Chapitre 1 : Introduction à la cryptographie

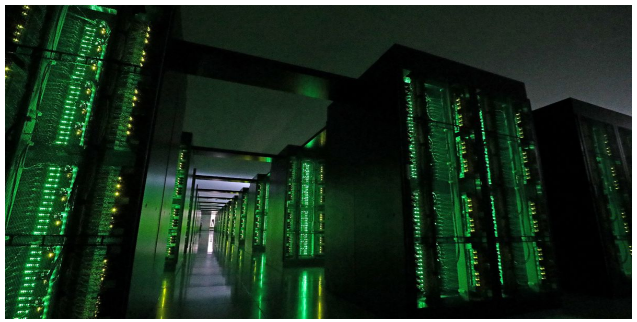
8 juin 2023

Sommaire

Introduction

Introduction

Les ordinateurs sont, de nos jours, partout dans notre quotidien.



Notre société virtuelle existe grâce aux données qui transitent à travers les réseaux. Cette transmission requiert

1. un niveau élevé de sécurité.
2. une certaine efficacité dans le traitement des opérations.

La cryptographie est au coeur de cette étude.

Concept de bases

Information

C'est un élément de connaissance tel qu' un texte, un son, une image, une vidéo, ... Traiter ou manipuler une information revient à lire, écrire/modifier, ou effacer cette information.

Canal

Tout moyen de transmission permettant de convoyer une information entre deux partenaires d'une communication. Cela peut être une ligne téléphonique, une fibre optique, un réseau sans fils, ...

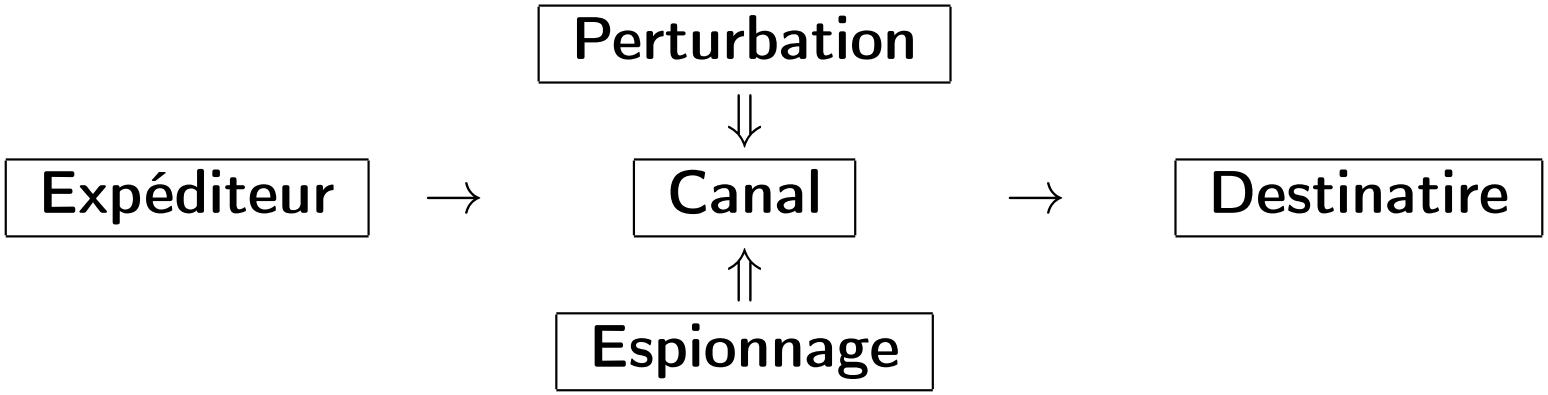
Entité

C'est l'un des partenaires d'une commmunication. Cela peut être une personne ou une machine capable d'envoyer, de recevoir, ou de traiter/manipuler une information.

Un schémas de communication

Met en excerce l'ensemble des composantes concernant un échange d'informations entre entités distantes. Ce schéma **fait internir :**

- **un expéditeur** et un **un destinataire** (**personne, machine, ...**),
- **un canal de transmission** (**ligne téléphonique, fibre optique, systèmes de communication sans fils,...**)
- **et un message** (**information : texte, son, image, vidéo, ...**).



Habituellement ou systématiquement

- le canal connait des perturbations (d'ordre électromagnétique) et/ou
- des entités tiers interviennent pour espionner ou compromettre les communications.

Pour prendre en charge tous les problèmes (d'efficacité, de sécurité, ...) qui peuvent se poser avant la transmission, le message subit des transformations particulières appélées codages. On distingue trois types de codes

1. les codes de compression,
2. les codes correcteurs d'erreur,
3. les codes secrets.

Les codes

Codes de compression

Lors d'une communication, l'information est transmise sous la forme d'une séquence de signaux. Pour des soucis de capacité du canal, on utilise des codes qui minimisent la longueur de la séquence : c'est la compression.

