction de hachage cryptographique

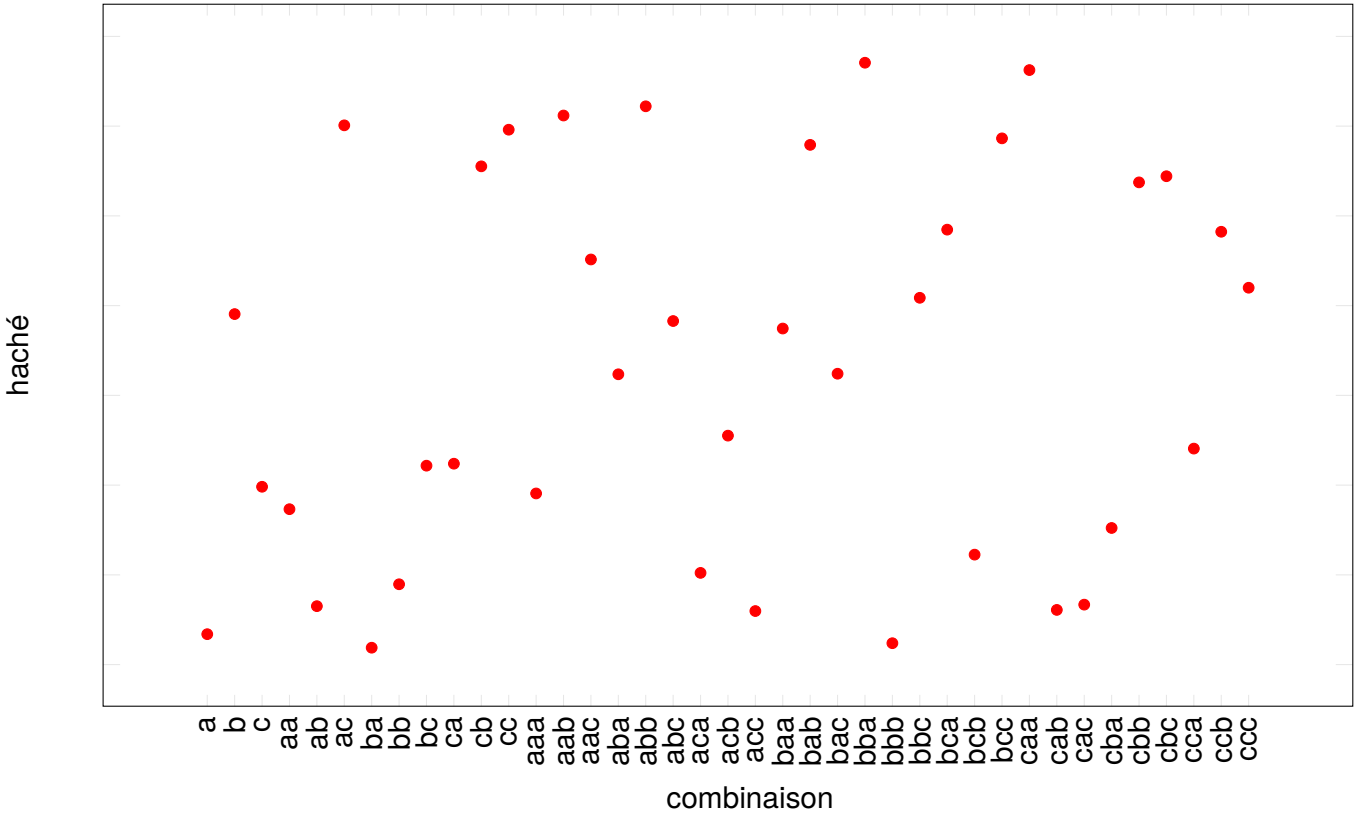


Imaginons que l'on veuille voir quelles sont les valeurs associées par la **fonction de hachage** aux différentes combinaisons possibles obtenues à partir des lettres«*a*» et «*b*», d'au plus 2 lettres :

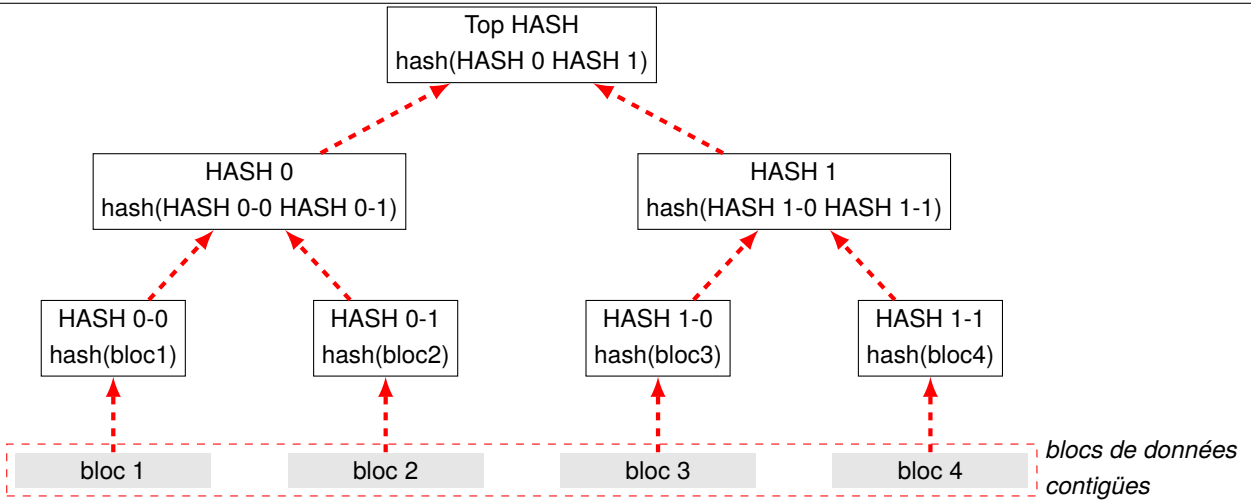
combinaison	**haché**
a	169552370019632401730582715598587264 97
b	19528942417061115912891101761279579534 3
ab	32560655549305688865853317129809488800
ba	941680395931154527312999502951431136 4
aa	865905563437731851846768541823880583 86
bb	447630314541533955979929907481056088 28



Tous les mots d'au plus 3 lettres à partir de l'alphabet { a,b,c }.



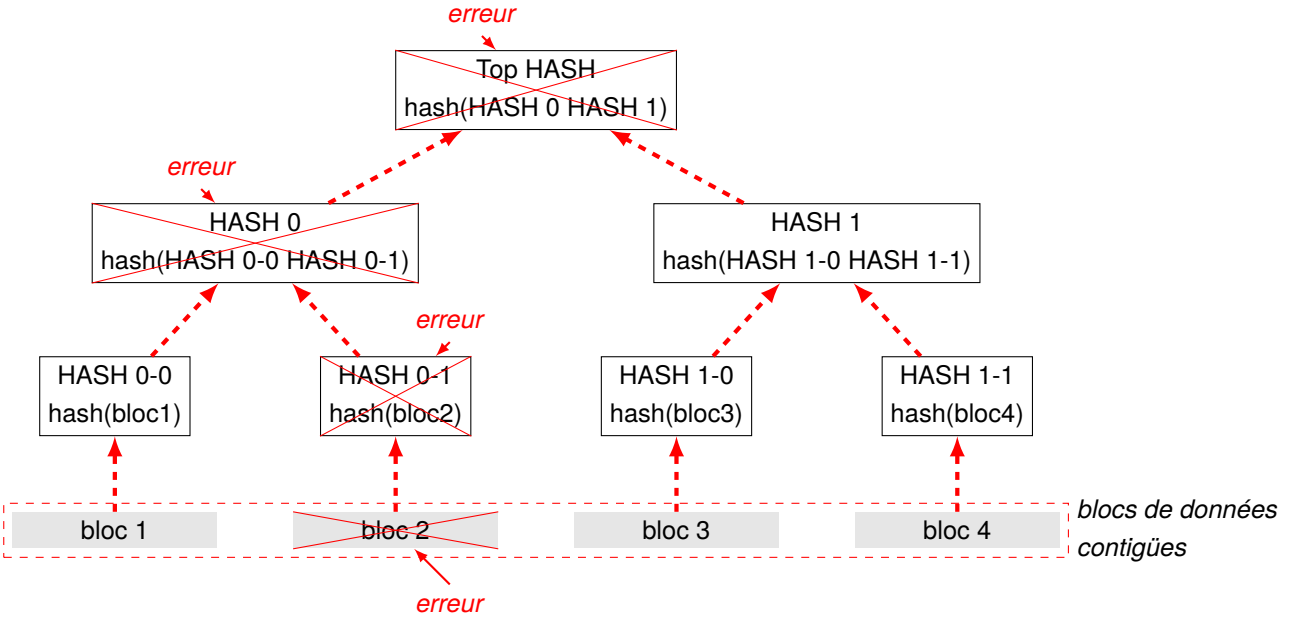
$\Longrightarrow$ ressemble à une **distribution aléatoire** !



L'utilisation de cette arbre permet **d'isoler une erreur** dans un fichier transféré d'Alice vers Bob :

1. Bob veut vérifier que le fichier reçu depuis Alice est sans erreur : il calcule l'abre de merkle sur sa copie de fichier ;
2. Alice transmets le haché Top HASH à Bob, c-à-d celui de la racine de l'arbre ;
3. Bob compare le haché qu'il a calculé avec celui qu'il a reçu d'Alice :
   - ◇ identique ? Le fichier a été transferré **sans erreur**.
   - ◇ différent ? Bob demande à Alice les hachés de la racine de chaque sous-arbre : HASH 0 et HASH 1 ;
4. pour chacun de ses hachés, HASH 0 et HASH 1, Bob peut vérifier par rapport à la valeur qu'il a lui-même calculé dans son abre de Merkle :
   - ◇ dès qu'il trouve une différence de haché, il peut identifier le sous-arbre concerné et descendre jusqu'à la vérification d'une **feuille** de l'arbre, c-à-d le haché de chaque bloc de données en comparant avec la version d'Alice ;
   - ◇ dans le cas où le haché d'un bloc de données n'est pas bon, il peut demander à Alice de lui retransmettre les données de ce bloc uniquement.

Détection d'une erreur et identification du ou des blocs concernés



Si une erreur se produit sur le bloc 2 :

- ▷ Top HASH différent de celui d'Alice ⟹ Bob demande le haché de **chaque sous-arbre** ;
- ▷ HASH 0-1 différent ⟹ Bob demande le haché de **chaque sous-arbre** ;
- ▷ HASH 0 différent ⟹ la feuille correspondant au haché du bloc bloc 2 ⟹ le bloc 2 doit être **retransmis** par Alice ou par **quiconque en possédant une copie** ;

⟹ **application au réseau «*peer-to-peer*».**

Principaux algorithmes

Il existe différents algorithmes réalisant de traitement :

- MD2, MD4 et **MD5** (MD signifiant «*Message Digest*»), développé par Ron Rivest (société RSA Security), créant une empreinte digitale de 128 bits pour MD5.
  Il est courant de voir des documents en téléchargement sur Internet accompagnés d'un fichier MD5, il s'agit du résumé du document permettant de vérifier l'intégrité de ce dernier.
  Son usage est maintenant déconseillé car il possible de choisir la valeur de l'empreinte obtenue.
- **SHA**,«*Secure Hash Algorithm*», pouvant être traduit par Algorithme de hachage sécurisé
  développé par le NIST en 1995. il crée des empreintes d'une longueur de 160 bits.
  C'est un standard SHA0 et SHA1 (devenu le standard SHS).
  Son usage est maintenant déconseillé car il possible de choisir la valeur de l'empreinte obtenue.
  Il a été étendu en SHA256 ou SHA512.
- **RIPEMD** «*Race Integrity Primitives Evaluation Message Digest*», développé par Hans Dobbertin, Antoon Bosselaers et Bart Preneel,
  RIPEMD-128 et RIPEMD-160, créé entre 88 et 92 ;
- **Tiger**, développé par Ross Anderson et Eli Biham, plus rapide que MD5 (132Mb/s contre 37Mb/s sur une même machine, optimisé pour processeur 64bit).

