



Cours
Administration des Systèmes d'Exploitation
Ecole Supérieure de Technologie – Guelmim
Université Ibn Zohr –Agadir-

Prof. ASIMI Younes
asimi.younes@gmail.com

2020/2021

Fonction de hachage



Les fonctions de hachage permettent **d'assurer l'intégrité** des données. Les **signatures numériques**, en plus d'assurer l'intégrité, permettent de vérifier **l'origine** de **l'information** et son **authenticité**.

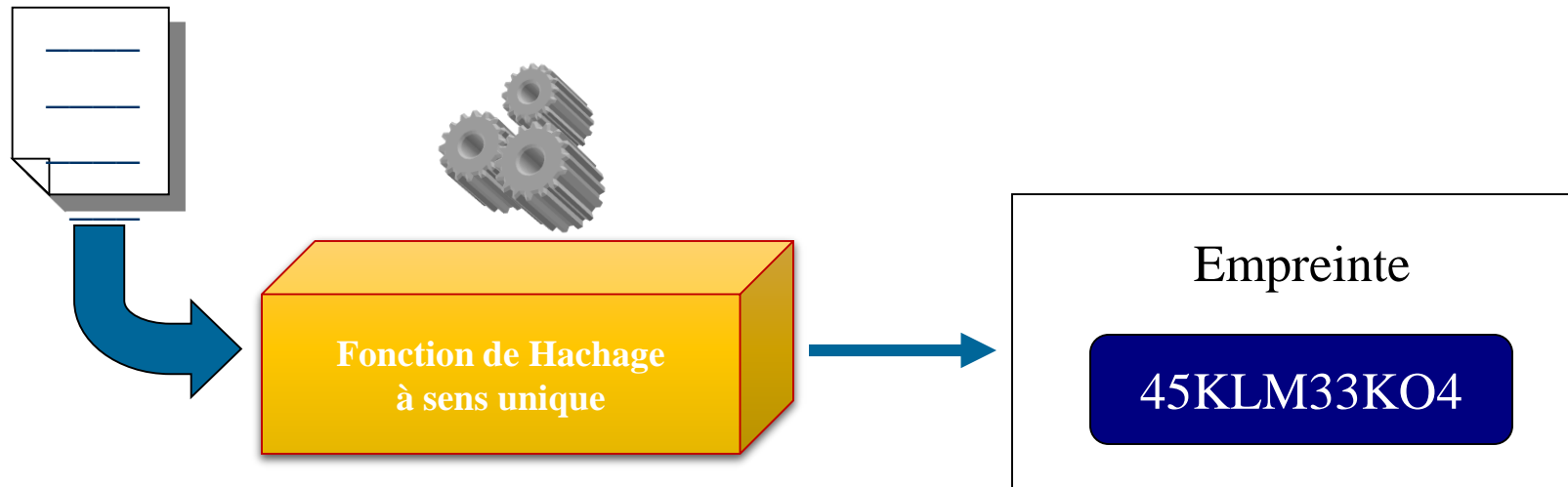
La robustesse de ces fonctions repose essentiellement sur leurs capacités de **résister** contre **différentes attaques**. Elles dominent un grand espace d'application de point de vue **sécurité** :

- ❖ **Intégrité de fichier (signatures numériques);**
- ❖ **Stockage de mots de passe sécurisé ;**
- ❖ **Intégrité de communications (messages échangés, mot de passe,...) ;**
- ❖ **Signature numérique (certificat numérique).**

Fonction de hachage

● Principe :

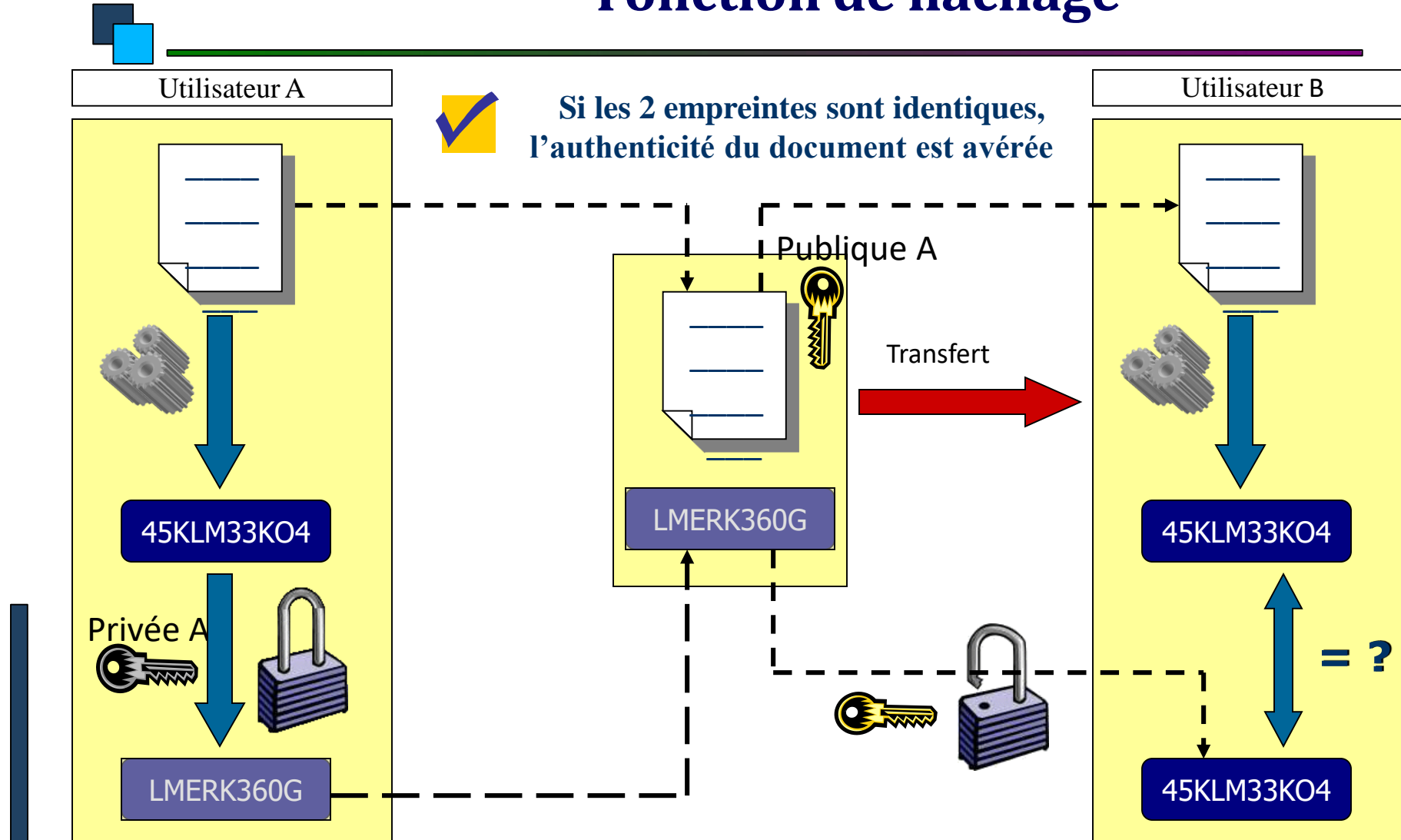
Transformation d'une chaîne de caractères de longueur quelconque à une chaîne de caractères de longueur fixe:



● Algorithmes :

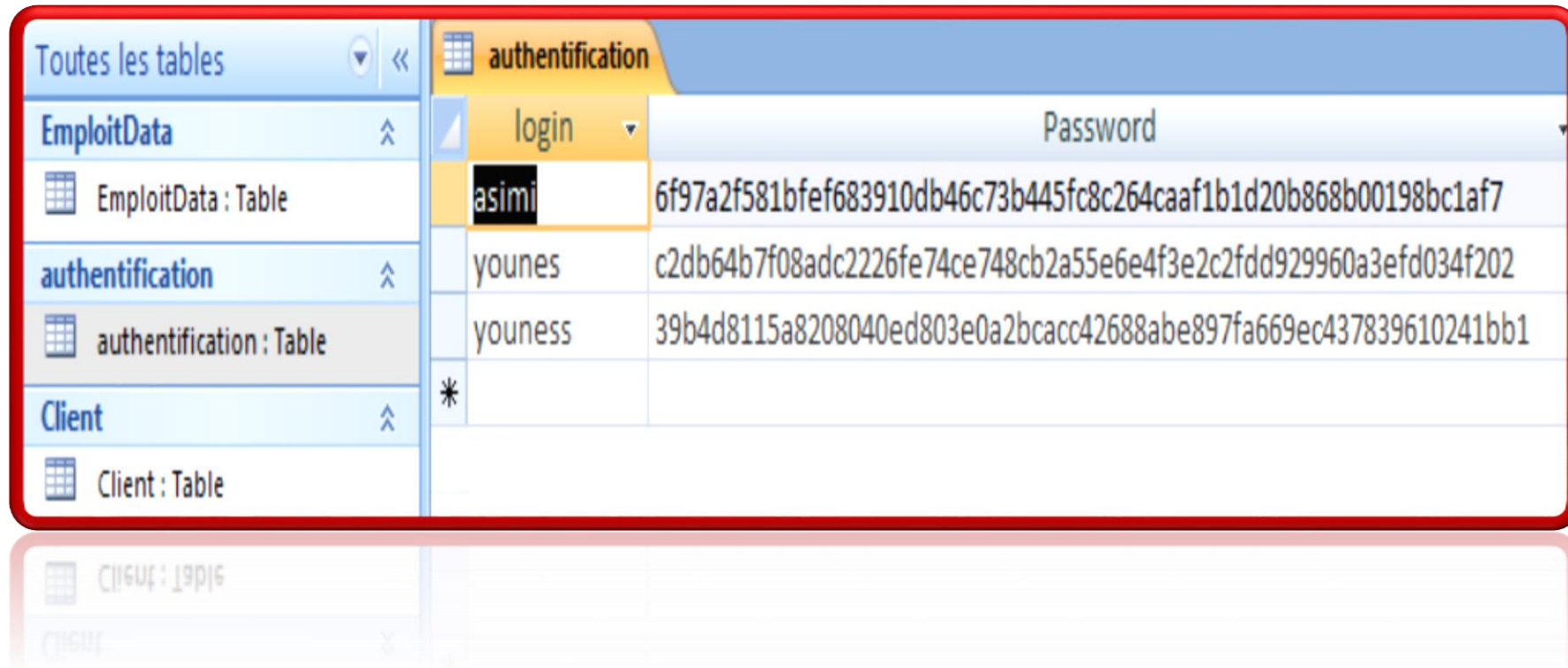
- MD5 : calcul d'empreinte sur 128 bits,
- SHA-1 : empreinte de 160 bits, plus sûr que MD5

Fonction de hachage



Fonction de hachage

Hachage des mots de passe sous VBA:



Toutes les tables	authentification	login	Password
EmploitData		asimi	6f97a2f581bfef683910db46c73b445fc8c264caaf1b1d20b868b00198bc1af7
EmploitData : Table		younes	c2db64b7f08adc2226fe74ce748cb2a55e6e4f3e2c2fdd929960a3efd034f202
authentification		youness	39b4d8115a8208040ed803e0a2bcacc42688abe897fa669ec437839610241bb1
authentification : Table		*	
Client			
Client : Table			

Fonction de hachage

Calculer un Haché pour un mot de passe : « asimi »

Lien: <http://www.sha1-online.com/>

Home Page | [SHA1 in JAVA](#) | [Secure password generator](#) | [Linux](#)

SHA1 and other hash functions online generator

Result for md5: **7df35e168b25555daec0e802a60f8af7**

SHA1 and other hash functions online generator

Result for sha1: **e0fe2f4ba6b1436c44348a9e5a06c178ee75f024**

SHA1 and other hash functions online generator

Result for
sha256: **5835dd2c323bccf0a8946ce4ad560bb68377527ff26cb5c55be3a653345a5a76**

Fonction de hachage

Craquer un Haché de mot de passe : « asimi »

Crack Md5:

<https://hashkiller.co.uk/sha1-decrypter.aspx>

Status: We found 1 hashes! [Timer: 132 m/s] Please find them below...