Codes correcteurs d'erreurs :

Lors d'une transmission, des erreurs peuvent apparaitre car il y'a des signaux qui sont perdus ou altérés. A la réception, il est nécessaire de pouvoir détecter et si possible de corriger les erreurs survenues.

Codes secrets

Lors d'une communication, un espion peut tenter de violer la confidentialité des données, de détourner et de modifier les données ou d'essayer d'usurper l'identitité de l'un des partenaires de la communication. Ainsi pour des raisons de sécurité, lors de l'envoie, un protocole bien spécifique doit etre utilisé pour protéger la communication par rapport à des besoins de sécurité bien identifiés. On fait appel à la cryptographie.

La sécurité informatique et la cryptographie

Contexte

Pour introduire la cryptographie, une compréhension des problèmes liés à la sécurité de l'information est nécessaire. En effet toutes les parties à une transaction doivent être convaincues que certains objectifs associés à la sécurité de l'information ont été atteints.

On distingue les objectifs suivants

- **confidentialité** : garder les informations secrètes de tous sauf de ceux qui sont autorisés à les voir.
- **intégrité des données** : s'assurer que les informations n'ont pas été modifiées par des moyens non autorisés ou inconnus.
- **authentification ou identification d'entité** : corroboration de l'identité d'une entité (par exemple, une personne, un terminal informatique, une carte de crédit, etc.).
- **authentification du message** : corroborant la source de l'information ; également appelée authentification de l'origine des données.

- **validation** : un moyen de fournir en temps opportun l'autorisation d'utiliser ou de manipuler des informations ou des ressources.
- **contrôle d'accès** : restriction de l'accès aux ressources aux entités privilégiées.
- **propriété** : un moyen de fournir à une entité le droit légal d'utiliser ou de transférer une ressource à d'autres.
- **anonymat** : dissimulation de l'identité d'une entité impliquée dans un processus.
- **non-répudiation** : empêcher le déni d'engagements ou d'actions antérieurs.
- **révocation** : retrait de la certification ou de l'autorisation.
- **signature** : un moyen de lier des informations à une entité. C'est un outil fondamental utilisé dans la sécurité de l'information et un élément constitutif de nombreux autres services tels que la non-répudiation, l'authentification de l'origine des données, l'identification et le témoignage.

Assurer la sécurité de l'information dans une société électronique nécessite un large éventail de

- compétences techniques et
- juridiques.

Les moyens techniques sont fournis par la cryptographie.

Definition

La cryptographie est l'étude des techniques mathématiques liées aux aspects de la sécurité de l'information tels que la confidentialité, l'intégrité des données, l'authentification de l'entité et l'authentification de l'origine des données.

La cryptographie n'est pas le seul moyen permettant d'assurer la sécurité de l'information, mais plutôt un ensemble de techniques s'attelant à cette tache.

Parmi tous les objectifs de sécurité de l'information qu'on a énumérés, les **quatre objectifs de la cryptographie** suivants forment un cadre sur lequel les autres seront dérivés :

1. *Confidentialité* : Il existe de nombreuses approches pour assurer la confidentialité, allant de la protection physique aux algorithmes mathématiques qui rendent les données inintelligibles.
2. *Intégrité des données* : pour assurer l'intégrité des données, il faut avoir la capacité de détecter la manipulation des données par des parties non autorisées.
3. *Authentification* : Cet aspect de la cryptographie est généralement subdivisé en deux grandes classes : l'authentification de l'entité et l'authentification de l'origine des données.
4. *Non-répudiation* : Une procédure impliquant un tiers de confiance peut être nécessaire pour assurer ce service.

L'objectif de la cryptographie est d'aborder adéquatement ces quatre domaines à la fois en théorie et en pratique.

