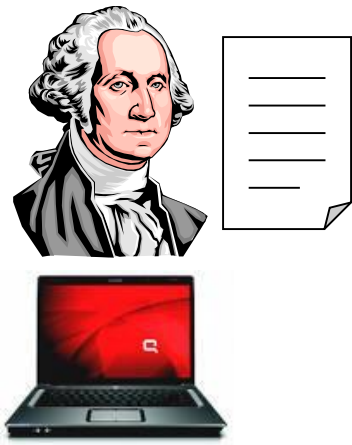


LES MÉCANISMES DE SECURITÉ

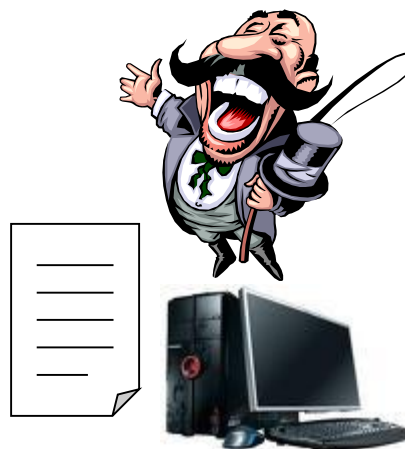
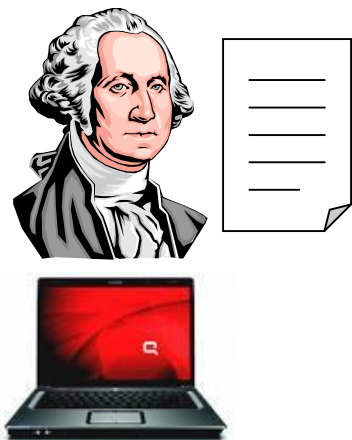
2021

Préambule

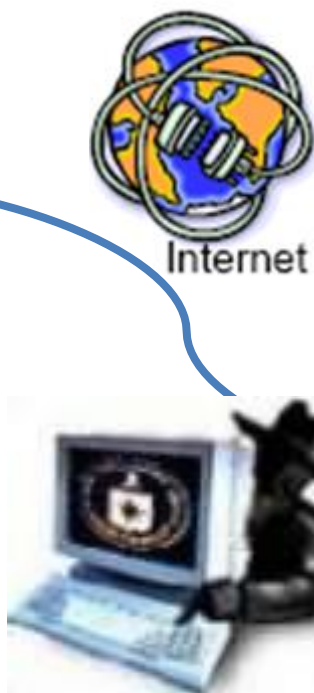
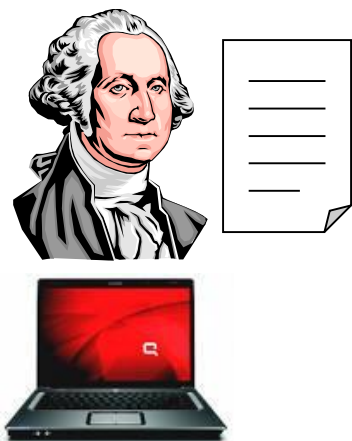


Le scénario...

Envoi de emails
Surf sur le web
Transactions bancaires
Téléchargements
Téléphonie sur IP
...



Les acteurs (les bons)...



Protéger les communications
les transactions
tout transfert de documents



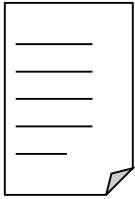
Le méchant...

<http://www.digitalattackmap.com>

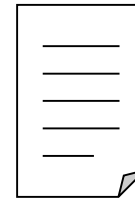
<http://map.norsecorp.com/#/>

<http://cybermap.kaspersky.com/>





Les protocoles doivent assurer...



Confidentialité

Maintenir le secret

Authentification

Vérifier l'identité de l'émetteur et celle du récepteur

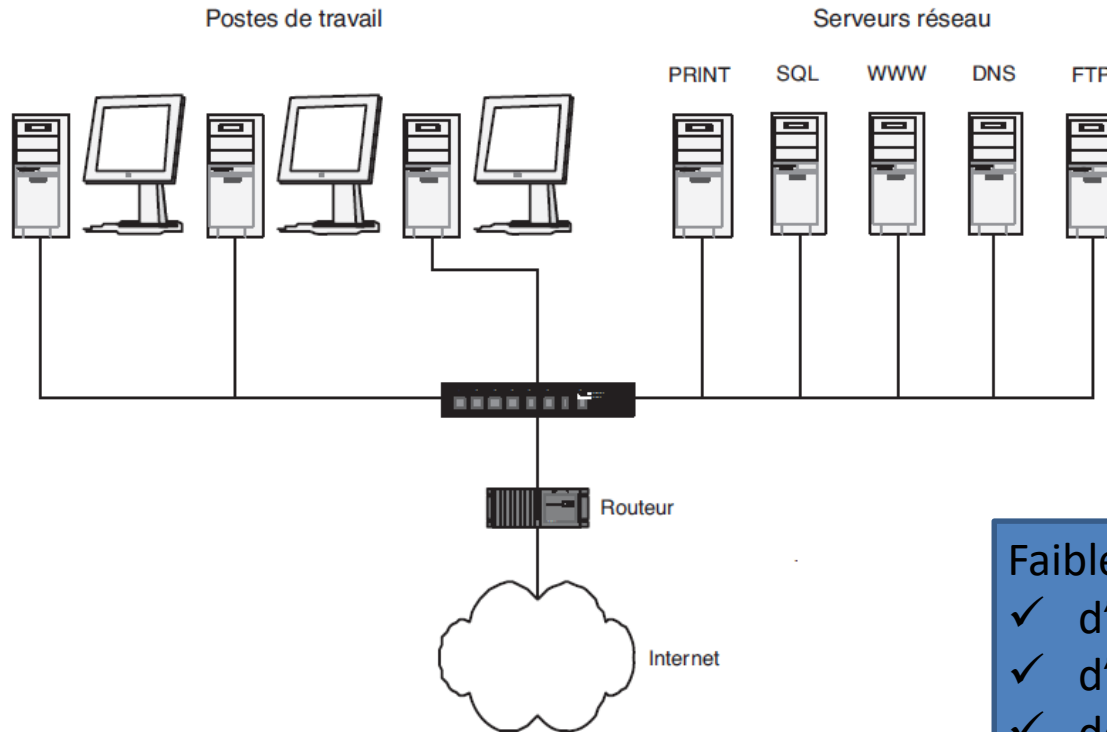
Intégrité

Détecter la modification des données

Non Répudiation

L'émetteur ne peut pas nier avoir émis le message

Ce qu'il ne faut pas faire !



Faiblesses des protocoles

- ✓ d'authentification
- ✓ d'implémentation
- ✓ de configuration

- Le câblage favorise l'écoute frauduleuse et donc la capture des informations sensibles qui transitent entre machines
- Pas de cloisonnement du réseau → écoute de l'ensemble des communications
- Les protocoles utilisés sont fragiles : FTP, TELNET, IMAP, HTTP
- Pas d'outils de surveillance
- La gestion des accès au réseau en entrée de site est inexistante

la sécurité du protocole IP en question

Lorsqu'ils ont été conçus, le protocole IP et les protocoles associés (TCP, UDP, ICMP, routage...) n'ont pas pris en compte la sécurité

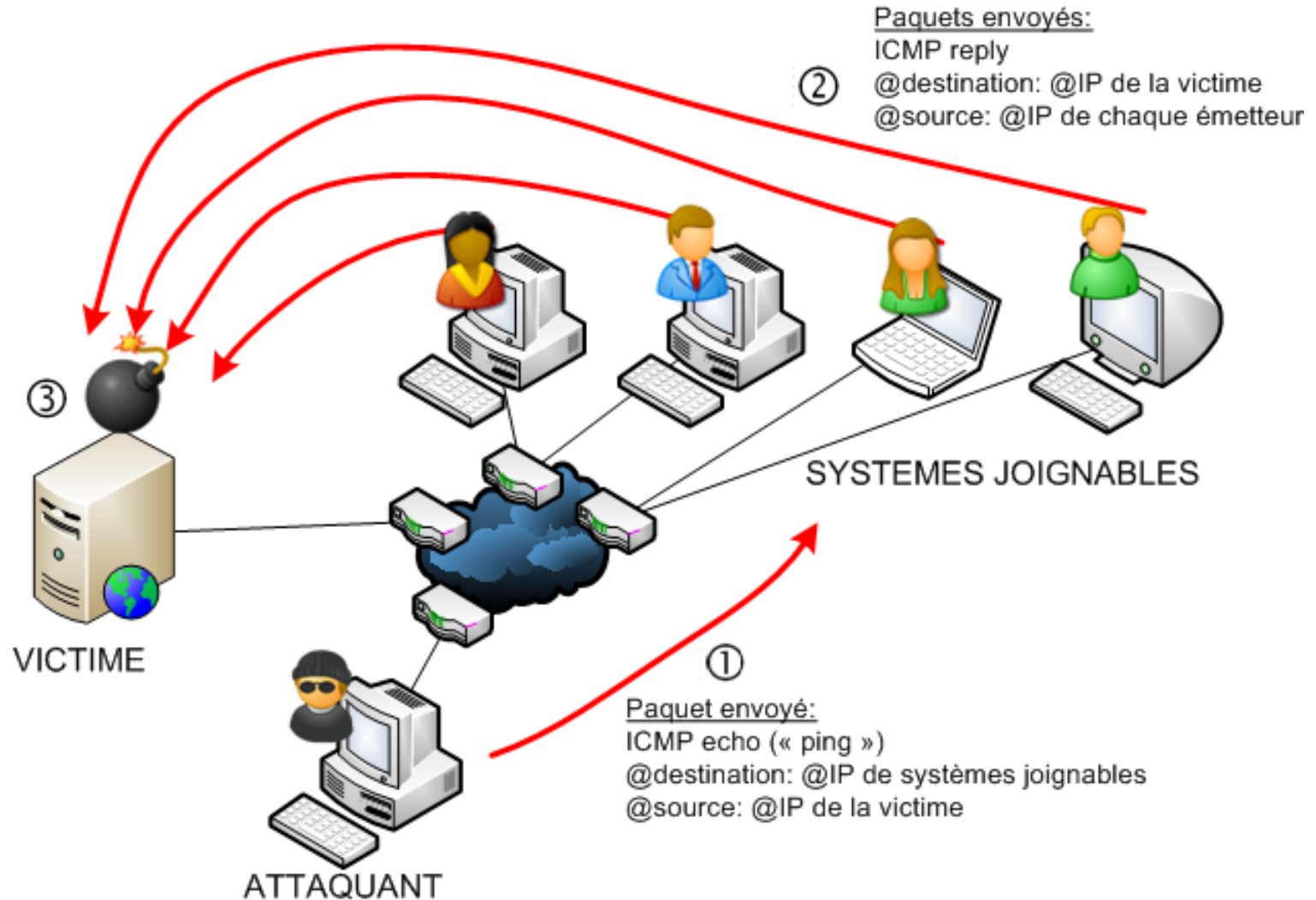
- « Concept sécurité » inconnu à l'époque, personne n'imaginait que ces protocoles pourraient être détournés à des fins malveillantes ;
- **Aucun mécanisme de sécurité n'est donc implémenté au sein de ces protocoles.**

Quelques exemples de faiblesses de ces protocoles

- **Absence d'authentification des émetteurs et récepteurs** d'un datagramme : usurpation d'adresse IP possible ;
- **Absence de chiffrement des données**, celles-ci sont donc transmises en clair. Un hacker positionné sur un réseau peut donc écouter les connexions et accéder aux données ;
- **Le routage des datagrammes peut être modifié** de façon à rediriger les datagrammes vers un autre destinataire ;
- Note : l'exploitation de ces faiblesses nécessite des prérequis techniques, i.e. elles ne sont pas systématiquement applicables à tous les réseaux.

Les diapositives suivantes illustrent le problème de l'authentification.

Exemple d'attaque par réflexion



Exemple d'attaque par réflexion

But de l'attaque

- porter atteinte aux performances d'un système cible (dédi de service).

Quelles sont les caractéristiques de l'attaque ?

- usurpation d'adresse IP ;
- réflexion de trafic en ayant recours à des systèmes tiers « innocents ».

Séquences de l'attaque

- ① Un attaquant envoie des paquets PING à des systèmes tiers joignables en indiquant l'@IP de la future victime comme @IP source ;
- ② Chaque système pense ainsi recevoir un PING de la part d'un système distant, et chacun va répondre à ce PING ;
- ③ Avec suffisamment de ressources, l'attaquant sera en mesure de faire générer suffisamment de trafic pour affecter les performances de la victime.

```
sendp(Ether(src='00:0a:f7:4d:59:58',dst='00:50:b6:0d:65:37')/IP(src='192.168.0.173',dst='192.168.0.41')/ICMP())
```

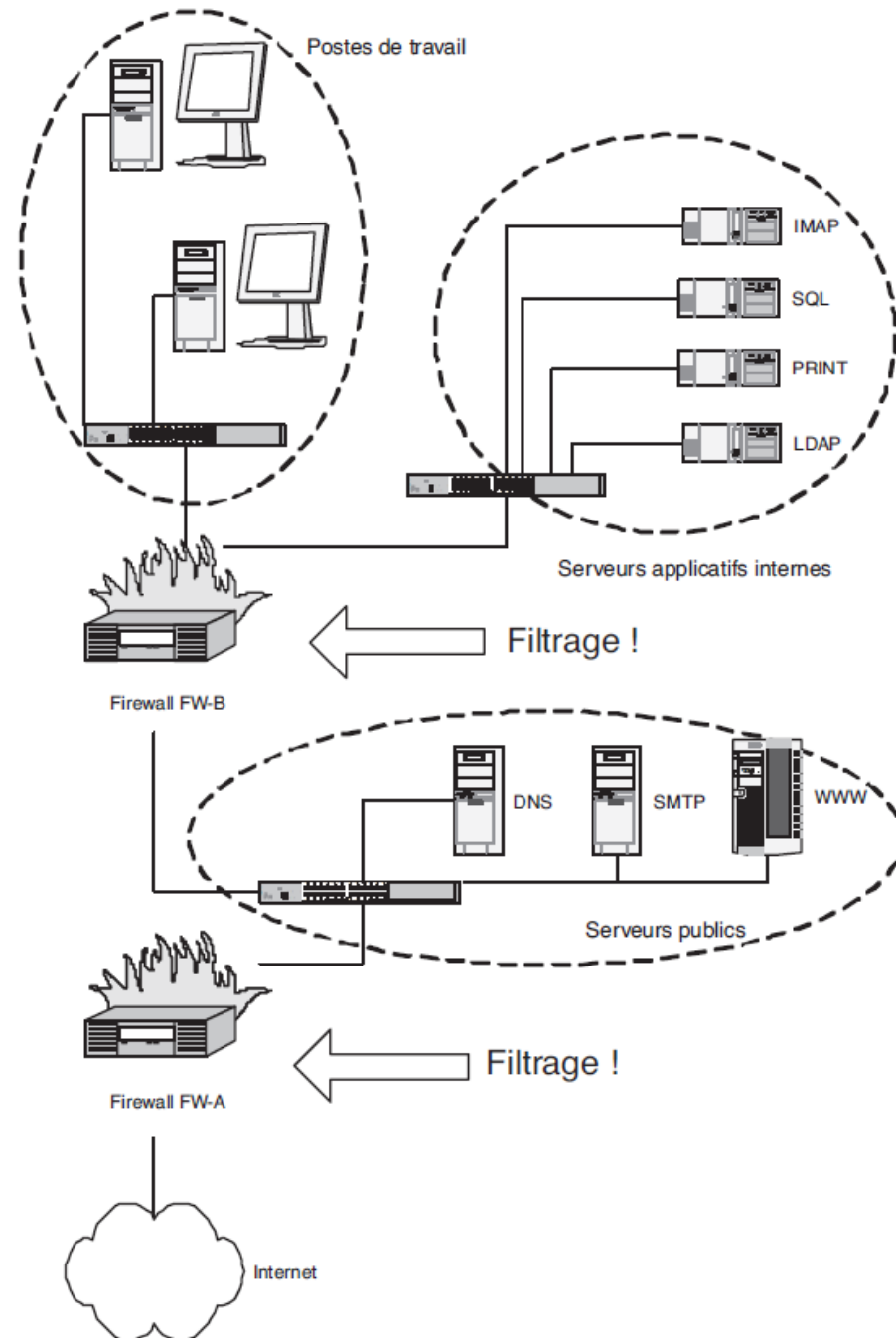
```
192.168.0.41 → 192.168.0.173 ICMP Echo (ping) reply
```