SHA1 Hashes: e0fe2f4ba6b1436c44348a9e5a06c178ee75f024

Max: 64

e0fe2f4ba6b1436c44348a9e5a06c178ee75f024 SHA1 : asimi

Status: We found 1 hashes! [Timer: 148 m/s] Please find them below...

MD5 Hashes: 7df35e168b25555daec0e802a60f8af7

Max: 64

7df35e168b25555daec0e802a60f8af7 MD5 : asimi

Certificat numérique

Un **certificat numérique** est aussi appelé **certificat électronique** ou **certificat de clé publique** peut être vu comme une carte **d'identité numérique**. Il est utilisé principalement **pour identifier et authentifier** une personne physique ou morale, mais aussi pour **chiffrer** des échanges.

➤ **Classes des certificats numérique:**

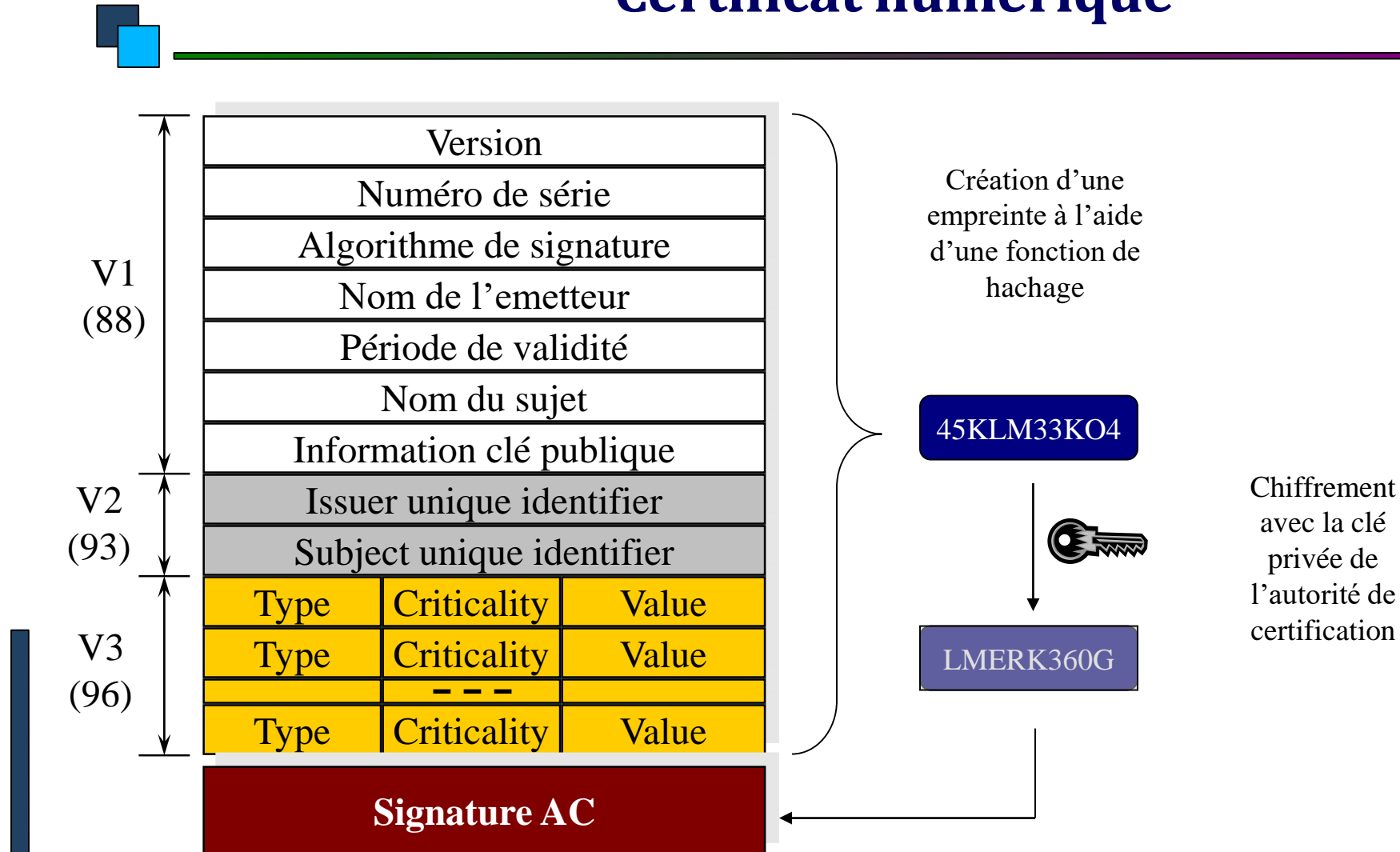
- ❖ **Classe I** : elle garantit uniquement l'existence d'une **adresse email**, mais pas l'identité du titulaire du certificat ;
- ❖ **Classe II**: elle garantit **l'identité** du titulaire du **certificat** et de son **entreprise**. Les pièces justificatives ont été transmises et vérifiées par l'autorité de certification qui a délivrée certificat numérique ;
- ❖ **Classe III**: Comme la classe II et la classe III, elle garantit la vérification de l'identité du titulaire du certificat mais sa présentation physique est requise.

Certificat numérique

Un certificat est un **document électronique** émis par une **tierce partie de confiance** qui permet de garantir **l'authenticité d'une clé publique**.

- Il s'agit d'une **carte d'identité numérique** pour :
 - Certifier une clé **publique**;
 - Identifier et authentifier une personne physique ou morale,
 - Chiffrer et déchiffrer des données échangées dans le réseau,
 - Stocker des données sécurisées dans une base de données;
 - Assurer une communication sécurisée entre des serveurs web et des navigateurs (**certificat SSL**);
 - Signer en ligne en toute sécurité des documents....
- Un certificat est l'équivalent d'une **carte d'identité ou d'un passeport**.
- Il est délivré par une **Autorité de Certification**.

Certificat numérique



Certificat numérique



Certificate

Version : 3 (0x2)
Serial Number : 7 (0x7)
Signature Algorithm : **md5 With RSA Encryption**
Issuer : C=FR, ST=France, L=Paris, O=EPITA, OU=ADM, CN=ROOT
 Email=murphy@tcom.epita.fr
Validity : Not Before: Sep 11 09:49:27 1998 GMT
 Not After : Sep 11 09:49:27 1999 GMT
Subject : C=FR, ST=France, L=Paris, O=EPITA, OU=TCOM, CN=MURPHY
 Email=murphy@tcom.epita.fr
Subject Public Key Info : **Public Key Algorithm: rsaEncryption**
RSA Public Key: (1024 bit)
00:d3:8a:78:15:90:bb:7f:62:50:37:e1:7f:ee:fd:7c:0e:86:c2:1f:50:d9
X509 v3 extensions : Netscape CA Revocation Url : <http://anjou.dsi.cnrs.fr/ca-crl.pem>
 Netscape Comment : Autorite de Certification CNRS-DSI
Signature Algorithm : md5 With RSA Encryption
47:27:8b:b6:4e:7c:22:aa:00:93:9a:c1:e0:04:ad:55:cf:51:c7:11

-----BEGIN CERTIFICATE-----

MIIC7TCCAlagAwIBAgIBBzANBgkqhkiG9w0BAQQFADCBhjELMAkGA1UEBhMCRIIxfgK
khXGEkWafhxb3ilCqAFxif4J7DPEX2fgmLEcwDqccR

-----END CERTIFICATE-----

Certificat numérique

La CNIE, identité de la personne vérifiée par les empreintes digitales.

Un document:

- Lettre, contrat, facture ...

Un stylo ou un marqueur, un crayon, une plume...

Signature manuscrite



Un certificat électronique unique à la personne contrôlé par une autorité de certification: Banque;

Un document:

- Word, PDF, XML...
- Contrat, lettre, données...

Un certificat électronique:

- Une clef USB,
- Une carte à puce,
- Certificat logiciel...

Un code secret:

Que le signataire est le seul à connaître (ou un mot de passe...)

Certificat numérique

Types de certificats

Certificat Personnel



- Hébergé sur un **PC**, carte à puce, jeton **USB** ...
- Usage **privé**;
- **Messagerie**, chiffrement, achat en ligne ...

Certificat Serveur



- Hébergé sur un **serveur Web**;
- Lié à une adresse de type **Internet** (<http://...>);
- Sécuriser les échanges électroniques (**SSL**);

Certificat numérique

Certificat Développeur



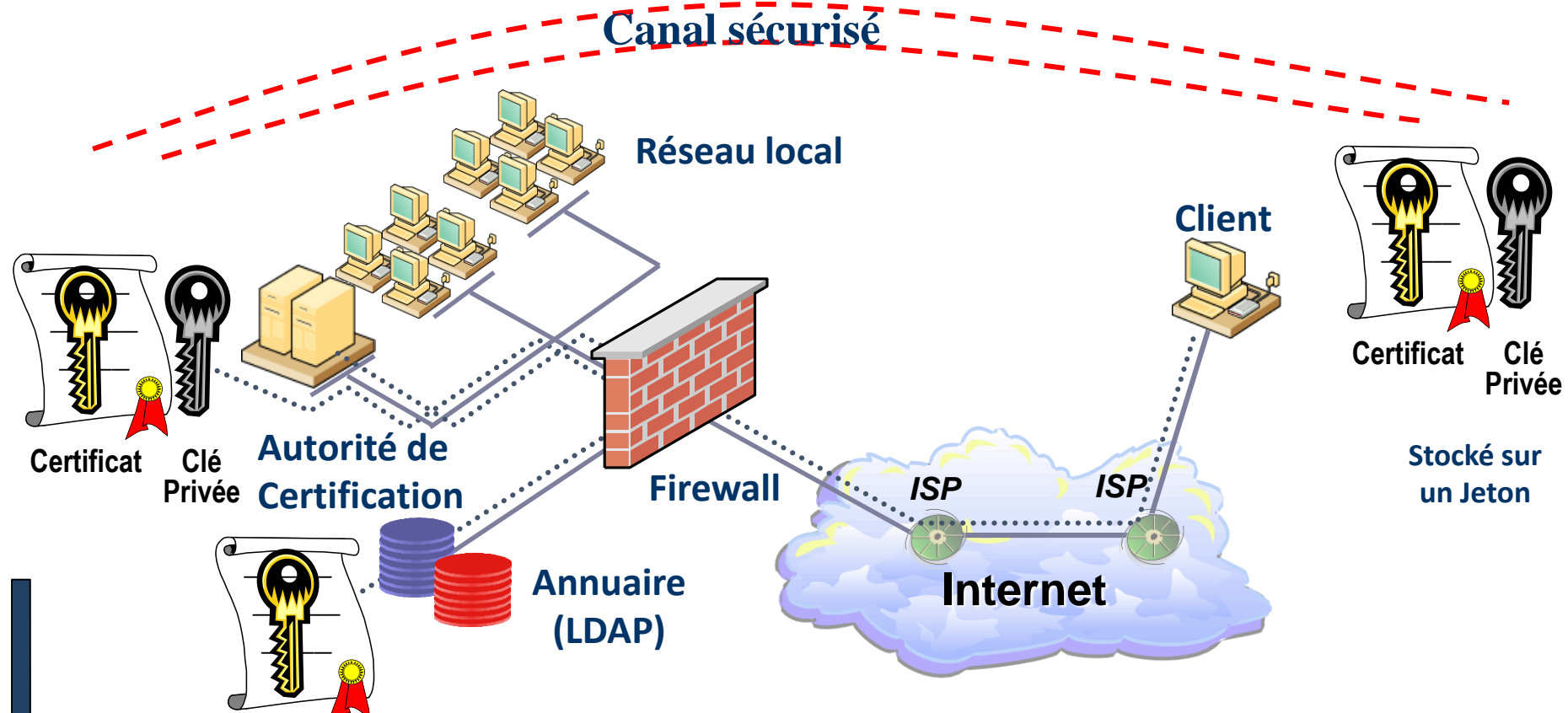
- Intégré à certains **browser** (IE, Firefox....);
- Donne le droit à certaines **applications** de se lancer;

