LA CRYPTOGRAPHIE

POURQUOI FAIRE?

DEBAT

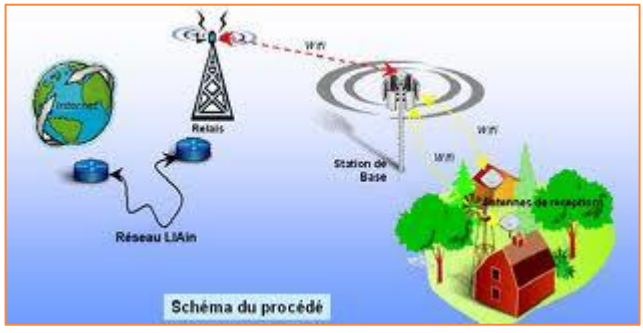
Nous avons vu précédemment les moyens techniques mis en œuvre pour transférer une image version papier à une image version écran en restant dans notre réseau local (chez moi).
Mais la peur d'un virus nous pousse à vouloir sauvegarder cette image ailleurs que sur une clé USB ou notre propre ordinateur.

Nous décidons de l'enregistrer sur l'ENT de l'école.

Néanmoins, comment faire pour que les données transmises par mon réseau local (chez moi) à l'ENT de mon école (Skydrive) restent confidentielles?
Le sont-elles obligatoirement?
Quels moyens pouvons nous utiliser?

Donner d'autres exemples d'applications.

Quelques exemples d'applications de la cryptographie



INTRODUCTION

La **cryptographie** est l'une des deux composantes de la **science du secret** nommée la **cryptologie**.
L 'autre composante s'appelle la **cryptanalyse**.

- **La cryptographie construit des outils pour le chiffrement des messages en préservant le secret des données lors des transmissions.**

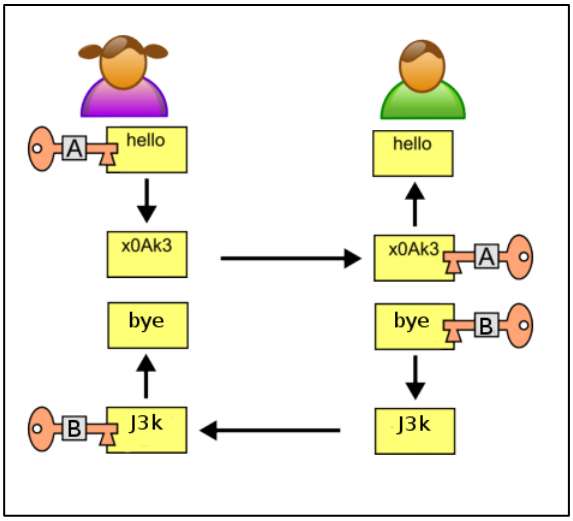
- La cryptanalyse consiste à analyser les faiblesse de ces constructions et à proposer des attaques pour compromettre la sécurité d'un système.

La cryptographie remonte aux origines de l'homme.
La cryptographie connut une réelle expansion entre les deux guerres.
La machine Enigma de cryptage des allemands pendant la seconde guerre mondiale en est un exemple.

Depuis l'apparition de la carte bleue, de la popularisation des ordinateurs, d'internet et des téléphones portables, la cryptographie connait une avancée considérable.

C'est une filière source d'emplois à l 'avenir car le besoin de sécurité ne fera que s'amplifier avec l'émergence de l'enregistrement de données privées sur un serveur web, de la dématérialisation papiers des contrats au profit d'une sauvegarde sur un serveur X et du besoin d'authenticiter l'origine d'une donnée.

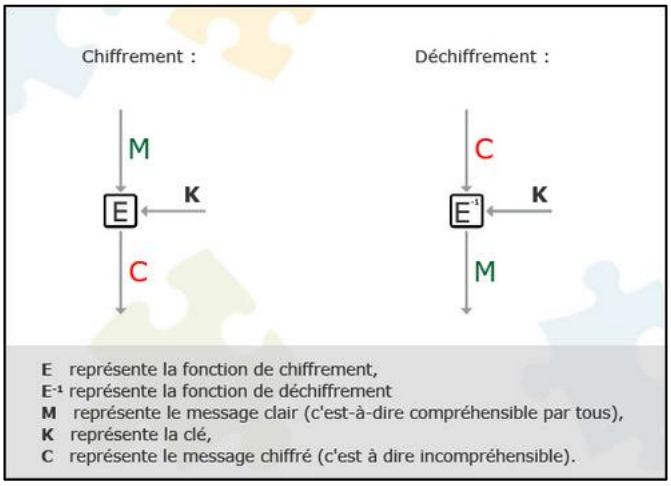
Système à cryptage symétrique dit à clé secrète



Le système repose essentiellement sur la connaissance de la clé secrète par l'émetteur du message (Alice) et le destinataire (bob).
La conception des clés secrètes peuvent s'appuyer sur différents algorithmes:

- **Le chiffre de Cesar.**
- **Le chiffre de Vigenère.**
- **Le chiffre de Vernam.**
- et bien d'autres encore…

La transcription mathématique pour représenter cela:
E est une fonction bijective.



