TNSI	Architectures matérielles & réseaux Sécurisation des communications	Cours – Sécurisation des communications

Objectifs :

- ⇨ Savoir ce qu'est un chiffrement
- ⇨ Connaitre les deux types de chiffrements
- ⇨ Comprendre le principe d'une communication https

I – Un peu d'intimité

Lorsqu'on utilise internet, les informations que l'on échange transitent par tout un tas de routeurs dont on ne maîtrise pas le fonctionnement et qui peuvent, en plus d'acheminer l'information, la lire et même la copier.
Cela pose des problèmes à la fois en termes de vie privée (ais-je vraiment envie que des firmes américaines puissent connaître la totalité des forums que je consulte, ce que j'y lis et y écris ?), mais aussi en termes de sûreté.

Lorsqu'on se connecte à un site de banque en ligne par exemple, on voudrait :

- que la totalité des informations échangées (y compris le mot de passe de connexion) ne soient pas visibles par d'autres entités que la banque et nous-même ;
- être sûr que le site qu'on consulte est bien celui de notre banque ;
- être sûr que les informations transmises n'ont pas été altérées lors de leur transit su le réseau et sont bien complètes.

Pour répondre à ces problématiques (....., ..., ...), les informaticiens ont développé des systèmes basés sur le chiffrement.

Il faut noter que le chiffrement est très encadré en France sur le plan légal. Si l'utilisation de logiciels de chiffrement est maintenant autorisée, leur création ou leur distribution doit faire l'objet de déclaration ou d'autorisation préalables (sauf exceptions).

II – Qu'est-ce que le chiffrement ?

Le **chiffrement** est un procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de (dé)chiffrement.

Les militaires et les politiques ont de tout temps[1] utilisé des procédés de chiffrement pour rendre inintelligibles leurs messages internes à leurs adversaires.

Faisons tout de suite une clarification du vocabulaire :

- ➢ La ..... est la « science du secret ». Elle comprend la **cryptographie** (qui assure la protection de l'information en la rendant incompréhensible), mais aussi la **cryptoanalyse** (étude des messages crypté et des techniques de cryptographie pour en tirer des renseignements) et la stéganographie.
- ➢ Le ..... est le procédé visant à rendre l'information non compréhensible en utilisant un algorithme et une clé de chiffrement.
- ➢ Le ..... est l'opération permettant à partir de l'information chiffrée et de la clé de chiffrement de reconstituer l'information de départ.

[1] La première utilisation attestée de techniques de chiffrement remonte aux égyptiens, vers 2000 avant JC

- Le ..... consiste à retrouver l'information originale d'un message chiffré *sans en connaître la clé* de chiffrement.
- En français, ... un fichier est un terme impropre parce qu'il ne renvoie pas à la notion de clé de chiffrement. Il s'agit juste de rendre l'information incompréhensible. Concrètement, crypter un fichier est possible : cela signifie chiffrer un document sans connaître la clé de chiffrement.

Il existe deux catégories de système de chiffrement : les systèmes symétriques et les systèmes asymétriques.

III – Cryptage symétrique

Le chiffrement symétrique ou chiffrement à clé secrète repose sur l'utilisation d'un algorithme réversible pour le chiffrement : ..... sert à chiffrer le message et à le déchiffrer.

Un tel système repose donc sur la communication sûre de la clé de chiffrement.
La sécurité offerte par le chiffrement est liée à la complexité de l'algorithme utilisé et à la longueur de la clé : plus l'algorithme est complexe, plus il est difficile à décrypter et plus la clé est longue, moins il est aisé de casser le chiffrement[2].

Par « difficile à décrypter », on entend « nécessite beaucoup de puissance de calcul (donc de temps) pour le décrypter ».

Les systèmes les plus utilisés reposent sur des algorithmes connus de tous et dont seule la clé secrète assure la sûreté. Il s'agit de DES (Data Encryption Standard), Blowfish, IDEA (International Data Encryption Algorithm) ou AES (Advanced Encryption Standard).

Ces algorithmes sont assez complexes et sont souvent basés sur l'opérateur logique OU EXCLUSIF (XOR) noté $\oplus$ qui est un opérateur par nature réversible.