Exemple d'une petite architecture PME/TPE

Les postes de travail sont invisibles depuis l'extérieur

Les serveurs d'applications à usage interne sont isolés du monde
Ils ne seront accessibles que par les postes de travail du personnel ou par l'intermédiaire des machines offrant les services publics

DNS, HTTP, FTP, MAIL : accès depuis l'extérieur autorisé mais contrôlé



Encapsulation de protocoles Insécurisés

SSH (Secure Shell) :

sécurise les connexions Interactives et les transferts de fichiers entre machines

OpenSSH : ensemble d'outils informatiques Libres permettant des communications sécurisées en utilisant le protocole SSH

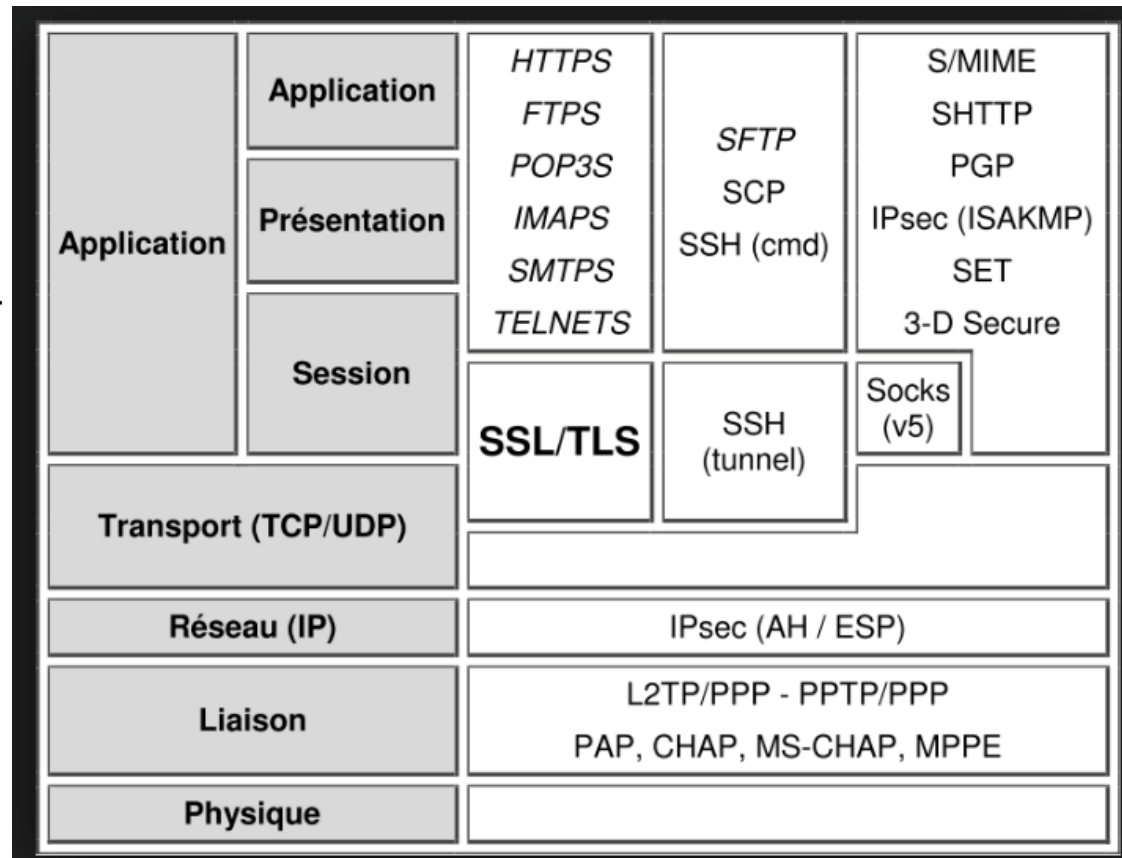
OpenSSL (Open Secure Sockets Layers):

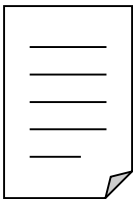
sécurise les accès aux informations confidentielles diffusées par le serveur Web et le serveur IMAP

Boite à outils de chiffrement comportant

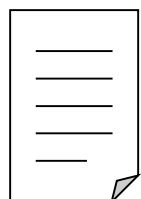
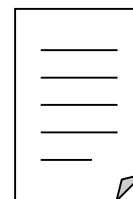
- deux bibliothèques cryptographie générale implémentant le protocole SSL
- une commande en ligne

SOCKS est un protocole réseau qui permet à des applications [client-serveur](#) d'employer d'une manière transparente les services d'un [pare-feu](#).
SOCKS : « [sockets](#) » et « *Secured Over Credential-based Kerberos* ».





Protéger les communications
les transactions
les documents multimédias



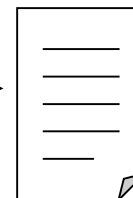
Chiffrement

- »gr
^e(\$
^ù*
%£μ!

... grâce aux mécanismes de sécurité

- »gr
^e(\$
^ù*
%£μ!

Déchiffrement



Mécanismes de sécurité

Les protocoles et les outils cryptographiques

Exercice 1

On distingue généralement trois grandes catégories de procédés d'authentification, parfois dénommées, « je sais », « je possède » et « je suis ».

Donnez un exemple de système d'authentification pour chacune de ses catégories.

Exercice 1

On distingue généralement trois grandes catégories de procédés d'authentification, parfois dénommées, « je sais », « je possède » et « je suis ».

Donnez un exemple de système d'authentification pour chacune de ses catégories.

Je sais	Je possède	Je suis
<ul style="list-style-type: none">• Couple login / mot de passe• Passphrase• Code secret• Code pin• ...	<ul style="list-style-type: none">• badge• Carte à puce• Carte magnétique• Token• ...	<ul style="list-style-type: none">• Biométrie empreintes digitales, de la main, IRIS, visage,...• Comportement• Statut : droit et privilège• ...

Exercice 2

Alice et Bob veulent transmettre un message sur une ligne non sécurisée. Alice possède un cadenas pour fermer un coffre et deux clés pouvant l'ouvrir. Ils peuvent se transmettre le coffre.

Proposez un protocole permettant l'échange de ce message.

Quel est l'inconvénient de ce protocole ?


Exercice 2

Alice et Bob veulent transmettre un message sur une ligne non sécurisée. Alice possède un cadenas pour fermer un coffre et deux clés pouvant l'ouvrir. Ils peuvent se transmettre le coffre.

Proposez un protocole permettant l'échange de ce message.

Quel est l'inconvénient de ce protocole ?

Comment créer une ligne sécurisée ?

- 
- 1 - Alice transmet sur une ligne sécurisée une clé à Bob
 - 2 - Alice place son message dans le coffre, ferme le coffre avec le cadenas
(→ chiffrement symétrique : Alice et Bob utilisent la même clé)
 - 3 - Alice transmet le coffre à Bob

Inconvénient : on doit créer une ligne sécurisée au préalable ...

Protocole incomplet

- vérifier que Bob l'a bien reçu
- vérifier que c'est bien Bob
- vérifier que seul Bob l'a bien reçu

Exercice 2 (suite)

Alice et Bob veulent transmettre un message sur une ligne non sécurisée et sans échanger de clés. Ils possèdent chacun une clé qu'ils ne peuvent donc échanger. Ils peuvent utiliser un coffre qu'ils peuvent s'envoyer. Ils possèdent chacun un cadenas que seule leur clé peut ouvrir.

Proposez un protocole permettant de transmettre un message en toute sécurité.

Exercice 2 (suite)

Alice et Bob veulent transmettre un message sur une ligne non sécurisée et sans échanger de clés. Ils possèdent chacun une clé qu'ils ne peuvent donc échanger. Ils peuvent utiliser un coffre qu'ils peuvent s'envoyer. Ils possèdent chacun un cadenas que seule leur clé peut ouvrir.

Proposez un protocole permettant de transmettre un message en toute sécurité.



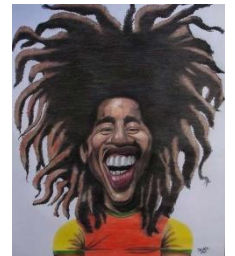
1 - Alice place son message dans le coffre, et le ferme avec son cadenas

2 – Alice transmet le coffre à Bob

3 – Bob place son cadenas sur le coffre et transmet le coffre à Alice

4 – Alice enlève le cadenas et transmet une nouvelle fois le coffre à Bob

5 – Bob enlève le cadenas avec sa clé et prend le message



Exercice 2 (suite)

Alice et Bob veulent transmettre un message sur une ligne non sécurisée et sans échanger de clés. Ils possèdent chacun une clé qu'ils ne peuvent donc échanger. Ils peuvent utiliser un coffre qu'ils peuvent s'envoyer. Ils possèdent chacun un cadenas que seule leur clé peut ouvrir.

Proposez un protocole permettant de transmettre un message en toute sécurité.

Protocole refusé !

Inconvénient : protocole long

Protocole incomplet (confidentialité uniquement)

- *Bob doit être sûr que l'expéditeur est bien Alice*
- *Il n'existe pas de preuve de liens entre Alice et sa clé, ni entre Bob et sa clé*
- *problème de non répudiation*

Exercice 2 (suite)

Bob possède maintenant plusieurs cadenas identiques qu'il peut diffuser.
Proposez un protocole qui utilise cette possibilité de diffusion et qui permet moins de trajets

Exercice 2 (suite)

Bob possède maintenant plusieurs cadenas identiques qu'il peut diffuser.
Proposez un protocole qui utilise cette possibilité de diffusion et qui permet moins de trajet

Protocole incomplet (confidentialité seulement)

- être sûr du lien entre le cadenas et Bob (preuve de son identité)
- être sûr qu'Alice est bien l'expéditeur
- problème de non répudiation

Protocole incomplet!
Mais début prometteur



- 2 - Alice ferme le coffre avec le cadenas de Bob
- 3 - Alice transmet le coffre à Bob



- 4 - Bob ouvre le coffre avec sa clé

Exercice 2 (suite)

Chiffrement asymétrique ou à clé publique.

En cryptographie, la clé publique équivaut au cadenas, qui est disponible par exemple dans des annuaires, tandis que la clé qui ouvre ce cadenas est la clé privée, détenue uniquement par leur propriétaire et qui n'est jamais divulguée.



2 - Alice demande **la clé publique** de Bob au serveur et chiffre le message avec cette clé

1 – Bob dépose **sa clé publique** sur un serveur de clé



3 – Bob utilise **sa clé privée** (qui a été générée avec **la clé publique**) pour déchiffrer le message.

Exercice 3

Un groupe de n personnes souhaite utiliser un système cryptographique pour s'échanger deux à deux des informations confidentielles. Les informations échangées entre deux membres du groupe ne devront pas pouvoir être lues par un autre membre. Le groupe décide d'utiliser un système symétrique de chiffrement.

Quel est le nombre minimal de clés symétriques nécessaires ?
Donnez le nom d'un algorithme de chiffrement symétrique reconnu.

Exercice 3

Un groupe de n personnes souhaite utiliser un système cryptographique pour s'échanger deux à deux des informations confidentielles. Les informations échangées entre deux membres du groupe ne devront pas pouvoir être lues par un autre membre. Le groupe décide d'utiliser un système symétrique de chiffrement.

Quel est le nombre minimal de clés symétriques nécessaires ?
Donnez le nom d'un algorithme de chiffrement symétrique reconnu.

Nombre de combinaison de 2
parmi n

$$C_2^n = \frac{n!}{2!(n-2)!} = \frac{n(n-1)}{2}$$

DES, TRIPLE-DES, AES,...

Exercice 3 (suite)

Le groupe décide ensuite de remplacer ce système par un système asymétrique.

Quel est le nombre minimal de couples de clés asymétriques nécessaires pour que chaque membre puisse envoyer et recevoir des informations chiffrées et/ou signées ?

Bob souhaite envoyer des informations chiffrées à Alice (Bob et Alice appartiennent tous les deux au groupe). Quelle clé Bob doit-il utiliser ?

Donnez le nom d'un algorithme de chiffrement asymétrique reconnu.

Exercice 3 (suite)

Le groupe décide ensuite de remplacer ce système par un système asymétrique.

Quel est le nombre minimal de couples de clés asymétriques nécessaires pour que chaque membre puisse envoyer et recevoir des informations chiffrées et/ou signées ?

Bob souhaite envoyer des informations chiffrées à Alice (Bob et Alice appartiennent tous les deux au groupe). Quelle clé Bob doit-il utiliser ?

Donnez le nom d'un algorithme de chiffrement asymétrique reconnu.

n personnes $\rightarrow 2n$ clés (clé privée/ clépublique)

$$2n \leq \frac{n(n-1)}{2} \Leftrightarrow n \geq 5$$

À partir de cette valeur le système asymétrique est plus économe en clé

Bob doit utiliser la clé publique d'Alice. Alice utilisera sa clé privée

Algorithme RSA



Comparaison

Chiffrement symétrique

Avantages

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

Inconvénients

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

Chiffrement asymétrique

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

- 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.

Exercice 3 (suite)...

Le groupe décide finalement d'utiliser un système hybride pour le chiffrement (c'est-à-dire qui utilise la cryptographie symétrique et asymétrique).

Donnez les raisons qui ont poussé ce groupe à utiliser un tel système.

Exercice 3 (suite)...

Le groupe décide finalement d'utiliser un système hybride pour le chiffrement (c'est-à-dire qui utilise la cryptographie symétrique et asymétrique).

Donnez les raisons qui ont poussé ce groupe à utiliser un tel système.

Le système symétrique est beaucoup plus rapide en temps d'exécution que le système asymétrique

Il nécessite cependant un canal sécurisé pour le partage de clé

Le système asymétrique (à clé publique) ne nécessite pas de canal sécurisé. Par contre il est beaucoup plus lent.

- on chiffre **la clé de session** avec **la clé publique** du destinataire (**chiffrement asymétrique**)
- le destinataire déchiffre la clé de session avec **sa clé privée**
- il peut ainsi déchiffrer le message avec la clé de session (**chiffrement symétrique**)



- Chiffrement

Objectif

- Consiste à modifier un message, ou un document, ou un fichier de nombre binaires de façon à le rendre inintelligible par un tiers qui ne possède pas l'outils requis

Moyen

- Recours à une opération mathématique, un algorithme de chiffrement, contrôlé par un code, une clé (key). Plus la clé est longue, plus le système est sûr.

