Module: Cryptographie

3ème année licence en Informatique

Par : Prof. Cherif Foudil

Chapitre 6 : Gestion des clés

- Sécurité et attaques des systèmes actuels
- Gestion des clés

Sécurité et attaques des systèmes actuels

- Nous vous présentons ici une liste des types d'attaques sur les algorithmes :
- 1- **L'attaque en force (ou Brute force attack, Exhaustive key search attack**) Le cryptographe essaie toutes les combinaisons de clefs possibles jusqu'à l'obtention du texte clair. Avec des ordinateurs de plus en plus performants et des méthodes de calculs distribuées, l'attaque en force restera toujours un moyen de casser des systèmes de chiffrement.
- **2- L'attaque à l'aide de l'analyse statistique (ou Statistical analysis attack**) Le cryptographe possède des informations sur les statistiques du message clair (fréquences des lettres ou des séquences de lettres). Les systèmes tels que ceux par substitution ne résistent pas à une telle attaque.

Sécurité et attaques de systèmes actuels

- **3- L'attaque à l'aide de textes chiffrés seulement (ou Ciphertext-only attack)** Le cryptographe dispose de messages chiffrés par l'algorithme et fait des hypothèses sur le texte clair (présence d'expressions, de mots, le sens du message, format ASCII etc.). Il peut grâce à cela soit retrouvé les textes en clair, soit retrouver la clef.
- **4- L'attaque à l'aide de textes clairs (ou Known-plaintext attack)** Le cryptographe dispose des messages ou parties de message clairs et de leur version chiffrée. Le but du cryptographe est alors de retrouver la clef. Ce type d'attaque est très répandu

Sécurité et attaques de systèmes actuels

- **5- L'attaque à l'aide de textes clairs choisis (ou Chosen-plaintext attack)** Le cryptographe dispose des messages clairs et de leur version chiffrée. Il a aussi la possibilité de tester des messages et d'obtenir le résultat chiffré.
- **6- L'attaque d'une tierce personne (ou Man-in-the-middle attack)** Cette attaque est appelée l'attaque de «l'homme du milieu» intervient dans une transaction entre deux personnes(groupes…). Une troisième personne s'interpose de manière transparente entre les deux et termine la transaction normalement en captant les messages et en transmettant d'autres messages. Il peut donc ainsi intercepter et même modifier les messages envoyés sans que les deux entités s'en aperçoivent. Cette attaque peut être évitée avec les signatures digitales.

Gestion des clés

- La **sécurité du processus** des chiffrement repose en grande partie sur la **sécurité** et la **confidentialité des clés** utilisées, sur la robustesse des algorithmes et sur la sécurité des plates-formes matérielles et logicielles qui les supportent.

- **La durée de vie** d'une clé de chiffrement (et de déchiffrement) dépend de son utilisation. Il est conseillé de changer la clé périodiquement(changement des clés), tout en évitant les modification trop fréquentes qui rendent difficile la gestion des clés. En revanche, pour toutes les applications ouvertes au réseau, il est hautement souhaitable d'utiliser une clé à usage unique, particulière à chaque session de travail.
- **Le système de gestion de clés** basé sur l'usage d'une carte à puce (et d'un lecteur de carte) autorise l'usage d'une clé unique à chaque session de travail.

Gestion des clés

- **Les fonctions d'un système de gestion de clés** :permettent de réaliser les services suivants:

  - Génération d'une clé en fonction des besoins et des systèmes de chiffrement;
  - Distribution des clés aux entités (vérification, authentification des entités, etc.);
  - Stockage des clés de manière sécurisée (chiffrement des clés , sécurité du serveur, archivage fiable afin d'assurer la confidentialité et l' intégrité des clés);
  - Surveillance(monitoring), d' enregistrement, d'audit , de traçage, de sécurité, de test de bon fonctionnement, d'alarme de contrôle d' accès aux clés, etc.;
  - Destruction des clés inutiles (destruction physique, etc.);

- Dans un système d'information, plusieurs clés de chiffrement sont généralement utilisées. Il peut alors exister une certaine **hiérarchie des clés** (notion de clé maitresse, physiquement protégée, et de clés filles chiffrées à partir de celle-ci).

Protocole cryptographique

Définition:

ensemble de règles d'échange entre les participants d'un réseau , basé sur les notions de crypto-systèmes qui permettent de sécuriser les communications dans un environnement hostile afin de réaliser une certaine fonctionnalité (Confidentialité, Authentification, Echange de clé,…).