E1	E2	S = E1 $\oplus$ E2
0	0	0
0	1	1
1	0	1
1	1	0

Table de vérité du OU exclusif

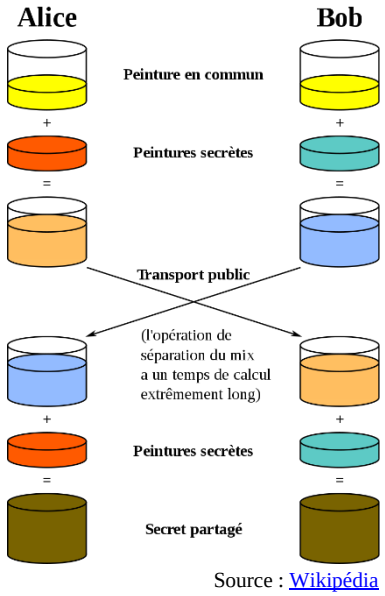
Le chiffrement symétrique permet de solutionner le problème de la ....., mais il est ne permet pas de traiter celui de ..... ou celui de .....

IV – Chiffrement asymétrique

Le chiffrement asymétrique, ou chiffrement à clé publique permet de résoudre certains problèmes qu'il y avait avec les chiffrements symétriques, notamment la nécessité d'échanger par un moyen sûr la clé de chiffrement sur laquelle repose toute l'efficacité du cryptage.

Les cryptologues américains Whitfield Diffie et Martin Hellman imaginent en 1976 une méthode d'échange de clé par un canal peu sûr.
Le schéma ci-contre explique le principe en utilisant des couleurs, mais la méthode présentée par Diffie et Hellman est basée sur des nombres exponentiés.

C'est en 1977 que Ronald Rivest, Adi Shamir et Leonard Adleman découvrent le premier chiffrement asymétrique : RSA (d'après les initiales des 3 mathématiciens). Ce chiffrement est encore utilisé de nos jours et c'est lui dont nous allons exposer le principe dans les parties suivantes.



Source : Wikipédia

[2] « Casser le chiffrement » est un synonyme de « décrypter » (déchiffrer sans connaître la clé).

1) Principe

Le cryptage asymétrique repose sur l'utilisation de **deux clés qui sont liées entre elles** :

- une ..... que l'utilisateur doit donner à des tiers pour communiquer ensuite avec eux de manière sécurisée. Comme son nom l'indique elle peut (et doit) être rendue publique sans que cela compromette la sécurité du système.
- une ..... (ou clé secrète) qui elle doit rester secrète et qui servira à déchiffrer les messages qui ont été chiffrés avec la clé publique.

Les clés sont générées aléatoirement (et non choisies comme un mot de passe peut l'être) et conjointement par un programme. La longueur de la clé est ici un critère important de sûreté[3].

On note M_{clair} le message en clair (non chiffré), $C_K(M)$, le chiffrement par l'algorithme de chiffrement C en utilisant la clé K du message M et $M_{chiffré}$ le message chiffré.
On a donc $M_{chiffré} = C_{clé}(M_{clair})$

Notons également KP la clé publique et KS la clé secrète correspondante. Les propriétés mathématiques des clés font que :

$$C_{KS}(C_{KP}(M)) = M \quad \text{et} \quad C_{KP}(C_{KS}(M)) = M$$

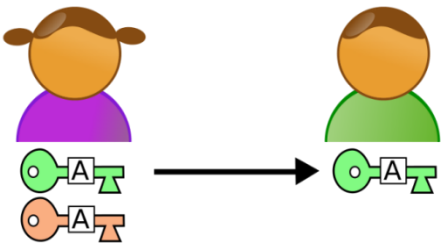
Autrement dit :

- ✓ ce que la clé publique chiffre, ... ;
- ✓ ce que la clé secrète chiffre, ...