Une forme particulière de fonction de hachage : MAC ou HMAC

Combiner Intégrité + chiffrement symétrique : MAC, «*Message Authentication code*», code d'authentification de message.
Combiner une fonction de **hachage** et une **clé secrète** : HMAC, «*keyed-hash message authentication*».
On transmet l'empreinte du message chiffrée avec une clé secrète qui protège contre toute modification du message : si l'intrus modifie le message et ne connait pas la clé, il ne peut créer un MAC correspondant au nouveau document (le document peut, lui-même, être transmis chiffré ou non).

Le scellement ou sceau ou signature électronique

Signer : **joindre** à un document sa **signature**, c-à-d le **chiffré asymétrique par clé privée**, de l'empreinte du document, obtenue à l'aide d'une fonction de **hachage**.

La **signature** assure :

- ▷ **Authentification** : le document peut être **identifié** comme provenant de la personne ;
- ▷ **Non-répudiation** : l'utilisation de la **clé privée** ne peut être faite sans le **consentement** de son propriétaire ;
- ▷ **Intégrité** : la correspondance de l'empreinte déchiffrée, avec celle courante du document implique qu'il n'y a pas eu de modification par rapport à la version du document utilisée lors du chiffrement.

La **confidentialité** peut être assurée par un **chiffrement symétrique** du document.

Utilisation pour la sécurité du courrier électronique

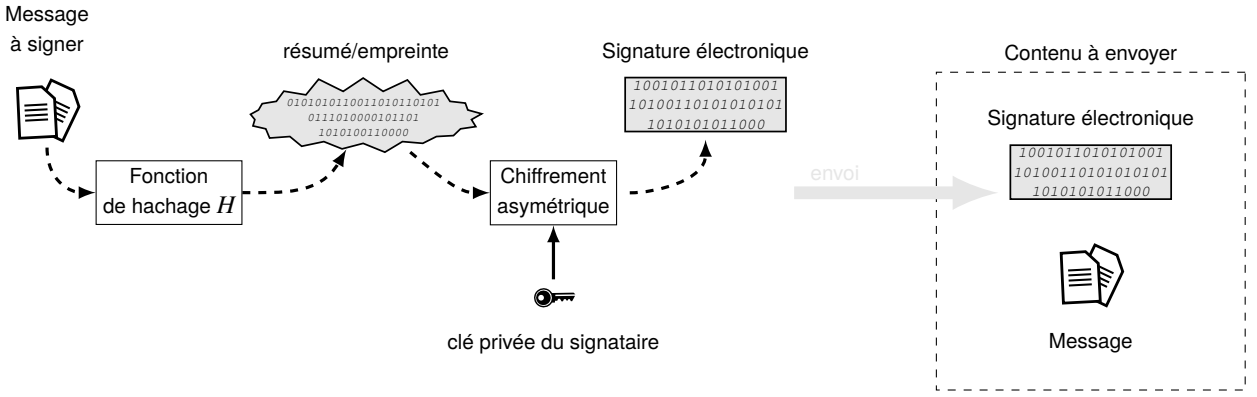
1. L'expéditeur calcule **l'empreinte** de son **texte en clair** à l'aide d'une fonction de hachage ;
2. L'expéditeur chiffre **l'empreinte** avec sa **clé privée** $\Longrightarrow$ signature ;
3. *Le chiffrement du document est **optionnel** si la confidentialité n'est pas nécessaire.*
4. L'expéditeur chiffre le **texte en clair** et **la signature** à l'aide d'un **chiffrement symétrique** dont la **clé secrète** est chiffrée à l'aide de la **clé publique du destinataire** et jointe au message (enveloppe sécurisée).
5. L'expéditeur envoie le **document chiffré** au destinataire ;
6. Le destinataire **déchiffre la clé secrète symétrique** avec **sa clé privée**, puis déchiffre le document ;
7. Le destinataire déchiffre **l'empreinte** avec la clé publique de l'expéditeur (*authentification*) ;
8. Le destinataire calcule **l'empreinte du texte clair** à l'aide de la même fonction de hachage que l'expéditeur ;
9. Le destinataire **compare les deux empreintes**.

optionnel

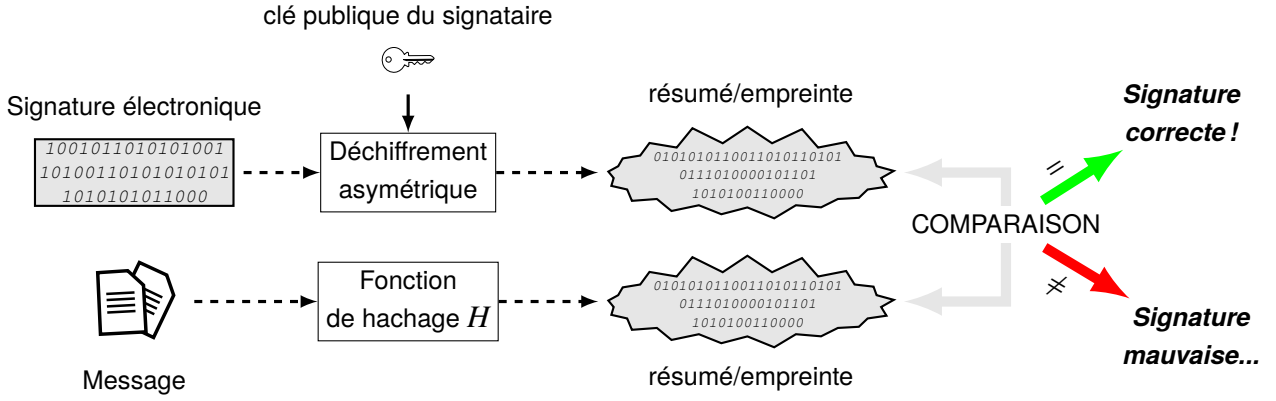
Deux empreintes identiques impliquent que le texte en clair n'a pas été modifié (intégrité).

Le standard américain est le **DSS**, «*Digital Signature Standard*», qui spécifie trois algorithmes : le DSA, «*Digital Signature Algorithm*», **RSA** et **ECDSA** «*Elliptic Curves Digital Signature Algorithm*».

Créer une signature électronique



Vérifier une signature électronique



La société RSA a établit des **standards** pour l'organisation des **échanges cryptographiques** et permettre l'interopérabilité «*PKCS*» ou «*Public Key Cryptographic Standards*» :

- **PKCS#1** : décrit comment chiffrer des données en utilisant l'algorithme à clé publique RSA, afin de pouvoir signer un fichier ou le chiffrer :
  - pour les signatures, le contenu doit d'abord être «hashé» par un algorithme de hachage afin de produire une empreinte.
    C'est cette empreinte qui sera signée avec l'algorithme RSA en utilisant la clé privée du signataire. *La manière de génèrer et signer une empreinte est décrite dans PKCS#7.*
  - pour le chiffrement d'un fichier, le fichier doit d'abord être chiffré par un algorithme à clé secrète comme AES et la **clé secrète** est ensuite elle-même **chiffrée** avec l'algorithme **RSA** en utilisant la **clé publique du destinataire** (il sera donc le seul à pouvoir déchiffrer la clé secrète avec sa clé privée).
    Le chiffrement du fichier et le chiffrement de la clé sont décrits dans PKCS#7.
  - PKCS#1 définit également différents algorithmes de hachage, MD5, SHA1, SHA256.
- **PKCS#3** : standard de **négociation de clé Diffie-Hellman** :
  - PKCS#3 décrit comment implémenter l'algorithme Diffie-Hellman qui sert à «négocier» un secret partagé entre deux parties, sans qu'aucune information privée n'ait à être échangée.
  - Ce secret partagé peut servir à générer une clé de session, qui pourra être utilisée dans un algorithme à clé secrète comme AES.
- **PKCS#7** : Standard de la syntaxe pour un message chiffré, on parle «d'enveloppe sécurisée»
  PKCS#7 décrit une syntaxe générale pour les données devant être chiffrées, comme les signatures numériques par exemple.
  Cette syntaxe supporte la récursivité, ce qui permet de signer un fichier déjà signé par quelqu'un d'autre par exemple.

Donc au final, la signature électronique reprend les principes du courrier...papier ?

Notion de copie et d'original d'un document papier

Une photocopie est différente de l'original (*ou presque...*). *Essayez de présenter la photocopie d'un billet pour acheter dans une boutique !*

Une personne est identifiée par sa signature (analyse graphologique) Cette signature engage la personne qui l'a écrite :

- ▷ c'est une preuve **d'acceptation** pour un contrat et **d'engagement** à le remplir ;
- ▷ c'est une **autorisation** de transfert d'argent dans le cas d'un chèque ;
- ▷ c'est une **identification** dans le cas d'une lettre que l'on envoie.

Cette signature est **reconnue** par la législation francaise.

Notion de copie «certifiée conforme» réalisable auprès de la mairie ou bien d'un commissariat. Cette notion a d'ailleurs **disparue**, face à l'avancée des moyens de reproduction et de l'utilisation systématique de l'impression machine pour les documents administratifs (plus ou presque de partie manuscrite présente sur le document ou bien reproduite électroniquement).

Signature

Une signature manuscrite idéale est réputée posséder les propriétés suivantes :

- ☐ elle ne peut être imitée ;
- ☐ elle **authentifie** le signataire ;
- ☐ la signature appartient **à un seul document** (elle n'est pas réutilisable) ;
- ☐ le document ne peut être partiellement ou totalement modifié ;
- ☐ la signature ne peut être **reniée** ;
- ☐ la signature peut être **contrôlée**.

Le cas du document électronique

Il est **reproductible** à l'infini sans modification.
C'est ce qui le rend virtuellement éternel.

Le **droit de copie**, dite de sauvegarde, est apparu avec l'apparition de «programme informatique» sur support duplicable (bande magnétique, disquette, CD...).