Problème du Logarithme discret

- Si g $\in Z_p^*$ avec p un nombre premier, cette fonction est définie par:

$$F_g : \begin{array}{ccc} \mathbb{Z}_p^* & \longrightarrow & \mathbb{Z}_p^* \\ x & \longrightarrow & g^x \bmod p \end{array}$$

- Etant donné x, il est facile de calculer $y = g^x \bmod p$ (exponentiation rapide).
- Par contre, on ne connait pas à ce jour de méthode rapide pour calculer $x = \log_g y \bmod p$, qui est appelé logarithme discret de y.

- Le protocole de Diffie Hellman

Merkle-Hellman-Diffie

Gestion des clés

- Echange de clés: Protocole Diffie et Hellman

  - Premier schéma de clé publique proposé en 1976.
  - Repose sur la notion de la fonction à sens unique et basé sur le problème du Logarithme discret..
  - C'est une méthode pratique pour l'échange public d'une clé secrète(ou de session), qui est souvent utilisée dans des produits commerciaux (SSL,...).

Gestion des clés (clé partagée)

Exemple de l' algorithme de Diffie Hellman pour créer une clé partagée

- Les deux participants (Alice et Bob) partagent deux paramètres non-secrets : un nombre premier p et un nombre g tel que $1 < g < p$.

  Chacun d'eux choisit une clé privée dans l'intervalle [1,.., p - 2], Alice choisissant une valeur a et Bob une valeur b .
- Chacun des participants calcule alors une valeur publique qu'ils s'échangent : Alice envoie $A = g^a \bmod p$ à Bob qui lui envoie $B = g^b \bmod p$.

  Bob calcule $A^b \bmod p$ et Alice calcule $B^a \bmod p$.
- Cette valeur étant nécessairement la même, ainsi, ils disposent d'une valeur k qui fait office de clé secrète partagée puisque on a :

  $k = B^a \bmod p = (g^b \bmod p)^a = g^{ba} \bmod p$

  $k = A^b \bmod p = (g^a \bmod p)^b = g^{ba} \bmod p$

Gestion des clés (clé partagée)

Exemple numérique de l' algorithme de Diffie Hellman

- Supposons à titre d'exemple, qu'Alice et Bob partagent les deux informations suivantes : p = 233 et g = 45 .