Techniques

- **Chiffrement symétrique** : la clé de chiffrement est la même que la clé de déchiffrement : *AES (Advanced Encryption Standard) avec une clé de 128 bits*
- **Chiffrement asymétrique** : la clé de chiffrement qui peut être connue de tous, est différente de la clé de déchiffrement : paire de clé publique/clé privée) : *RSA (Rivest Shamir Adelman) avec des longueurs de clés de 1024 à 2048 bits.*



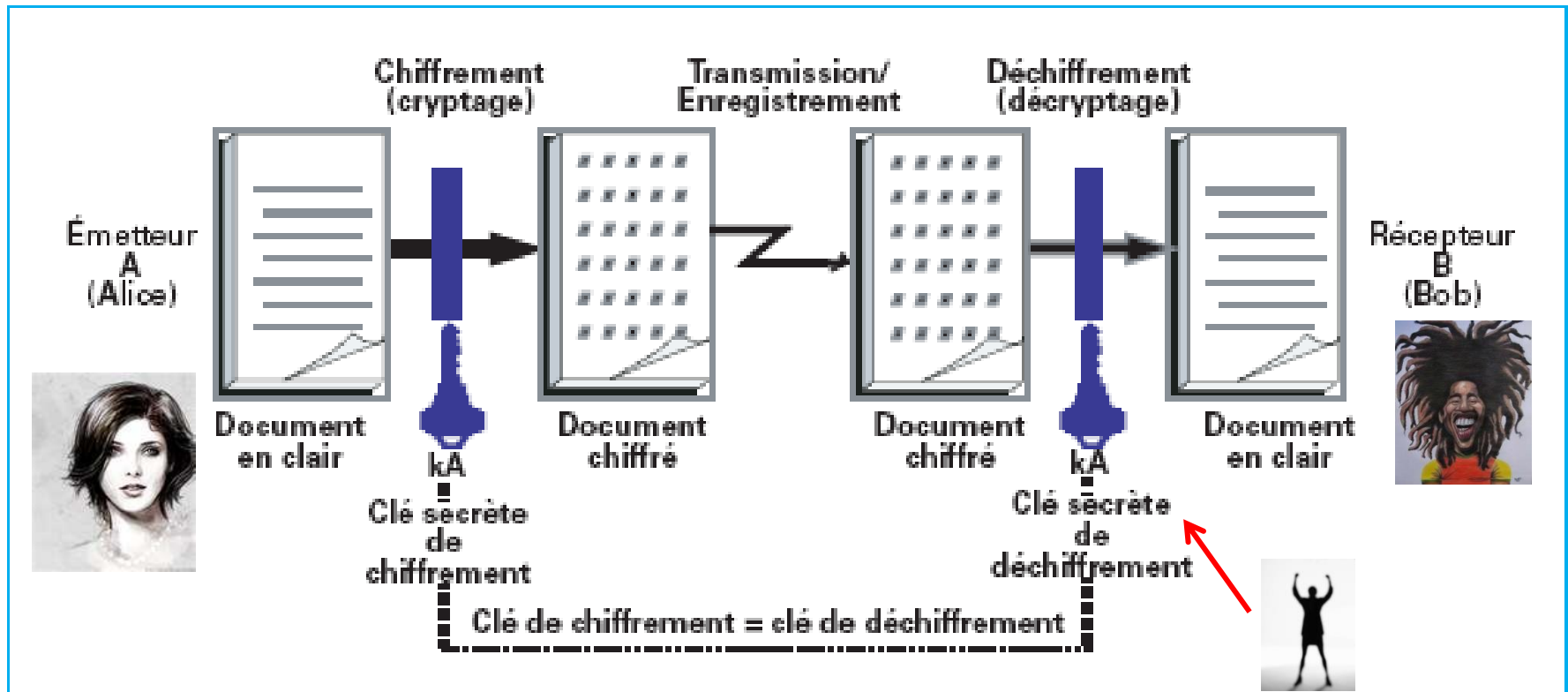
- Chiffrement symétrique

Le DES (Data Encryption Standard) : 56 bits (+ 6 bits de parité)

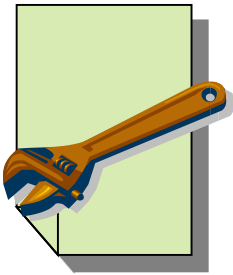
Le Triple DES : 3 applications successives de l'algorithme DES

L'AES (Advanced Encryption Standard) : successeur du DES

Le RC4 (Ron's Code {4}), mode de chiffrement d'une chaîne de caractère



- Chiffrement symétrique



Chiffrement du message M avec la clé K : $E_k(M)$

Déchiffrement avec la même clé K : $D_k(E_k(M)) = M$

```
mnenard@yabasic ~
$ echo "Ce contenu est confidentiel" > fichier.txt

mnenard@yabasic ~
$ ls
fichier.txt  xterm.exe.stackdump

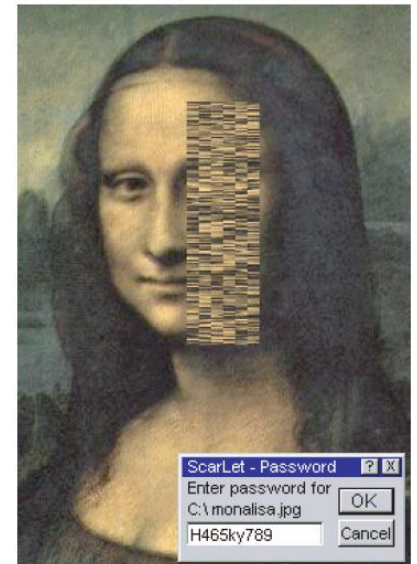
mnenard@yabasic ~
$ openssl rc4 -e -in fichier.txt -out crypto.dat
enter rc4 encryption password:
Verifying - enter rc4 encryption password:

mnenard@yabasic ~
$ more crypto.dat
Salted__1J;8i?+\\>T42

mnenard@yabasic ~
$ openssl rc4 -d -in crypto.dat -out fichier1.txt
enter rc4 decryption password:

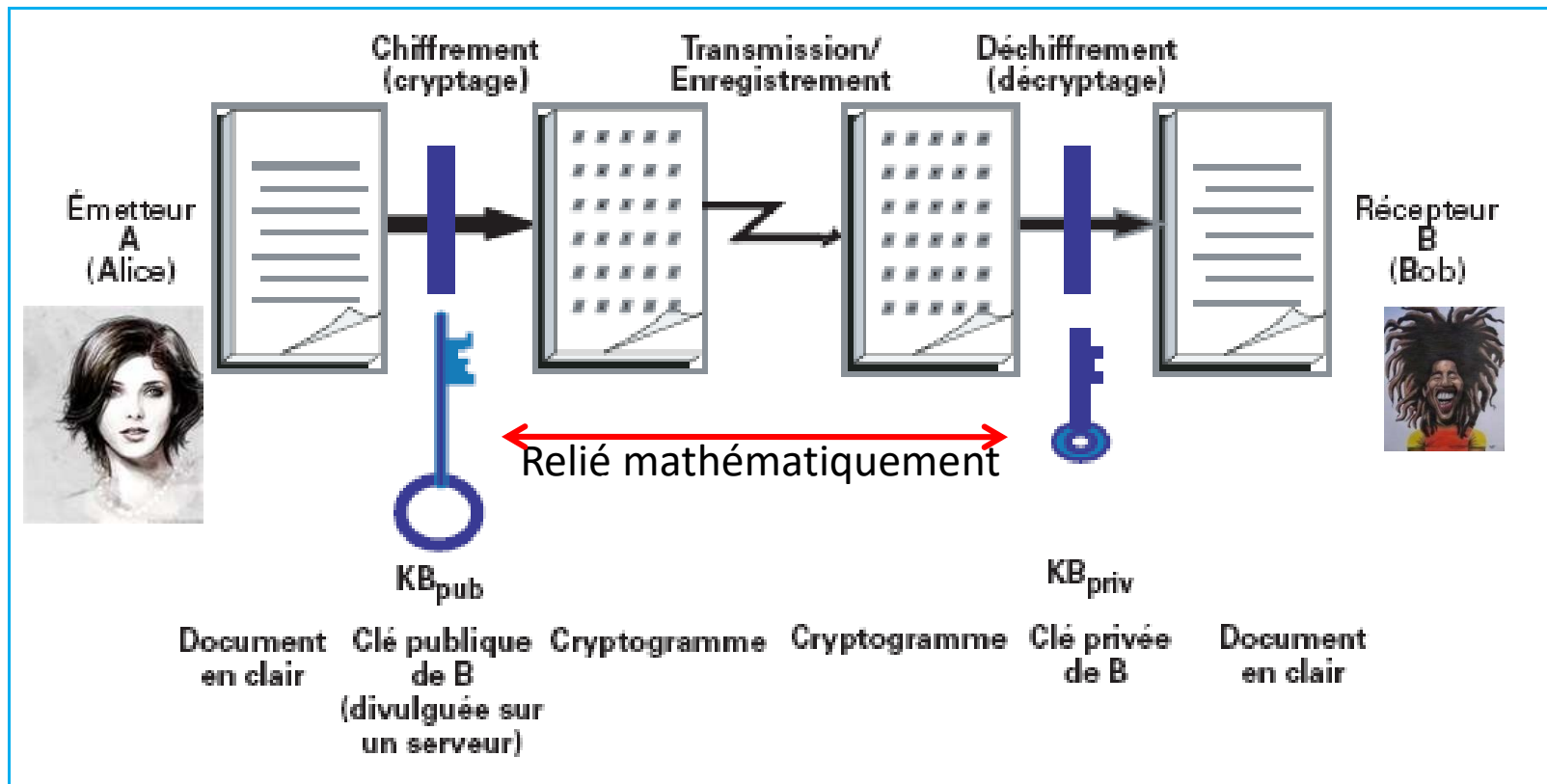
mnenard@yabasic ~
$ more fichier1.txt
Ce contenu est confidentiel

mnenard@yabasic ~
$
```





- Chiffrement asymétrique ou à clé publique
 - **pour transporter une clé symétrique (de session)** entre l'émetteur et le destinataire
 - pour créer des signatures numériques (inversement du rôles des clés)

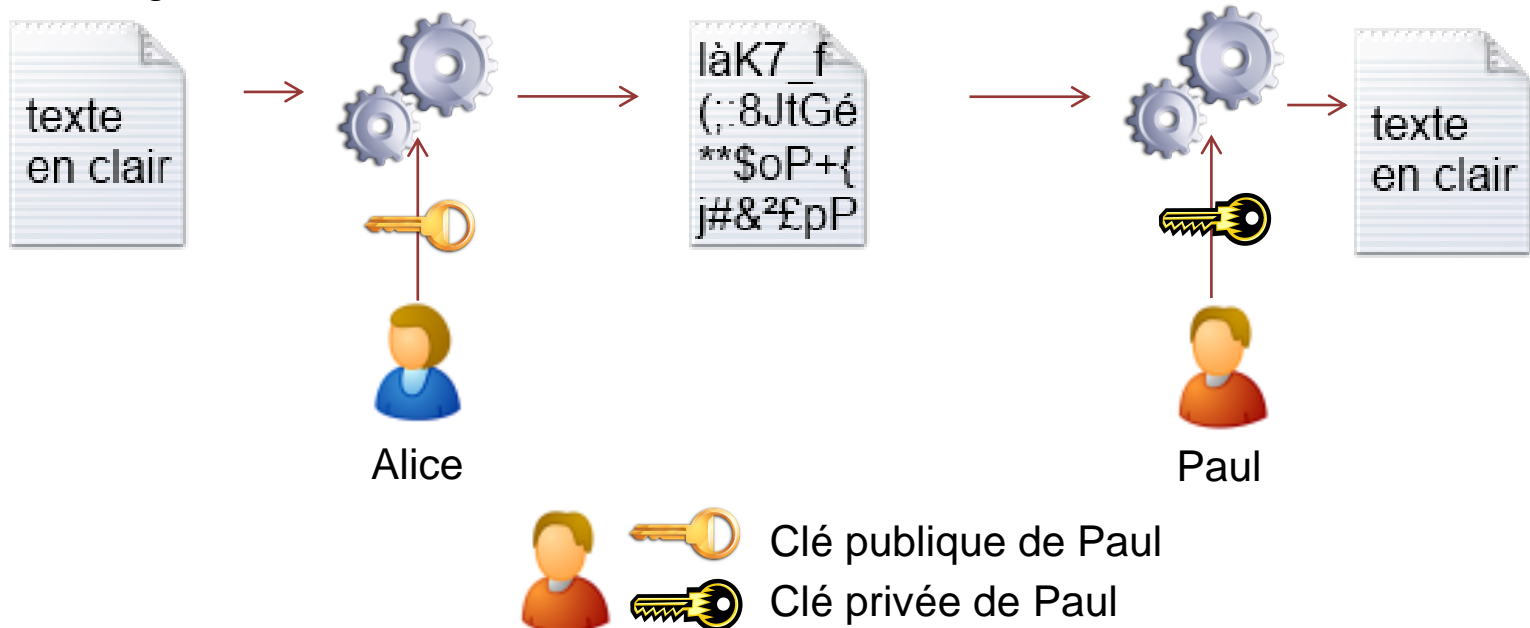




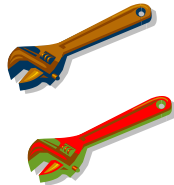
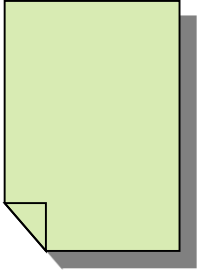
- Chiffrement asymétrique ou à clé publique

Exemple : Alice souhaite envoyer un **message** confidentiel à Paul (en général une clé)

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



- Chiffrement asymétrique ou à clé publique



clé publique

clé privée

générées par le même algorithme

Chiffrement du message M avec la clé publique du destinataire : $E_{k_{public}}(M)$

Déchiffrement avec la clé privée du destinataire : $D_{k_{privée}}(E_{k_{public}}(M)) = M$

- Chiffrement asymétrique ou à clé publique

```
hmenard@yabasic ~  
$ openssl genrsa -out cle.pem 1024  
Generating RSA private key, 1024 bit long modulus  
.....++++++  
.....++++++  
e is 65537 (0x10001)  
  
hmenard@yabasic ~  
$ openssl rsa -in cle.pem -pubout -out pub.pem  
writing RSA key  
  
hmenard@yabasic ~  
$ echo secret | openssl rsautl -inkey pub.pem -pubin -out crypto.dat -encrypt  
  
hmenard@yabasic ~  
$ more crypto.dat  
eK5JlL@l[?Q8?#  
UWNiMb u2;M/H?  
  
hmenard@yabasic ~  
$ openssl rsautl -inkey cle.pem -in crypto.dat -decrypt  
secret  
  
hmenard@yabasic ~  
$
```




- Le hachage : calcul d'empreinte, condensation et hash

Objectif

- Algorithme qui prend en entrée une donnée qui peut avoir n'importe quelle taille, et qui rend en sortie une chaîne d'octets de longueur fixe qui dépend de chacun des bits de l'entrée mais ne permet pas de retrouver l'entrée.

