CHAPITRE 1

INTRODUCTION À LA CRYPTOGRAPHIE

1.1 Introduction

La cryptographie, appelée science du secret, a vu ses possibilités décuplées au cours des siècles. Avec l'arrivée de l'Informatique, elle fait partie de notre quotidien. De par ses diverses possibilités et méthodes, cette discipline, servant à assurer la sécurité et la confidentialité des communications. La cryptographie, est l'un des éléments principaux ayant rendu possible l'invention des crypto-monnaies et des blockchains modernes. Les techniques cryptographiques utilisées aujourd'hui sont cependant le fruit d'une longue histoire de développement. Depuis l'Antiquité, la cryptographie permet de transmettre des informations de manière sécurisée.

1.2 Qu'est ce que la cryptographie

La cryptographie vient du grec, **kryptos** qui veut dire **cacher** et **graphein** qui signifie **écrire**. C'est l'art de garder le secret, de crypter, de coder, un message pour ceux qui ne sont pas habilités à en prendre connaissance. Il s'agit donc d'un ensemble de techniques basées sur des théories mathématiques (algorithmes) permettant de protéger une communication au moyen d'un code secret.

1.3 Cryptographie : aperçu historique

Tout au long de l'histoire, la cryptographie s'est insérée dans les différents contextes historiques, et a progressé avec les évolutions mathématiques. La plupart du temps utilisée dans un milieu politique ou militaire, elle s'oppose à son rival, la cryptanalyse, qui est l'action de décrypter un message préalablement codé suivant des règles bien définies.

- De l'Antiquité au début du Moyen-Âge : Les 1ères traces de cryptographie remontent au XVIe siècle avant J-C. On a retrouvé à cette époque :
  - Le chiffre Atbash : Datant du Ve siècle avant J-C, ce procédé consiste à faire correspondre l'alphabet classique avec l'alphabet inversé, et d'associer ainsi à chaque lettre la lettre correspondante en position dans l'alphabet inversé.

- Le chiffre de César : Durant l'antiquité, le premier système de cryptographie à base mathématique fut inventé par Jules César. Un grand empereur militaire, son véritable intérêt à l'époque est son utilisation militaire.
- La scytale : Est une des premières techniques de codage par transposition. Elle date du Ve siècle av J-C. Le principe est le suivant : celui qui est l'auteur du message va préalablement enrouler une bande en hélice autour d'un bâton régulier de diamètre fixé sur laquelle il va pouvoir écrire. Après écriture, l'auteur déroule la bande qui présente alors une succession de caractères n'ayant aucun sens logique. Celui qui veut lire le message doit alors connaître le diamètre du bâton initial puis y enrouler de nouveau la bande.
- Le chiffre affine : Il existe un autre type de cryptage dont le code César est un cas particulier. Cette méthode est connue sous le nom de chiffrement affine.

- De la Renaissance au début du XIXe siècle

  - Le carré de Vigénère

  Bien que les systèmes de cryptographie par substitution étaient connus pour être facilement décryptés, il n'y eut pas, depuis le code César (et tous ses dérivés) apparu vers le Ve siècle avant J-C, de réels nouveaux systèmes cryptographiques à la fois sécurisés et commodes à employer. Il fallut attendre le XVIe siècle pour que Blaise de Vigénère révèle enfin un nouveau mode de codage basé sur un chiffrement polyalphabétique, procédé qui primera sur la plupart des autres modes de cryptage pendant près de 3 siècles.

- De la 1ère guerre mondiale aux débuts de l'informatique : La période que nous étudions ici englobe les deux guerres mondiales. De nombreuses nouveautés dans le type de systèmes apparaissent : il y a apparition de machines à crypter (comme la bien connue machine Enigma), mais également l'utilisation d'outils mathématiques développés.

  - La machine Enigma : est l'une des plus remarquables machines à crypter toutes périodes confondues ; elle a longtemps servi de modèle et a marqué son époque. La naissance de la machine Enigma est initiée en 1919 par un ingénieur hollandais, Hugo Alexander, qui brevete un dispositif de codage électromécanique.
  - Le système ADFGVX : Le chiffre ADFGVX a été inventé durant la Première Guerre Mondiale par le colonel allemand Fritz Nebel. Ce système de chiffrement avait l'avantage que le texte obtenu après une première substitution était ensuite soumis à une permutation des colonnes du carré ADFGVX.
  - Le chiffre de Hill : Cette méthode de chiffrement fut inventée par Lester Hill en 1929. L'idée de Lester Hill est de changer de méthode générale de cryptage : il cherche à oublier la façon de crypter caractères par caractères, pour la remplacer par un chiffrement en blocs de manière simultanée de plusieurs caractère en utilisant un outil mathématique intéressant : les matrices.

- Des débuts de l'Internet à aujourd'hui : Dans les années 1970, l'apparition des ordinateurs de troisième et de quatrième générations, dotés des microprocesseurs, ainsi que de l'internet va considérablement augmenter la facilité à communiquer et à casser certains algorithmes grâce à la puissance de calcul des ordinateurs. De nouveaux procédés cryptographiques vont alors apparaître justement dans le but de déjouer la puissance nouvelle de ces machines ; les plus célèbres seront présentés parmi les nouveaux systèmes décrits ci-après.