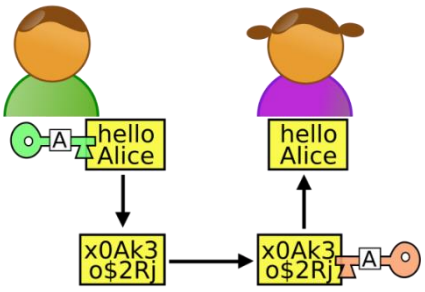
C'est cette propriété très particulière qui fait que le système permet ensuite de chiffrer un message à destination d'un utilisateur particulier mais également d'authentifier l'origine d'un message (signature numérique).

a. Chiffrement

Lorsque deux personnes (Alice et Bob[4]) veulent échanger des informations par un canal non sécurisé (comme le courriel), elles doivent tout d'abord chacune générer un couple clé publique/clé privée. Elles échangent ensuite leurs clés publiques (Bob communique sa clé publique à Alice et Alice communique sa clé publique à Bob).
Pour chiffrer un message à destination d'Alice, Bob utilisera alors la clé publique d'Alice (et un programme de cryptographie asymétrique). Par la suite ce message ne pourra être déchiffré qu'avec la clé privée d'Alice (et donc par Alice seule). De même si Alice veut répondre à Bob, elle chiffrera le message avec la clé publique de Bob. Bob pourra alors déchiffrer le message avec sa propre clé privée.



1re étape : Alice génère deux clefs. La clef publique (verte) qu'elle envoie à Bob et la clef privée (rouge) qu'elle conserve précieusement sans la divulguer à quiconque.



2ème et 3ème étapes : Bob chiffre le message avec la clef publique d'Alice et envoie le texte chiffré. Alice déchiffre le message grâce à sa clef privée.