Il peut être modifié pour faire disparaitre ou apparaitre des éléments supplémentaires. *Suppression du nom de l'auteur d'un document de traitement de texte, ajout d'un texte de propriété sur une image...*

Il peut être **attribuer** à n'importe quel propriétaire. *Un fichier MP3 peut appartenir à une personne disposant du CD qui a servi de source à son encodage ou bien à une autre...*

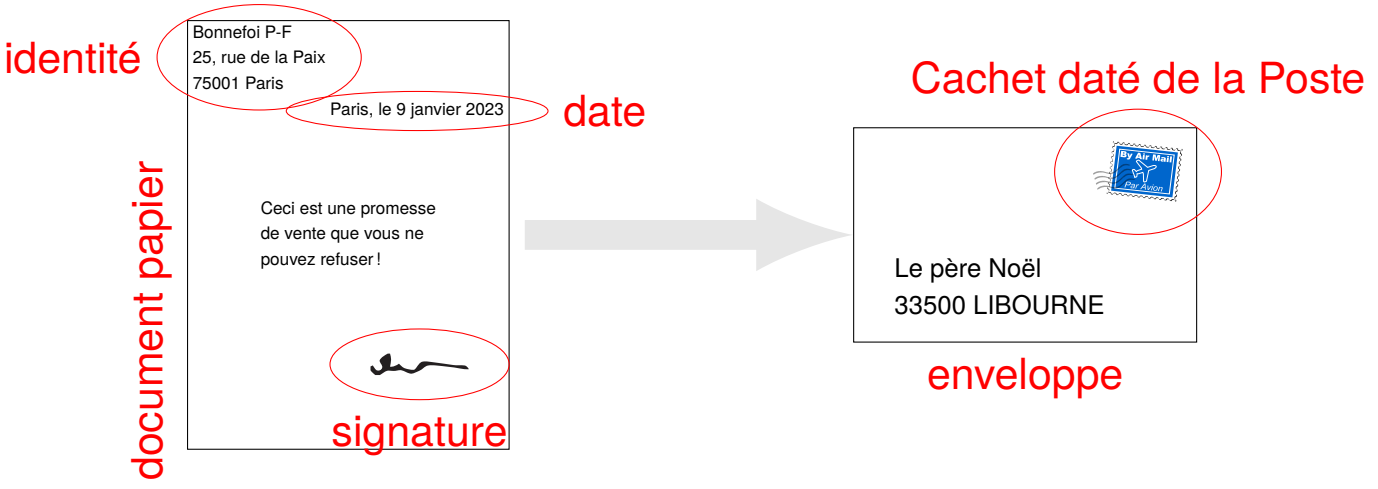
Limitation à la consultation

Une **nouvelle forme de propriété** est apparue avec lui : celle liée à la **consultation** du contenu sans possibilité d'exploitation ou de reproduction en vu de conservation.
C'est le cas du DVD ou du Bluray dont le contenu ne peut (ne pouvait) être accéder que pour le visionner mais pas pour l'enregistrer ou le modifier.

La sécurité «écrite» : la signature et l'envoi par la Poste

Pour être recevable comme document engageant la responsabilité de celui qui l'envoi le document doit posséder :

- une indication claire de **l'identité** ;
- une **signature** ;
- ces deux indications doivent être apposés **sur un même papier** (pas de collage, ...) ;
- mis dans une **enveloppe** avec le **cachet de la Poste**.



Les aspects juridiques nécessaires pour la version électronique

Vers la signature électronique : des considérations juridiques

Les régimes juridiques doivent admettre les écrits numériques comme :

- **recevables** (le juge a le droit de les considérer) ;
- potentiellement **probants** (ils apportent la preuve s'ils sont difficilement falsifiable).

Les travaux de normalisation se concentrent sur deux aspects :

- **l'interopérabilité** pour une signature électronique universellement interprétée et reconnue

  définition de standards d'interprétation **non ambigüe** des signatures ;
  des **algorithmes** de calcul et des **modes** de fonctionnement ;
  des initiatives privées (RSA Security Inc) ont déjà établi des formats de messages ;

- la **sécurité** :
  la norme internationale des «critères communs» de **spécification** et **d'évaluation sécuritaire** ouvre la perspective de la reconnaissance des signatures **entre pays** par le fait que leurs niveaux de sécurité soient équivalents.

La vérification des **caractéristiques de sécurité** des systèmes est effectuées par des **sociétés spécialisées**, les *évaluateurs* ; dont les compétences sont surveillées entre autres, par une autorité émanant de l'état **l'ANSSI**, «Agence Nationale de la Sécurité des Systèmes d'Information» (anciennement appelée la DCSSI).
Vous trouverez à `http://www.ssi.gouv.fr/administration/reglementation/`*, les documents relatifs au RGS, Référentiel Général de Sécurité définissant les exigences francaises en matière de sécurité relative à la cryptographie.*
Le **risque zéro** n'existe pas et **l'arsenal juridique** et technique doit **prendre en compte ce fait**, en prévoyant les **conséquences d'accidents majeurs** (fraudes ou dysfonctionnement) dans des **plans de secours**.

Le 13 décembre 1999, de la directive 1999/93/CE relative à «un cadre communautaire pour les signatures électroniques»

La loi du 13 mars 2000

Au contraire de la directive, la loi francaise ne rentre dans aucune considération technique. Elle définit de facon générale la signature, au regard des fonctions assurées par celle-ci : «*La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte*» (art. 1316-4 du Code Civil).

Le code civil définit également les conditions de l'équivalence du support électronique et du support papier à titre de preuve, sous réserve que quatre conditions soient respectées :

Les quatre conditions posées par le code civil pour que le support numérique soit admissible comme preuve au même titre que le support papier

1. **pouvoir identifier** la personne dont émane l'écrit électronique au moyen d'un procédé fiable ;
2. l'écrit électronique a été **créé** dans des conditions de nature à en **garantir l'intégrité** ;
3. l'écrit électronique est **conservé** dans des conditions de nature à en **garantir l'intégrité** ;
4. utiliser un procédé fiable **garantissant le lien** de la **signature électronique** avec **l'acte** auquel elle s'attache.

Le décret du 30 mars 2001

Le décret est un texte technique, qui constitue la transposition de la **directive européenne** sur la signature électronique.

Il distingue la «signature électronique» de la «signature électronique sécurisée» :

- la **signature électronique** est celle qui respecte les conditions posées par le code civil ;
- la **signature électronique sécurisée** est celle qui répond de plus aux exigences du décret, et présente de ce fait une présomption de fiabilité.

Le décret précise les conditions de mise en œuvre de la «signature électronique sécurisée», qui bénéficie d'une présomption de fiabilité :

- elle est établie grâce à un dispositif sécurisé de création de signature électronique ;
- sa vérification repose sur l'utilisation d'un **certificat électronique qualifié**.

23 juillet 2014 : adoption règlement n° 910/2014/UE, eIDAS, «electronic identification and trust services»

- **abroge** la 1999/93/C à partir du 1er juillet 2016 et s'appliquera en effet directement à partir de cette date **dans tous les états membres de l'UE**
  viendra remplacer les lois nationales, ce qui engendra des modifications profondes dans la législation de certains pays en matière de signature et d'identification électronique.

- **création d'un nouvel objet juridique** : **la signature électronique de personne morale** :
  - nouveau concept juridique – qui n'existait pas en droit Francais – à savoir la **signature de personne morale** ou **cachet électronique**.
    Jusqu'à présent, seules les personnes physiques pouvaient créer une signature électronique. Les entreprises, les administrations et les associations vont désormais pouvoir signer en leur nom des documents qui seront recevables comme preuve en justice.
- **pas d'obligation de carte à puce** : le recours à un **support physique qualifié** ne fait pas partie des exigences applicables aux dispositifs de création de signature électronique qualifiés, permettant d'obtenir un niveau de sécurité juridique maximal sur les documents signés.

Le règlement consacre le marché européen de la signature électronique dans le secteur public et les relations avec les administrés, ainsi que le principe de reconnaissance mutuelle des moyens d'identification électronique délivrés par les Etats membres, tout en exigeant un haut niveau de sécurité pour l'ensemble des méthodes utilisées.

https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-reglement-eidas/

http://www.droit-technologie.org/actuality-1663/l-europe-remet-a-plat-les-regles-en-matiere-de-signature-electronique.html

Tous les acteurs intéressés – les citoyens/consommateurs ainsi que les entreprises et les autorités publiques – doivent être en mesure de recourir aux ***technologies de l'information et de la communication*** *(et notamment l'internet) en* ***toute confiance*** *et avec un* ***niveau de sécurité élevé****. Cela suppose notamment qu'ils puissent* ***identifier avec certitude*** *un cocontractant potentiel et que les obstacles à l'utilisation de certains outils (tels que des services de signature, d'horodatage ou de recommandé électroniques) soient levés.*

Par ailleurs, ces objectifs doivent être atteints dans un ***contexte transfrontalier paneuropéen*** *de sorte que, par exemple, un citoyen belge puisse s'identifier auprès d'une administration publique italienne, en utilisant des technologies fournies par une entreprise allemande (ce qui requiert, entre autres, que les moyens techniques utilisés soient* ***interopérables****).*

D'une part*, elles consacrent la reconnaissance mutuelle des* ***moyens d'identification électronique*** *délivrés par un Etat membre et qui seraient utilisés dans un autre Etat membre. On songe à l'hypothèse d'un étudiant belge qui souhaiterait s'inscrire en ligne dans une université espagnole, en établissant son identité au moyen de sa carte d'identité électronique. Pour les entreprises, cette reconnaissance mutuelle est importante dans le cadre des marchés publics et des réponses aux appels d'offres. Une procédure est mise en place, pour organiser la coopération entre les Etats membres et les autorités européennes (spécialement la Commission), et garantir l'interopérabilité des moyens d'identification utilisés.*

D'autre part*, le* ***règlement eIDAS*** *établit un* ***cadre juridique*** *pour* ***plusieurs services de confiance****. Outre la signature électronique, sont également visés le* ***cachet électronique*** *(qui doit permettre de garantir l'origine et l'intégrité d'un document électronique délivré par une personne morale),* ***l'horodatage électronique*** *(pour prouver l'existence des données à un moment particulier), les services d'envois recommandés et* ***l'authentification de site internet*** *(pour s'assurer qu'un site web est géré par celui qui s'en prétend titulaire).*

Il y a violation de secret de la correspondance lorsqu'une tierce personne en prend connaissance sans le consentement préalable de l'émetteur d'un courrier à caractère privé ou en dehors du cadre de la Loi.

Une correspondance reste la **propriété intellectuelle** de son auteur bien que le support physique soit la propriété du destinataire.

La convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales du 4 novembre 1950, rappelle en son article 8, «le droit au respect de la correspondance».

Union européenne

Au sein de l'Union européenne, le secret de la correspondance est garanti par la directive européenne 97/66 du 15 décembre 1997 qui fait obligation aux états membres de garantir par leur législation :

- la **confidentialité** des communications passées par la voie des télécommunications et d'interdire «à toute autre personne que les utilisateurs, sans le consentement des utilisateurs concernés, d'écouter, d'intercepter, de stocker les communications ou de les soumettre à quelque autre moyen d'interception ou de surveillance, sauf lorsque ces activités sont légalement autorisées».

France

En France, la **violation de secret** de la correspondance est actuellement réprimée par les articles 226-15 et 432-9 du code pénal et par l'article L 33-1 du code des postes et télécommunications.

Le ministre délégué au Budget et à la Réforme de l'Etat, Jean-Francois Copé, a présenté un projet de loi ratifiant l'ordonnance du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives, et entre les autorités administratives elles-mêmes.

Cette ordonnance, prise sur le fondement de la loi du 9 décembre 2004, de simplification du droit, vient renforcer l'attirail juridique nécessaire au bon développement de «l'administration électronique» dans le pays.

L'e-administration

Elle concerne :

- l'ensemble des **échanges électroniques** ;
- télé-services ou courriels échangés avec les administrations, qu'il s'agisse des administrations de l'Etat, des collectivités territoriales, de leurs établissements publics administratifs, des organismes de sécurité sociale ou des autres organismes de droit privé gérant des services publics administratifs.

L'ordonnance a établi une **équivalence juridique** entre le **courrier électronique** et le **courrier sur support papier** en prévoyant notamment que la *saisine de l'administration par voie électronique est régulière* et doit faire l'objet d'un *accusé de réception* ou d'un *accusé d'enregistrement* informant l'usager que sa demande a été prise en compte.