Moyen

- c'est une fonction mathématique irréversible et injective (one-way function ou checksum)

Techniques

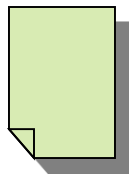
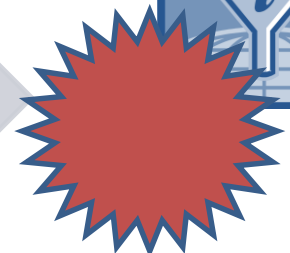
- L'algorithme de hash actuellement recommandé est SHA256 (pour Standard Hash Algorithm) 256 bits étant la taille des données obtenues en sortie.
- La sortie a une taille constante, indépendante de l'entrée.
- La sortie est pseudo-aléatoire, très dépendante de l'entrée.
- Le hash est une fonction à sens unique.

- Le hachage : calcul d'empreinte, condensation et hash

Propriétés de la fonction

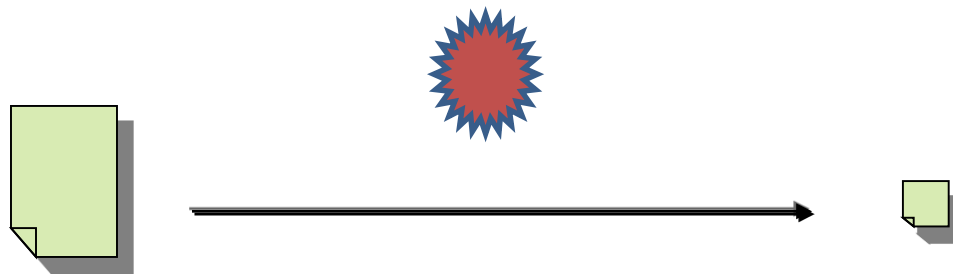
- Elle doit rendre impossible la reconstitution du document original à partir du condensé
- Elle doit rendre impossible l'obtention du même condensé à partir de deux documents distincts

SHA (Secure Hash Algorithm)
Message



- Le hachage : calcul d'empreinte, condensation et hash

SHA (Secure Hash Algorithm) SHA1, 256, 512
MD5 (Message digest)



```
C:\OpenSSL\bin>openssl dgst -sha1 -out empreinte file.txt
```

```
C:\OpenSSL\bin>more file.txt
```

Ce fichier va bientôt être crypté en utilisant OpenSSL

```
C:\OpenSSL\bin>more empreinte
```

```
SHA1(file.txt)= dbc25535351f4f8d7c034b1254e6d0f7b7c64709
```

Le hachage : calcul d'empreinte, condensation et hash (suite) :
sel et empreinte de mot de passe sous linux présents dans le
fichier /etc/shadow

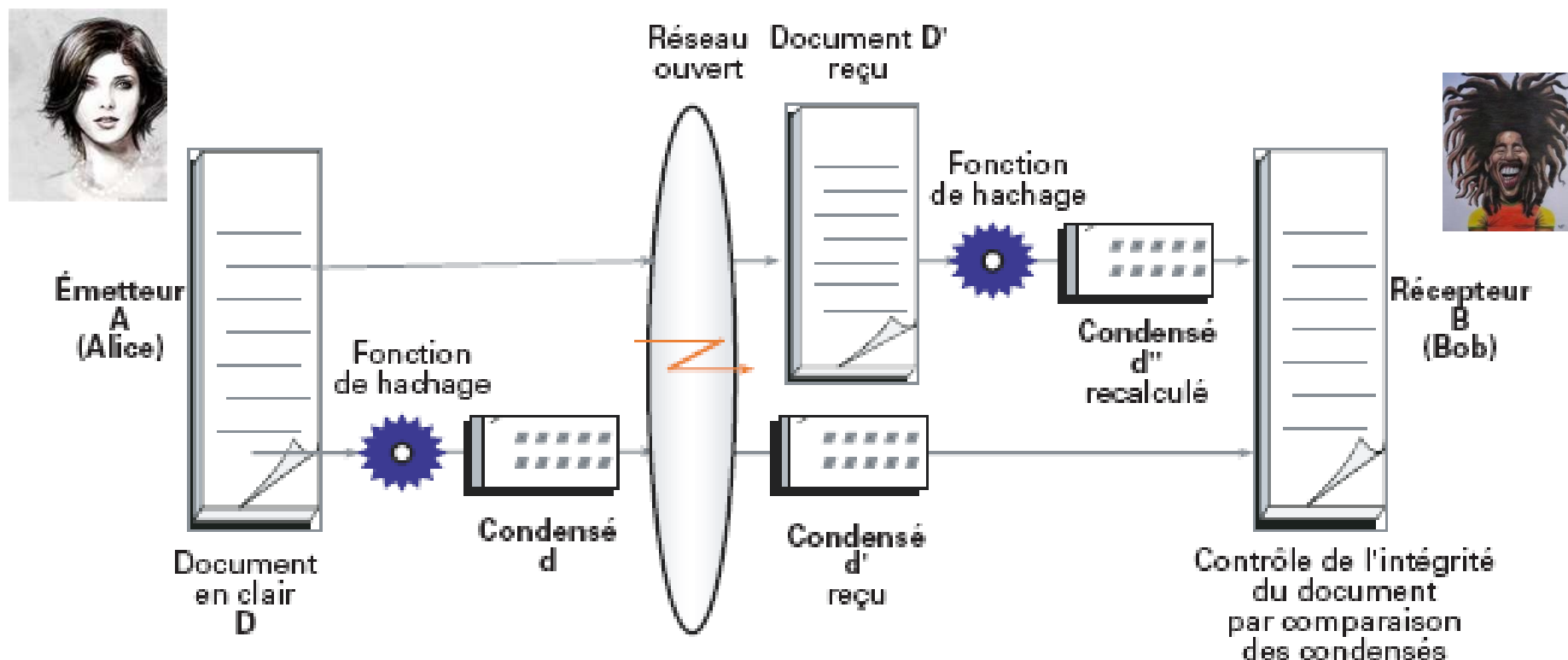
```
[root@arch01 ~]# cat /etc/shadow | sed 's/michael/test/' | sed 's/mbo/joe/'
root:$6$4GxAA08J$AB7vFkLSCxtVdVMcPav8jZ5u4ZsyG22hy1cqWPdnQgqL84VesJNQYFXSwhfwkhT
UeHNxYwjJUGe8U/sjITBhq/:16672::::::
bin:x:14871::::::
daemon:x:14871::::::
mail:x:14871::::::
ftp:x:14871::::::
http:x:14871::::::
uidd:x:14871::::::
dbus:x:14871::::::
nobody:x:14871::::::
systemd-journal-gateway:x:14871::::::
systemd-timesync:x:14871::::::
systemd-network:x:14871::::::
systemd-bus-proxy:x:14871::::::
systemd-resolve:x:14871::::::
systemd-journal-upload:!!:16672::::::
systemd-journal-remote:!!:16672::::::
avahi:!!:16672::::::
polkitd:!!:16672:0:99999:7:::
joe:$6$TA4PslzF$ch961z/ppk1VrmVAqSjSEdf75FIahttse1x/bsDdjSXLt8cmsIoX9eAKfVm8epuD
KGVYV1xkohA37aeEvmu8d1:16672:0:99999:7:::
git:!!:16683::::::
test:$6$PNkLwU7L$2Hm8YRMGgRoxxt4srAzGBZJFfxU7Sn1DbAUwb6APg5dyXSiQvQwSxHY1j0i5t2eM
kZ1PwBzY1aHAVZu29wSBpJ0:16735:0:99999:7:::
```



Les mécanismes principaux : INTEGRITE

- **Vérification d'intégrité d'un document par hachage**

- Association de l'information et du condensé.
- Le condensé peut être crypté.





Les mécanismes principaux : SIGNATURE

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

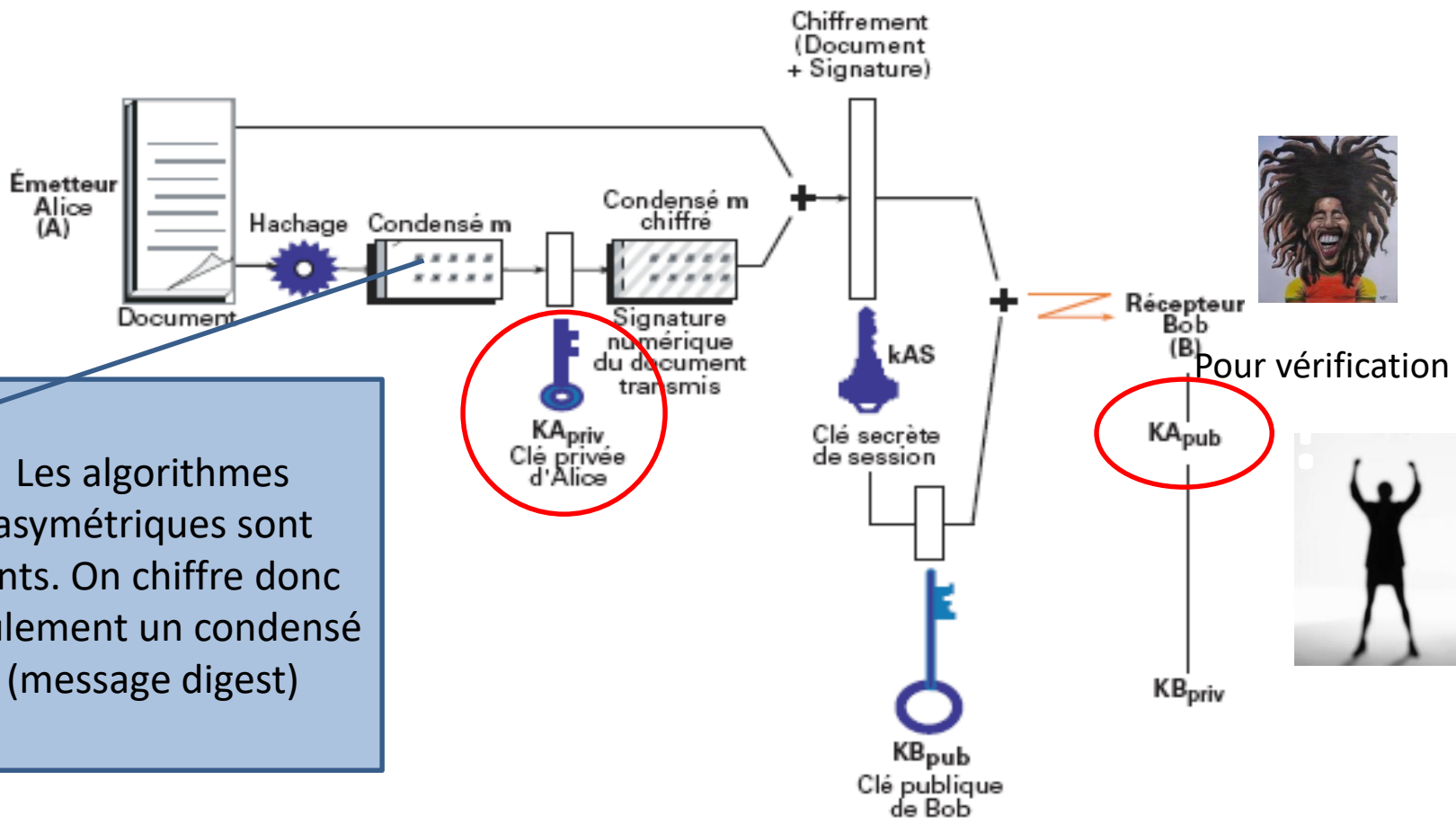
Notes :

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



- **Authentification de l'expéditeur d'un document par signature électronique**

- authentification et non-répudiation
- hachage + chiffrement asymétrique (les clés sont inversées)



Les algorithmes asymétriques sont lents. On chiffre donc seulement un condensé (message digest)

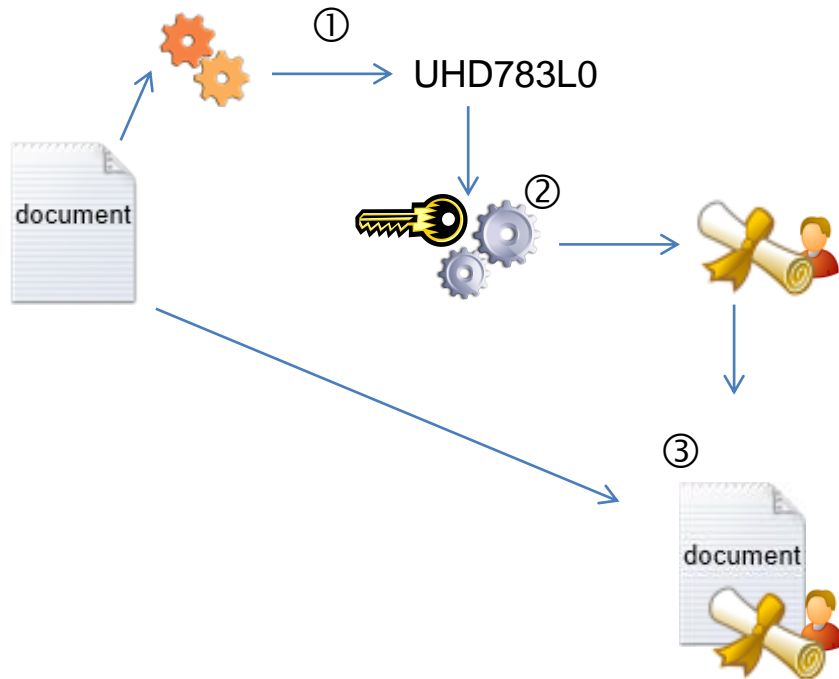


Principe de la signature

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



Principe de la signature



Etapes de la signature :

- ① Le signataire génère le condensat unique associé au message ;
- ② Le signataire utilise l'algorithme de signature, qui prend en entrée sa clé privée et le condensat précédent, pour produire une signature électronique ;
- ③ Le signataire envoie (ou stocke) le message et la signature électronique, permettant ainsi à un lecteur d'en prendre connaissance ;

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



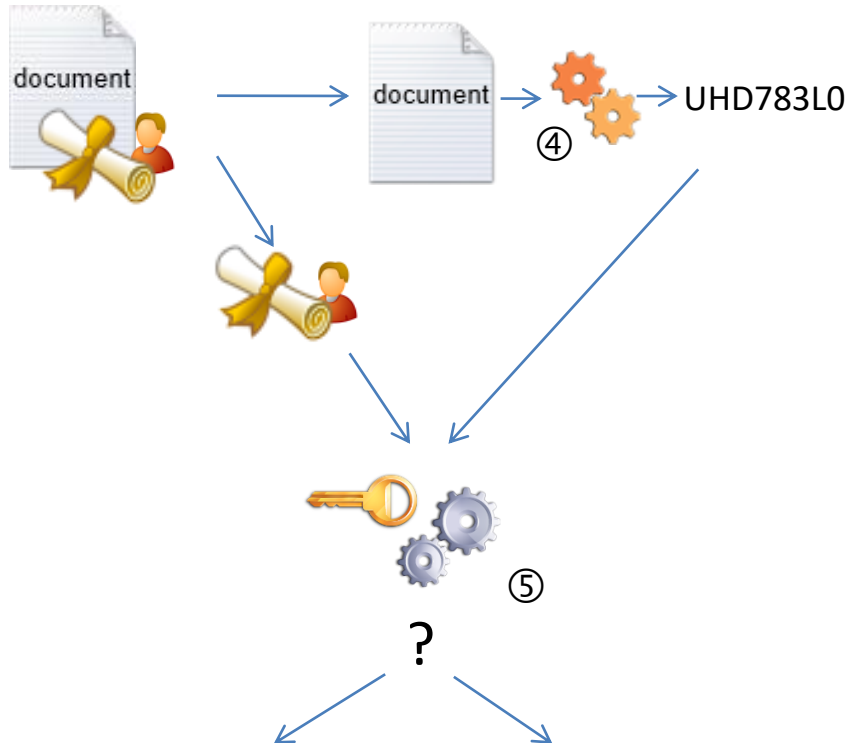
Clé publique du signataire



Clé privée du signataire



Principe de la signature



✓ La signature est valide. Le message est intègre.