Source : Wikipédia

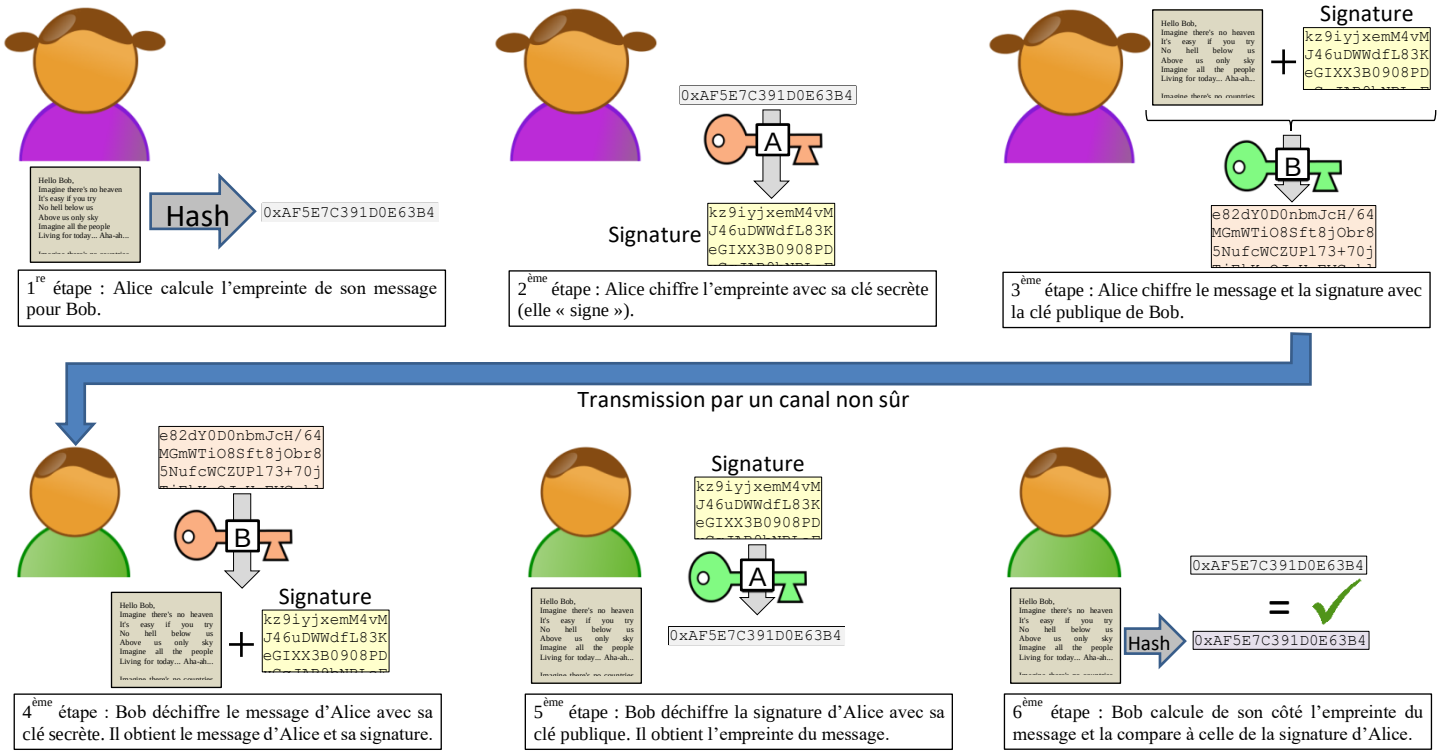
b. Authentification

Le chiffrement asymétrique est réversible, ce qui veut dire que si comme on vient de le voir ce qui est chiffré avec la clé publique peut être déchiffré uniquement avec la clé privée correspondante, l'inverse est également vrai : on peut chiffrer un message avec une clé privée qui ne sera déchiffrable qu'avec la clé publique correspondante.

[3] En 2022, des clés de moins de 2048 bits pour RSA sont considérées comme non sûres. Les transactions bancaires utilisent des clés de 4096 bits.
[4] Plutôt que A et B, les ouvrages sur le chiffrement utilisent généralement ces deux prénoms pour représenter les partenaires d'une communication numérique chiffrée.

Ainsi lorsqu'Alice envoie un message à Bob, elle peut calculer l'empreinte[5] du message et chiffrer celle-ci avec sa clé privée (on appelle cela « signer numériquement ») avant de chiffrer le tout (message + signature) avec la clé publique de Bob.

Lorsque Bob reçoit le message, il commence par le déchiffrer avec sa clé privée, ce qui lui permet de voir le message d'Alice et sa signature. Puis il déchiffre la signature avec la clé publique d'Alice ce qui lui donne l'empreinte du message. Il n'a plus alors qu'à comparer l'empreinte du message reçu (qu'il calcule lui-même) avec celle contenue dans la signature d'Alice. Si elles correspondent, c'est qu'Alice est bien l'auteur de ce message et que le message n'a pas été altéré.



Ce procédé de calcul d'empreinte est aussi utilisé pour vérifier que l'on a bien téléchargé le bon programme par exemple.

Application 1 :
Aller sur la page de téléchargement du logiciel avidemux : https://www.fosshub.com/Avidemux.html et télécharger la version 64 bits pour windows (« Avidemux 64-bits Windows Installer » - premier choix de la liste). Pour vérifier que vous avez téléchargé le bon fichier, utiliser l'application portable « hashtool.exe » qui se trouve dans le répertoire de l'activité. Comparer l'empreinte du fichier téléchargé avec celle indiquée sur le site (cliquez sur « signature » sur la ligne du fichier dans la page web). Est-ce le bon fichier ?

Le chiffrement asymétrique demande beaucoup de puissance de calcul et il est donc généralement utilisé pour chiffrer une petite quantité de données (un courriel, un certificat, une clé de chiffrement, …). Pour chiffrer de gros volumes de données, on utilisera de préférence un algorithme symétrique.

[5] L'empreinte ou « hash » ou encore condensat est un nombre ou une chaîne de caractère permettant d'identifier rapidement, bien qu'incomplètement, la donnée initiale (ici le message). Elle est calculée par une « fonction de hachage » (comme CRC, MD5 ou encore SHA) et change si on modifie ne serait-ce qu'un seul bit de la donnée initiale, mais ne contient pas suffisamment d'information pour être capable de reconstituer la donnée d'origine. Une empreinte a une taille fixe (ex 128 bits) quelle que soit la taille de la donnée initiale (un texte, une image, une vidéo, …).

V – Vulnérabilités

Aucun système de chiffrement n'est infaillible, et avec l'évolution de la technologie et de la cryptologie, de nouvelles failles sont régulièrement trouvées dans des méthodes de chiffrement, tandis que des clés de plus en plus grandes sont « cassées » par les programmes. La cryptologie est donc un domaine en évolution constante et une méthode de chiffrement réputée « sûre » un jour peut être considérée comme « compromise » (et donc non fiable) le lendemain.
Nous allons dans cette partie lister quelques façons classiques d'attaquer des systèmes de chiffrement.

1) La force brute

On peut essayer de déchiffrer le message en essayant toutes les combinaisons de clé possibles.
Par exemple si la clé est un nombre entier positif, on essayera successivement 1, 2, 3, … jusqu'à ce que le résultat du déchiffrement donne un texte cohérent.