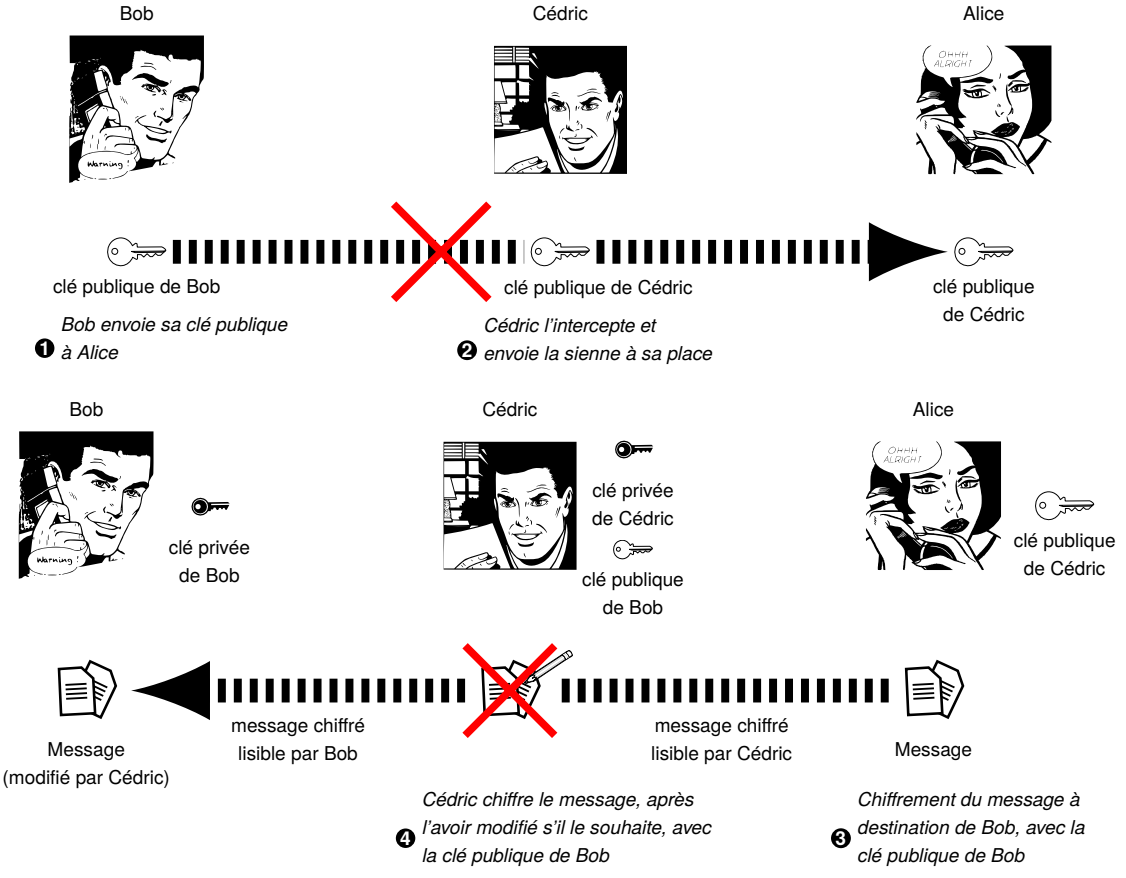
Elle offre ainsi la possibilité aux usagers de disposer d'un **espace de stockage en ligne**, personnalisé et personnalisable, qui a pour vocation d'accueillir les documents administratifs les concernant, ainsi qu'un bloc-notes contenant des formulaires en ligne.

Ce service sera expérimenté début 2006 avant sa mise en place en 2007. Le texte permet également la mise place des conditions permettant la **signature électronique** de leurs actes par les autorités administratives.

Alors ?

Plus de problème ?

Le problème de l'échange de clé publique



Le problème de la diffusion des clés publiques

Pour diffuser des clés publiques, on peut utiliser un **annuaire** (LDAP par exemple).

Le problème est de s'assurer que la clé que l'on récupère provient bien de la personne concernée : **rien ne garantit** que la clé est bien celle de l'utilisateur à qui elle est associée.

Attaque

Un pirate peut **remplacer** la clé publique de la victime présente dans l'annuaire par **sa clé publique**.

Ainsi, il peut **déchiffrer** tous les messages ayant été chiffrés avec cette clé.

Il peut même, ensuite, renvoyer à son véritable destinataire le message (modifié ou non) en le chiffrant avec la clé publique originale pour **ne pas être démasqué** !

But de la PKI

- Gérer les problèmes posés par le **maintien de lien entre des clés publiques et des identités** au travers de différentes applications.
  Sans PKI, il faudrait définir de nombreuses solutions de sécurité et espérer une certaine interopérabilité ainsi qu'un même niveau de protection entre elles.
- Gérer le **partage de la confiance** entre usagers, en utilisant un tiers pour **confirmer** la propriété d'un «credential», c-à-d un document conférant une identité ou une qualité, appelé «certificat».
- Être **reconnu** «comme de confiance» par les **différents usagers** :
  - un usager n'a plus à connaître directement un autre usager avec lequel il veut établir une relation de confiance :
    - il connaît un tiers de confiance partagé avec cet autre usager ;
    - il établit un lien de confiance avec cet autre usager au travers du tiers.

  C'est le modèle du «tiers de confiance».

Composants d'une PKI

- des **certificats électroniques** ;
- des **autorités d'enregistrement**, «*Registration Authority*», et de **certification**, «*Certification Authority*» ;
- un **procédé standardisé** de vérification.

La carte d'identité de la clé publique

Le certificat contient :

- une identité ;
- la clé publique associée à cette identité ;
- une **preuve de cette association** fournie par le tiers de confiance.

Comment fournir la **preuve de la confiance** du tiers ?

Utiliser la **signature électronique** de ce tiers !

La construction du certificat

L'ensemble des informations (le nom de l'autorité de certification, du propriétaire du certificat...) est **signé** par l'**autorité de certification**, représentant le tiers, à l'aide de la signature électronique :

- une fonction de hachage crée une **empreinte** de ces informations ;
- ce résumé est **chiffré** à l'aide de la **clé privée** de l'autorité de certification, la clé publique ayant été préalablement largement diffusée ou elle même signée par une autorité de niveau supérieur.

Grâce à cette signature électronique, il est possible de s'assurer de la fiabilité du certificat.

Cette méthode repose sur la confiance dans une structure dont on dispose de la clé publique, une autorité supérieure : VeriSign, GTE, Certinomis, CommerceNet, Thawte, ...

Fonctionnement

- **Si je fais confiance** à cette autorité de certification, **alors je fais confiance** aux certificats signés par elle ;
- Un certificat signé par elle associe une clé publique à une identité : **je fais confiance** à cette association (après vérification de la signature grâce à la clé publique de cette autorité de certification) ;
- **J'utilise la clé publique** contenue dans le certificat pour **l'identité associée**.

3. 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.

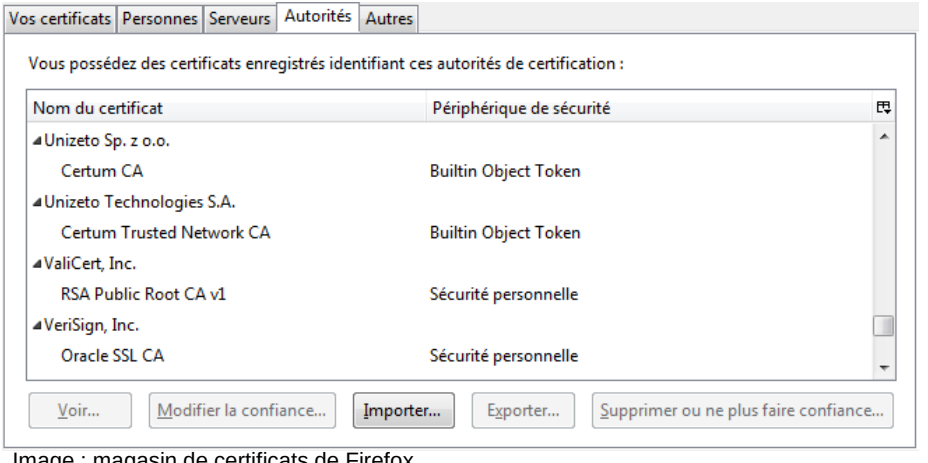


Image : magasin de certificats de Firefox

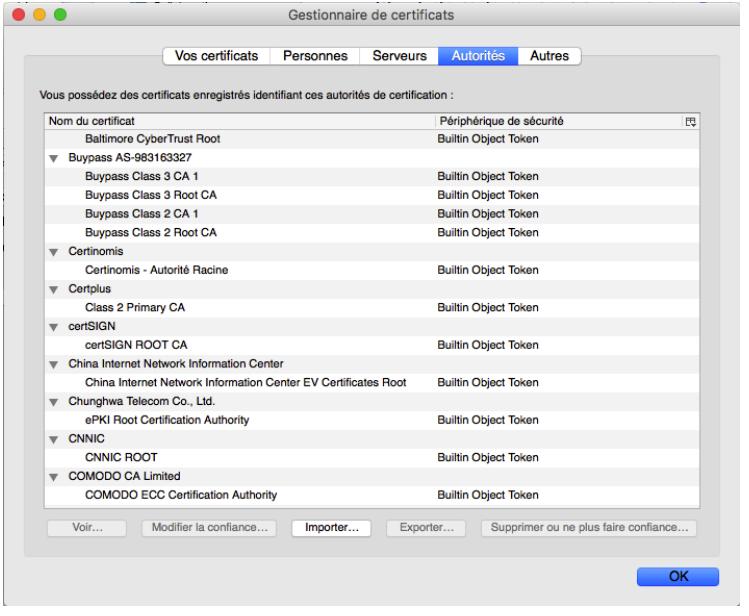
Connaissance et acceptation d'un tiers de confiance

Cela consiste à **adhérer** auprès de l'**autorité de certification** qui représente le tiers de confiance.

Cette CA, «*Certification Authority*», **émets** des certificats.

Cet organisme intègre sa **clé publique** au niveau :

- du **navigateur** de la machine dans le cas de la sécurisation d'une transaction web ;
- du **système d'exploitation** pour la vérification des mises à jour ou l'installation de logiciel.