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

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

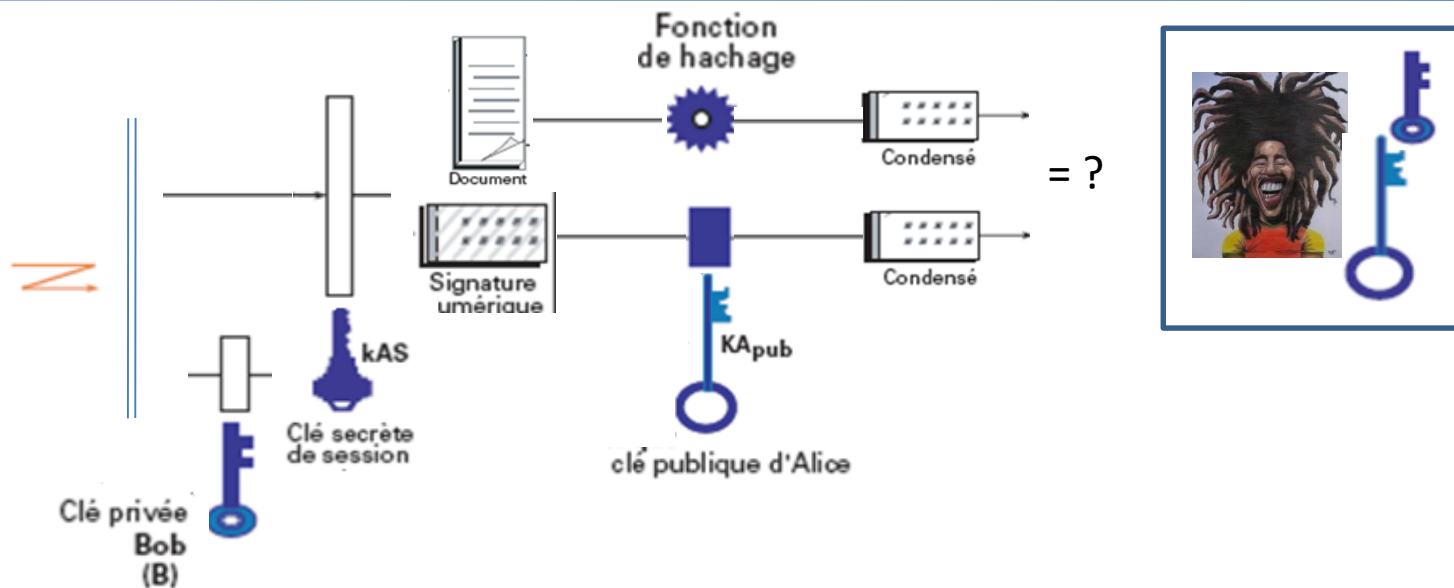
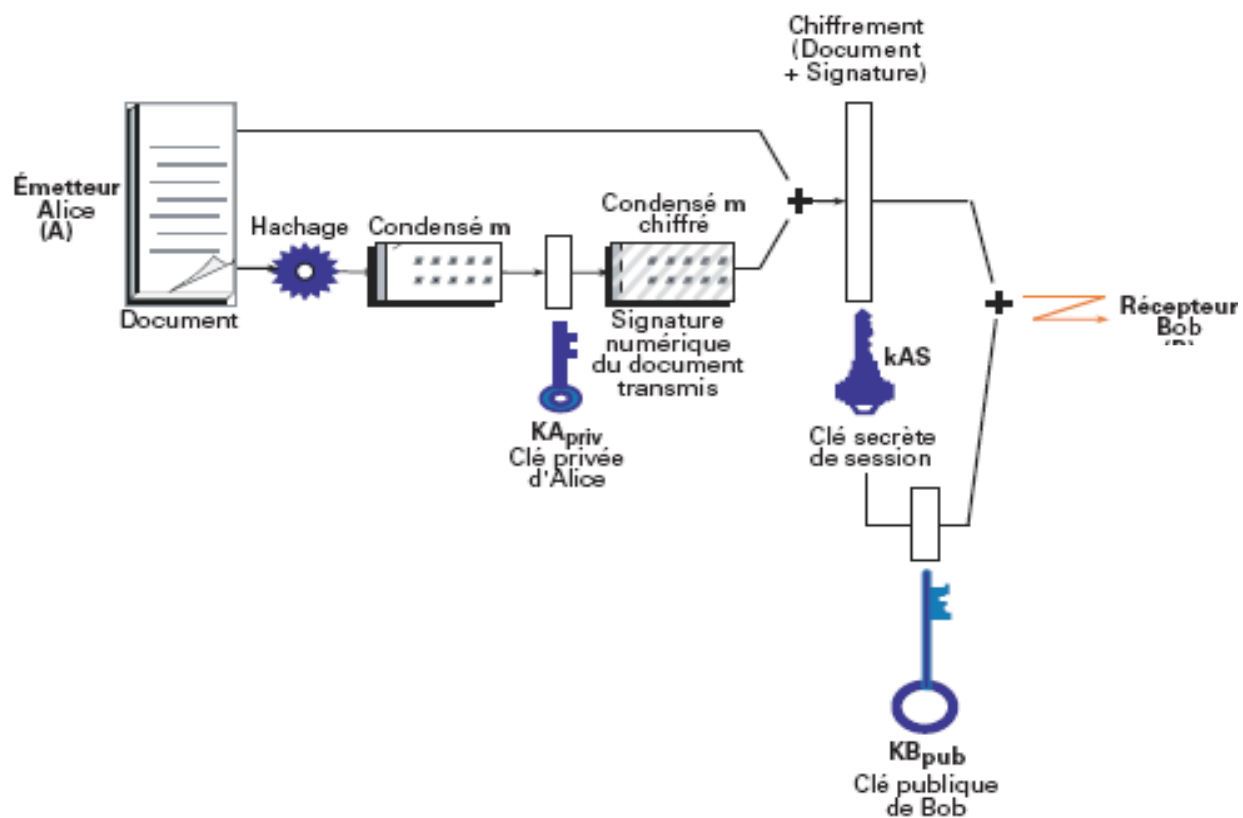
④ Le lecteur calcule le condensat du message en clair ;

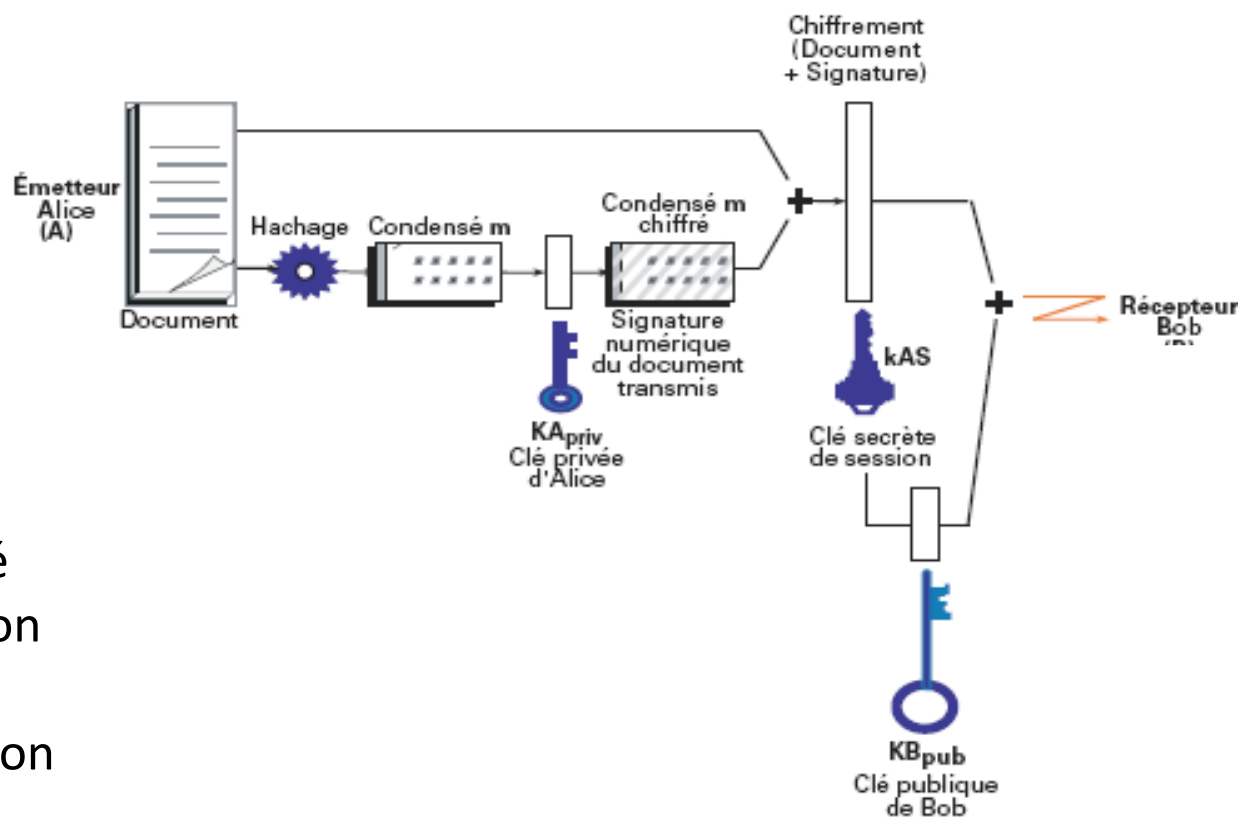
⑤ Le lecteur utilise l'algorithme de vérification de signature, qui prend en entrée la clé publique du signataire, le condensat et la signature, pour rendre un verdict. Si le verdict est négatif, alors il ne faut pas faire confiance au message reçu (celui-ci ne correspond pas — pour une raison que l'on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