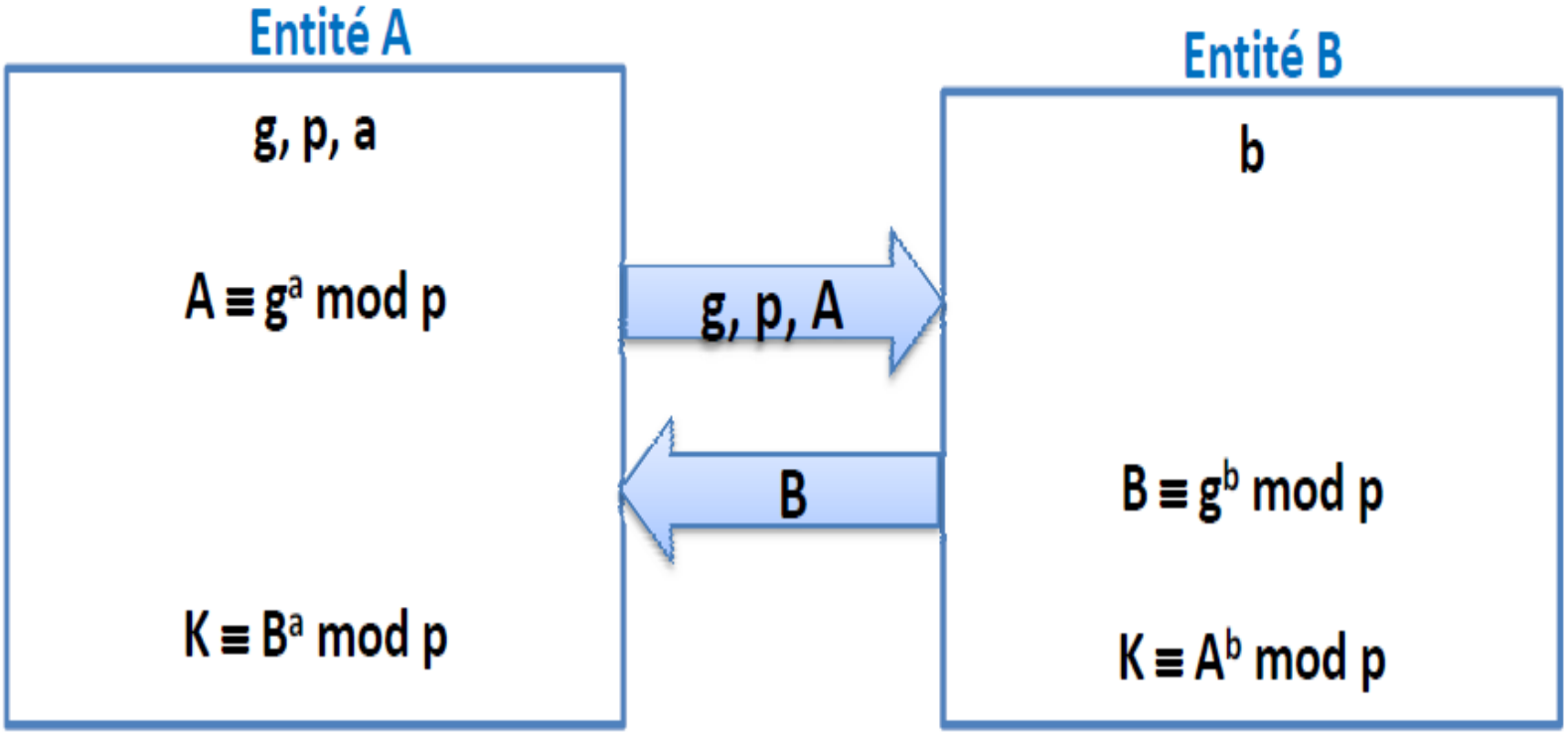
  Si Alice choisit a = 11 et Bob b = 20 , alors A = 45^{11} mod 233 =147 , B = 45^{20} mod 233 =195 .
- Aussi on a : B^a mod p=195^{11} mod 233=169 et A^b mod p=147^{20} mod 233 =169. Alice et Bob disposent d'une clé privée, k = 169 .
- La sécurité de cette technique repose sur la difficulté de calcul de k (= g^{ab} mod p) à partir de A= g^a mod p ou B= g^b mod p lorsque p est grand.

  La fonction utilisée dans cette méthode f (x) = g^x mod p est une fonction à sens unique : f (x) est facile à calculer, mais "retrouver x à partir de { f (x) , g et p }" est très délicat . L'algorithme de Diffie Hellman se base ainsi sur le problème du logarithme discret.

- **Question** : Comment casser l'algorithme de Diffie Hellman(DH)?

Gestion des clés (clé partagée)

Echange de clés: Protocole Diffie et Hellman



$$K \equiv B^a \bmod p \equiv (g^b)^a \bmod p \equiv (g^a)^b \bmod p \equiv A^b \bmod p$$

Gestion des clés (Clés partagée)

Les faiblesse de l' algorithme de Diffie Hellman

- 1- Quand Alice veut envoyer un message chiffré à Bob, elle doit d'abord entrer en contact avec lui afin de fixer la clé lors d'un premier échange; chaque transmission de message se trouve ainsi fortement ralentie et perd toute instantanéité. On parle dans ce cas du **problème d'authentification**.
- 2- Aussi l'algorithme de Diffie Hellman est menacé par le progrès en mathématiques car le problème difficile du logarithme discret peut être résolu dans le futur.

Gestion des clés (Clés partagée)

Les faiblesse de l' algorithme de Diffie Hellman

3- **Attaque active**: Le protocole est vulnérable aux attaques actives « par milieu» (*man-in-the-middle*):

Lors de l'échange des clés, l'intermédiaire choisit sa propre clé c et calcule $C = g^c \bmod p$. Il remplace a et b *par* cette valeur.