Cette technique est très rudimentaire :

- Elle nécessite de connaître l'algorithme de chiffrement (ce sera souvent le cas)
- Il faut également disposer d'un bout d'information chiffrée et si possible de connaître l'information en clair correspondante
- Elle peut nécessiter un temps de calcul rédhibitoire si la clé est trop grande ou trop complexe
- Elle fonctionne sur tous les types de chiffrement

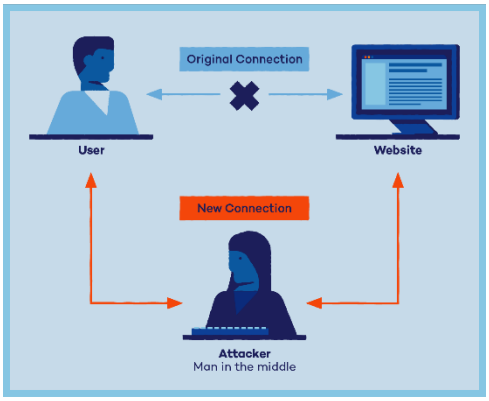
Application 2 :

1) Combien y a-t-il de mot de passe de 7 lettres utilisant uniquement des lettres minuscules ?
2) Même question si on utilise maintenant les majuscules également puis les chiffres.
3) Si on considère qu'un ordinateur puissant peut essayer 100 millions de combinaisons par secondes, combien de temps lui faudra-t-il dans le pire des cas pour casser le mot de passe dans chaque cas ?

2) L'attaque par dictionnaire

Comme pour l'attaque par force brute, on va essayer plusieur clé au hasard en espérant trouver la bonne. Ici on parie sur la faiblesse humaine et au lieu de tester tous les possible, on va juste essayer une série de mot de passe « classiques » repertoriés dans une base de donnée de mots de passe fréquents.
Cette méthode est bien plus rapide que la force brute (il suffit généralement d'une seconde pour tester tous les mots de passe du dictionnaire) mais inefficace si le mot de passe a été généré aléatoirement ou s'il s'agit d'une phrase complète par exemple.

3) L'attaque de l'homme du milieu (Man in the middle)



Dans ce type d'attaque, le pirate se place au milieu d'une communication entre deux postes A et B (par exemple un utilisateur et un serveur web). Toutes les informations vont alors transiter par lui, notamment les échanges de clés. Il peut ainsi récupérer la clé de A et fournir sa propre clé à B. qui croira que c'est celle de B. De même il reçoit la clé de B et transmet une autre clé à A qui croira qu'elle vient de B.

Ainsi A croit que le pirate est B et B croit que le pirate est A. Le pirate transférera toutes les requêtes de A vers B et inversement de manière à ce qu'auncun des deux ne se doute que la communication est écoutée.

Il doit pour cela être capable d'intercepter la requête originale (par exemple la demande de page web du client), ce qui peut se faire avec différentes techniques comme le DNS Spoofing.

VI - Le protocole https

Lorsqu'un navigateur demande une page à un serveur web, il utilise le protocole http (**H**yper**T**ext **T**ransport **P**rotocol). Celui-ci permet d'échanger facilement des données entre le serveur et le client mais il fait transiter les données en clair sur le réseau ce qui permet à n'importe quelle machine sur le parcours de prendre connaissance des informations échangées (notamment les mots de passe de connexion).

Pour palier à ce problème, le protocole **https** (**H**yper**T**ext **T**ransfer **P**rotocol **S**ecure) a été développé afin d'assurer la confidentialité et l'authentification.

Ceci est obtenu en chiffrant toutes les communications avec un chiffrement symétrique utilisant une clé aléatoire (valable uniquement le temps de la session) sur laquelle le client et le serveur se seront mis d'accord en utilisant un chiffrement asymétrique.