Avantages:

- Systèmes rapides (implémentation matérielle)
- Clés relativement courtes (128 ou 256 bits)
- A utiliser dans le cas où il y a peu d'interlocuteurs: communication point à point, chiffrement d'archives…

Inconvénients:

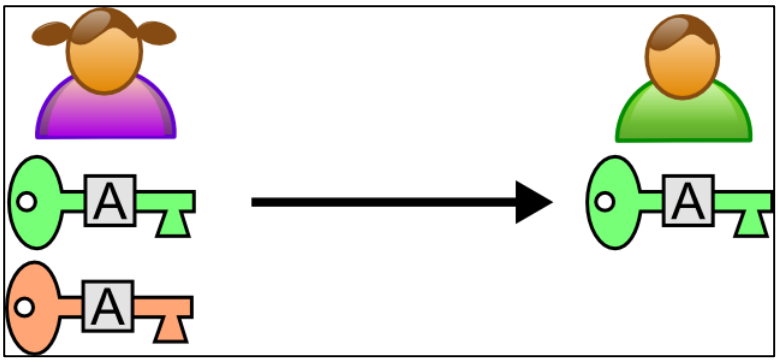
- Gestion des clés difficiles (nombreuses clés)
- GROS point faible = échange d'un secret

Des évolutions ont vu le jour pour résoudre en partie ces problèmes avec :

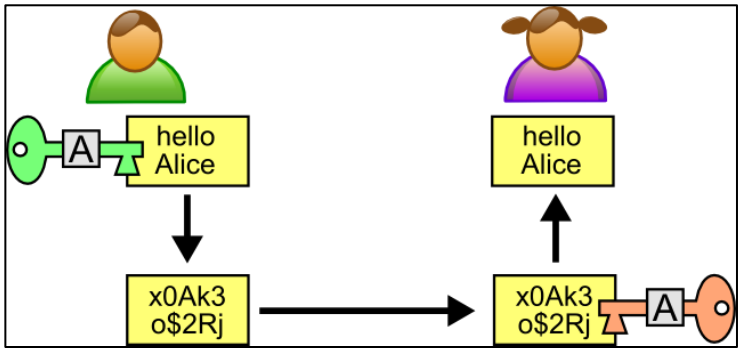
- **Le chiffrement par bloc.**
- **Le chiffrement par flot.**

Le principe de Kerckhoffs résume :
« **la sécurité d'un système cryptographique doit résider dans le secrèt de la clé** ».

Système à cryptage asymétrique dit à clé publique



Alice génère deux clés, l'une publique (verte) qu'elle transmettra à tout le monde par internet par exemple, et l'autre privée (rouge) qu'elle conservera précieusement.
La conception de ces deux clés reposent sur des fonctions mathématiques.
En effet, certaines fonctions mathématiques peuvent être calculées facilement mais en revanche l'opération inverse (obtenir la fonction réciproque) est beaucoup plus ardu.
Bob transmet son message en le codant à l'aide de la clé publique (verte).



Avantage immédiat:
Seule, Alice peut décrypter le message avec sa clé privée qu'elle seule détient.

Autre utilisation du cryptage asymétrique:
Alice peut utiliser sa clé privée pour crypter un message.
Intérêt: tout le monde peut le décrypter avec la clé publique en étant sûr que le message provient d'Alice.

Des exemples très répandus sont:

- Le cryptage RSA (carte bancaire entre autre…)
- Le cryptage SSL
- Le cryptage SSH (transfert de données sur réseau)

Aspects juridiques:

En France, et en vertu de l'article 30-I de la loi 2004-575 du 21 juin 2004, l'utilisation des moyens de cryptologie est libre. En revanche, la fourniture, l'importation et l'exportation sont réglementées. Il faut savoir que l 'importation comprend le téléchargement de logiciels.

Il n'est donc pas forcément légal d'utiliser un logiciel de cryptologie s'il n'est pas autorisé à l'importation.

Vous êtes libre de télécharger et d'utiliser un logiciel de cryptologie utilisant des clés dont la longueur ne dépasse pas 128 bits. En revanche, si vous souhaitez fournir un tel logiciel, vous êtes soumis à une déclaration préalable auprès de la DCSSI .

Si vous souhaitez télécharger puis utiliser un logiciel de cryptologie utilisant des clés dont la longueur dépasse 128 bits, vous devez vous assurer que ce logiciel est autorisé par la DCSSI. Par exemple, les logiciels GnuPG (similaire à PGP) et OpenSSL entrent dans ce cas.
Ils sont autorisés à l'importation, ainsi qu'à la fourniture générale. Vous avez donc le droit de redistribuer ces logiciels libres comme bon vous semble.

Pour aller plus loin:

- la loi LCEN (Loi pour la confiance dans l'économie numérique): Articles 30, 31 et 36 ainsi que les articles 30 à 40.

- **L'ANSSI**

- **Un lien intéressant**