1 Communication chiffrée

Sécuriser une communication consiste à la rendre incompréhensible par quiconque n'étant pas censé participer à cette communication. Typiquement, on cherchera à sécuriser la communication lorsqu'on souhaite échanger des informations sensibles comme des mots des passe ou des transactions financières par exemple.

> Le **chiffrement** est l'opération qui consiste à rendre illisibles les données à échanger lors de la communication.

Évidemment, la chiffrement n'a d'intérêt que si le destinataire des données reste capable de déchiffrer ces données !

2 Chiffrement symétrique

2.1 Principe

De multiples mises en œuvre de chiffrements sont possibles, mais toutes reposent sur l'utilisation d'une **clef de chiffrement**.

> Dans un chiffrement **symétrique**, **la clef** de chiffrement et de déchiffrement **est la même**.

Exemple basique : chiffre de César.
Ce chiffrement consiste simplement à décaler chaque lettre de l'alphabet d'un certain pas. La clef de chiffrement est simplement la valeur de ce décalage.
Ex avec un décalage de 1 : A $\rightarrow$ B, B $\rightarrow$ C, $\cdots$, Z $\rightarrow$ A.

 Déchiffrer le message suivant `JYFWAHUHSFZL` obtenu avec une clef de chiffrement de 7.

L'**inconvénient** majeur d'un chiffrement symétrique est qu'**il faut au départ s'échanger la clef commune** par un canal sécurisé autre que celui qui sera utilisé par la suite.

Une des méthodes les plus utilisées en matière de chiffrement symétrique se nomme **AES** (Advanced Encryption Standard). Son principe est une application plus complexe, mais reposant en partie sur le chiffrement présenté ci-dessous.

2.2 Chiffrement XOR

Un autre exemple de chiffrement repose sur l'opérateur Ou Exclusif (XOR) appliqué bit à bit entre les caractères à chiffrer et une clef de chiffrement. L'intérêt de cette opération est sa réversibilité : Si A XOR B = C, alors C XOR B = A.
( *à vérifier avec une table de vérité*).
Il suffit de considérer que A est le message clair, B la clef de chiffrement et C le message chiffré.
Si la clef de chiffrement est plus courte que le message à chiffrer, on la répète autant de fois que nécessaire.

 *Exemple* : on veut chiffrer `CRYPTOGRAPHIE` avec la clef `NSI`.

C	R	Y	P	T	O	G	R	A	P	H	I	E	
N	S	I	N	S	I	N	S	I	N	S	I	N	(répétition de la clef)

On commence par « traduire » chaque caractère par son encodage Unicode UTF8 (cf cours 1ère). Une rapide recherche sur le Web indique que l'alphabet majuscule porte les *points de code* en hexadécimal de 41 à 5A.
Exemple : Le C est encodé en hexa par 43, càd 67 en décimal, ou encore 01000011 en binaire. Le N par $4E_{16}$, ou 78_{10}, ou 01001110_2.

Chiffrement :

message clair	0	1	0	0	0	0	1	1	C
clef	0	1	0	0	1	1	1	0	N
message chiffré	0	0	0	0	1	1	0	1	C XOR N : 00001101 = code retour chariot

Déchiffrement :

message chiffré	0	0	0	0	1	1	0	1	retour chariot
clef	0	1	0	0	1	1	1	0	N
message déchiffré	0	1	0	0	0	0	1	1	C

1. Terminer le chiffrement du message.
   On s'appuiera sur une table UTF8 (ou ASCII) en ligne.
2. La vérification du chiffrement/déchiffrement peut être facilitée avec ce site de conversion : `https://www.rapidtables.com/convert/number/binary-to-ascii.html`
3. Automatiser ce travail en Python.
   Indications : les fonctions `ord(lettre)` ou `chr(entier)` permettent des conversions entre caractère et point de code. Et l'opérateur XOR s'écrit `^`.

```
>>> ord('C')
67
>>> ord('N')
78
>>> 67^78
13
>>> chr(13)
'\r' # retour chariot (carriage return CR)
```

   Écrire une fonction `chiffrement(message, clef)` qui renvoie le message chiffré (ou déchiffré).