Certificat IPSEC



- Hébergé sur des **routeurs**;
- Chiffre les flux transitant entre lui et un autre équipement réseau;
- **VPN**, Tunnel **IPSEC**;

Demande d'un Certificat numérique

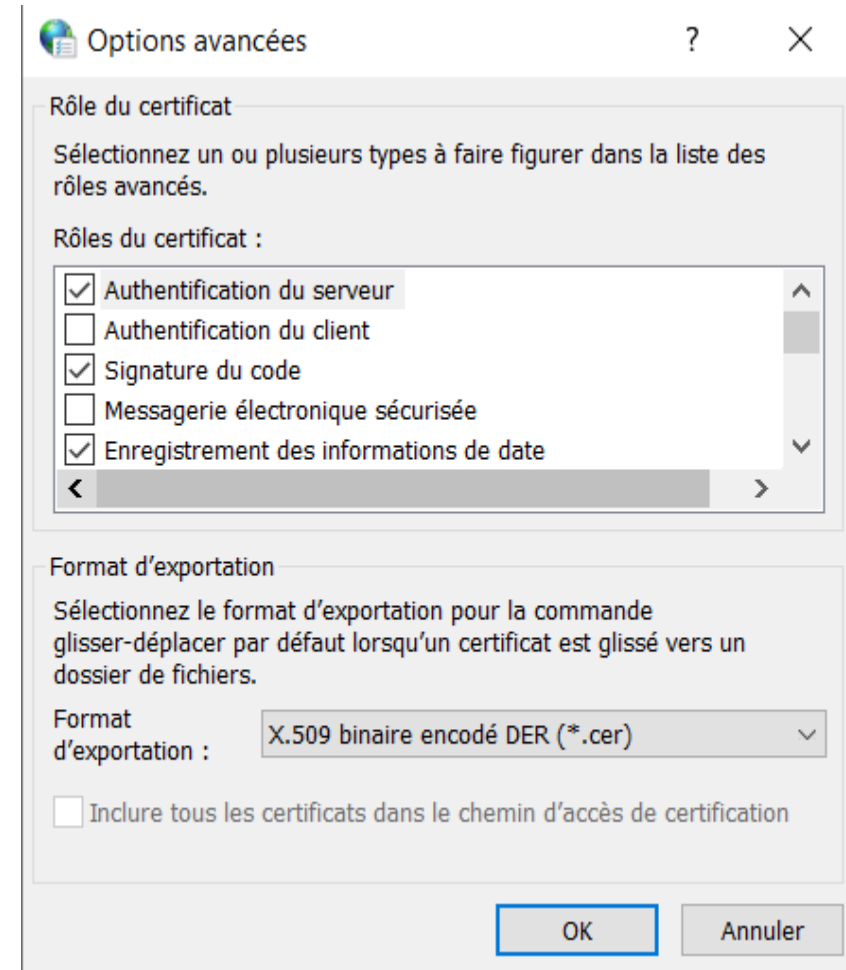


L'AC génère et distribue une clé publique et une clé privée.
L'AC crée un certificat numérique contenant la clé publique de façon sécurisée (transfert physique ou session cryptée).
L'utilisateur stocke les données dans un jeton matériel ou logiciel.

Certificat numérique

Le fichier d'un certificat contient au moins les **informations** suivantes :

- Le nom de l'autorité de certification qui a créé le certificat;
- Le nom et le prénom de la personne;
- Son entreprise (ESTG par exemple);
- Son adresse électronique;
- **Sa clé publique**;
- Les dates de validité du certificat;
- Une signature électronique.



Certificat numérique

Panneau de configuration\Réseau et Internet:

Propriétés de : Internet

Général Sécurité Confidentialité **Contenu** Connexions Programmes Avancé

Certificats

Utiliser des certificats pour les connections chiffrées et pour l'identification.

Effacer l'état SSL Certificats Éditeurs

Saisie semi-automatique

La saisie semi-automatique stocke les entrées précédentes sur des pages Web et suggère des correspondances.

Paramètres

Flux et composants Web Slice

Les flux et les composants Web Slice offrent un contenu mis à jour à partir de sites Web, lisible dans Internet Explorer et dans d'autres programmes.

Paramètres

Certificats

Rôle prévu : <Tout>

Autorités de certification racines de confiance Éditeurs approuvés Éditeurs non approuvés

Délivré à	Délivré par	Expiration	Nom convivial
AAA Certificate Services	AAA Certificate Se...	01/01/2...	Sectigo (AAA)
Actalis Authentication ...	Actalis Authenticat...	22/09/2...	Actalis Authen...
AddTrust External CA ...	AddTrust External ...	30/05/2...	Sectigo (AddT...
Avast Web/Mail Shiel...	Avast Web/Mail S...	01/01/2...	<Aucun>
Baltimore CyberTrust ...	Baltimore CyberTr...	13/05/2...	DigiCert Balti...
Buypass Class 3 Root ...	Buypass Class 3 R...	26/10/2...	Buypass Class...
Certum CA	Certum CA	11/06/2...	Certum
Certum Trusted Netw...	Certum Trusted N...	31/12/2...	Certum Trust...
Class 3 Public Primary...	Class 3 Public Pri...	02/08/2...	VeriSign Clas...
COMODO RSA Certific...	COMODO RSA Cer...	19/01/2...	Sectigo (form...

Importer... Exporter... Supprimer

Avancé

Détails de certificat

Authentification du client, Signature du code, Système de fichiers EFS (Encrypting File System), Messagerie électronique sécurisée, Fin du tunnel de sécurité IP, Utilisateur de sécurité IP, Authentification du serveur,

Affichage

Fermer

Certificat numérique

Certificats

Rôle prévu : <Tout>

Autorités de certification racines de confiance

Délivré à	Délivré par	Expiration	Nom convivial
AAA Certificate Services	AAA Certificate Se...	01/01/2...	Setigo (AAA)
Actalis Authentication ...	Actalis Authentica...	22/09/2...	Actalis Authen...
AddTrust External CA ...	AddTrust External ...	30/05/2...	Setigo (AddT...
Avast Web/Mail Shiel...	Avast Web/Mail S...	01/01/2...	<Aucun>
Baltimore CyberTrust ...	Baltimore CyberTr...	13/05/2...	DigiCert Balti...
Buypass Class 3 Root ...	Buypass Class 3 R...	26/10/2...	Buypass Class...
Certum CA	Certum CA	11/06/2...	Certum
Certum Trusted Netw...	Certum Trusted N...	31/12/2...	Certum Trust...
Class 3 Public Primary...	Class 3 Public Pri...	02/08/2...	VeriSign Clas...
COMODO RSA Certific...	COMODO RSA Cer...	19/01/2...	Setigo (form...

Importer...

Exporter...

Supprimer

Avancé

Détails de certificat

Authentification du client, Signature du code, Système de fichiers EFS (Encrypting File System), Messagerie électronique sécurisée, Fin du tunnel de sécurité IP, Utilisateur de sécurité IP, Authentification du serveur,

Affichage

Fermer

Certificats

Rôle prévu : <Tout>

Éditeurs approuvés

Délivré à	Délivré par	Expiration	Nom convivial
Microsoft Corporation	Microsoft Code Si...	11/08/2...	<Aucun>
OpenVPN Inc.	DigiCert EV Code ...	23/02/2...	<Aucun>
WZTeam	WZTeam	01/01/2...	<Aucun>

Importer...

Exporter...

Supprimer

Avancé

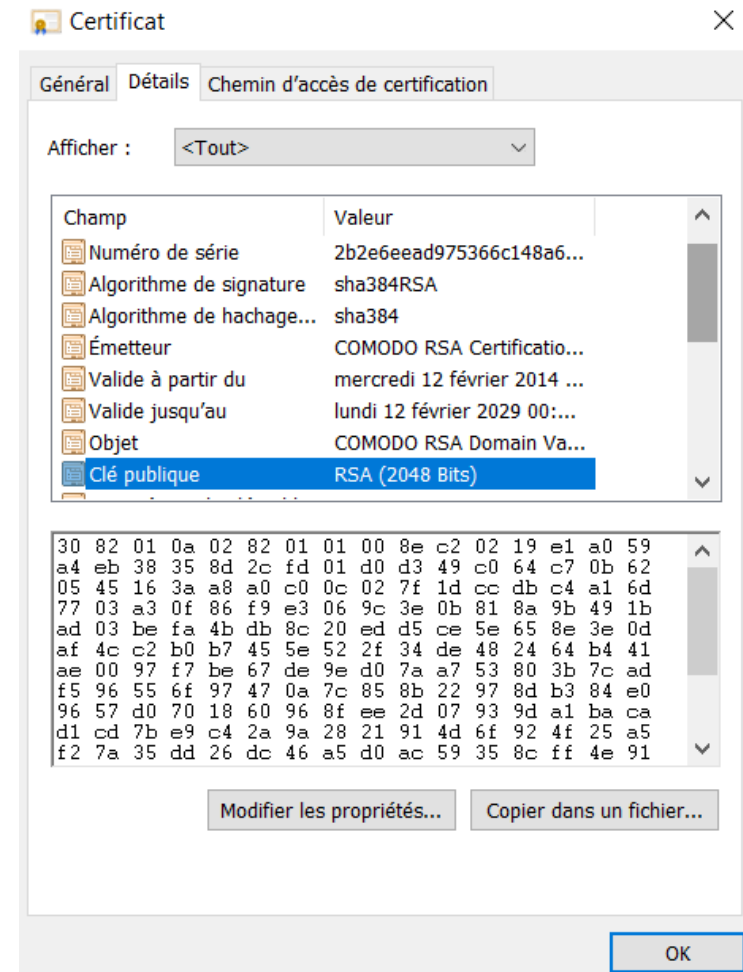
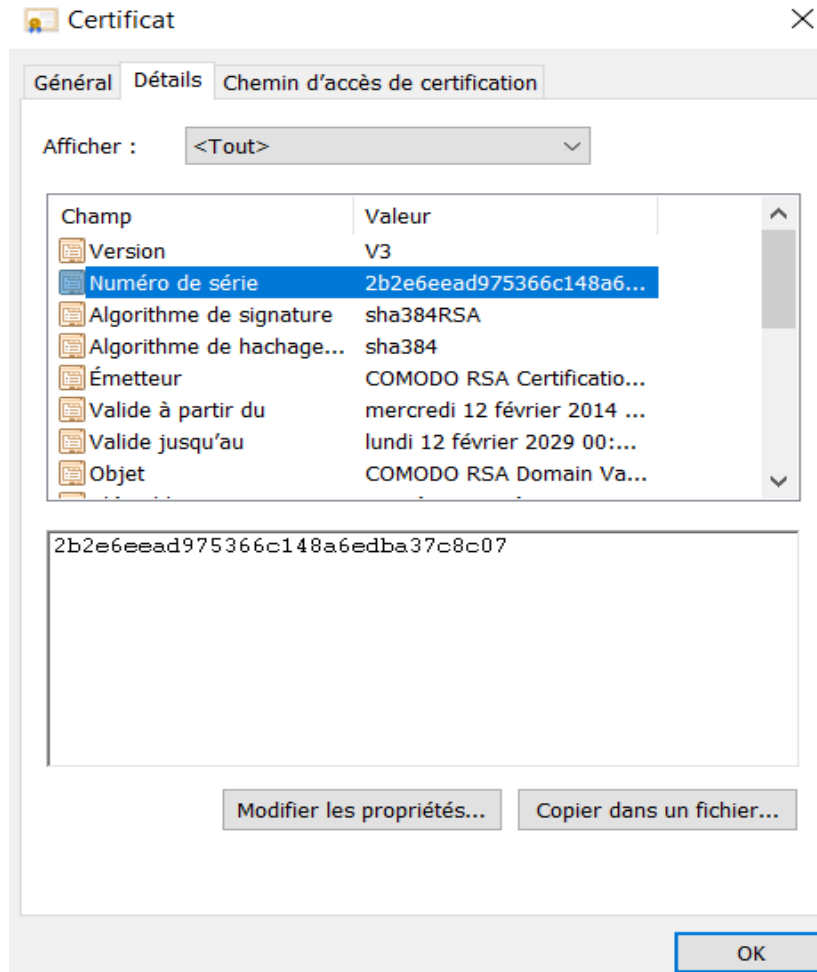
Détails de certificat