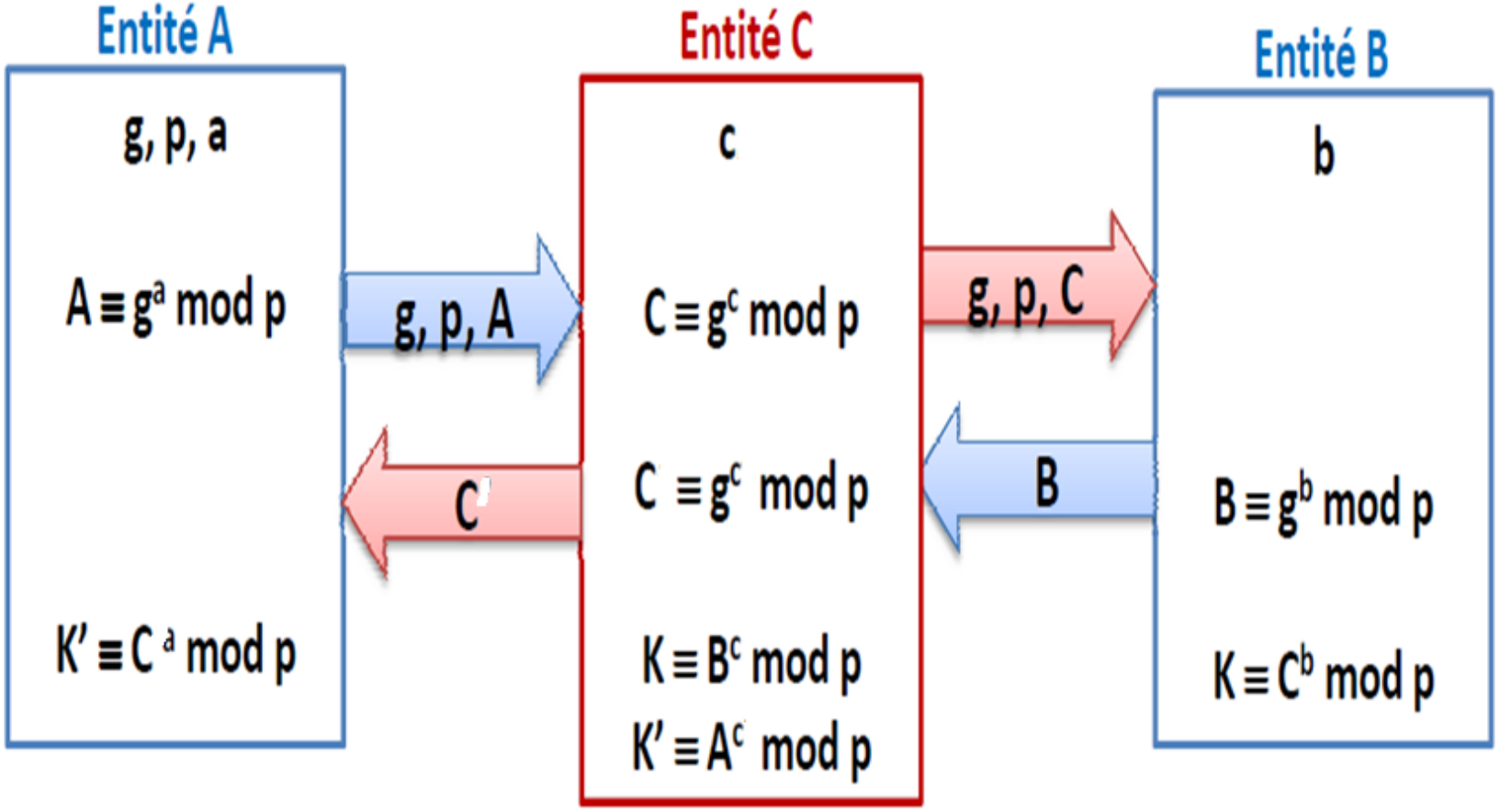
Alice va utiliser la clé $k_1 = g^{ac} \bmod p$ et Bob la clé $k_2 = g^{bc} \bmod p$.

Lors de l'échange d'un message chiffré, l'intermédiaire déchiffre les messages d'Alice à l'aide de la clé $k_1 = g^{ac} \bmod p$ qu'il partage avec Alice, puis les chiffre avec la clé $k_2 = g^{bc} \bmod p$ qu'il partage avec Bob.

Ce dernier va déchiffrer le message d'Alice sans s'apercevoir qu'il a été intercepté et manipulé.

Gestion des clés (Clés partagée)

Protocole de DH: Sécurité



Gestion des clés (Certificats de clés publiques)

•Les algorithmes de chiffrement asymétrique ne garantissent pas que la clé privée est bien celle de l'utilisateur à qui elle associée.

•Un certificat permet d'associe une clé publique à un utilisateur pour en assurer la validité (carte d'identité de la clé publique).