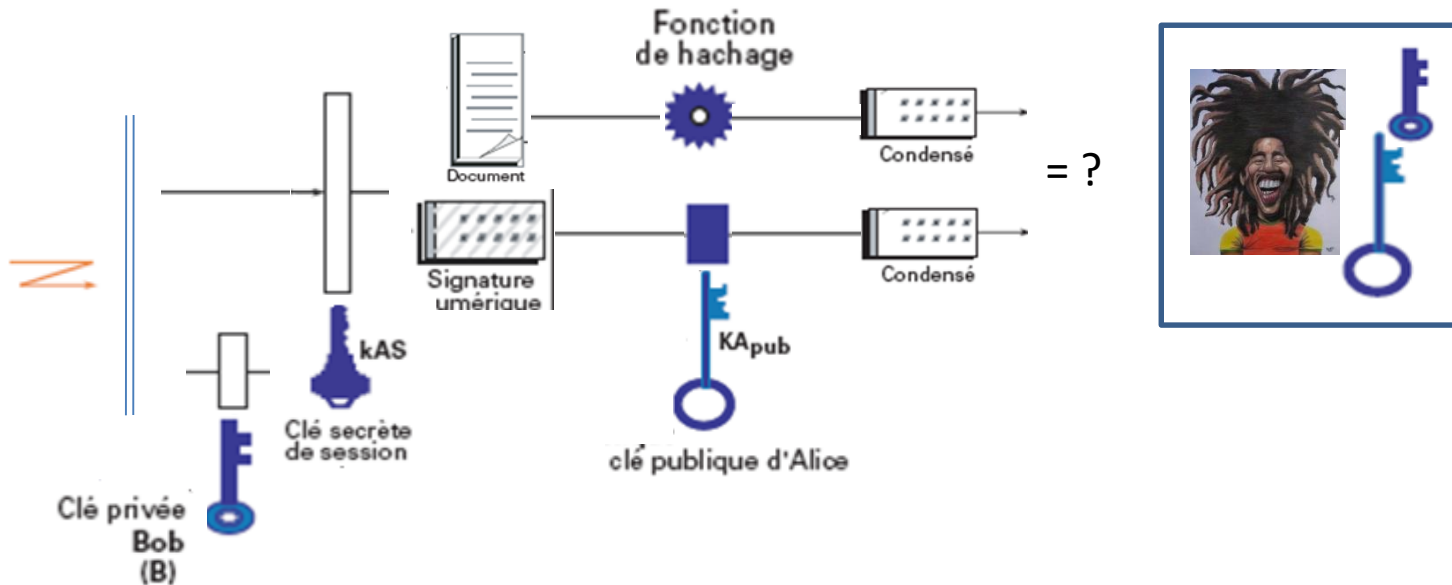
Clé publique du signataire

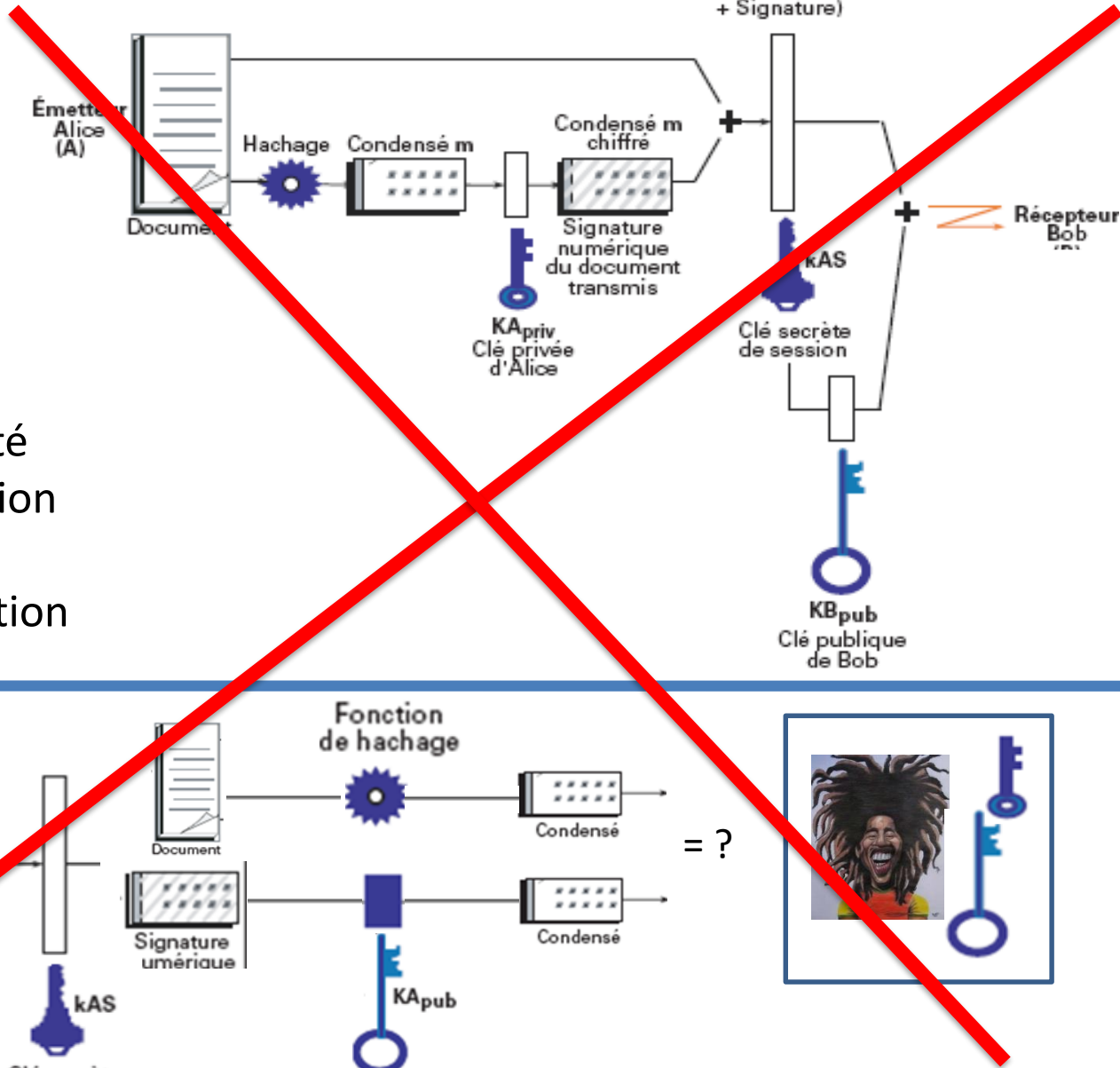
Clé privée du signataire



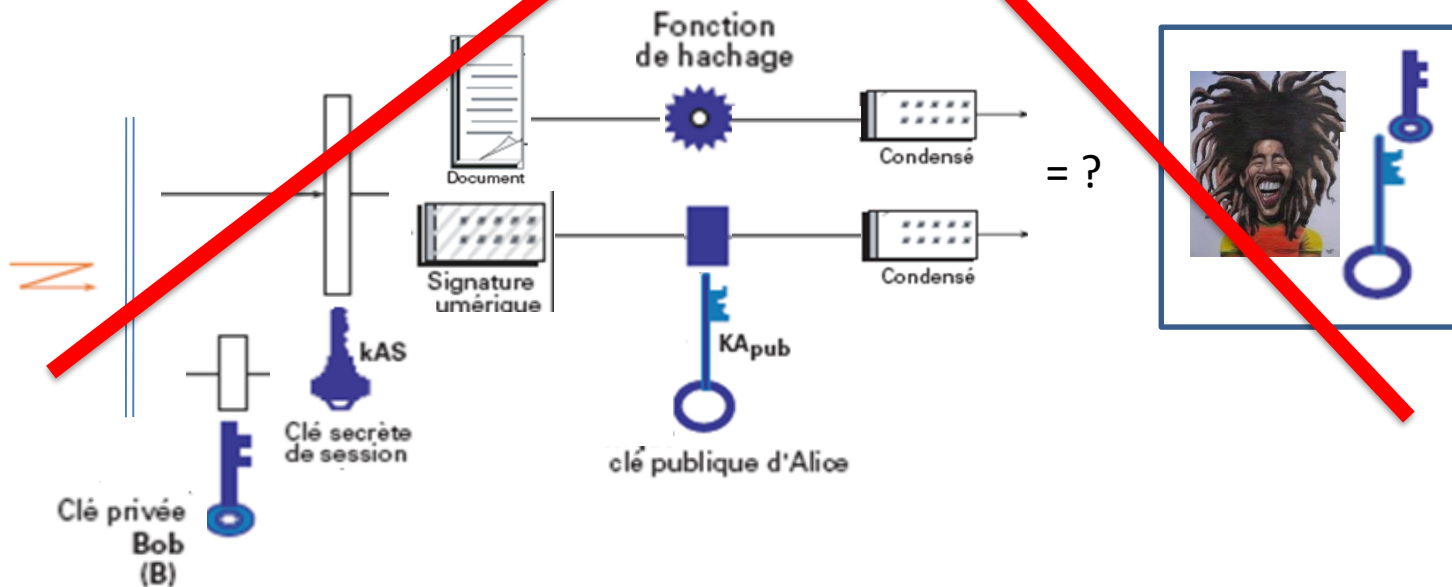


Confidentialité
Authentification
Intégrité
Non Répudiation





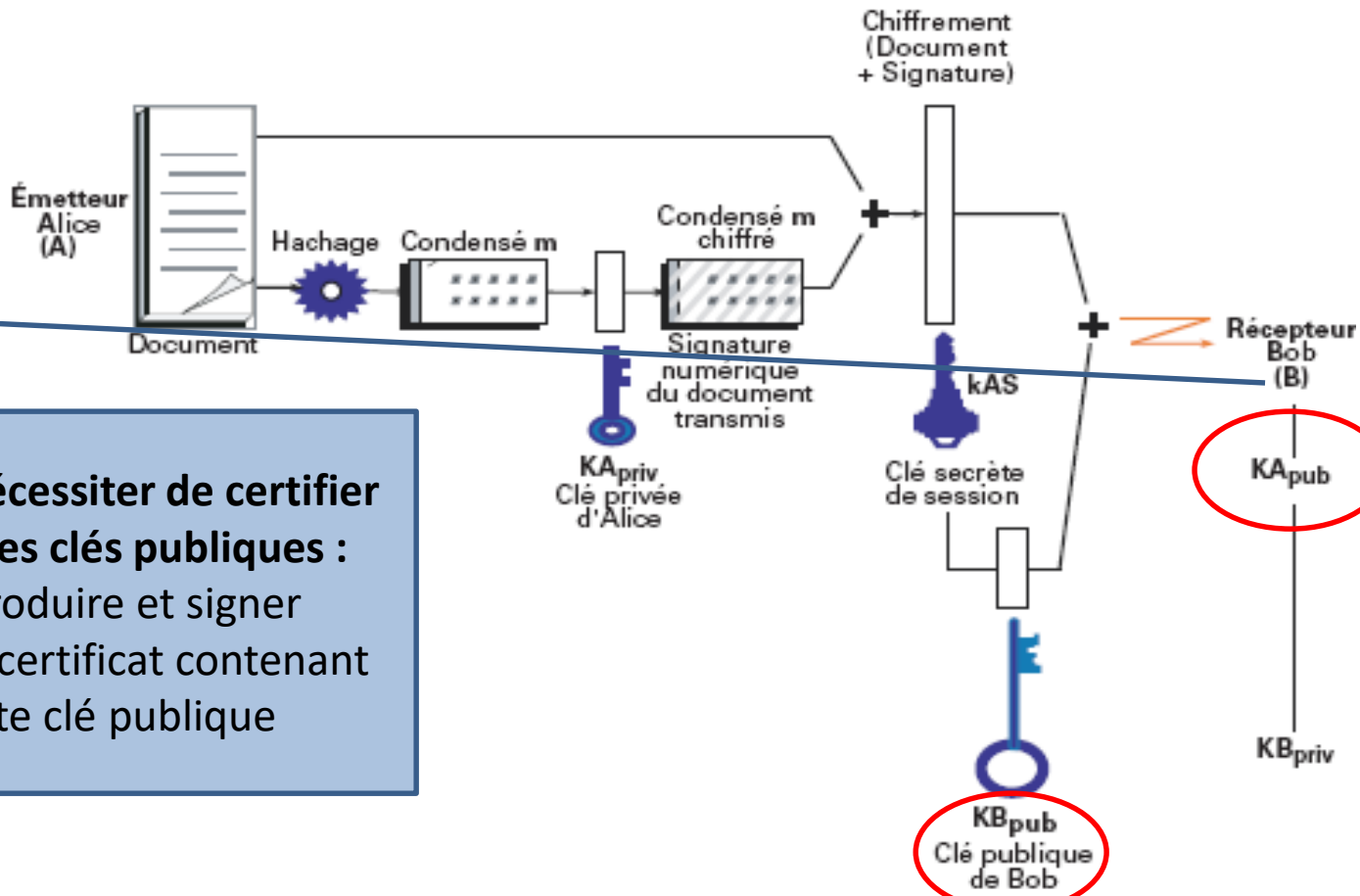
Confidentialité
Authentification
Intégrité
Non Répudiation



Les mécanismes principaux : CERTIFICATION

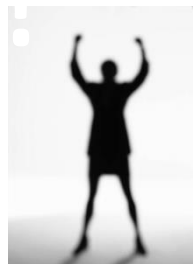
- **Authentification**

- Est-ce bien la clé publique d'Alice ?
- Est-ce bien la clé publique de Bob ?

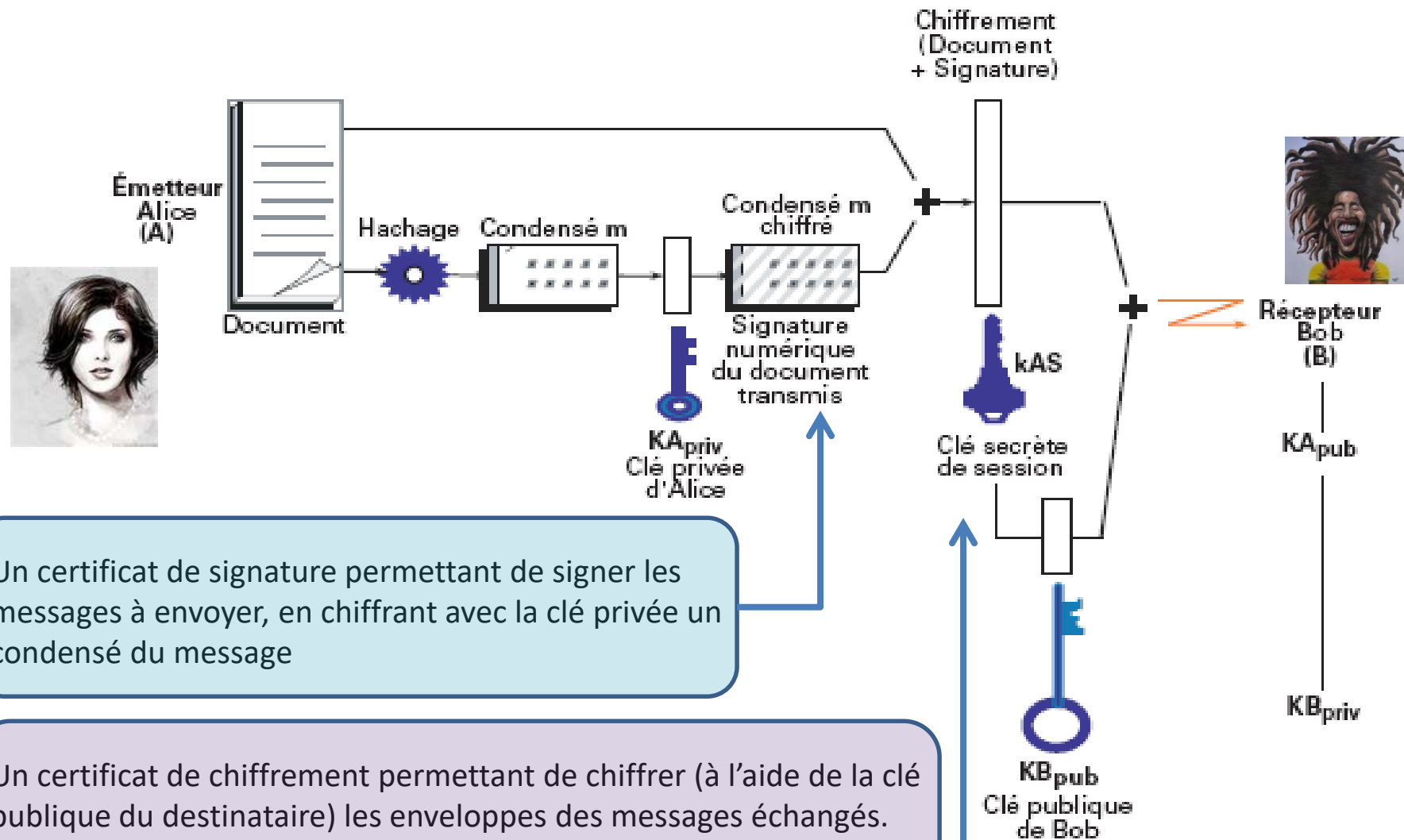


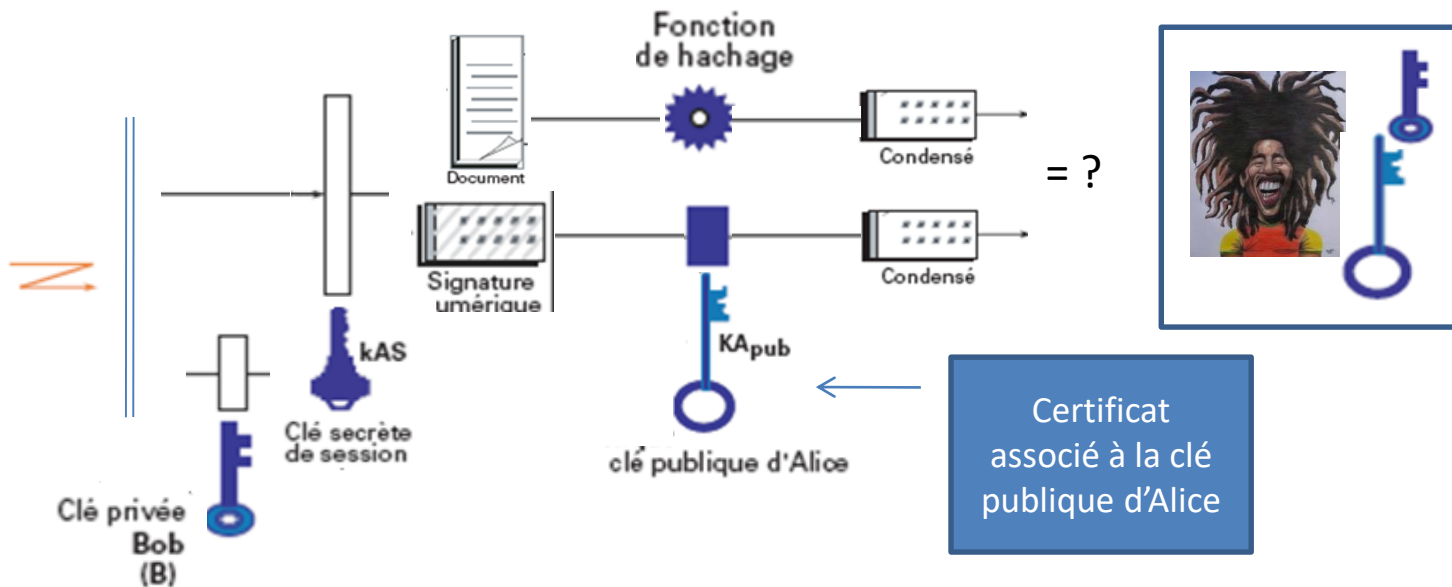
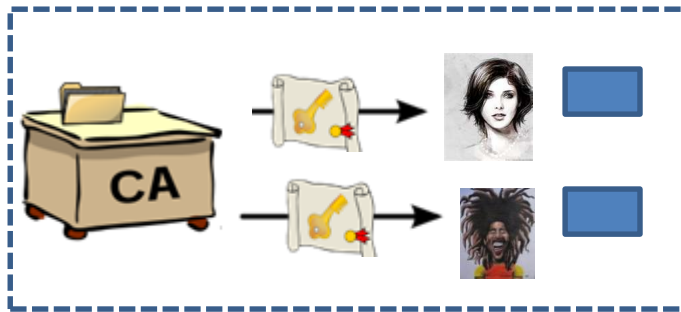
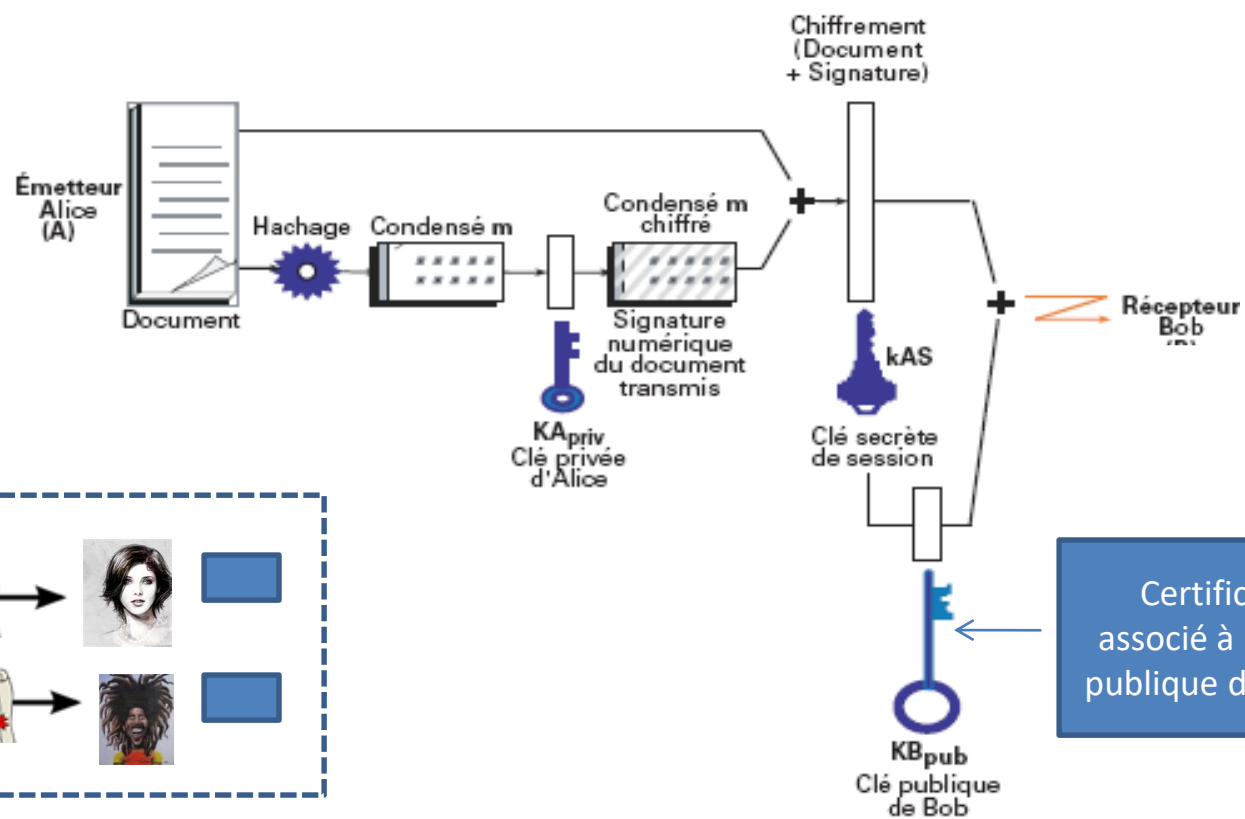
Nécessiter de certifier les clés publiques :