Microsoft Publisher, Signature du code

Affichage

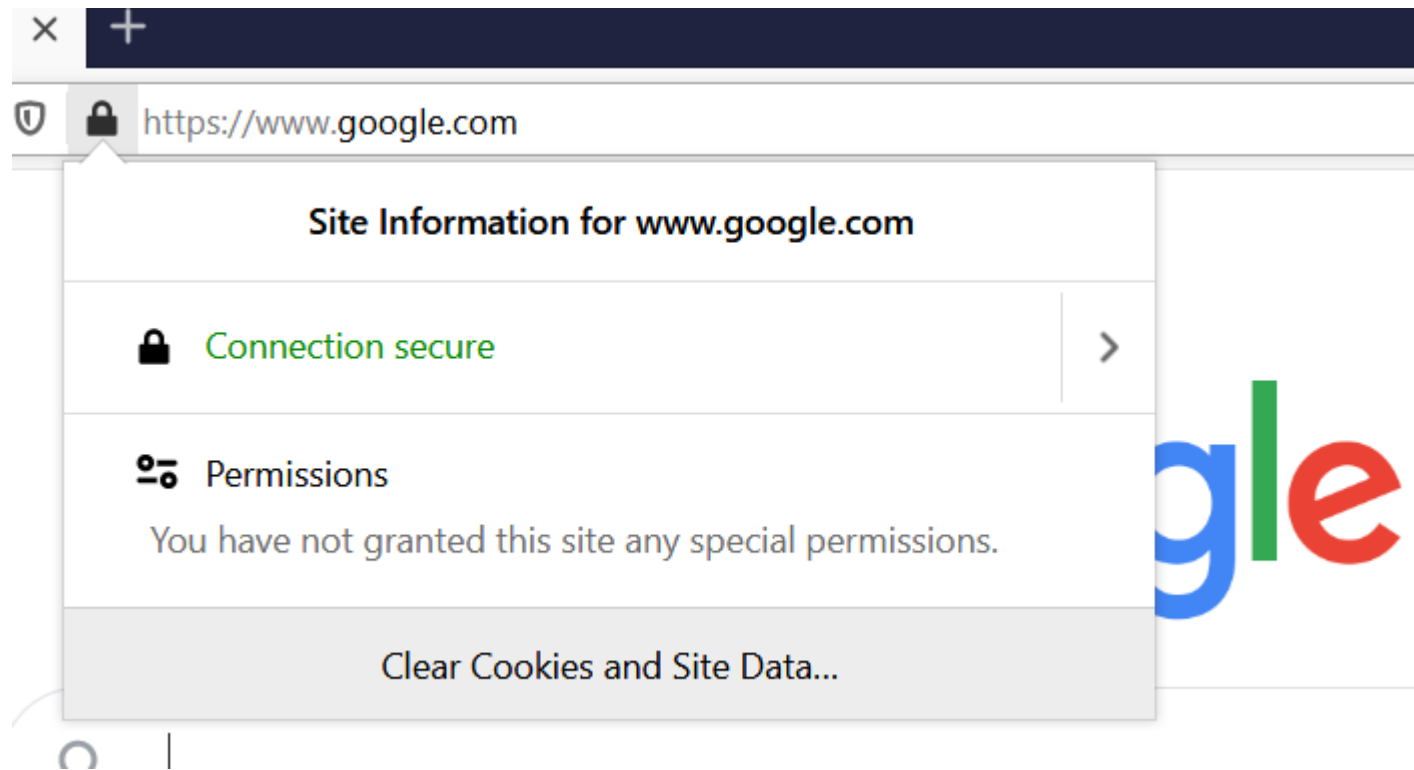
Fermer

Certificat numérique



Certificat numérique

Dans votre navigateur : Google



Certificat numérique



Page Info — https://www.google.com/

General Media Permissions **Security**

Website Identity

Website: www.google.com

Owner: This website does not supply ownership information.

Verified by: Google Trust Services [View Certificate](#)

Expires on: Tuesday, January 26, 2021

Privacy & History

Have I visited this website prior to today? Yes, 281 times

Is this website storing information on my computer? Yes, cookies and 11.3 MB of site data [Clear Cookies and Site Data](#)

Have I saved any passwords for this website? No [View Saved Passwords](#)

Technical Details

Connection Encrypted (TLS_AES_128_GCM_SHA256, 128 bit keys, TLS 1.3)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

[Help](#)

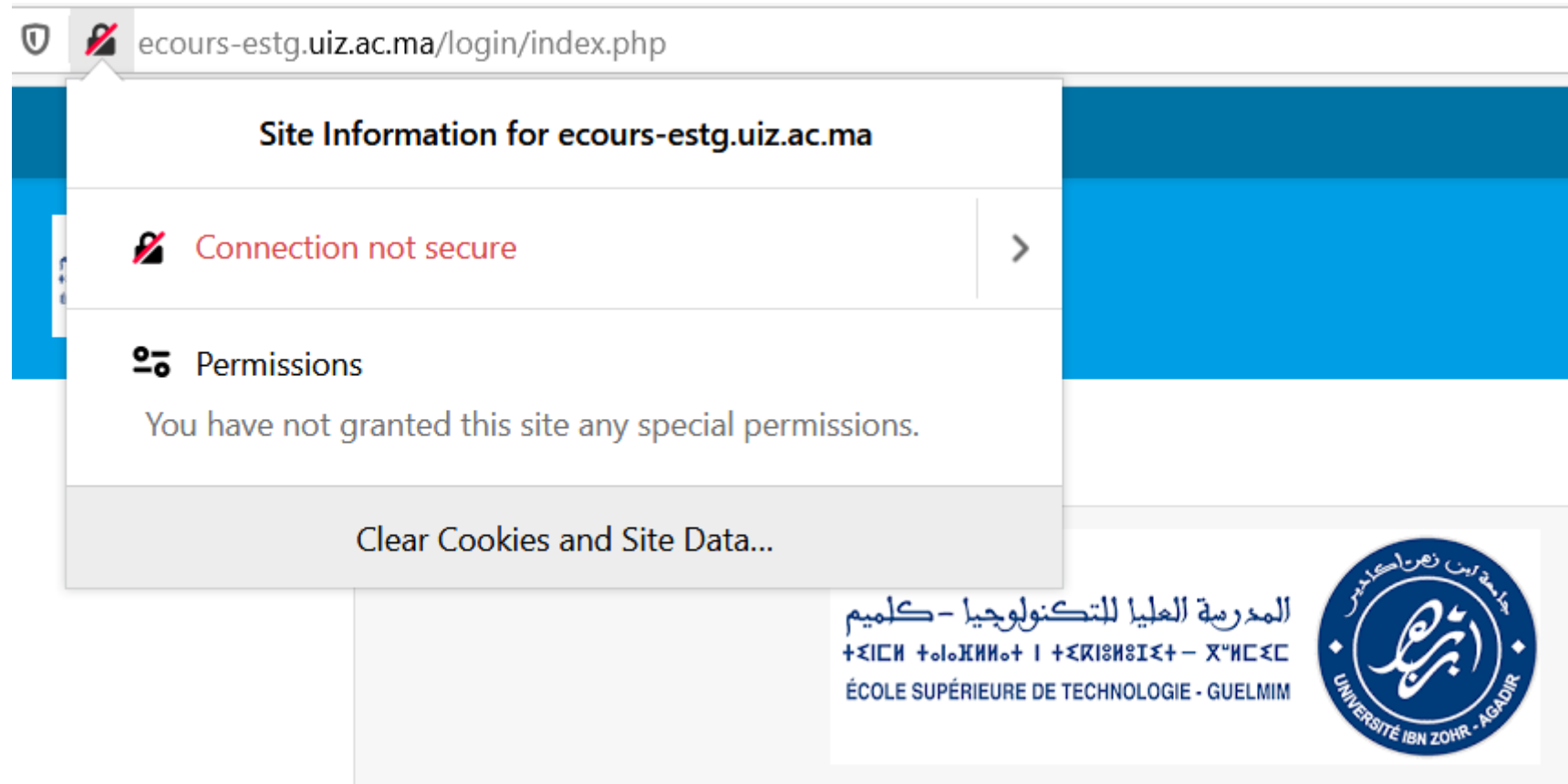
Certificat numérique



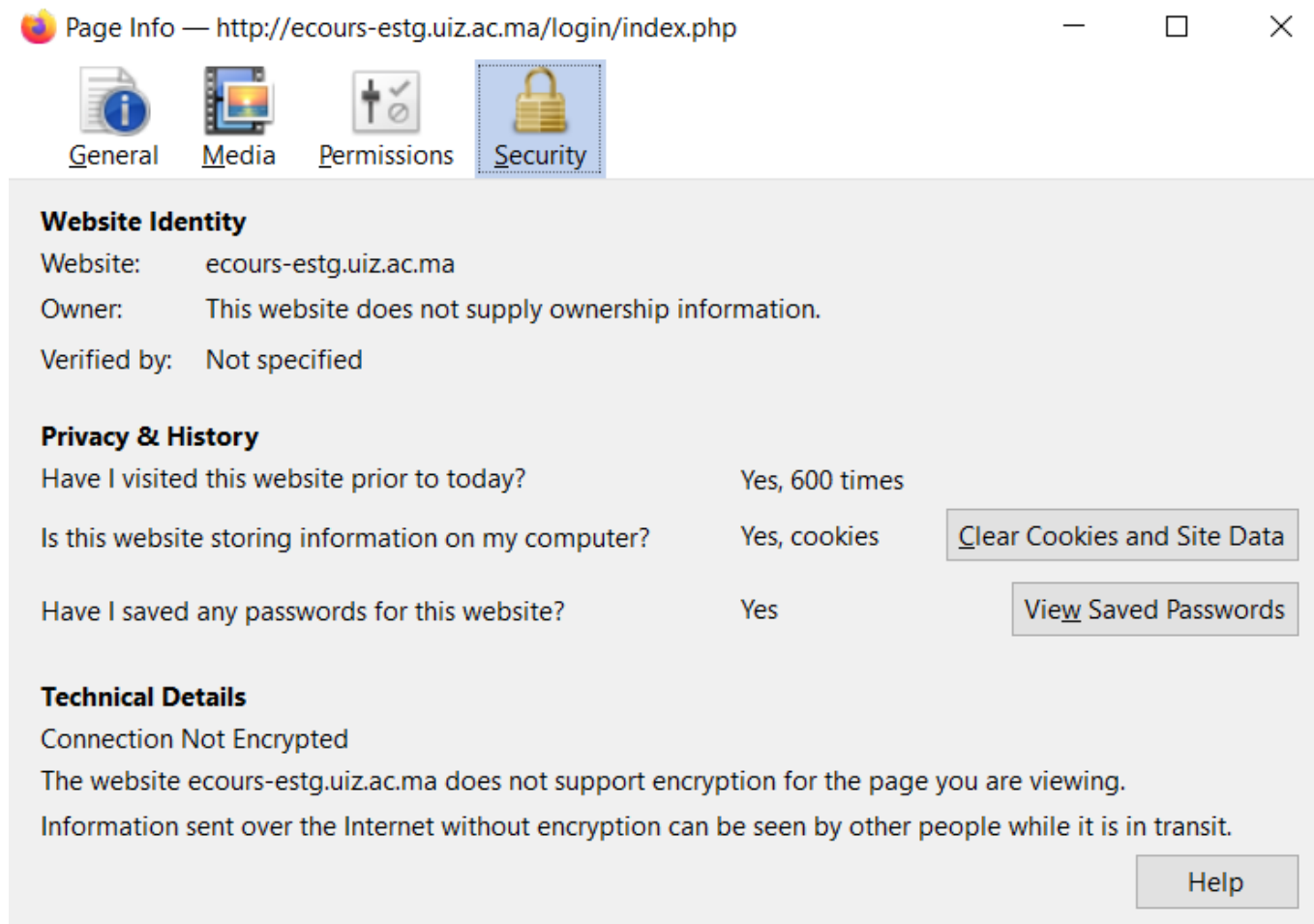
Subject Alt Names	
DNS Name	www.google.com
Public Key Info	
Algorithm	Elliptic Curve
Key Size	256
Curve	P-256
Public Value	04:A2:C8:48:9B:8D:97:BC:87:E6:3C:AC:2B:6C:A4:A9:51:44:2D:D6:4C:55:34:5B:14:...
Miscellaneous	
Serial Number	00:E5:89:50:14:FF:A6:56:CF:02:00:00:00:80:55:FE
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
Download	PEM (cert) PEM (chain)
Fingerprints	
SHA-256	8D:E8:36:F2:2B:52:79:56:94:47:54:94:8B:2B:CA:D6:CD:CF:87:AA:47:A7:E0:B0:F4:6...
SHA-1	71:51:3E:C3:A9:3E:54:97:03:53:B4:78:15:06:73:2B:16:EB:49:48