•Pour assurer l'intégrité des clés publiques, les clés publiques sont publiées avec un certificat.

Gestion des clés (Certificats de clés publiques)

Certificat délivré par un organisme appelé Autorité de certification (Certification Autority).

N'importe quel utilisateur ayant accès au CA peut obtenir un certificat de celui-ci, mais seul le CA peut modifier un certificat.

Gestion des clés (Certificats de clés publiques)

- Structure d'un certificat:

Ce sont des petits fichiers divisés en deux:

- Une partie informations
- Une partie contenant la signature de l'autorité de certification.

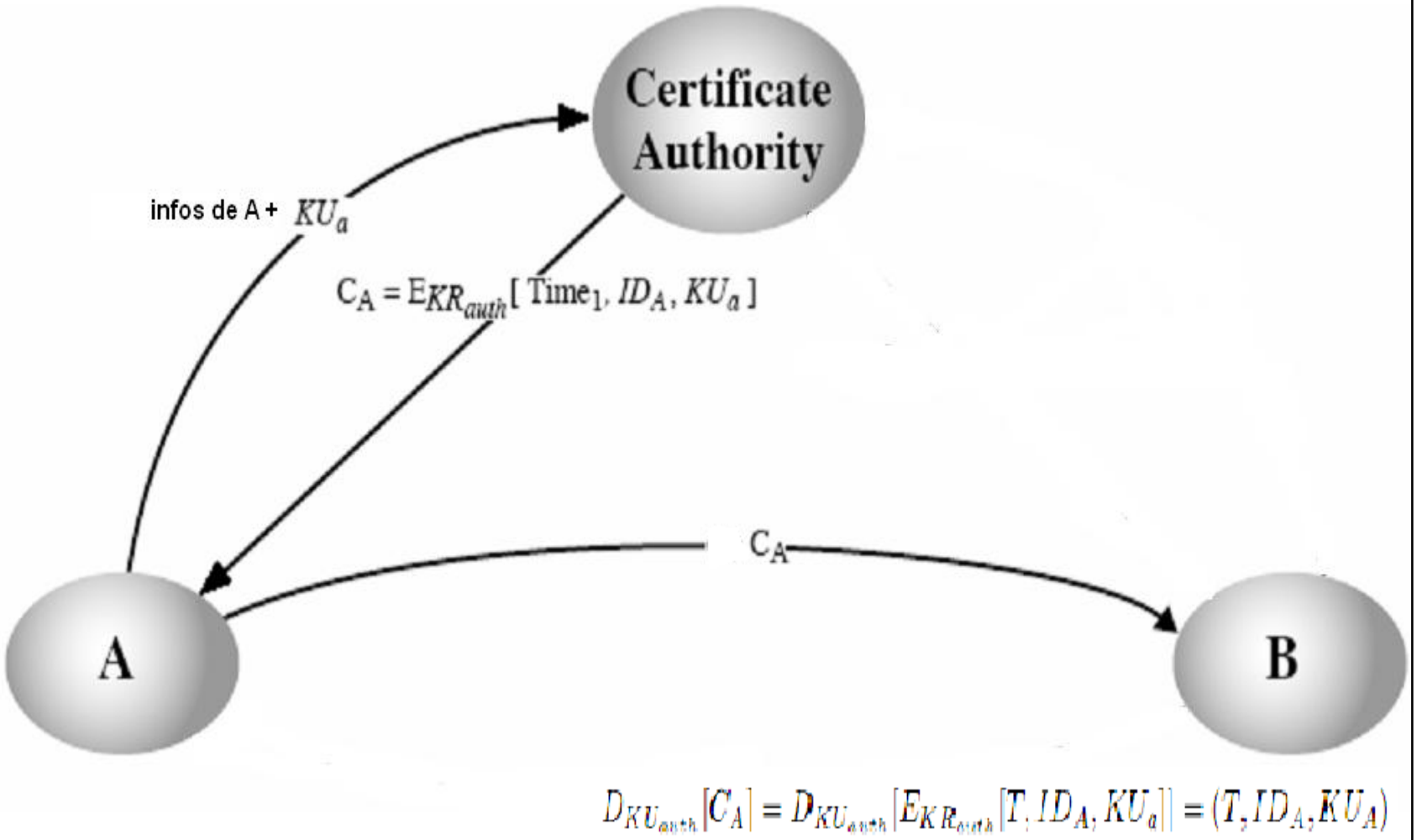
- Structure: normalisée par la norme X.509 de l'UIT (International Telecommunication Union)

Son contenu est signé par la clé privée du CA.