- produire et signer un certificat contenant cette clé publique



Les mécanismes principaux : CERTIFICATION







Certificats



Clé publique de Paul



Clé privée de Paul

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

- Solution : utilisation de certificats.



Certificats

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

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

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

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

Certificats

Comment connaître 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.

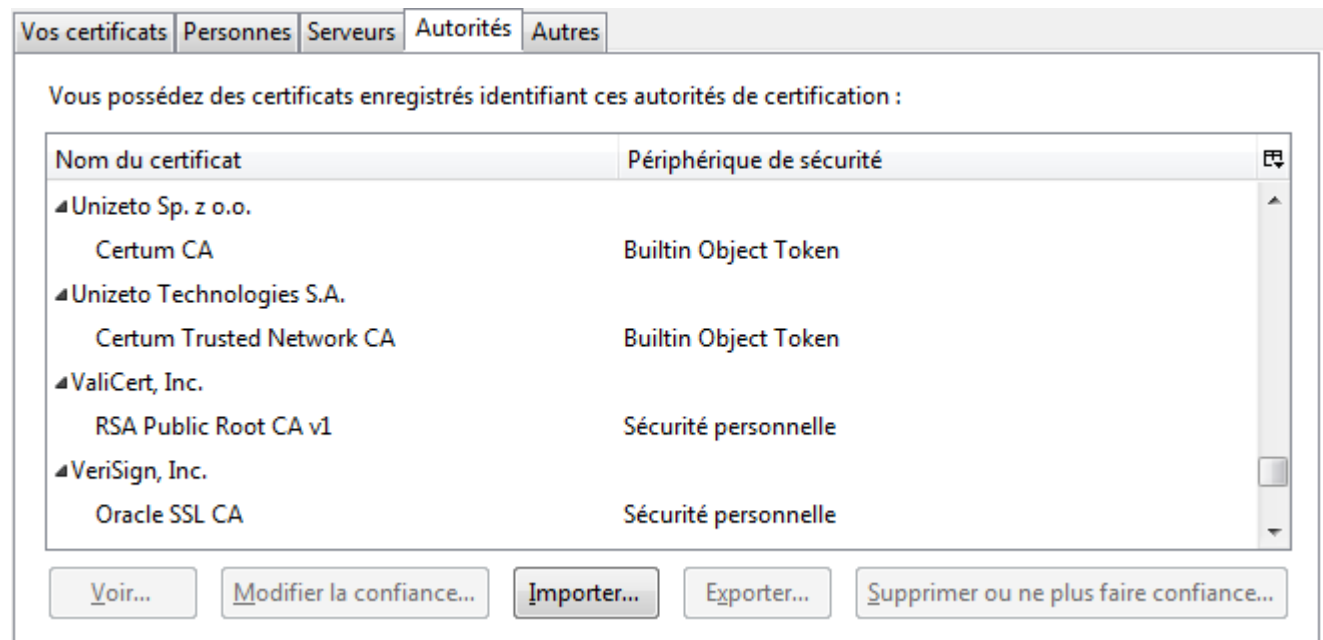
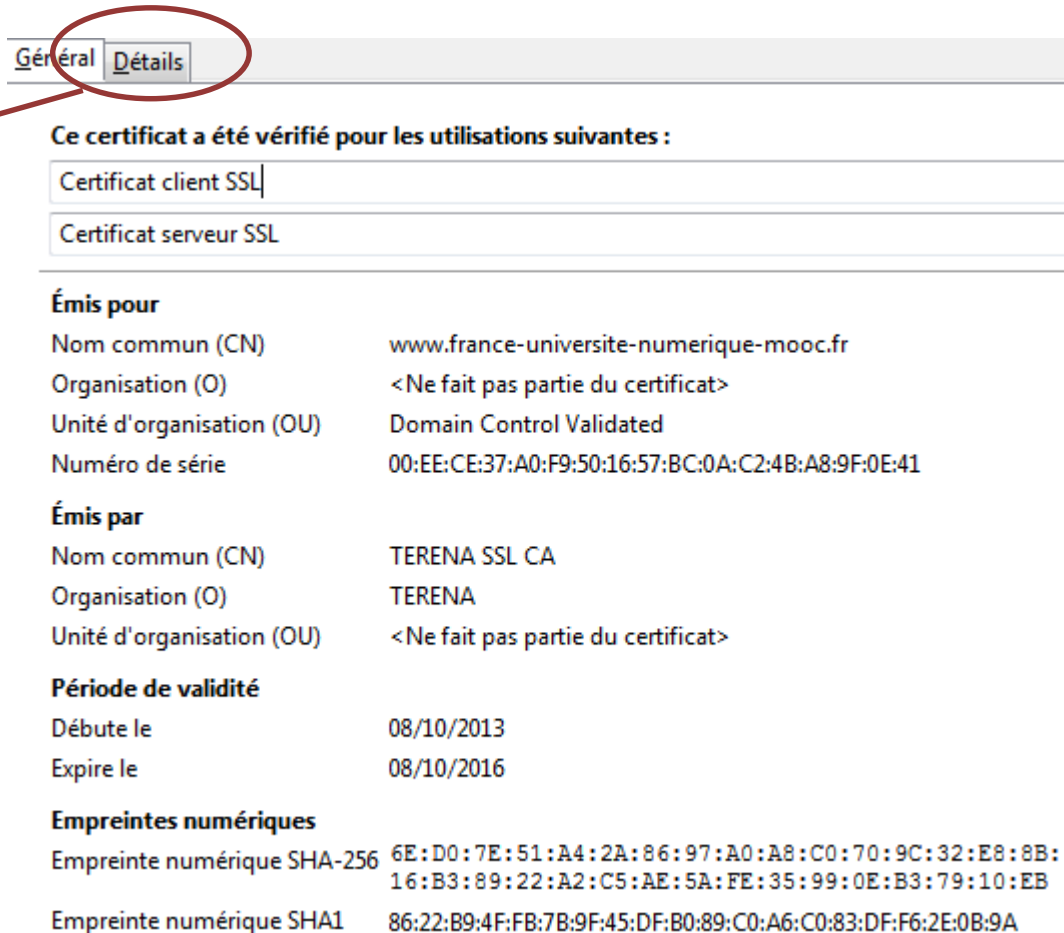


Image : magasin de certificats de Firefox

Certificats

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**



Général **Détails**

Ce certificat a été vérifié pour les utilisations suivantes :

- Certificat client SSL
- Certificat serveur SSL

Émis pour

Nom commun (CN)	www.france-universite-numerique-mooc.fr
Organisation (O)	<Ne fait pas partie du certificat>
Unité d'organisation (OU)	Domain Control Validated
Numéro de série	00:EE:CE:37:A0:F9:50:16:57:BC:0A:C2:4B:A8:9F:0E:41

Émis par

Nom commun (CN)	TERENA SSL CA
Organisation (O)	TERENA
Unité d'organisation (OU)	<Ne fait pas partie du certificat>

Période de validité

Début le	08/10/2013
Expire le	08/10/2016

Empreintes numériques

Empreinte numérique SHA-256	6E:D0:7E:51:A4:2A:86:97:A0:A8:C0:70:9C:32:E8:8B:16:B3:89:22:A2:C5:AE:5A:FE:35:99:0E:B3:79:10:EB
Empreinte numérique SHA1	86:22:B9:4F:FB:7B:9F:45:DF:B0:89:C0:A6:C0:83:DF:F6:2E:0B:9A

Détenteur de la clé publique

Autorité de certification

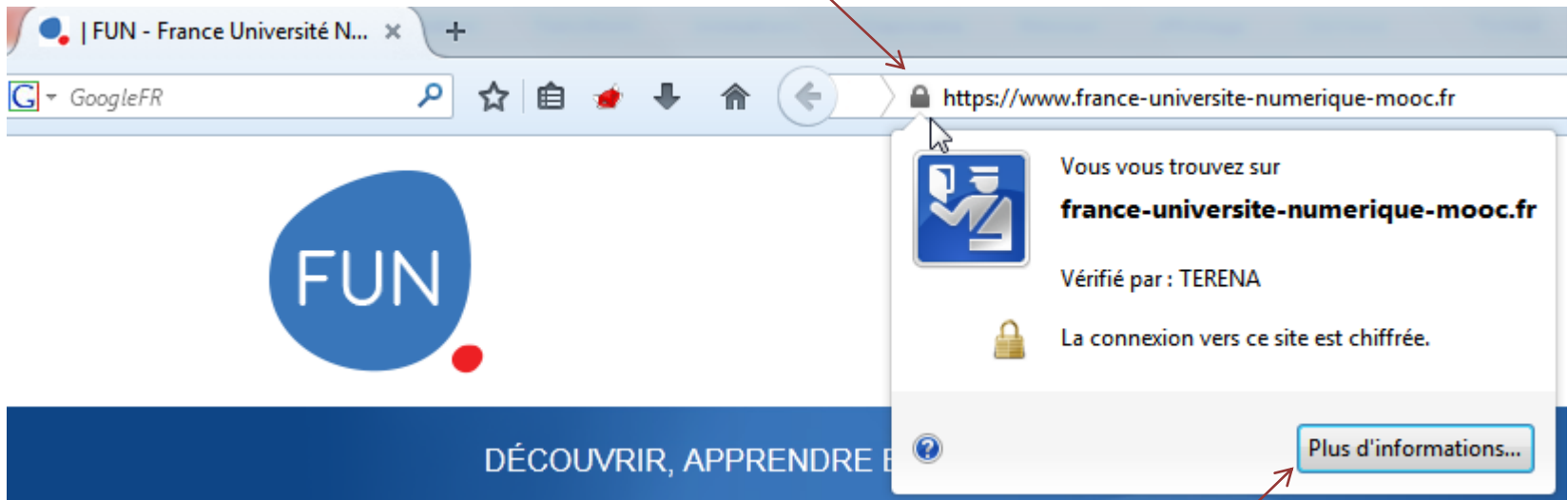
Dates de validité du certificat

Certificats

Où trouver les certificats dans un navigateur ?

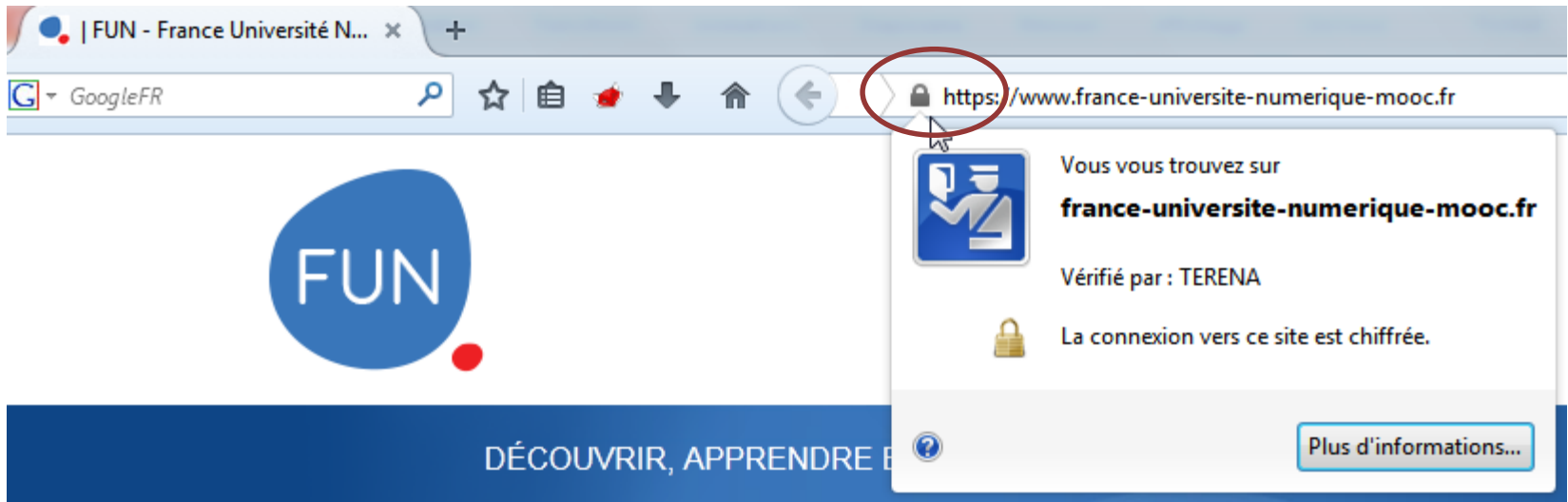
Exemple avec Firefox pour ouvrir le certificat d'un site WEB