Certificat numérique

Dans votre navigateur : <http://ecours-estg.uiz.ac.ma/login/index.php>



Certificat numérique



Cookies



Les cookies sont des fichiers créés par le serveur mais stockés coté client. Ils ont plusieurs utilités :

- Traçabilité de clients,
- Identification sécurisée des utilisateurs (admin) d'un site,
- Enregistrement de données sur l'utilisateur pour des sites.

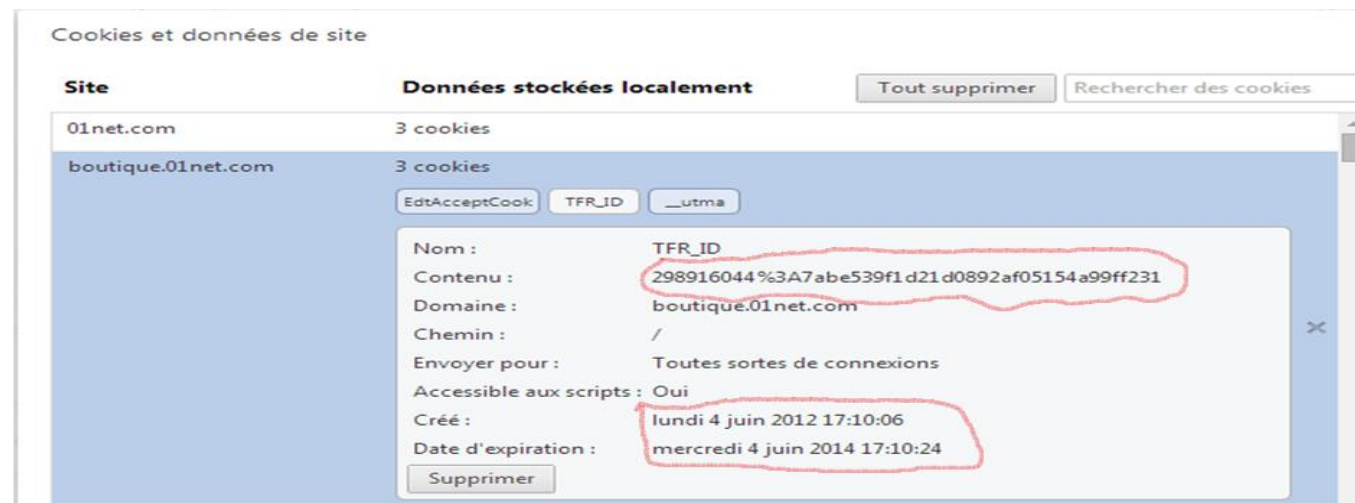
La transitions et le stockage de ces informations sur le réseau se fait en clair. Il existe deux types de cookies :

- ***Cookies Session*** : il s'expire à la fin de chaque session navigateur.
- ***Cookies Persistants*** : ce type n'est pas lié au navigateur. Il persiste à la longue de vie d'un compte utilisateur, mais on peut le supprimer manuellement.

Sessions

ID de session est un numéro d'identification généré par le serveur afin d'attribuer les demandes d'un utilisateur à la session en cours.

- Cet ID de session est localement sauvegardé par l'utilisateur sous la forme d'un cookie;
- Éviter l'utilisation des processus statique (comme l'incrémentation);
- Penser à l'utilisation des générateurs pseudo-aléatoires imprévisibles;
- Dans une communication réseau, il sert à identifier une [session](#);



Stockage et cryptage des mots de passe sous Linux

Premièrement, la sécurité des mots de passes sous UNIX étaient fondée sous un **algorithme de chiffrement symétrique DES**. Ils étaient stockés **dans le deuxième champ** de chaque ligne de **/etc/passwd** (fichier root avait le droit de lecture pour tout le monde).

Mais, suite à la **sensibilité** des **mots de passe**, ils ont changé :

- Le lieu de stockage **/etc/passwd** → **/etc/shadow**;
 - Il ont remplacé le mot de passe dans le fichier par le caractère x;
- La fonction de cryptage **DES** → **MD5**;

Exemple d'une ligne de stockage dans le fichier **/etc/passwd** :

asimi:x:1000:1000:ASIMI,,,:/home/asimi:/bin/bash

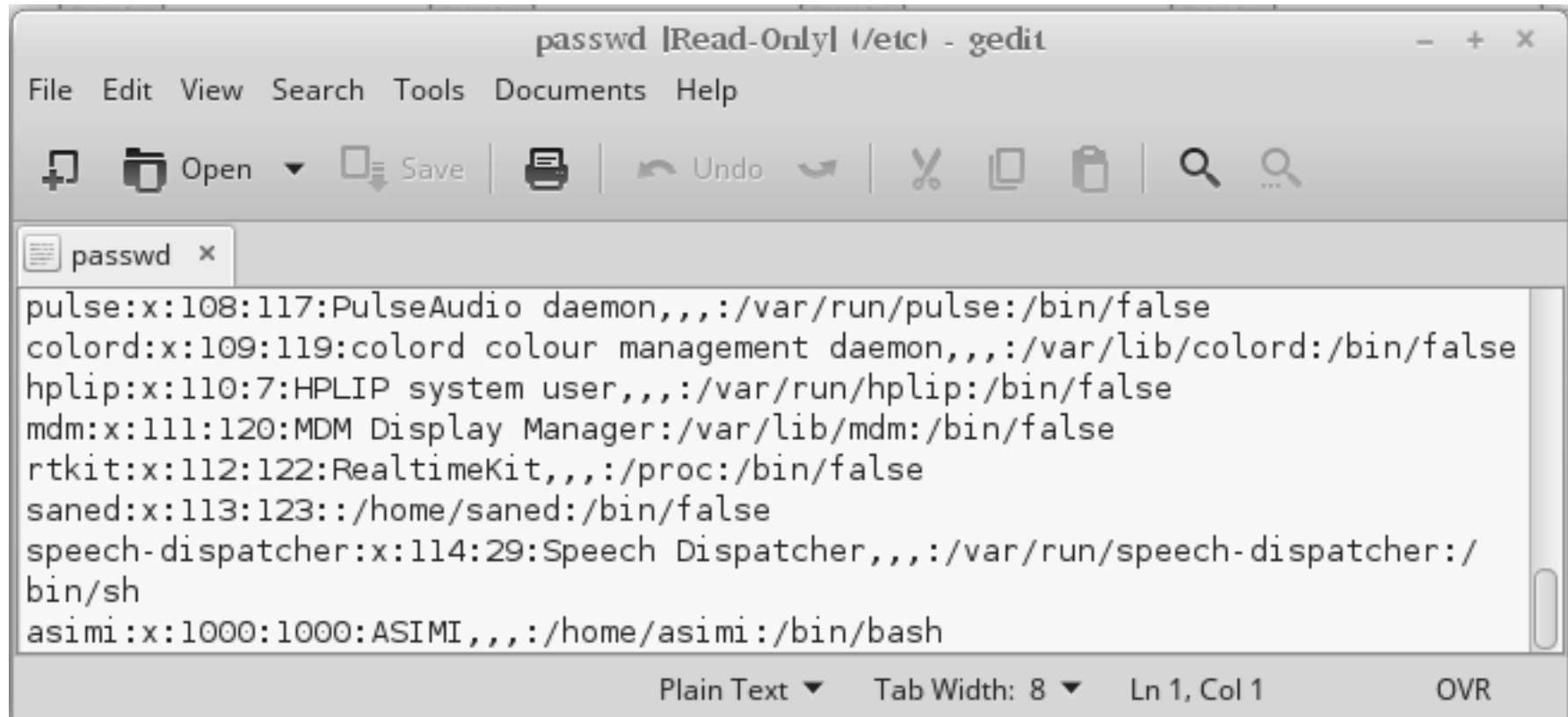
Field	Description
asimi	Login
x	Mot de passe crypté et stocké dans /etc/shadow;
1000	UID
1000	GID
ASIMI,,,	Infos ou commentaire
/home/asimi	répertoire de connexion;
/bin/bash	interpréteur de commandes

Stockage et cryptage des mots de passe sous Linux

La seule personne qui a le pouvoir de changer les informations propres à un utilisateur dans le fichier `/etc/passwd` est **le superutilisateur (root)**:

- **Login**: nom du compte de l'utilisateur ;
- **X**: mot de passe de l'utilisateur (chiffré) ;
- **UID**: identifie l'utilisateur pour le système d'exploitation (UID=User ID) ;
- **GID**: identifie le groupe de l'utilisateur (GID=Group ID) ;
- **Commentaire**: donne des informations sur l'utilisateur ou bien son nom réel;
- **Répertoire de connexion**: après s'authentifier, l'utilisateur se trouve dans ce répertoire **:/home/asimi**;
- **Interpréteur de commandes**: est l'interpréteur des commandes par défaut après connexion au système : **/bin/bash**;

Système d'exploitation



The image shows a screenshot of a gedit text editor window. The title bar reads "passwd [Read-Only] (/etc) - gedit". The menu bar includes "File", "Edit", "View", "Search", "Tools", "Documents", and "Help". The toolbar contains icons for opening, saving, printing, undo, redo, cut, copy, paste, and search. A single tab labeled "passwd" is open. The text area displays the contents of the /etc/passwd file, listing system users and the root user. The status bar at the bottom indicates "Plain Text", "Tab Width: 8", "Ln 1, Col 1", and "OVR".

```
passwd [Read-Only] (/etc) - gedit
File Edit View Search Tools Documents Help
+ Open Save | Print | Undo Redo | Cut Copy Paste | Search
passwd x
pulse:x:108:117:PulseAudio daemon,,,:/var/run/pulse:/bin/false
colord:x:109:119:colord colour management daemon,,,:/var/lib/colord:/bin/false
hplip:x:110:7:HPLIP system user,,,:/var/run/hplip:/bin/false
mdm:x:111:120:MDM Display Manager:/var/lib/mdm:/bin/false
rtkit:x:112:122:RealtimeKit,,,:/proc:/bin/false
saned:x:113:123::/home/saned:/bin/false
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/sh
asimi:x:1000:1000:ASIMI,,,:/home/asimi:/bin/bash
Plain Text Tab Width: 8 Ln 1, Col 1 OVR
```

Système d'exploitation

Le fichier `/etc/passwd` est public. Par contre certains systèmes ont introduit le fichier `/etc/shadow`, lisible seulement par **l'utilisateur root**.