Cet algorithme de chiffrement possède les avantages suivants :
- L'opération "ou exclusif" se calcule très rapidement.
- Le chiffrement fonctionne avec n'importe quel fichier binaire et pas seulement du texte.

3 Chiffrement asymétrique

Le chiffrement asymétrique permet d'éviter l'inconvénient de la diffusion secrète d'une clef commune de chiffrement/déchiffrement.

> Le chiffrement **asymétrique** repose sur l'utilisation d'une **paire de clefs** : la clef de chiffrement est différente de la clef de déchiffrement.
>
> La clef de chiffrement peut être diffusée publiquement (on parle d'ailleurs de **clef publique**), mais la clef de déchiffrement, quant à elle, doit rester secrète (on l'appelle **clef privée**).

Si Alice veut communiquer de façon sécurisée avec Bob (Alice et Bob sont les personnages clefs de la cryptologie), elle crée une paire de clefs publique/privée et diffuse ouvertement sa clef publique à Bob. Bob peut alors chiffrer son message avec la clef publique d'Alice et envoyer le message. Seule Alice, dotée de sa clef privée soigneusement protégée, sera capable de déchiffrer ce message.
Si Ève (le 3ème personnage de la cryptologie qui joue le rôle du méchant cryptanalyste) intercepte la clef publique, ou le message chiffré par Bob, elle ne pourra rien faire de mal. Sans la clef privée, elle ne peut pas déchiffrer le message, et avec la clef publique, elle peut seulement chiffrer un message (sans utilité ... !).

Si Alice doit envoyer un message sécurisé à Bob, elle pourra de la même manière utiliser la clef publique de Bob, et Bob déchiffrera le message avec sa propre clef privée.

> La sécurité de ce procédé réside dans le fait de pouvoir créer une paire de clefs qui sont intimement associées, mais tel que la connaissance de la clef publique ne rende toutefois pas possible de déduire la clef privée.

L'algorithme **RSA** (du nom de ses inventeurs **Rivest**, **Shamir** et **Adleman**) est le plus utilisé aujourd'hui pour le chiffrement asymétrique. La création des clefs repose sur l'utilisation de grands nombres premiers, et sur l'impossibilité de factoriser des grands entiers dans un délai raisonnable. **De façon générale la sécurité informatique compte plutôt sur la durée pour casser un code que sur la réelle impossibilité de le casser.**

L'inconvénient de ce type de chiffrement est qu'il est **assez long à mettre en œuvre**, ou tout du moins plus long qu'avec un chiffrement symétrique comme AES.

4 Communication sécurisée HTTPS

> L'idée retenue pour les communications sécurisées sur le Web, est d'**initier la communication par chiffrement asymétrique** (un peu long) pour décider d'une clef de chiffrement symétrique à s'échanger, et ensuite de **poursuivre la communication avec un chiffrement symétrique** (plus rapide).

Le protocole HTTPS repose donc sur le protocole HTTP non sécurisé, en ajoutant une couche TLS (Transport Layer Security) pour chiffrer les données échangées.

La suite d'opérations est la suivante :