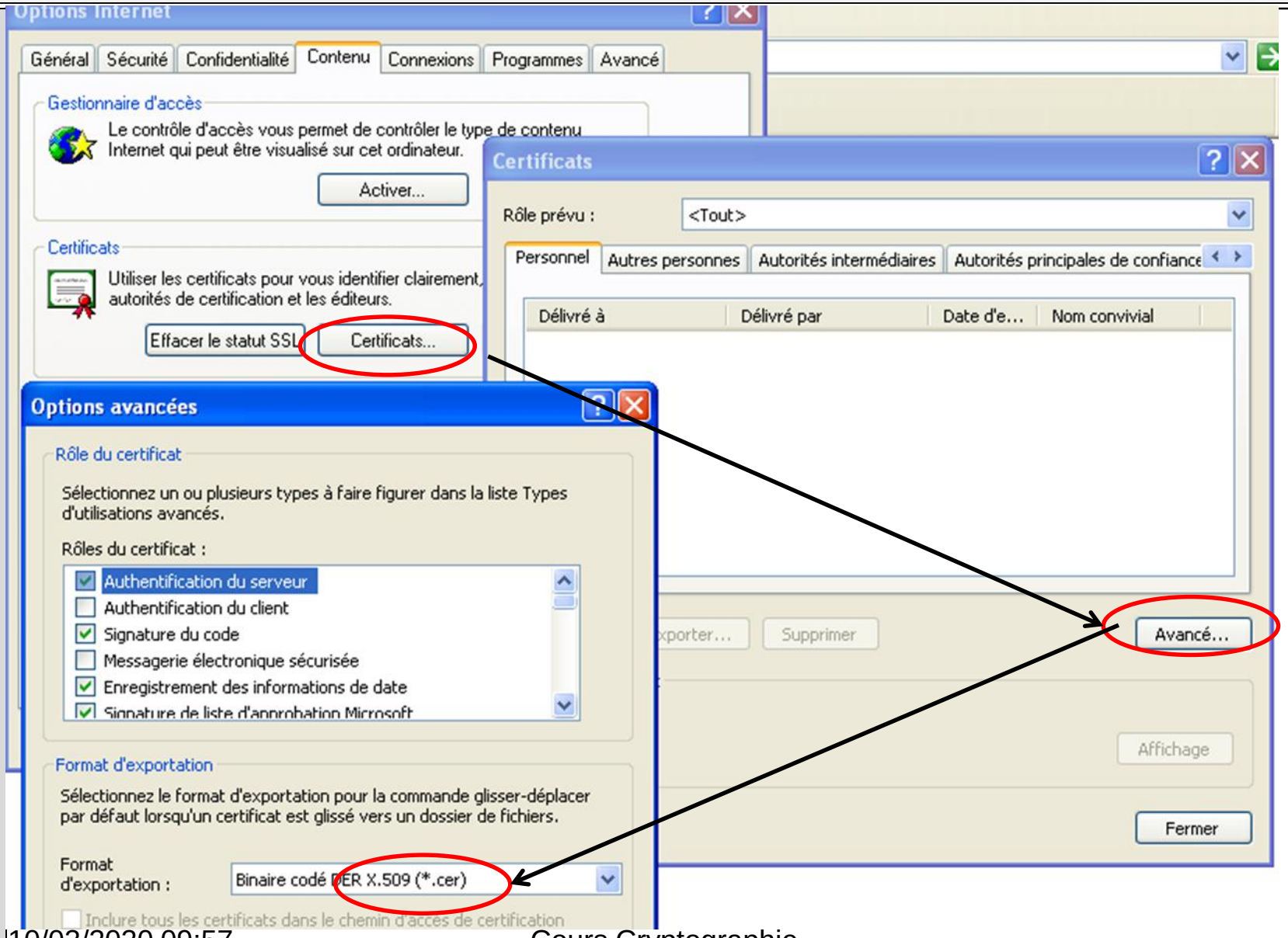
Gestion des clés (Certificats de clés publiques)

- Alice veut certifier que sa clé publique lui appartient.
- Alice envoie sa clé à un CA, ainsi que différentes informations la concernant (nom, email, etc...).
- Cet organisme vérifie les informations fournies par Alice, et ajoute au certificat son propre nom, une date limite de validité, et surtout une signature numérique.
- Cette signature est réalisée grâce à sa clé privée (de CA) et à un algorithme de hachage (ex.RSA et le SHA).