Stockage et cryptage des mots de passe sous Linux

Le résultat de **cryptage** d'un mot de passe crypté dans **/etc/shadow** ressemble à :

\$1\$s1f5m5j4\$oLyi.z6g6/.Fx4x0y6nxD0

Ce mot de passe crypté se compose de deux parties:

- **Première partie : \$1\$s1f5m5j4\$** correspond au **salt**:
 - Elle commence toujours par **\$1\$** et finit par **\$**;
 - Le "**salt**" est une chaîne aléatoirement, qui n'est pas secrète, et qui sert à **perturber** le **cryptage**;
 - Le "**salt**" devrait être régénérer par **régénérateur aléatoire**;
- **Deuxième partie : oLyi.z6g6/.Fx4x0y6nxD0** est le mot de passe **crypté** :
 - Il est crypté à l'aide de la **fonction** de **hachage MD5**;
 - **Cette fonction de hachage est montrée cassable**;

Connexion d'un utilisateur

Le rôle d'un administrateur est de veiller sur le bon fonctionnement des SE. Il peut également avoir la tâche d'administrer le réseau, les bases de données, ..., la gestion des utilisateurs et des groupes;

- ❖ Comment être « root »?

Le nom de l'administrateur d'un système Linux est « root ». Pour avoir les privilèges de root ou bien de super user, il faut prendre l'identité de root.

- ❖ Connexion en tant qu'utilisateur root:

Login: root

Password: caché

#

#exit ou bien logout

Connexion d'un utilisateur

Il est aussi possible de prendre les droits de root temporairement, grâce à la commande **su**:

\$su

password: caché

#(Administrateur)

#exit

\$ (utilisateur ordinaire)

Question : expliquer la différence entre les commandes suivantes : su et su -l ;

Remarques:

- Le caractère **tilde (~)** indique que vous êtes dans votre répertoire personnel.
- Le signe **dollar (\$ ou bien #)** indique que le **shell bash** attend la saisie d'une commande.

Connexion d'un utilisateur

Remarques

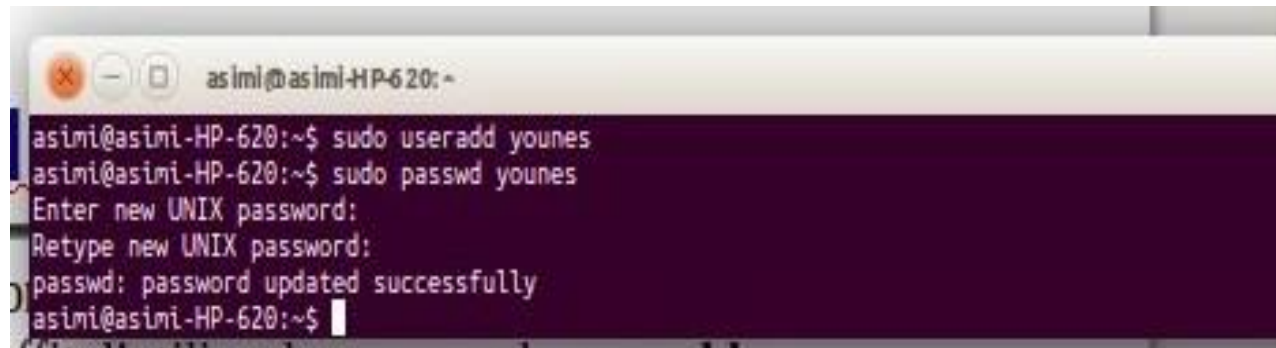
- Root peut changer l'invité du shell (#).
- Il est déconseillé de travailler toujours en tant que **root**.
- Il est préférable de disposer d'un compte ordinaire et d'exécuter la commande **su**.
- On utilise le symbole **\$** pour un utilisateur **ordinaire** et le symbole **#** pour **root**.
- Une erreur lors de la saisie du nom peut être annulée par la combinaison de touches **<ctrl-u>**.

Gestion des groupes et des utilisateurs

- ❖ **useradd, usermod, userdel:** gèrent les comptes utilisateurs;
- ❖ **groupadd, groupmod, groupdel:** gèrent les groupes;
- ❖ **passwd:** permet de gestion des mot de passe d'utilisateurs;

Création d'un utilisateur

Coté protection, la première action à réaliser par un administrateur est de créer un compte pour chaque utilisateur. Pour ceci, il suffit d'utiliser la commande **useradd**.



```
asimi@asimi-HP-620: ~$ sudo useradd younes
asimi@asimi-HP-620: ~$ sudo passwd younes
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
asimi@asimi-HP-620: ~$
```

- La commande **useradd** permet de créer un utilisateur en précisant des informations associées;
- Un utilisateur peut à tout moment changer son mot de passe par la **commande passwd**.

Modification de Super User

La commande **usermod** modifie les fichiers d'administration des comptes du système selon les modifications qui ont été indiquées sur la ligne de commande. Les options qui s'appliquent à la commande **usermod** sont :

- **-d --home** ou bien **-m --move-home**: nouveau répertoire de connexion de l'utilisateur.
- **-l --login**: Le nom de l'utilisateur passera de *login*.
- **-a, --append**: Ajouter l'utilisateur aux groupes supplémentaires (-G).
- **-c, --comment**: La nouvelle valeur du champ de commentaire du fichier de mots de passe pour l'utilisateur.
- **-p, --password**: Mot de passe chiffré (par MD5)
- **-e, --expiredate**: Date à laquelle le compte utilisateur sera désactivé (**format** AAAA-MM-JJ).
-

■ **Modification de Super User**

Quelques options doivent être passées à *usermod* afin qu'elles aient un résultat intéressant.

Exemple: `sudo usermod login nouvel_identifiant --home
nouvel_emplacement_du_dossier_personnel movehome
identifiant_actuel`

- ❖ *login* précise le nouvel identifiant qui devra être attribué au compte d'utilisateur. C'est la seule option qu'il est obligatoire de fournir ;
- ❖ *home* indique l'emplacement du dossier personnel de l'utilisateur. Si cette option n'est pas précisée, *l'emplacement actuel du dossier personnel est conservé* ;

Modification de Super User

❖ ***movehome***: déplace le contenu du dossier personnel actuel vers le nouvel emplacement, défini à l'option *home*.

❖ ***identifiant_actuel*** : désigne le nom du compte dont l'identifiant doit être changé.

```
asimi@asimi-HP-620:~$ sudo usermod -l youness -d /home/asimi -m kaka
usermod: directory /home/asimi exists
asimi@asimi-HP-620:~$
```

Limitations:

- L'identifiant d'un compte d'utilisateur ne peut pas être modifié lorsqu'une session est **ouverte** avec ce compte ;
- Seul un **superutilisateur** peuvent modifier l'identifiant d'un compte d'utilisateur..

Suppression de Super User

La suppression d'un compte utilisateur se décompose en deux phases :

- La suppression de l'utilisateur dans les fichiers de configuration (**/etc/passwd**, **/etc/group ...**)
- La suppression du répertoire et des fichiers de configuration d'un utilisateur.

La commande ***userdel*** permet de faire soit la première étape soit de réaliser les deux d'un coup.

Pour supprimer l'utilisateur ASIMI dans les fichiers de configuration du système, utilisez la commande suivante :

```
[root@root]# userdel ASIMI
```

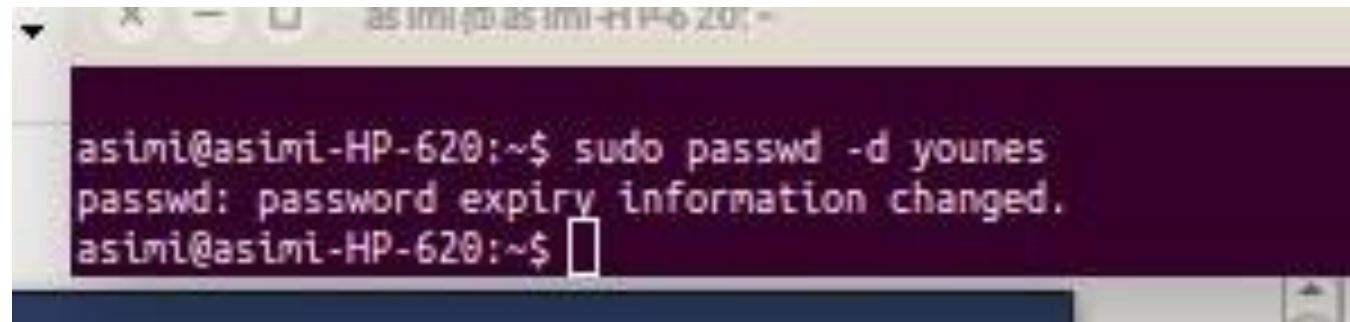
Pour supprimer d'un coup l'utilisateur et son répertoire (ici /home/asimi), on utilise la commande suivante :

```
[root@root]# userdel -r ASIMI
```


Suppression de Super User

Pour supprimer un mot de passe d'un compte utilisateur **asimi**, il suffit d'utiliser la commande *passwd*.

#passwd -d asimi

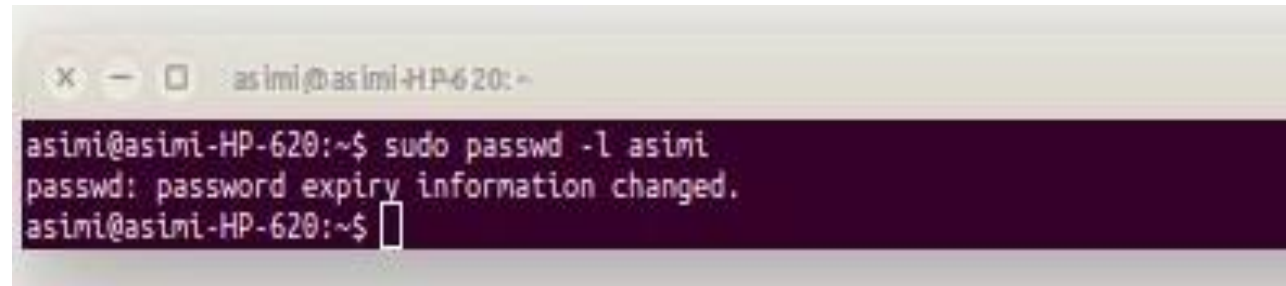


```
asimi@asimi-HP-620:~$ sudo passwd -d younes
passwd: password expiry information changed.
asimi@asimi-HP-620:~$
```

Verrouiller un compte

- Verrouiller le compte **asimi**, ce qui empêche sa connexion:

#passwd -l asimi



```
asimi@asimi-HP-620:~$ sudo passwd -l asimi
passwd: password expiry information changed.
asimi@asimi-HP-620:~$
```

usermod --expiredate 1 nom_utilisateur

Options de la commande **passwd**:

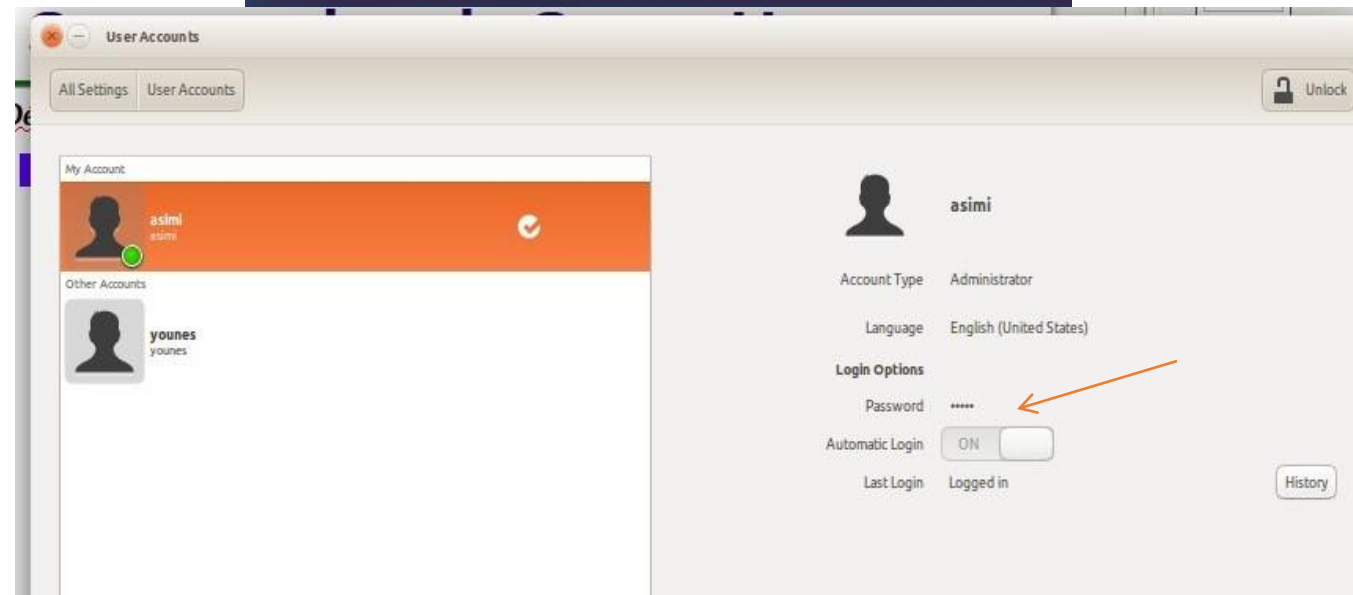
- l** : Permet de verrouiller le compte de l'utilisateur;
- f** : force le changement de mot passe à la prochaine connexion;
- d** : Supprime le mot de passe d'un utilisateur.

Déverrouiller un compte

■ Déverrouiller le compte **asimi**,

#passwd -u asimi

```
asimi@asimi-HP-620:~$ sudo passwd -u asimi
passwd: password expiry information changed.
asimi@asimi-HP-620:~$
```



Création de Groupe

Le fichier système **/etc/group** contient la liste des groupes systèmes ainsi que leurs membres. Le format d'une ligne est le suivant:

Nom_du_groupe:X:GID :membre1, membre2...

Exemple:

```
root:x:0:root
Bin:x:1:root,bin,daemon
Apache:x:43:
Joe:x:500:
Alex:x:501:
Developper:x:1000:Alex,Joe
```



Création de Groupe

Caractéristique du fichier /etc/group:

Nom:X:GID:utilisateurs appartenant à ce groupe

Détails

Nom :

Nom du groupe;

Mot de passe X :

Représente le mot de passe du groupe (déconseillé aujourd'hui);

GID :

Représente le Numéro du groupe;

Utilisateur(s) :

Mets tous les utilisateurs séparés par une virgule;

Création de Groupe

Pour créer un groupe des utilisateurs, il suffit d'utiliser la commande **groupadd**.

#groupadd -g [or -G] GID nameGroup

- **g initial_group**: le groupe initiale;
- **G group,...**: les groupes supplémentaires;

Créer des groupes de GID: 2017, 2018:

#groupadd -g 100 nameGroup

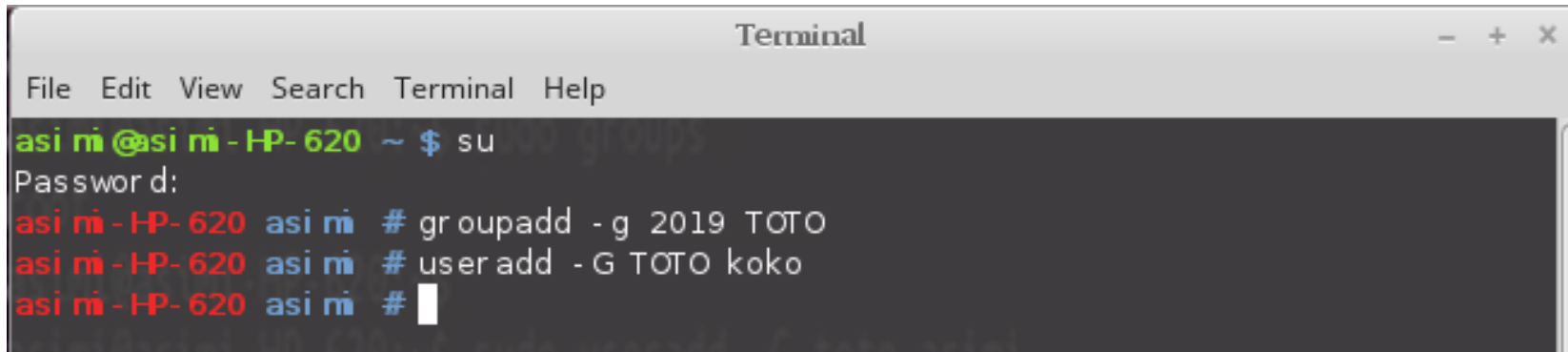
Ajouter un utilisateur à un groupe,

#useradd -G Groupe1, Groupe2, ... nameUser

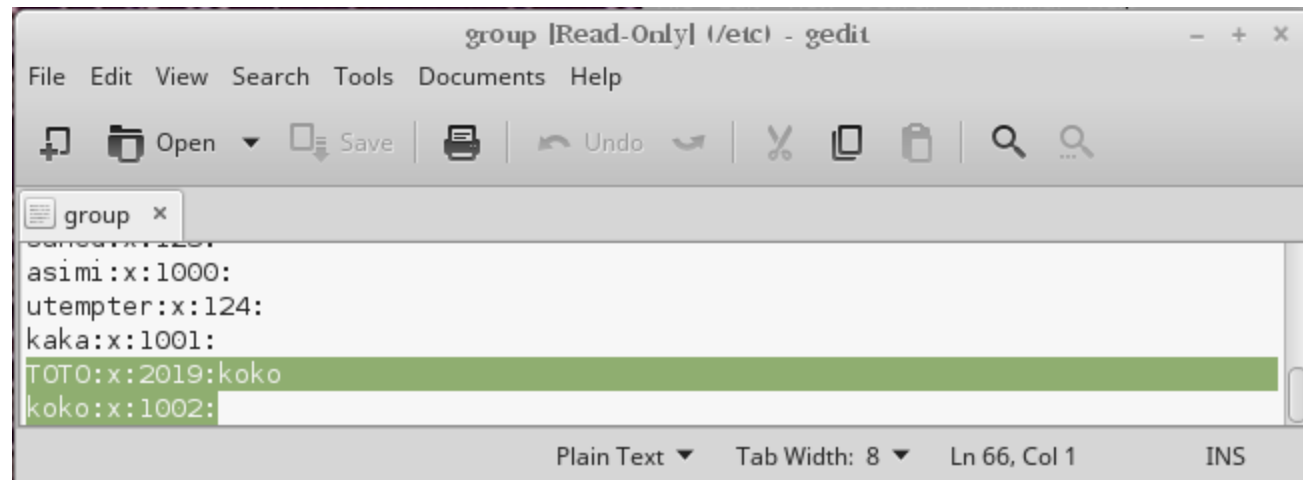
Lister les groupes d'utilisateur:

#groups nameUser

Création de groupe



```
Terminal
File Edit View Search Terminal Help
asi mi@asi mi -HP- 620 ~ $ su
Password:
asi mi -HP- 620 asi mi # groupadd -g 2019 TOTO
asi mi -HP- 620 asi mi # useradd -G TOTO koko
asi mi -HP- 620 asi mi #
```



```
group [Read-Only] (/etc) - gedit
File Edit View Search Tools Documents Help
[Icons] Open Save [Icons] Undo [Icons]
group x
asimi:x:1000:
utempter:x:124:
kaka:x:1001:
TOTO:x:2019:koko
koko:x:1002:
Plain Text Tab Width: 8 Ln 66, Col 1 INS
```

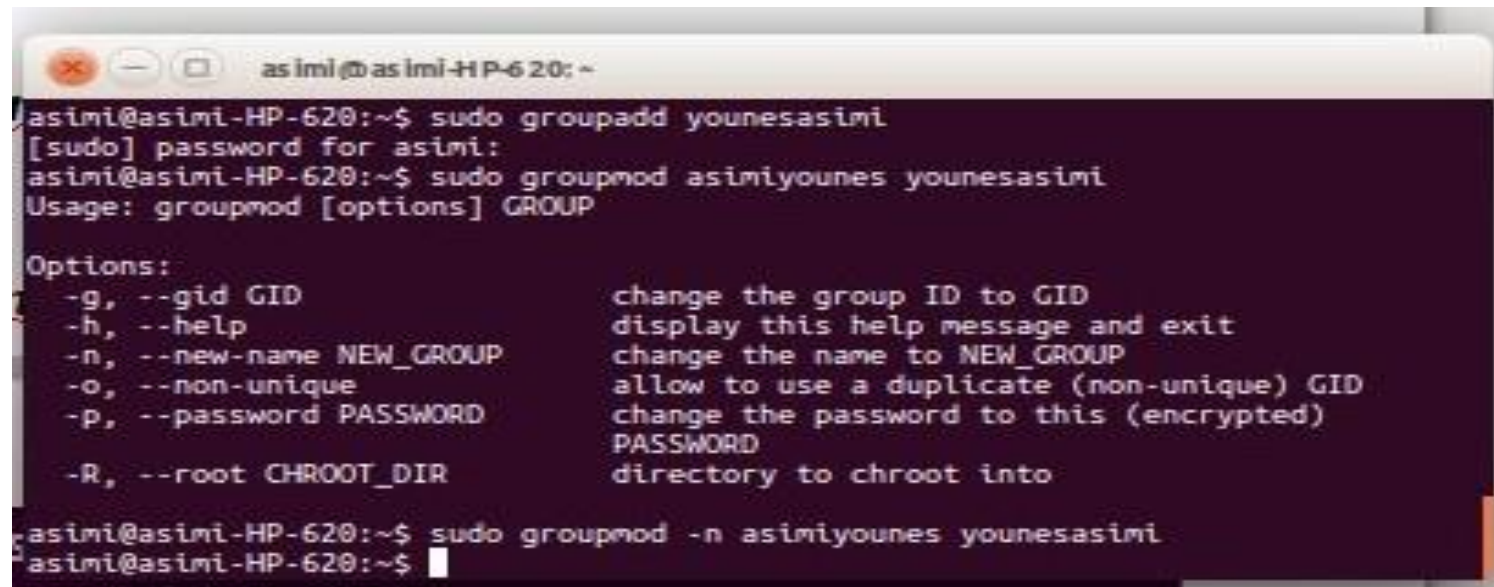
Modification de Groupe

Pour modifier le nom d'un groupe des utilisateurs, il suffit d'utiliser la commande **groupmod**.

#groupmod *newname* [-n] *nouveau_nom* *nom_actuel*

Exemple:

groupmod -n asimi younes

A terminal window titled 'asimi@asimi-HP-620: ~' showing a series of commands and their outputs. The user 'asimi' runs 'sudo groupadd younesasimi', then '[sudo] password for asimi:', then 'sudo groupmod asimiyounes younesasimi'. This last command results in a 'Usage' error. The user then views the help for 'groupmod' using 'man groupmod', which displays a list of options: -g, --gid, -h, --help, -n, --new-name, -o, --non-unique, -p, --password, and -R, --root. Finally, the user runs 'sudo groupmod -n asimiyounes younesasimi' successfully.

```
asimi@asimi-HP-620:~$ sudo groupadd younesasimi
[sudo] password for asimi:
asimi@asimi-HP-620:~$ sudo groupmod asimiyounes younesasimi
Usage: groupmod [options] GROUP

Options:
  -g, --gid GID                change the group ID to GID
  -h, --help                    display this help message and exit
  -n, --new-name NEW_GROUP      change the name to NEW_GROUP
  -o, --non-unique              allow to use a duplicate (non-unique) GID
  -p, --password PASSWORD       change the password to this (encrypted)
                                PASSWORD
  -R, --root CHROOT_DIR        directory to chroot into

asimi@asimi-HP-620:~$ sudo groupmod -n asimiyounes younesasimi
asimi@asimi-HP-620:~$
```


Suppression de groupe

Pour supprimer un groupe des utilisateurs, il suffit d'utiliser la commande *groupdel*.