3. Les bases de la cryptographie

g. Certificats électroniques

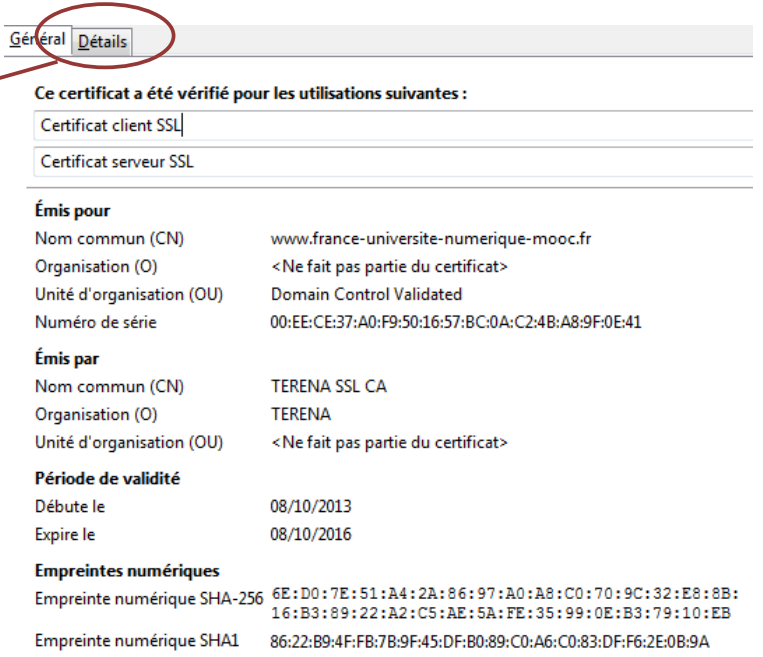
Exemple d'un certificat pour le site web www.france-universite-numerique-mooc.fr

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



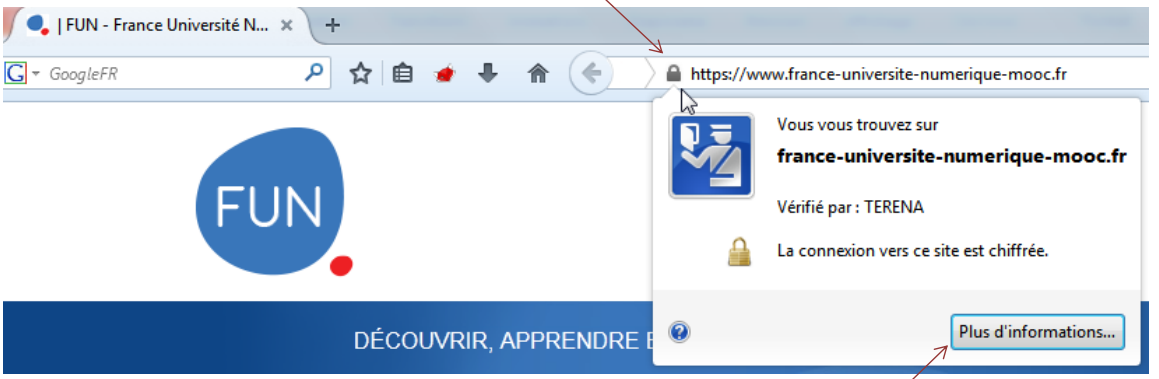
3. Les bases de la cryptographie

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

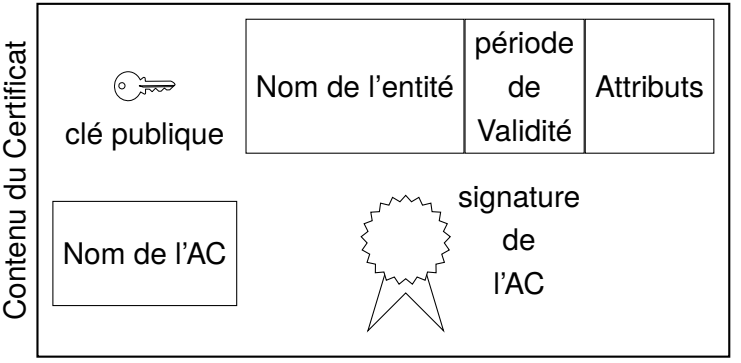


Cliquer ici pour afficher le certificat

Notion de certificat

Un **certificat** permet d'associer une **clé publique** à une **entité** (une personne, une machine, ...) afin d'en assurer la **validité**.

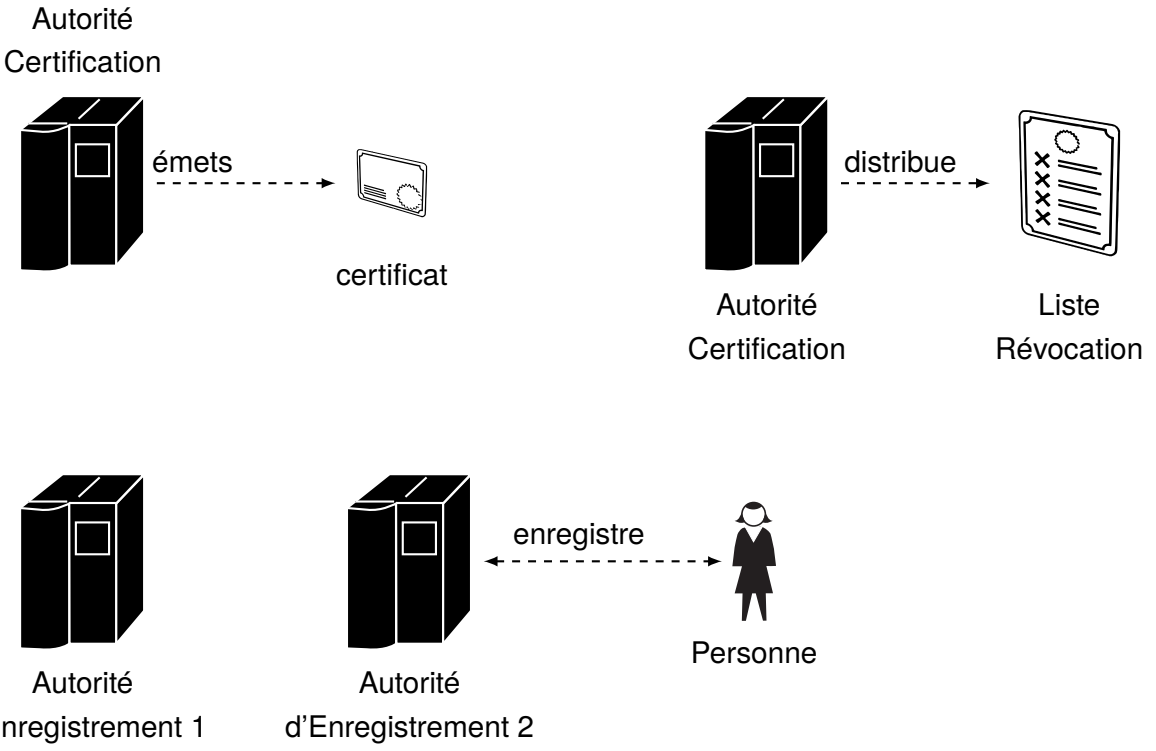
Ce certificat doit ne pas pouvoir être modifié, ni créer sans contrôle : il faut à la fois intégrité et authentification du créateur.



L'**Autorité de Certification** doit assurer des fonctions de **gestion** de certificats (émission, révocation, stockage, récupération et fiabilité des certificats), elle doit :

- **délivrer** les certificats ;
- assigner une **date de validité** aux certificats (équivalent à la date limite de péremption des produits alimentaires) ;
- **révoquer** éventuellement des certificats avant cette date en cas de compromission de la clé privée associée (ou du propriétaire).

Composition d'une PKI



peut exister en plusieurs exemplaires :
distribution géographiques,
catégories de clients...

Utilisation de PKI, reposant sur des AC déjà connues comme Verisign, Thawte *etc.*

Il existe plusieurs «classes» de certificat en fonction du niveau de confiance demandé et du prix du traitement.
Des informations d'identité plus ou moins précises sont demandées en fonction du niveau de confiance choisi.

- **Classe 1** = une **clé publique** associée à une **adresse email**.
  - le demandeur recoit automatiquement un mail de confirmation ;
  - il n'y a pas de vérification de l'identité du titulaire.

  Il permet de faire de la signature de courrier électronique et du chiffrement de contenu. suffisant pour un particulier, service parfois gratuit.

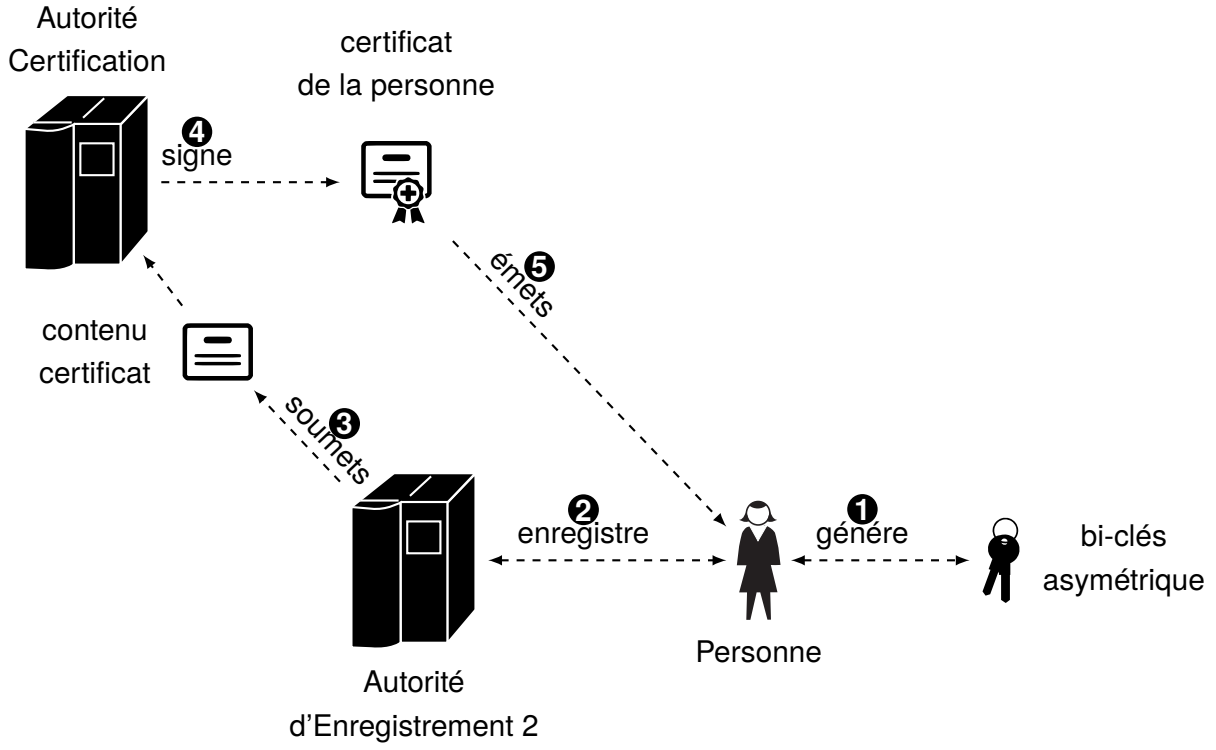
- **Classe 2** = la vérification des informations d'identité fournies est effectuée,
  - la présentation physique peut être nécessaire ;
  - il y aura compensation financière en cas de litige ;
  - il permet de faire :
    - la même chose qu'un classe 1, mais avec de plus grandes garanties
    - de la signature d'application : lors du déploiement de ce logiciel, on pourra vérifier qu'il provient bien de la société de développement et qu'il n'a subit aucune altération.

  Pour un usage professionnel le certificat de classe 2 ou supérieur est nécessaire.

- **Classe 3** = la vérification des informations d'identité fournies est effectuée,
  - la présentation physique est nécessaire ;
  - il y aura compensation financière en cas de litige ;

  Un certificat de classe 3 permet de créer sa propre CA et de délivrer des certificats en interne.