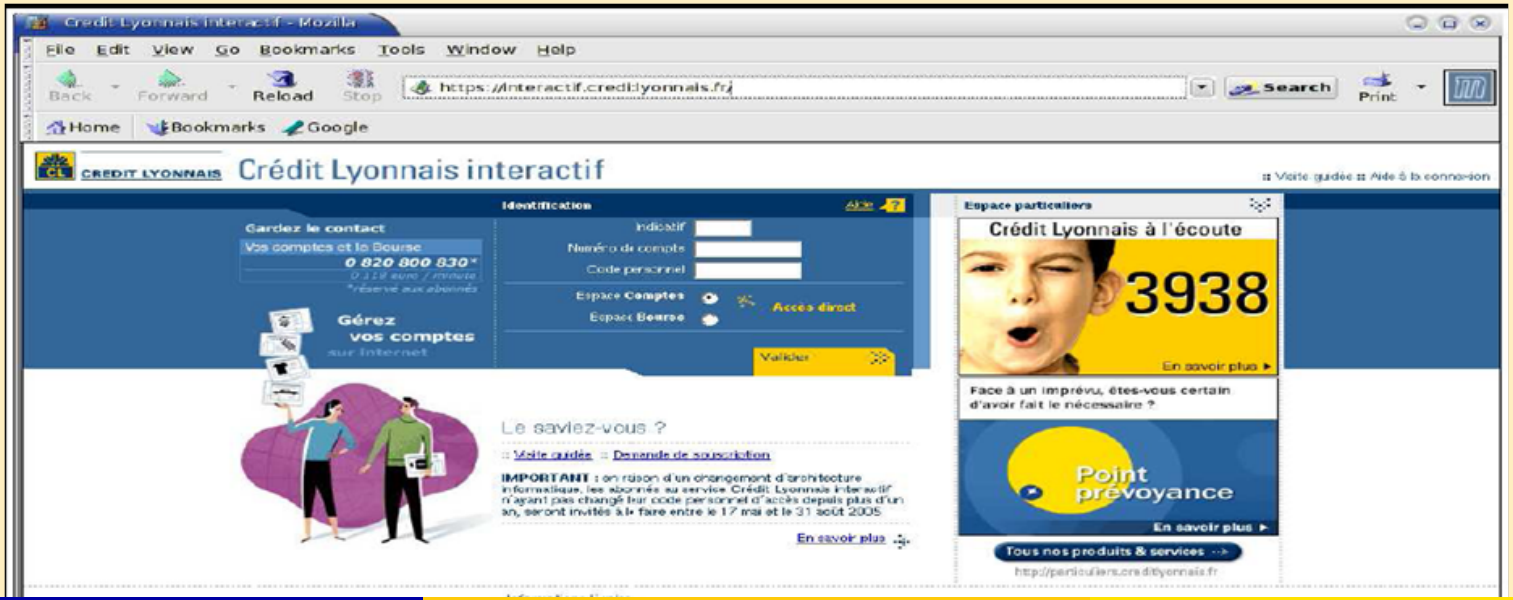
Les domaines d'application de la cryptographie

Où applique t-on la cryptographie ?

La cryptographie est très vaste et connait un progrès très rapide, surtout depuis qu'elle s'est dévelloppée dans le monde civil. Dans chacun des domaines ci dessous la cryptographie s'attéle à répondre à des questions relevant de la sécurité.

Internet : confidentialité, anonymat, authentification. Par exemple dans le cadre du e-Banking on peut se poser comme question "S'agit-il bien de ma banque ?"

Internet



Où applique t-on la cryptographie ?

Administration (vote électronique) : "S'agit-t-il d'un vote unique d'un quelconque électeur ?" En effet le résultat doit reflèter le vote qui reste confidentiel et seuls les électeurs peuvent voter et une seule fois.

Vote électronique

Où applique t-on la cryptographie ?

Paiement par carte bancaire : on peut se poser les questions suivantes : est-ce qu'il s'agit d'une vraie carte ? Est-ce que le montant débité sera égal au montant crédité ? Est-ce que le code secret est bien protégé ?

Paiement par carte bancaire

Où applique t-on la cryptographie ?

Décodeurs et abonnement TV : vérification de l'abonné, impossibilité de retransmettre les données décodées à une tierce personne.
"L'abonnement est-t-il vérifiable ? est-t-il à jour ?"

Décodeurs

Où applique t-on la cryptographie ?

Porte monnaie électronique : La monnaie utilisée est-t-elle autorisée ?
Est-t-il possible de créer un faux porte-monnaie ?

Porte monnaie électronique

Où applique t-on la cryptographie ?

Assurance maladie : Il s'agit d'un secteur sensible utilisant des bases de données sécurisées. Seules les personnes habilitées ont accès à la vue partielle à laquelle elles ont droit, les données peuvent être échangées entre un médecin, un laboratoire, un hôpital.

Bases de données sécurisées

Les outils cryptographiques

Les services offerts par la cryptographie peuvent reposer sur différents domaines de la science.

Outils en Physique.

1. Electronique,
2. Théorie du signal et transmission des données,
3. Physique quantique

Outils en Informatique

1. Génie logiciel,
2. Réseaux informatique et télécom,
3. Equipements informatique et télécom.

La cryptographie s'appuie sur différentes branches des mathématiques notamment sur la théorie des nombres et la géométrie algébrique.

Prérequis mathématiques

1. Théorie des ensembles
2. Groupes, anneaux, corps, espace vectoriel
3. Arithmétique sur les entiers
4. Calcul modulaire et Résiduosité quadratique
5. Calcul sur les polynomes
6. Corps finis et base d'espace vectoriel
7. Les courbes elliptiques
8. Probabilités et variables aléatoires (pseudo-aléatoire)

Dans ce cours on s'en tient aux mathématiques reliés à la cryptographie classique et/ou communément utilisée.