#groupdel nameGroup

A terminal window titled 'asimi@asimi-HP-620: ~' with standard window control buttons. The terminal shows the following commands and output:

```
asimi@asimi-HP-620:~$ sudo groupdel younesasimi
asimi@asimi-HP-620:~$ sudo useradd -G younesasimi younes
useradd: group 'younesasimi' does not exist
asimi@asimi-HP-620:~$
```

Cryptographie Asymétrique

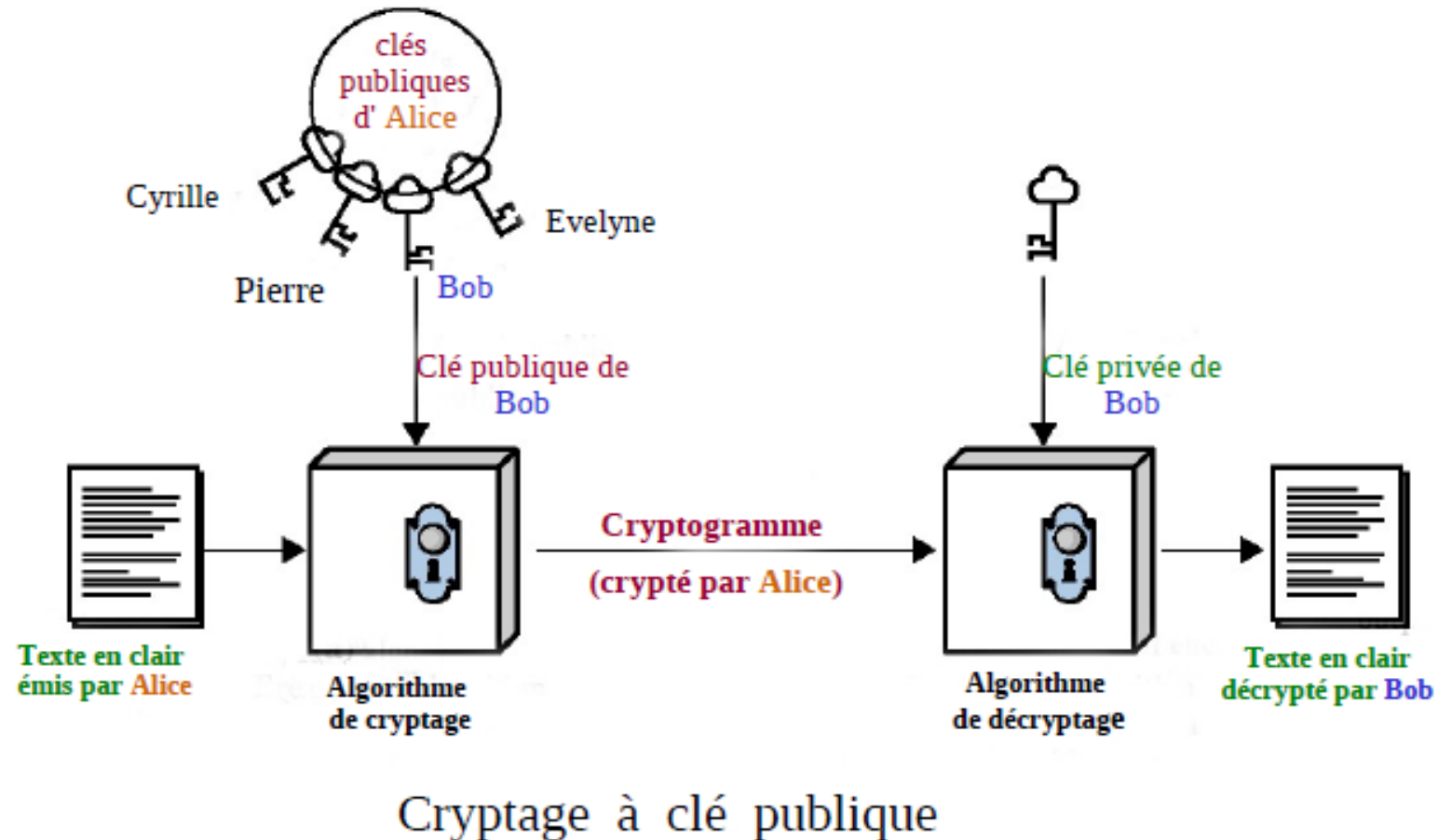


La cryptographie à clef publique repose sur un schéma asymétrique qui utilise une paire de clefs pour le chiffrement : **une clef publique**, qui chiffre les données, et **une clef privée correspondante**, aussi appelée clef **secrète**, qui sera utilisée pour le déchiffrement.

Parmi les crypto-systèmes à clef publique, on cite:

- Elgamal (Taher Elgamal);
- **RSA**;
- Diffie Hellman;
- DSA, l'Algorithme de Signature Digitale;

Cryptographie Asymétrique



Cryptosystème RSA

Supposons que Alice souhaite communiquer avec Bob en utilisant RSA, chacune de deux personnes crée:

- une clef publique qu'elle diffuse à ses correspondants ;
- une clef privée qu'elle **cache soigneusement**.

Algorithme de création des clefs :

- Elle choisit deux grands nombres premiers distincts p et q .
- Elle calcule $n = pq$ et $\varphi(n) = (p - 1)(q - 1)$.
- Elle choisit un entier $e \in \{2, \dots, n - 1\}$ premier avec $\varphi(n)$.
- Elle détermine $e^{-1} = d \in \{2, \dots, n - 1\} : de = 1 \bmod \varphi(n)$.
- La clef *privée* d'Alice est d et sa *clef publique* est (n, e) .

Cryptosystème RSA

Algorithme de chiffrement

Lorsque Alice veut envoyer un message confidentiel à Bob :

- Alice code le message en code ASCII de taille trois.
- Il représente le message par un nombre $m \in \{1, \dots, n-1\}$;
- Il se procure la **clef publique (n, e) de Bob**; *il doit s'assurer qu'il s'agit effectivement de la clef publique de Bob (Certificat numérique).*
- Il calcule $c \equiv m^e \bmod n$ *qui est un bloc chiffré.*
- Il transmet la concaténation des **c à Bob**.

Cryptosystème RSA

Algorithme de déchiffrement

Lorsque Bob reçoit le message **c**, il calcule le texte en clair en utilisant sa clef privée **d** : $m = c^d \bmod n$.

Remarques:

- La compréhension de RSA nécessite quelques connaissances mathématiques plus précisément des connaissances sur **l'arithmétique ou calculs modulaires**.
- Le RSA est encore le système cryptographique à clef publique le **plus utilisé dans le monde de nos jours**.

ETUDE DE RSA

Les fonctions composantes de RSA :

- Calcul de n et $\ell(n)$.
- Génération de la clé publique e (recherche des nombres premiers avec $\ell(n)$).
- Génération de la clé privée d (calcul d'inverse).
- Cryptage (chiffrement).
- Décryptage (déchiffrement).

Les opérations utilisées dans RSA :

- Soustraction;
- Multiplication;
- Puissance;
- Modulo;
- Division.

ETUDE DE RSA

Description du fonctionnement des composantes:

- *Calcul de n et $\ell(n)$* : après avoir choisis les deux nombre p et q qui sont deux paramètres d'entrée de RSA, l'algorithme procède au calcul de $n = p * q$ et $\ell(n) = (p-1)(q-1)$.
- *Génération de e* : pour la génération de la clé publique e l'algorithme recherche l'ensemble des nombres qui *seront premiers avec $\ell(n)$ et inférieurs à n* .
- *Génération de d* : la génération de la clé privée consiste à trouver l'inverse de e de tel sorte que : $e * d = 1 \% n$.
- *Cryptage* : le chiffrement se fait comme suit : $C = M^e \% n$.
- *Décryptage* : $M = C^d \% n$.

ETUDE DE RSA

Si une clé public e accepte son propre inversible d , *on* aura $e = d$. *Dans ce cas*, la clé est utilisée pour le chiffrement et le déchiffrement du message (chiffrement symétrique).

- ❖ On propose $p = 7$ et $q = 11$;
- ❖ On détermine toutes des clés pour que RSA soit **symétrique & asymétrique**;
 - $n = p * q = 7 * 11 = 77$;
 - $\ell(n) = (p-1)(q-1) = (7-1)*(11-1) = 60$;
 - $e \in \{2, \dots, 77\} \setminus \text{PGCD}(e, 60) = 1$;
 - $e \in \{7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 51, 53, 57, 59, 61, 71, 73\}$;
- ❖ Pour que RSA soit symétrique, on doit vérifier que chaque clé accepte son propre inversible: $x * x = 1 \% 60$;
 - RSA symétrique: $\{11, 19, 29, 31, 41, 49, 59, 61, 71\}$;
 - RSA asymétrique: $\{7, 13, 17, 23, 37, 43, 47, 53, 67, 73\}$.

ETUDE DE RSA



Cas clé publique $e = 7$:

- Dans ce cas RSA est asymétrique puisque la clé 7 se trouve dans l'ensemble asymétrique démontré dans la question précédente.
- Calcul de la clé privée d :

$$d \in \{7, 13, 17, 23, 37, 43, 47, 54, 67, 73\} \setminus d \cdot 7 = 1 \% 60$$

- On trouve alors dans cet ensemble que $d = 43$.

ETUDE DE RSA



Chiffrement avec RSA

Pour chiffrer un message avec RSA on commence tout d'abord par la conversion du message en code ascii de taille 3 le message choisis est « misr » :

$$M = \text{Misr} = \{109, 105, 115, 114\} : \text{code ASCII}$$

Ensuite il faut représenter le message en blocs de même taille que n qui est égale à 77 dans notre cas ; chaque bloc sera de taille 2 :

$$M = \{10, 91, 05, 11, 51, 14\}$$

Il faut aussi vérifier que les blocs contiennent des nombres inférieurs à n (77) ce qui nous pousse à réduire la taille de chaque bloc on obtient alors :

$$M = \{1, 0, 9, 1, 0, 5, 1, 1, 5, 1, 1, 4\}$$

ETUDE DE RSA



Chiffrement avec RSA

Maintenant on procède au calcul de C (message chiffré) :

$$C = \{1^7 \% 77, 0^7 \% 77, 9^7 \% 77, 1^7 \% 77, 0^7 \% 77, 5^7 \% 77, 1^7 \% 77, \\ 1^7 \% 77, 5^7 \% 77, 1^7 \% 77, 1^7 \% 77, 4^7 \% 77\}$$

$$C = \{1, 0, 37, 1, 1, 0, 47, 1, 1, 47, 1, 1, 60\}$$

ETUDE DE RSA

Déchiffrement du message

Pour le déchiffrement du message on aura :

$$M = \{1^{43} \% 77, 0^{43} \% 77, 37^{43} \% 77, 1^{43} \% 77, 1^{43} \% 77, 0^{43} \% 77, \\ 47^{43} \% 77, 1^{43} \% 77, 1^{43} \% 77, 47^{43} \% 77, 1^{43} \% 77, 1^{43} \% 77, \\ 60^{43} \% 77\}$$

$$M = \{1, 0, 9, 1, 0, 5, 1, 1, 5, 1, 1, 4\}$$

Ensuite on reprend la représentation en bloc de code ascii de taille 3 on obtient :

$$M = \{109, 105, 115, 114\} = \text{Misr}$$