Composition d'une PKI : enregistrement



L'autorité de certification doit être de confiance

- Elle doit être plus «*qu'un logiciel*» : elle englobe des procédures, des «policies», du matériel, des bâtiments, des gens pour vérifier les informations d'identité etc.
- Chaque CA doit avoir un CPS, «*Certification Practices Statement*» qui précise :
  - Comment les identités sont vérifiées ;
  - Quelles sont les étapes suivies par la CA pour générer un certificat, le maintenir et le distribuer ;
  - Les éléments qui permettent de justifier la confiance que l'on peut lui apporter et comment elle va s'acquitter de ses responsabilités ;
  - Les recours juridiques possibles dans le cas où l'AC est compromise ;
  - Que faire en cas de compromission de sa clé privée ou de sa perte ;
  - Les données qui seront inscrits dans le certificat ;
  - La gestion de la révocation ;
- Ce sont des documents qui doivent être rédigés par : les ressources humaines, le responsable des ressources informatiques et le service juridique.
- Cette CPS doit **être consultée** afin de **vérifier** que l'entreprise ou l'individu peut l'utiliser **conformément** à ses exigences.

Confiance dans la PKI

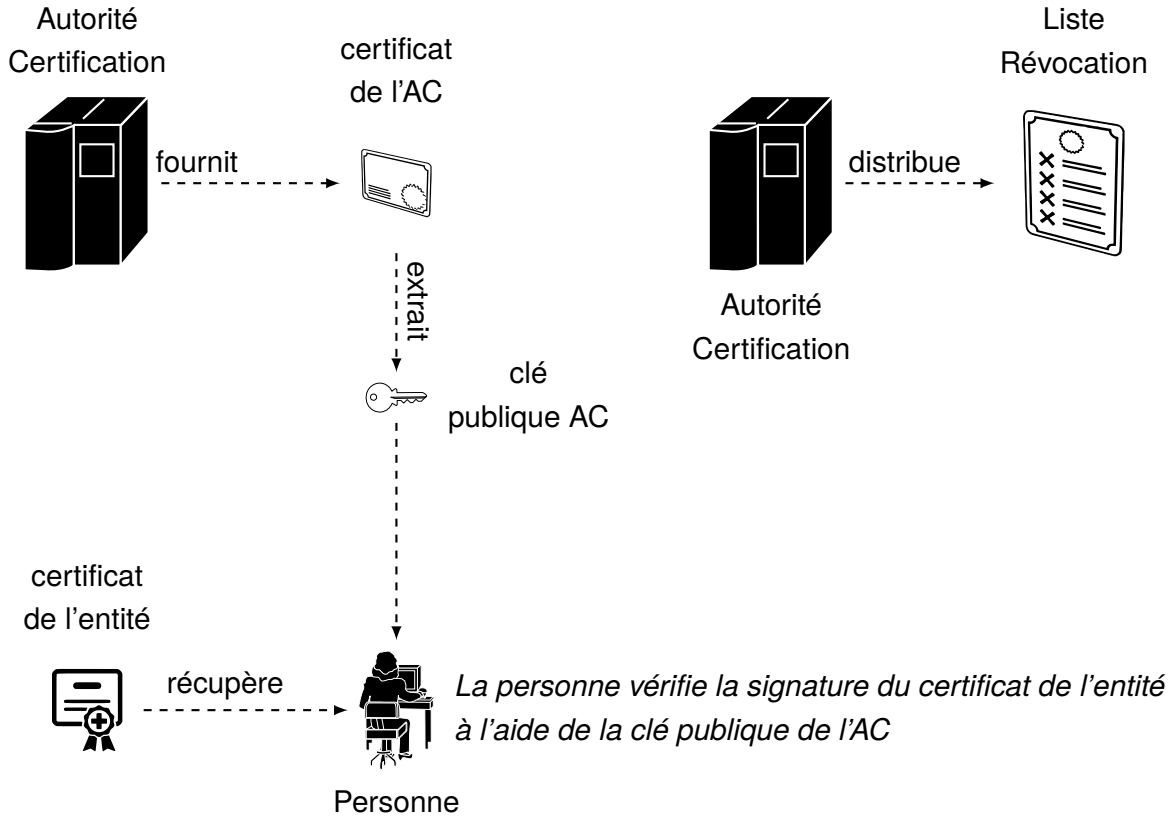
L'ensemble des personnes et des services doivent faire confiance à la PKI pour :

- signature des courriers;
- chiffrement ;
- authentification sur des applications maison…

Ils doivent être capable de :

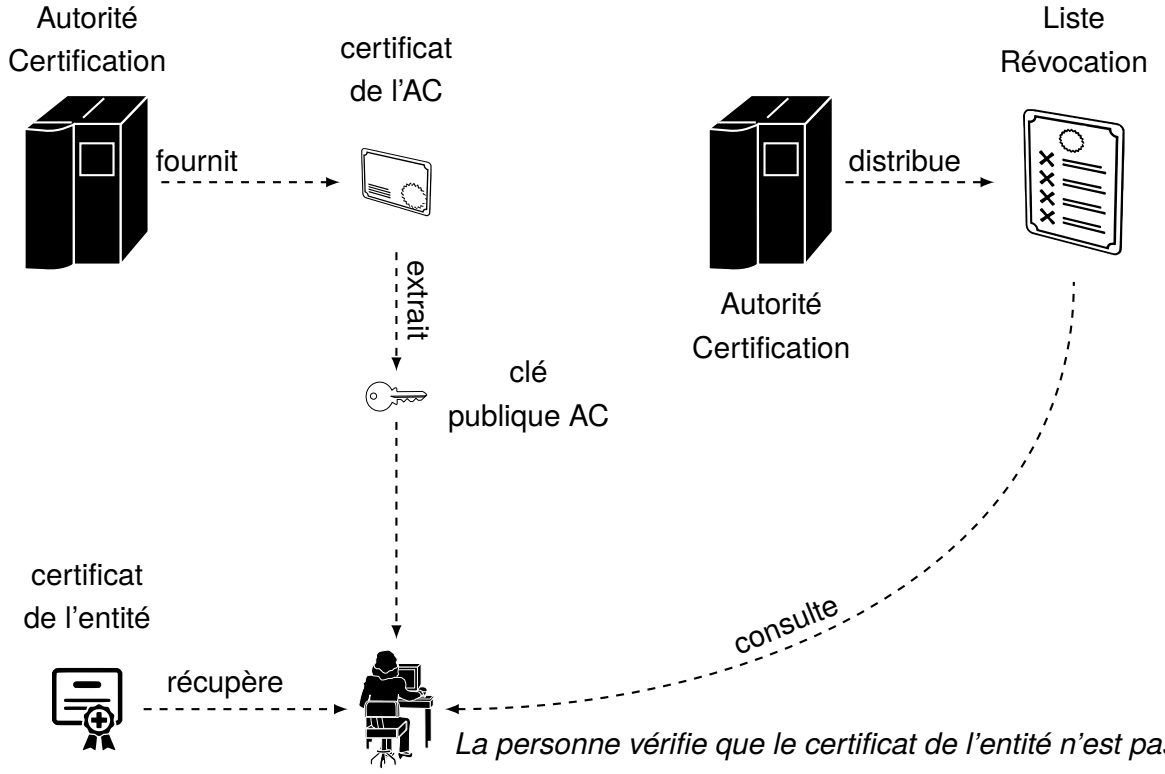
- **vérifier** un certificat ;
- contacter l´Autorité de Certification afin de vérifier la **validité du certificat** auprès de la **liste de révocation**.

Composition d'une PKI : utilisation et vérification du certificat



La personne vérifie la signature du certificat de l'entité à l'aide de la clé publique de l'AC

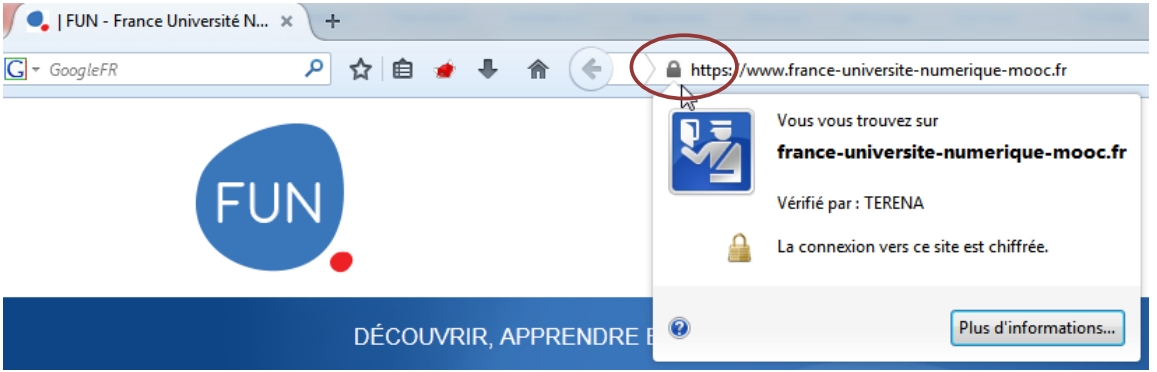
Composition d'une PKI : consultation liste révocation



La personne vérifie que le certificat de l'entité n'est pas révoqué (la liste de révocation est elle-même signée par l'AC)

3. Les bases de la cryptographie

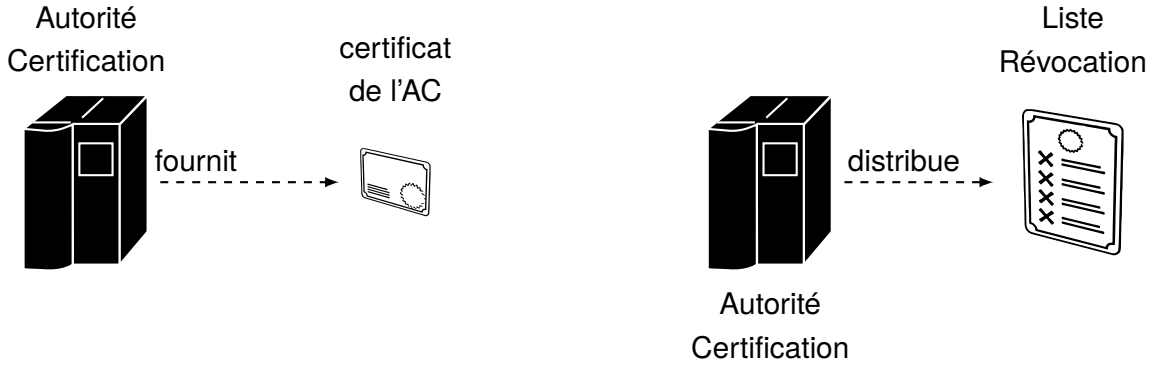
g. Certificats électroniques

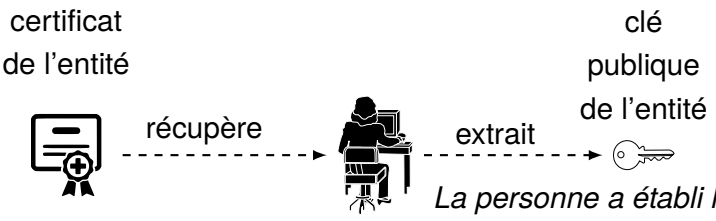


Puisque le certificat du site WEB est disponible et valide, cela amène donc deux avantages à l'utilisateur, caractéristiques du HTTP**S**

- 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).