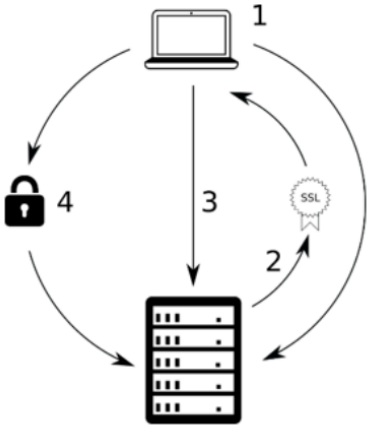
1. le client effectue une requête HTTPS vers le serveur, et en retour le serveur lui envoie sa clef publique.
2. le client génère alors une nouvelle clef (symétrique, commune pour la suite) qu'il renvoie au serveur après l'avoir chiffrée avec la clef publique du serveur.
3. le serveur la déchiffre en utilisant sa clef privée. À partir de ce moment-là, le client et le serveur sont en possession de la clef commune. L'échange de cette clef symétrique s'est bien fait de façon sécurisée.
4. le client et le serveur poursuivent désormais les échanges des données en les chiffrant et en les déchiffrant avec cette clef.

Il reste toutefois un problème à régler. Ève, la méchante, pourrait s'intercaler entre Alice et Bob (attaque dite de « l'homme du milieu » MitM, **Man in the Middle**) et leur faire croire qu'ils communiquent directement ensemble de façon sécurisée, alors que c'est elle qui relaie la communication.

Voyons comment cela se déroule :

- Eve intercepte la clef publique d'Alice et renvoie à Bob sa propre clef publique en se faisant passer pour Alice.
- Lorsque Bob veut envoyer un message à Alice, il utilise donc, sans le savoir, la clef publique d'Ève. Bob chiffre le message avec la clef publique d'Ève et l'envoie à celle qu'il croit être Alice.
- Ève intercepte le message, le déchiffre avec sa clef privée et peut lire le message. Puis elle chiffre à nouveau le message avec la clef publique d'Alice, après l'avoir éventuellement modifié.
- Alice déchiffre le message avec sa clef privée, et ne se doute de rien puisque tout fonctionne. Ainsi, Alice et Bob sont chacun persuadés d'utiliser la clef de l'autre, alors qu'ils utilisent en réalité tous les deux la clef d'Ève.

Pour éviter ce problème, **il faut que le serveur puisse justifier de son identité**. Pour ce faire, chaque site désirant proposer des transactions HTTPS doit demander un **certificat d'authentification** auprès d'une **autorité de confiance** habilitée à fournir ce genre de certificats. Le serveur envoie le certificat au client en même temps que sa clef publique. Le certificat contient entre autres un exemplaire de la clef publique du serveur, chiffrée avec la clef privée de l'autorité de confiance. Le navigateur Web, possédant toutes les clefs publiques des autorités de confiance, vérifie donc que cette clef déchiffrée avec la clef publique de l'autorité est bien identique à celle que le serveur lui a envoyée : la correspondance assure l'identité du serveur.



1. Demande d'initialisation d'une connexion par le protocole SSL.

2. Présentation du certificat :
- validité,
- signature par un tiers de confiance.

3. Transmission d'une clé de chiffrement unique, encodée avec la clef publique du serveur.

4. Déchiffrement de la clé de chiffrement par le serveur, à l'aide de sa clef privée :
- établissement de la connexion sécurisée.

Tout ceci est bien résumé dans la vidéo suivante :

`https://www.youtube.com/watch?v=7W7WPMX7arI&feature=youtu.be`

5 Mise au point du vocabulaire

- **Chiffrer** : il s'agit de rendre un document illisible avec une clef de chiffrement, excepté pour son destinataire.
- **Déchiffrer** : il s'agit de rendre lisible un document chiffré, en ayant connaissance de la clef de chiffrement.
- **Décrypter** : il s'agit de rendre lisible un document chiffré, sans avoir connaissance de la clef de chiffrement : c'est l'aspect « piratage ».
- **Cryptologie** : il s'agit de la science du secret, c'est son sens étymologique. Elle regroupe deux disciplines :
  - La **cryptographie** : vise à étudier comment protéger par le chiffrement.
  - La **cryptanalyse** : vise à analyser les méthodes de chiffrement pour les casser.
- *Crypter* : ça n'existe pas.
- *Chiffrage* : ça existe, mais dans le domaine de la comptabilité ou de la musique !