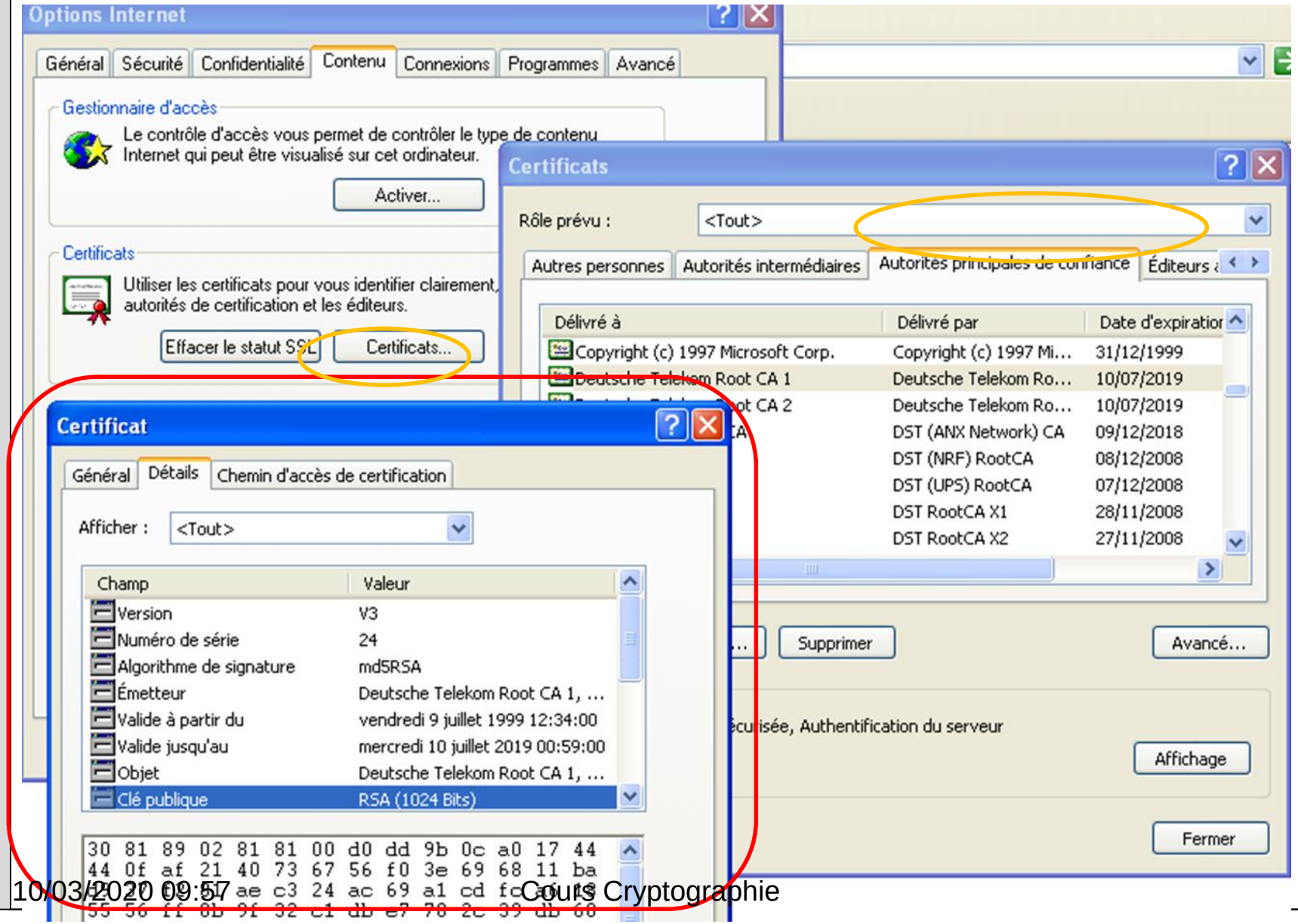
Gestion des clés (Résumé Certificat)