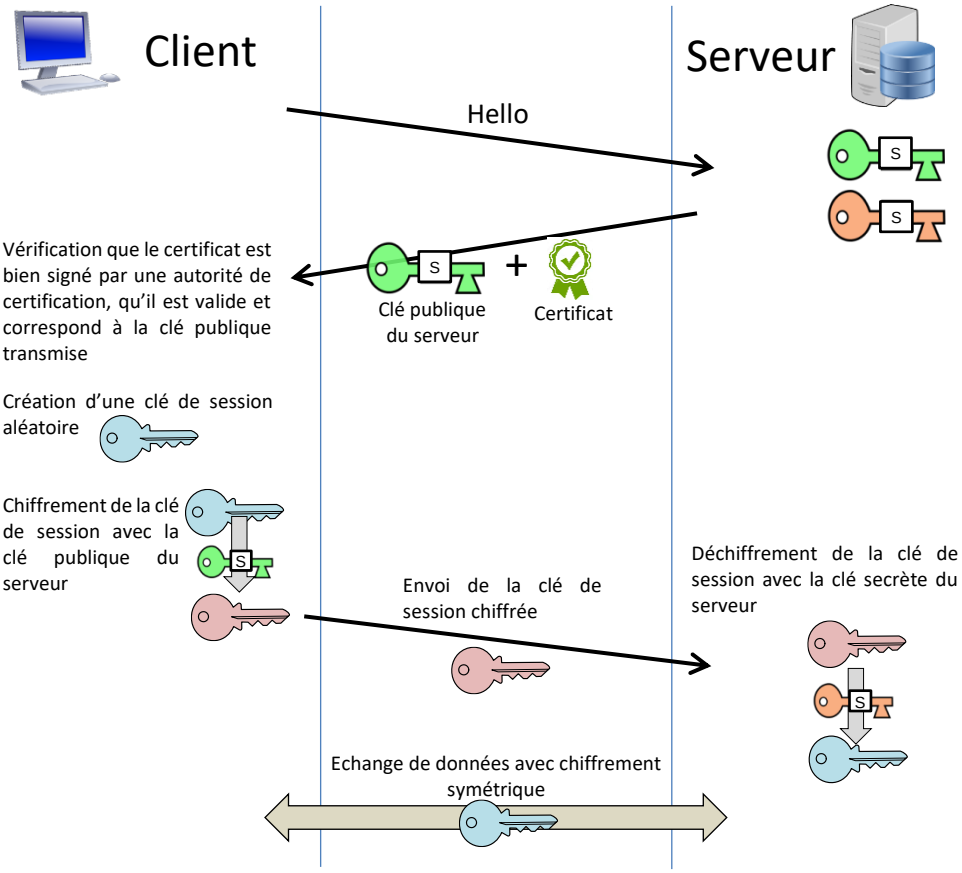
Le client initie une connexion avec le serveur et les deux se mettent d'accord sur une méthode de chiffrement à utiliser.

Puis le serveur envoi au client sa clé publique ainsi que son certificat.

Le client vérifie le certificat en utilisant la clé publique de l'autorité qui l'a certifié (les navigateurs possèdent les clés publiques des principales autorités de certification). Il vérifie aussi que la clé publique correspond bien à celle décrite dans le certificat et que le certificat est encore valide et n'a pas été révoqué.

Le client est alors certain de s'adresser véritablement au serveur (et pas à un pirate).

Le client génère alors une clé de session aléatoire et suffisamment forte qu'il chiffre avec la clé publique du serveur. Il peut ensuite transmettre la clé chiffrée par le canal de transmission car seul la clé secrète du serveur pourra déchiffrer son message.



Le serveur récupère donc la clé de session en déchiffrant l'envoi. La phase de concertation (Handshake) est terminée et les deux pourront désormais communiquer en chiffrant leurs communications avec la clé de session en utilisant l'algorithme de chiffrage symétrique dont ils étaient convenu au départ.

Application 3 :
Aller sur la page du site web du lycée et récupérer les informations sur le certificat utilisé (il faut cliquer sur le cadenas à côté de l'url). Quelles informations importantes peut-on y trouver ?

Références :
RSA : https://interstices.info/nombres-premiers-et-cryptologie-lalgorithme-rsa/ et https://samuelgallay.github.io/CryptoTPE/rsa/
Chiffrement asymétrique : https://technique-et-droit-du-numerique.fr/chiffrement-asymetrique-a-cle-privee-et-cle-publique/
Histoire du chiffrement : https://repo.zenk-security.com/Cryptographie%20.%20Algorithmes%20.%20Steganographie/RSA.pdf
Fonctions de hachage : https://www.dcode.fr/fonction-hash
https : https://www.ionos.fr/digitalguide/hebergement/aspects-techniques/le-https-cest-quoi/
Diaporama assez complet : http://perso.inforoutes.fr/grozanne/cryptographie/sld001.htm