Composition d'une PKI : établissement de la confiance

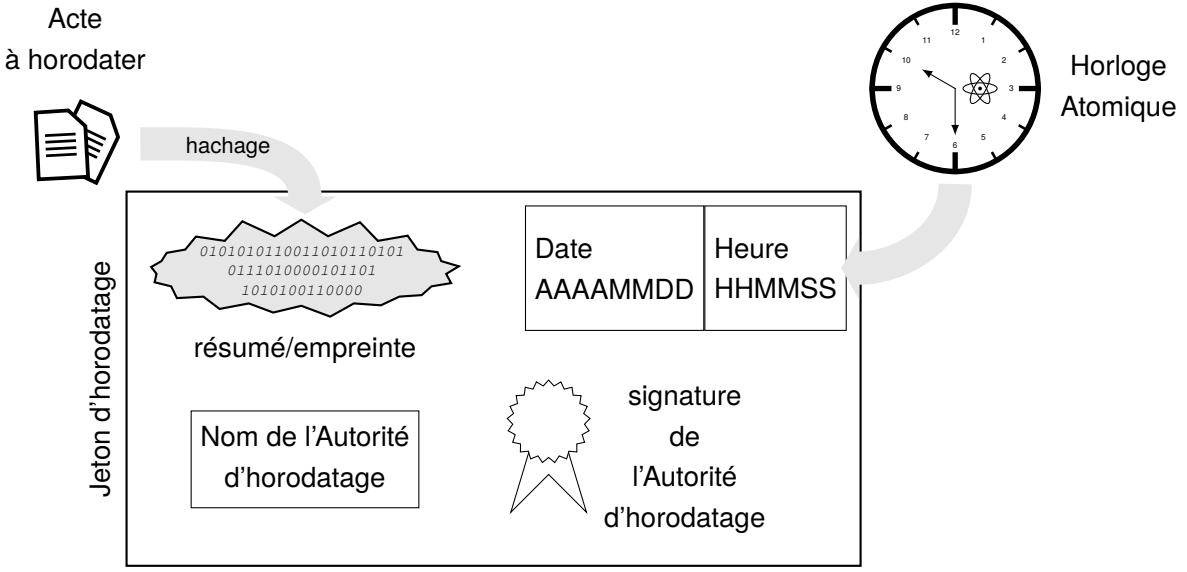




La personne a établi la confiance dans l'entité,
elle extrait la clé publique de l'entité
elle peut ***authentifier*** *l'entité ou lui transmettre un* ***message chiffré****.*

L'autorité d'horodatage, délivre des «*jetons d'horodatage*» pour **certifier l'existence de données** ou **l'établissement d'une transaction**, à une **date** et une **heure précise** à la seconde près, tel le «*cachet de la poste*» qui fait foi.

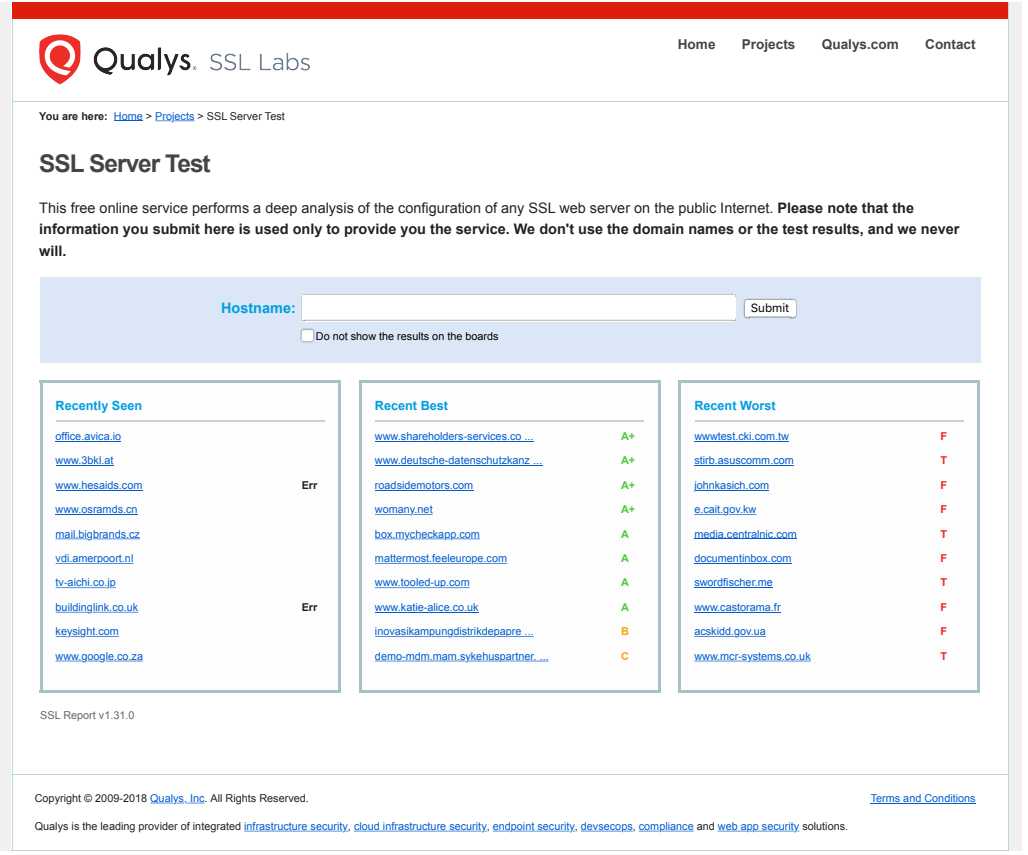
⟹Certifier l'intégrité d'un fichier ou d'une opération entre la date d'horodatage et celle de vérification.



L'heure et la date sont **absolues** données en référence UTC, «*Universal Time Coordinated*», et correspondent à l'heure et la date **courante** lors de la création du jeton.

Le jeton assure **l'intégrité**, **l'antériorité** et **l'opposabilité** (protection contre la contestation liée au temps).

Audit externe `https://www.ssllabs.com/ssltest/`



Qualys. SSL Labs

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test

SSL Server Test

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. **Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.**

Hostname: Submit

Do not show the results on the boards

Recently Seen		Recent Best		Recent Worst	
office.avica.io		www.shareholders-services.co ...	A+	wwwtest.cki.com.tw	F
www.3bkl.at		www.deutsche-datenschutzkanz ...	A+	stirb.asuscomm.com	T
www.hesaids.com	Err	roadsidemotors.com	A+	johnkasich.com	F
www.osramds.cn		womany.net	A+	e.cait.gov.kw	F
mail.bigbrands.cz		box.mycheckapp.com	A	media.centralnic.com	T
vdi.amerpoort.nl		mattermost.feeleurope.com	A	documentinbox.com	F
tv-aichi.co.jp		www.tooled-up.com	A	swordfischer.me	T
buildinglink.co.uk	Err	www.katie-alice.co.uk	A	www.castorama.fr	F
keysight.com		inovasikampungdistrikdepapre ...	B	acskidd.gov.ua	F
www.google.co.za		demo-mdm.mam.sykehuspartner. ...	C	www.mcr-systems.co.uk	T

SSL Report v1.31.0

Copyright © 2009-2018 Qualys, Inc. All Rights Reserved. Terms and Conditions

Qualys is the leading provider of integrated infrastructure security, cloud infrastructure security, endpoint security, devsecops, compliance and web app security solutions.

Vérification qu'un certificat est bien émis depuis la bonne AC

Site de référence `https://www.grc.com/fingerprints.htm`

Gibson Research Corporation · Privacy Recovery

Home ▾ | SpinRite ▾ | Services ▾ | Freeware ▾ | Research ▾ | Other ▾ | Search

Fingerprints

Is your employer, school, or Internet provider **eavesdropping** on your **secure** connections?

1,077 sets of fingerprints checked per day
1,588,775 sets of fingerprints checked for our visitors

Secure browser connections can be intercepted and decrypted by authorities who spoof the authentic site's certificate. But **the authentic site's fingerprint CANNOT be duplicated!**

Domain Name	Certificate Name	EV	Security Certificate's **Authentic** Fingerprint
www.grc.com	grc.com	●	15:9A:76:C5:AE:F4:90:15:79:E6:A4:99:96:C1:D6:A1:D9:3B:07:43
www.facebook.com	*.facebook.com	–	BD:25:8C:1F:62:A4:A6:D9:CF:7D:98:12:D2:2E:2F:F5:7E:84:FB:36
www.paypal.com	www.paypal.com	●	BB:20:B0:3F:FB:93:E1:77:FF:23:A7:43:89:49:60:1A:41:AE:C6:1C
www.wikipedia.org	*.wikipedia.org	–	4B:3E:D6:B6:A2:C7:55:E8:56:84:BE:B1:42:6B:B0:34:A6:FB:AC:24
twitter.com	twitter.com	●	26:5C:85:F6:5B:04:4D:C8:30:64:5C:6F:B9:CF:A7:D2:8F:28:BC:1B
www.blogger.com	*.blogger.com	–	80:72:8D:F5:50:E1:78:55:2E:4E:EA:2C:41:6E:EF:B8:13:48:21:36
www.linkedin.com	www.linkedin.com	–	3A:60:39:E8:CE:E4:FB:58:87:B8:53:97:89:8F:04:98:20:BF:E3:91
www.yahoo.com	*.www.yahoo.com	–	AE:69:9D:5E:BD:DC:E6:ED:57:41:11:26:2F:19:BB:18:EF:BE:73:B0
wordpress.com	wordpress.com	●	79:1A:83:83:21:20:F6:6D:9D:1E:77:5F:ED:89:16:FC:8E:A0:E0:C3
www.wordpress.com	*.wordpress.com	–	54:E0:89:DF:28:53:83:00:10:5D:D4:37:64:FD:E7:D0:F5:ED:5B:C0

Each site's authentic security certificate fingerprint (shown above) was just now obtained by GRC's servers from each target web server. If your web browser sees a different fingerprint for the same certificate (carefully verify the Certificate Name is identical) that forms strong evidence that something is intercepting your web browser's secure connections and is creating fraudulent site certificates.

Custom Site Fingerprinting

In addition to the well-known web sites listed above, GRC's web server can obtain and display the "fingerprint" of any HTTPS-capable public web server's secure connection certificate. Simply enter the domain name of the server you wish to fingerprint, then press Enter or click the "Fingerprint Site" button:

https:// [ ] Fingerprint Site

Google and Apple are different: Some visitors are being confused by Google's and Apple's certificate fingerprints which change and may not match. Please see the "What can go wrong with this test?" section at the bottom of this page for an explanation of the complexities.

Des problèmes persistent pour l'utilisation de certificat

Lacune du côté technique :

- la révocation des certificats est basée sur une liste qu'il faut **télécharger régulièrement**, ceci est contraignant et lourd.
  Des standards, comme OCSP, «*Online Certificate Satus Protocol*» permettent d'accéder à cette liste dynamiquement et automatiquement et ils sont implémentés dans Firefox ou Internet Explorer mais aussi dans les serveurs par exemple (Apache).

La confiance peut être un danger

Toute la mécanique de la PKI nécessite des procédures strictes et sérieuses (dans la gestion des certificats…) pour assurer les garanties qui sont affichées.

Mais si les procédures ne sont pas fiables, il y aura des malversations, des faux certificats…

Si ces incidents sont trop nombreux, alors plus personne ne fera confiance aux certificats et ceux-ci n'auront plus aucune valeur.

Ce sera la mort des certificats.

Pas de service public

Tout le secteur est totalement **libéralisé**, il est complètement laissé aux entreprises privées.

Or, celles-ci peuvent avoir tendance à négliger les procédures (coûteuses) pour un profit à court terme.

Des certifications et des vérifications par des organismes gouvernementaux sont mis en place dans certains pays, mais pas partout et ils tardent à s'imposer.

Il n'y a par exemple pas encore d'autorité de certification gouvernementale française...