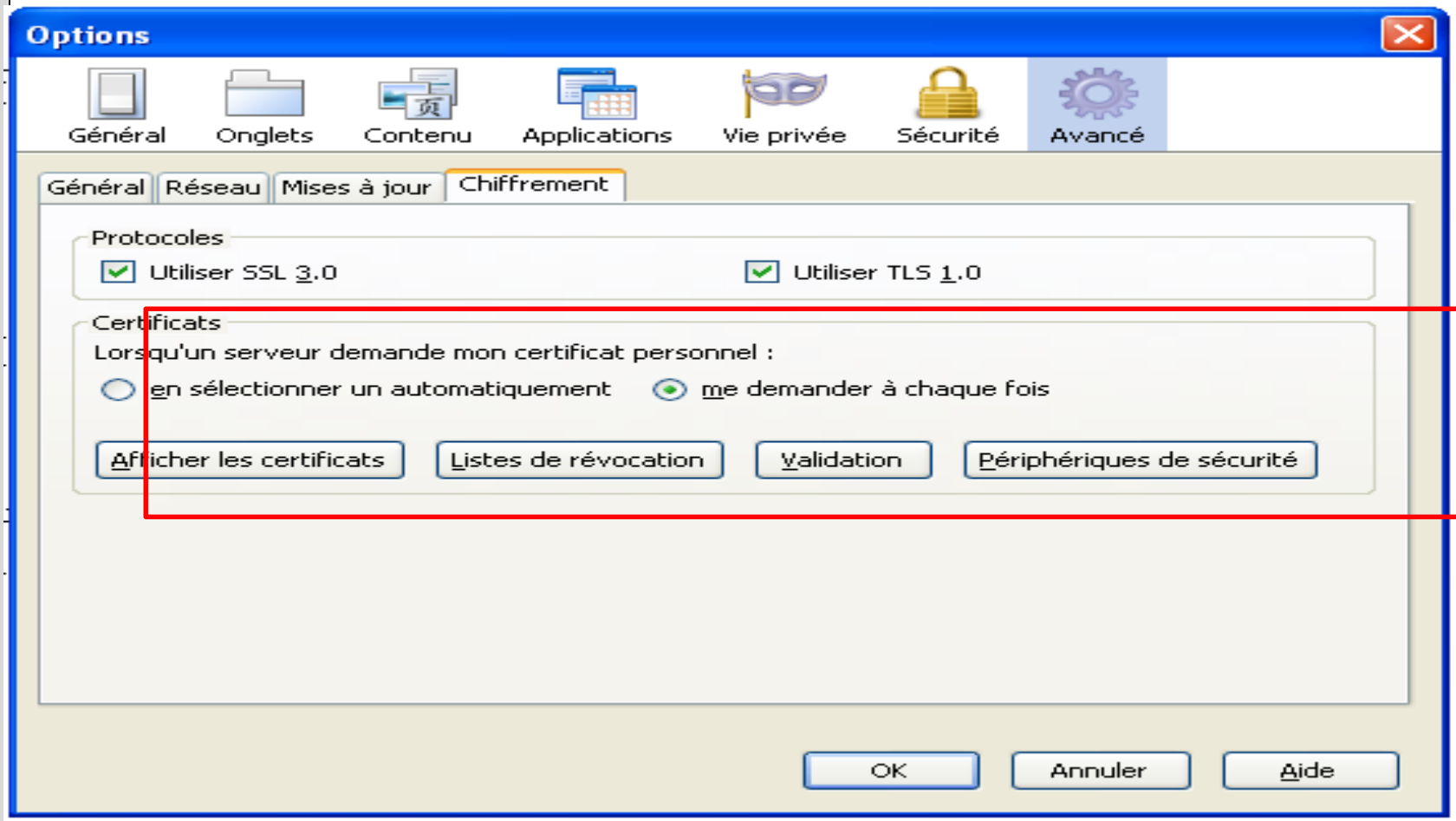
Gestion des clés (exemple de certificat)



Gestion des clés (exemple de certificat)



Gestion des clés (exemple de certificat)



Conclusion générale

La cryptographie est un domaine très intéressant et très délicat, il touche:

- La sécurité du pays, des personnes
- L'économie des entreprises, des banques
- Les relations de la société …
- C'est un domaine qui reste toujours ouvert puisque on cherche toujours à casser les clés de chiffrement.

Références

http://www.bibmath.net/crypto/index.php?action=affiche&quoi=moderne/md5

Ce site est très intéressant, il résume le module de cryptographie