Cliquer sur le cadenas à côté de l'URL



Cliquer ici pour afficher le certificat

Certificats



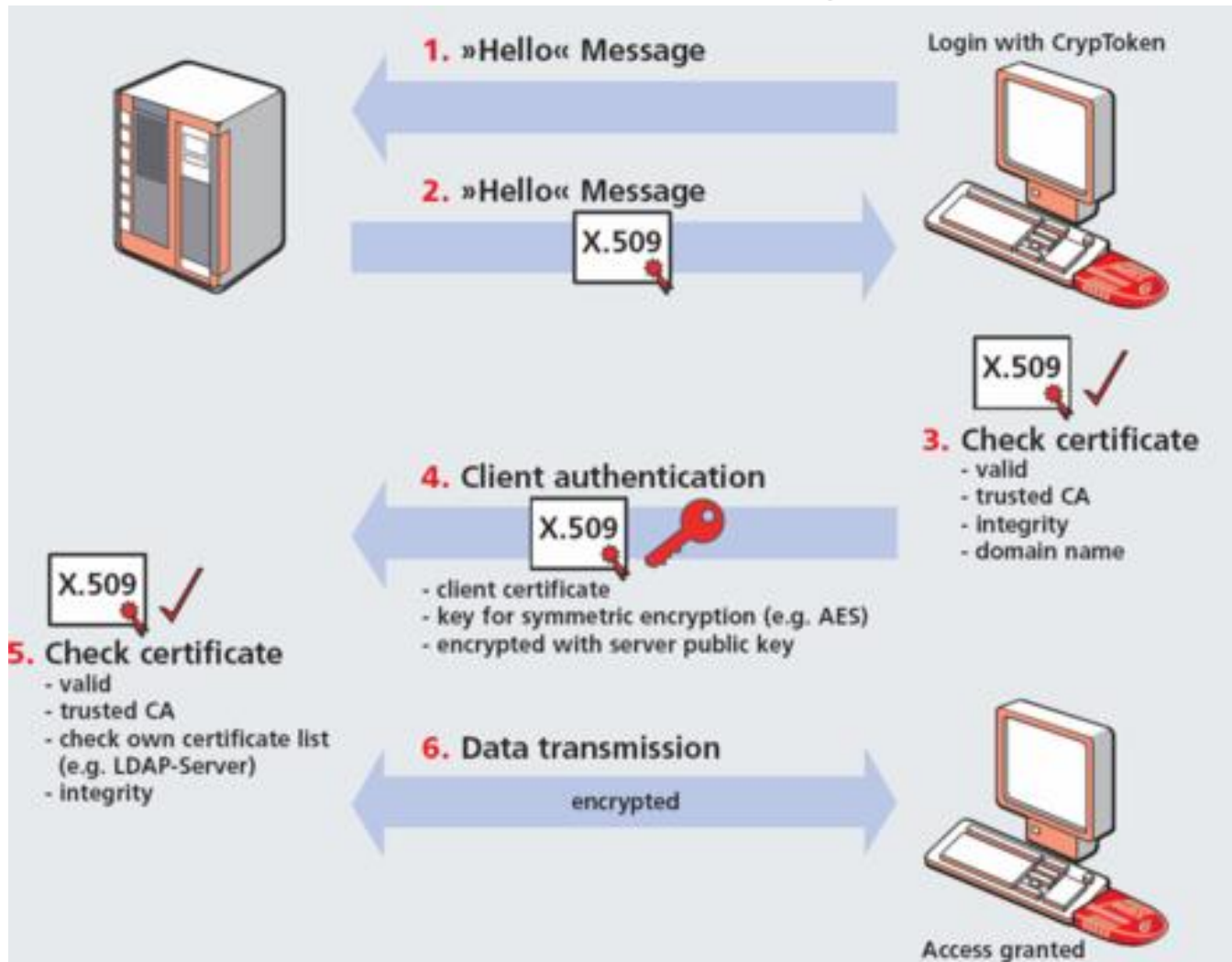
Puisque le certificat du site WEB est disponible et valide, cela amène donc deux avantages à l'utilisateur, caractéristiques du HTTPS

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



Les mécanismes principaux

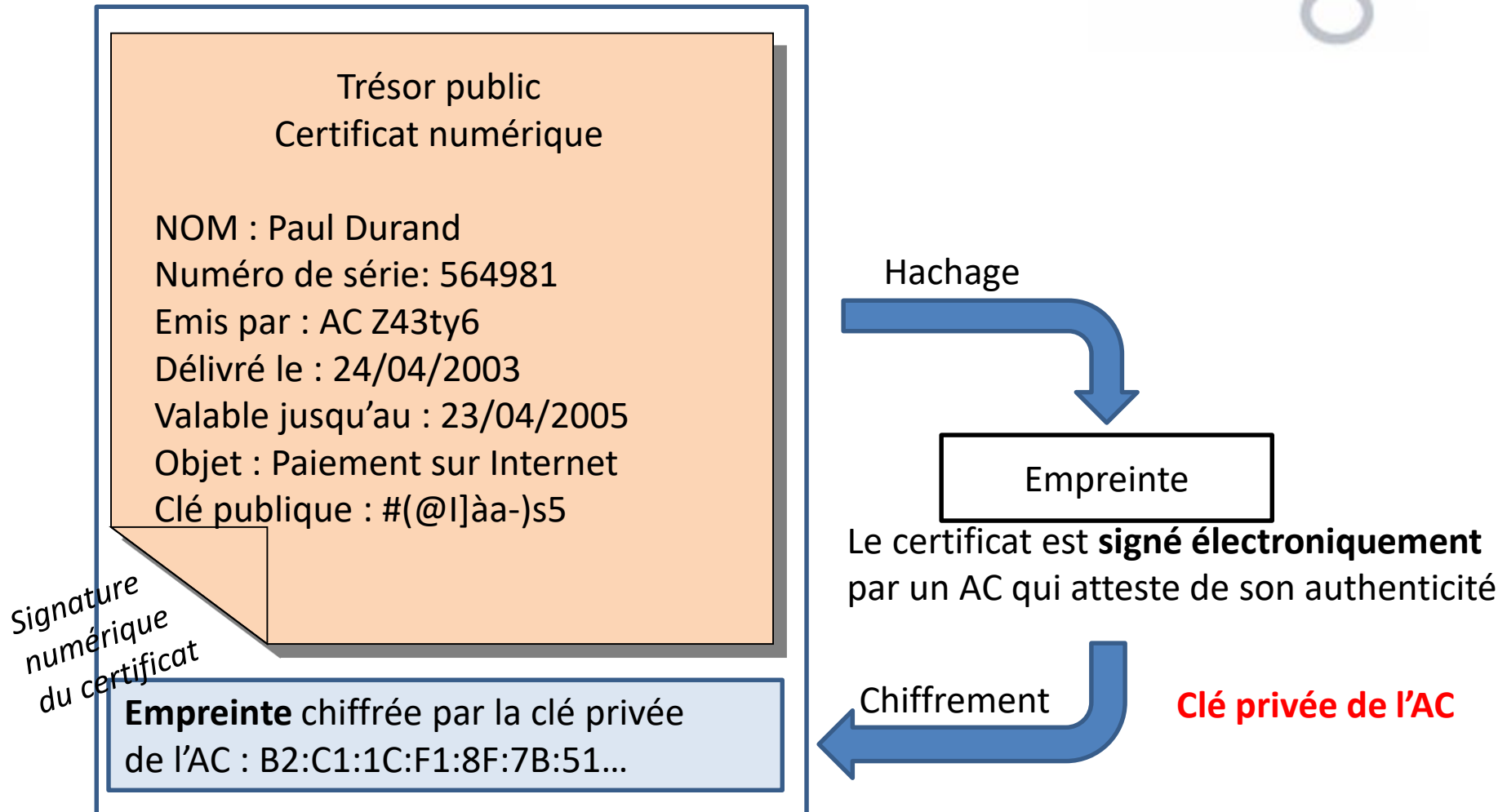
- **Authentication et certificat / Sécuriser ses échanges**





Les mécanismes principaux

- **Certificats X.509 et X.509 v3** / Empreinte et signature





Les mécanismes principaux

- **Certificats X.509 et X.509 v3 / Vérification**



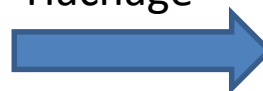
Trésor public
Certificat numérique

NOM : Paul Durand
Numéro de série: 564981
Emis par : AC Z43ty6
Délivré le : 24/04/2003
Valable jusqu'au : 23/04/2005
Objet : Paiement sur Internet
Clé publique : #(@I]àa-)s5

Signature
numérique
du certificat

Empreinte chiffrée par la clé privée
de l'AC : B2:C1:1C:F1:8F:7B:51...

Hachage



Empreinte
calculée

La vérification du certificat peut être
effectuée par tout service qui possède
la clé publique de l'AC
Ex: un navigateur

Déchiffrement



Empreinte
déchiffrée

Clé publique de l'AC

#



Synthèse

Résumer des techniques classiquement utilisées dans les protocoles de sécurité

- **Le chiffrement** d'une **quantité importante** de données utilisent les **clés symétriques**
- **La signature** est obtenue en **chiffrant** avec la **clé privée** du **signataire**; la **clé publique**, accessible à tous permet de **vérifier** la signature
- **Le transport des clés symétriques** se fait dans une enveloppe **chiffrée** par la **clé publique** du destinataire; ce dernier est le seul à posséder **clé privée** permettant de **déchiffrer** (ouvrir) cette enveloppe
- **La gestion et la certification** des **clés publiques** sont effectuée par une **PKI (voir aussi certificat étendu et let's encrypt)**

<https://blog-fr.orson.io/comment-passer-http-vers-https>

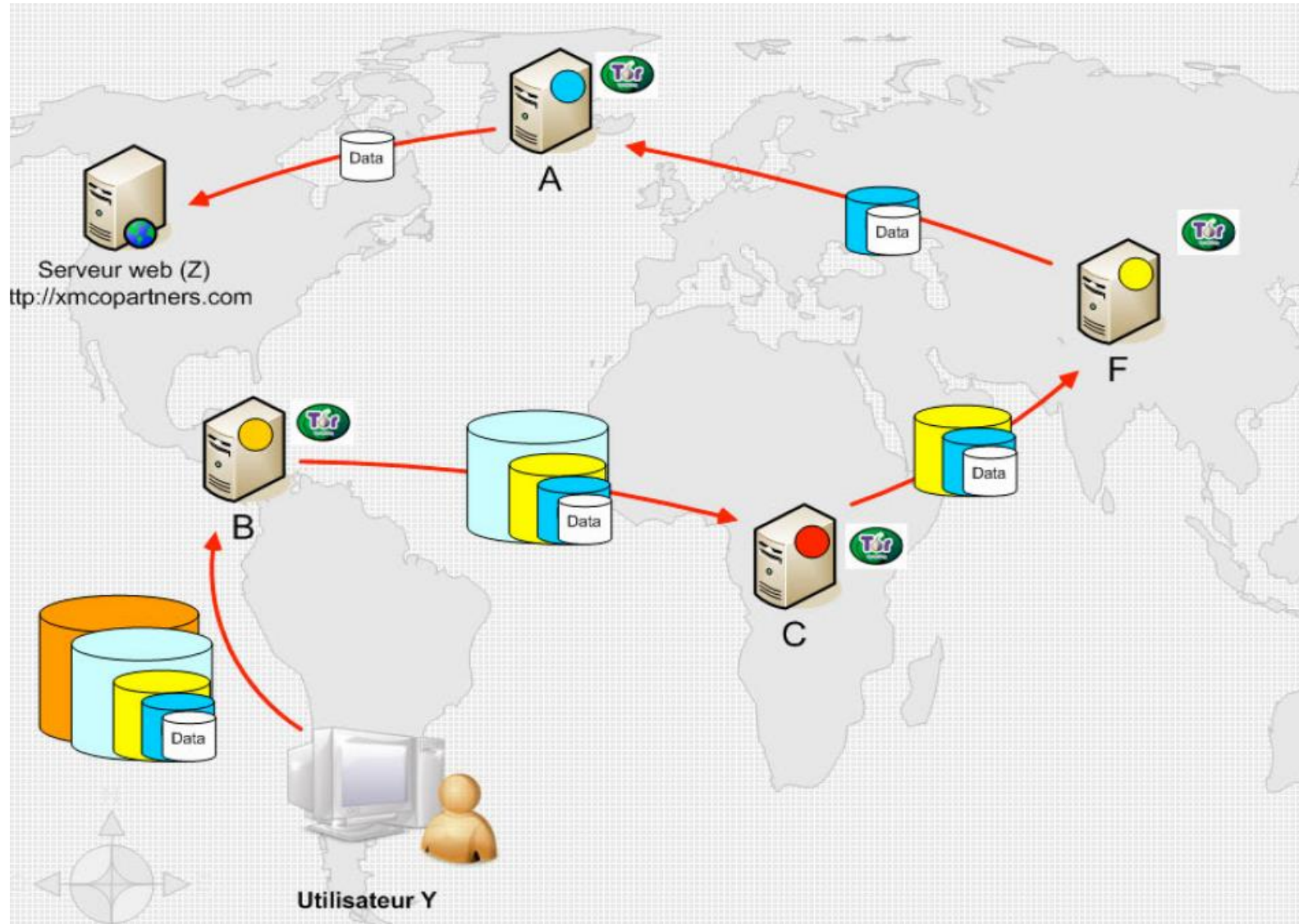
<https://korben.info/les-attaques-ssltls.html>

<https://korben.info/detecter-config-ssl-vulnerabilites-associees.html>

<https://www.numerama.com/tech/149306-drown-un-tiers-des-serveurs-https-est-vulnerable-a-une-nouvelle-faible-critique.html>

<https://connect.ed-diamond.com/MISC/MISCHS-006/Revue-d-attaques-du-protocole-TLS-et-de-l-implementation-OpenSSL>

Annexe : principe du réseau TOR



Synthèse : algorithmes

Chiffrement
Confidentialité/
Authentification

Signature numérique
Authentification / Intégrité
Non-répudiation

Fonctions auxiliaires
*combinées à la SN
pour l'intégrité*

MD5
RIPEMD
OAEP
SHA-1

Systèmes
symétriques

Systèmes
asymétriques

Gestion de
clé

Algo par
flux

A5
PKZIP
RC4
SEAL
WAKE

Algo par
bloc

AES RC2
CAST RC5
DES
3DES
IDEA
Blowfish
Rijndael

MAC

HMAC
MAC
MDC

Log discret

DSA
ECDSA
ElGamal

Factorisation

RSA
RW

DH
MQV
ISAKMP
Oakley

*La signature numérique est une
technique informatique
La signature électronique est une
solution technico-organisationnelle qui
répond à un besoin juridique*

Synthèse : clés

Clés cryptographiques

Exemple 1 : clé DES sur 64 bits représentée par 16 caractères hexadécimaux



6F 40 A2 F3 73 1D EB F9

Exemple 2 : clé RSA de 512 bits



6b f5 fe 1c 67 d4 f2 04 47 6a dc f4 15 f4 27 05 b7 79 15 e2 dc b3
9a 29 25 93 07 2c c9 59 14 39 18 76 1d f0 67 3d 3f cc ac e8 a5 95 fd
a2 eb 46 06 13 32 c8 aa ca cf ef 12 23 f4 27 67 1c f5 25 9a ac e8 3d b3 79