Mais parfois ce sont les états qui créent des «vrais/faux» certificats pour espionner leurs citoyens !

Un projet ambitieux d'entreprise

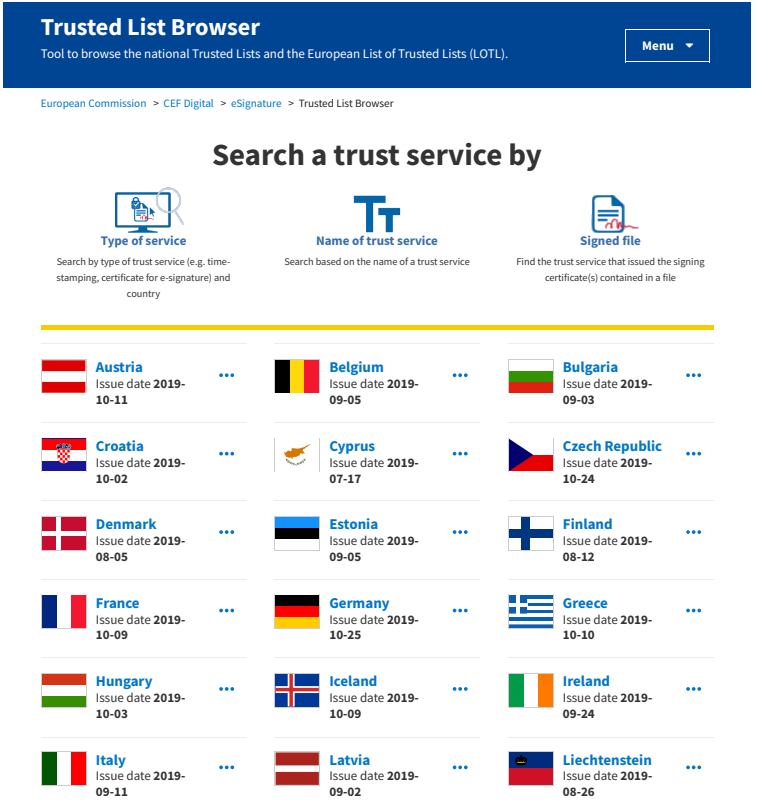
Pour une entreprise la démarche est lourde et pas toujours nécessaire :

- pour signer des e-mails ou faire du chiffrement, il existe des méthodes plus légères (PGP ou GPG)
- pour participer à des places de marché, fédérer ses fournisseurs ou ses partenaires, ou unifier les fonctions de signature électronique, alors la PKI est **nécessaire** au sein de l'entreprise.

La liste des Autorités de certification en Europe

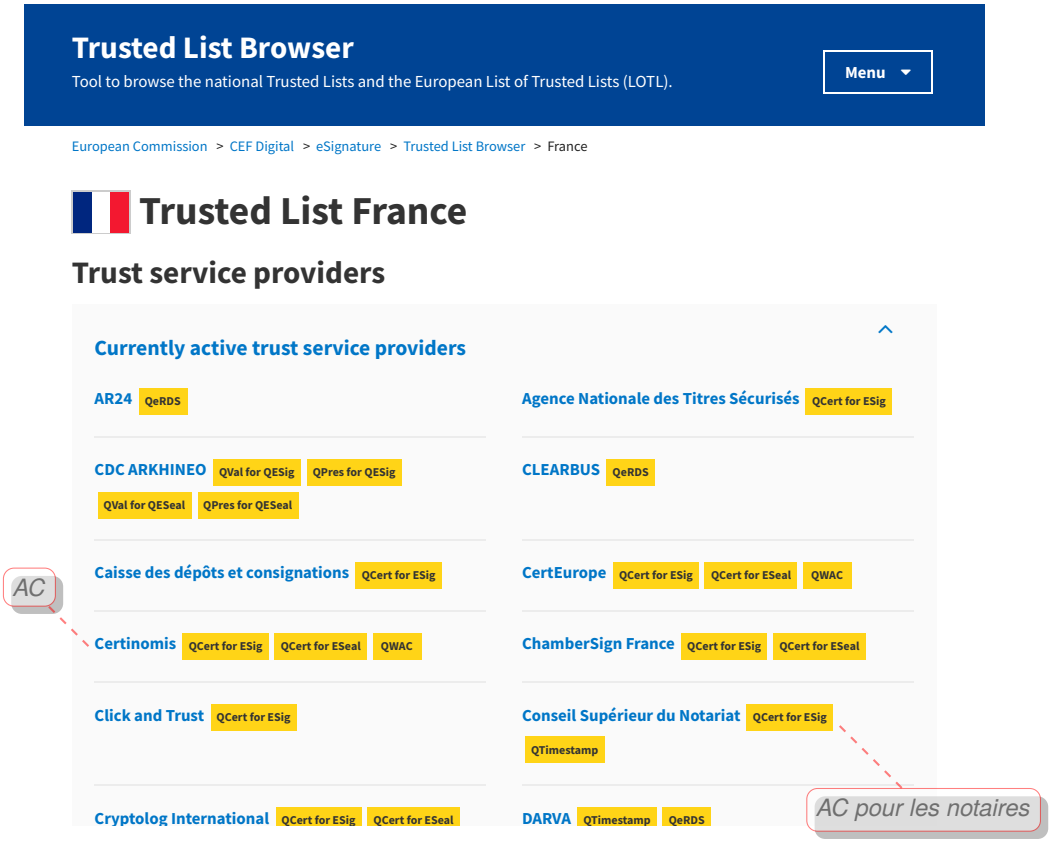
Une liste des différentes Autorités compilée par l'Europe est accessible à :

https://webgate.ec.europa.eu/tl-browser/####/



La liste des Autorités de certification en France

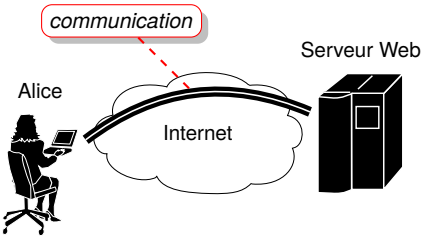
https://webgate.ec.europa.eu/tl-browser/####/tl/FR



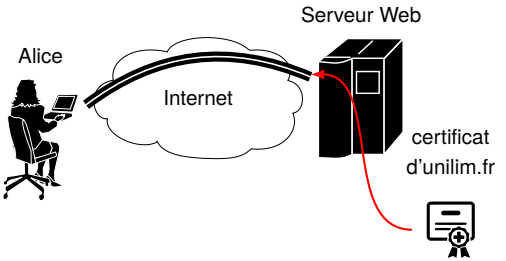
Alors plus de problèmes ?

La connexion httpS : un «*tiers de confiance*» est nécessaire

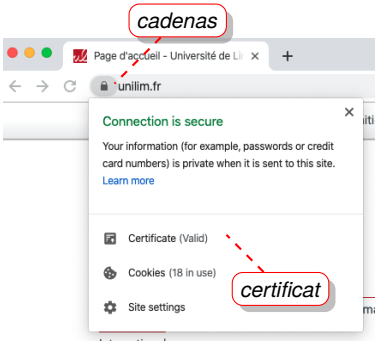
Alice veut consulter le site de l'Université de Limoges :
Elle se connecte à https://www.unilim.fr/

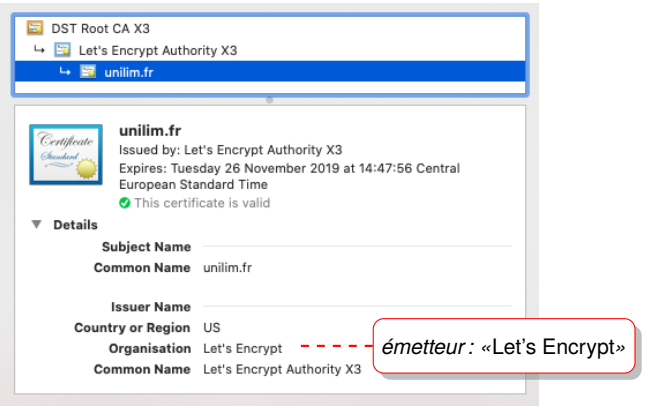


Dans la communication, le serveur Web envoie son «*certificat*» :



Dans son navigateur, elle voit un cadenas qui lorsqu'elle clique dessus, lui indique que le «*certificat*» est valide :



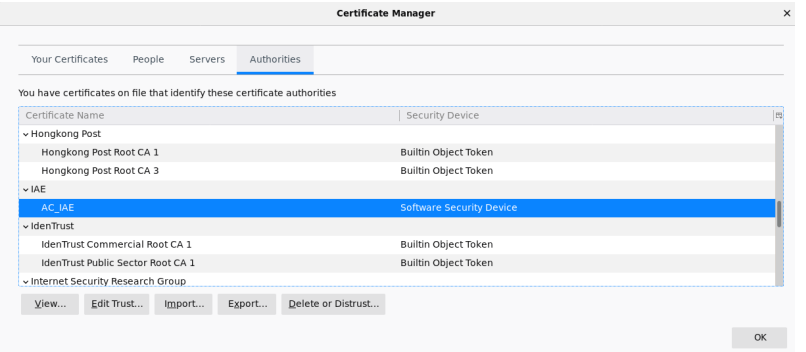


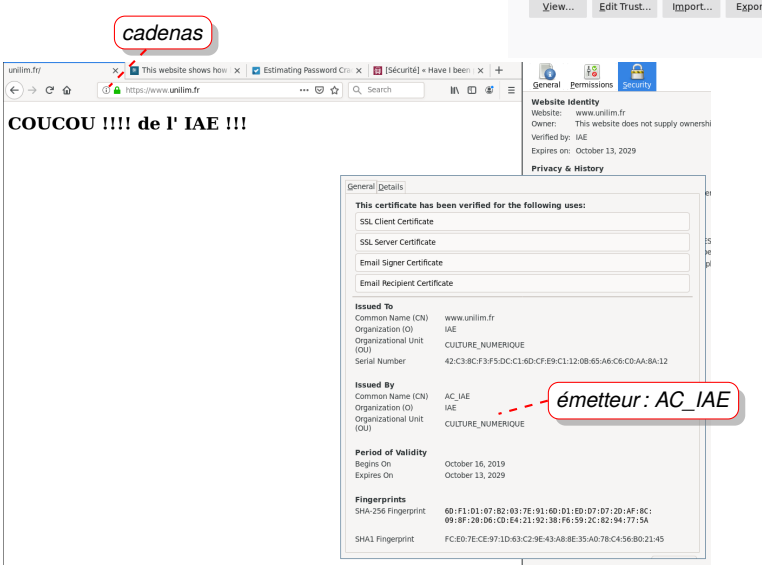
- ☐ Le certificat **authentifie** le site «*www.unilim.fr*» ;
- ☐ Le certificat est émis par l'organisation «*Let's Encrypt*» ;

⟹ Let's Encrypt est un **tiers de confiance** entre Alice et «*www.unilim.fr*» !

Alice s'est absentée et a laissé son poste de travail sans protection.

À son insu, j'installe un nouveau **tiers de confiance**, «*AC_IAE*» dans son navigateur Firefox :





Lorsqu'elle revient et consulte le site «*www.unilim.fr*», elle trouve un message «*Coucou !!!*» à la place de la page de l'Université.

⟹J'ai ajouté un «*Tiers de confiance*» qui donne de la **confiance** à mon mon **faux site** «*www.unilim.fr*» à l'aide d'un **faux certificat** !

⟹**La confiance d'Alice a été trahie !**