- Le Pretty Good Privacy, communément appelé PGP. Ce dernier présente comme grand intérêt que c'est un des premiers logiciels de cryptographie à la fois puissant et rendu public, d'utilisation accessible à toute personne possédant un ordinateur, ce qui a eu pour effet de voir son auteur poursuivi par le FBI.
- Le chiffrement DES : dont les initiales signifient : Data Encryption Standard (standard de chiffrement de données), fut inventé dans la société IBM. Jusqu'à cette époque, seuls les états-majors possédaient des algorithmes à clés secrètes fiables.
- Le système RSA (du nom des trois auteurs Ronald Rivest, Adi Shamir et Leonard Adleman) est l'un des meilleurs exemples de procédés capables de mettre en échec la puissance des ordinateurs s'il est bien utilisé. Ce système de cryptographie asymétrique à clé publique créé à la fin des années 1970 tire sa force de la difficulté à factoriser un grand nombre entier en produit de nombres premiers.

- Demain : la cryptographie quantique ? Les progrès en sciences physiques et notamment les connaissances en mécanique quantique permettent aujourd'hui d'imaginer un nouveau procédé de cryptographie inédit et très différent de ce que l'on a connu jusqu'ici. Différent, excepté le fait que cette méthode réutilise comme outil un système de codage inventé en 1917 par Gilbert Vernam : le masque jetable, qui est le seul procédé à être théoriquement incassable. Pourtant, on remarquera que le principe est simplissime : il s'agit d'une version évoluée du code César ou l'on choisit une clé de la longueur du message à chiffrer. Ensuite, on décale chaque lettre du message du nombre de lettre indiqué par la lettre de la clé correspondante. Aujourd'hui, les avancées de la physique ont peut-être trouvé une voie au masque jetable : effectivement, ils ont trouvé un moyen de transmettre la clé secrètement en manipulant les photons polarisés.

1.4 Principes de Kerckhoffs

En 1883 dans un article paru dans le Journal des sciences militaires, Auguste Kerckhoffs (1835-1903) posa les principes de la cryptographie moderne. Ces principes et en particulier le second stipulent entre autre que la sécurité d'un cryptosystème ne doit pas reposer sur le secret de l'algorithme de codage mais qu'elle doit uniquement reposer sur la clé secrète du cryptosystème qui est un paramètre facile à changer, de taille réduite (actuellement de 64 à 2048 bits suivant le type de code et la sécurité demandée) et donc assez facile à transmettre secrètement. Ce principe a été très exactement respecté pour le choix du dernier standard de chiffrement, l'algorithme symétrique AES, par le NIST. Ce dernier a été choisi à la suite d'un appel d'offre international et tous les détails de conception sont publics. Ce principe n'est que la transposition des remarques de bon sens suivantes :

- Un cryptosystème sera d'autant plus résistant et sûr qu'il aura été conçu, choisi et implémenté avec la plus grande transparence et soumis ainsi à l'analyse de l'ensemble de la communauté cryptographique.

- Si un algorithme est supposé être secret, il se trouvera toujours quelqu'un soit pour vendre l'algorithme, soit pour le percer à jour, soit pour en découvrir une faiblesse ignorée de ses concepteurs. A ce moment-là c'est tout le cryptosystème qui est à changer et pas seulement la clé.

1.5 Un peu de vocabulaire

Avant d'aller plus loin, précisons le sens de certains termes.

- Cryptanalyse : c'est l'ensemble des procédés d'attaque d'un système cryptographique. Autrement dit, est l'art pour une personne non habilitée, de décrypter, de décoder, de déchiffrer un message.
- Cryptologie : Une Science mathématique qui comporte les deux branches ; la cryptographie et la cryptanalyse.
- Crypto-système (un système de chiffrement) : Un système cryptographique ou cryptosystème est composé d'un algorithme de cryptage (chiffrement) et d'un algorithme de décryptage (déchiffrement). Un système cryptographique est un quintuple (P, C, K, E, D) tel que :

  P : ensemble fini de textes clairs possibles.
  C : ensemble fini de textes chiffrés possibles.
  K : ensemble fini de clés possibles.
  E : un ensemble de fonctions e_k k $\in$ K de chiffrement de P vers C.
  D : un ensemble de fonctions d_k |k $\in$ K de déchiffrement de C vers P,satisfaisant aux conditions suivantes : pour tout $k \in K$, il y a une fonction de chiffrement $e_k \in E$ et une règle de déchiffrement correspondante $d_k \in D$. $e_k : P$ vers C et $d_k : C$ vers P sont des fonctions telles que $d_k(e_k(x)) = x$ pour tout $x \in P$.
- Cryptogramme : Est un message écrit a l'aide d'un système de chiffrement.
- Clé: Dans un système de chiffrement, elle correspond a un nombre, un mot, une phrase, etc. qui permet, grâce à l'algorithme de chiffrement, de chiffrer ou de déchiffrer un message.
- Chiffrement : procédé qui consiste à transformer un texte clair en cryptogramme.
- Déchiffrement : procédé inverse du chiffrement qui consiste à obtenir la version originale d'un message qui a été chiffré en connaissant la méthode de chiffrement et les clés.
- Canal : Moyen de transport de l'information.
- Canal sécurisé : Canal où l'intrus n'a pas la possibilité d'altérer les messages.
- Canal sécuritaire : Canal qui n'est pas physiquement accessible à l'intrus.

1.6 Qualité d'un cryptosystème

Les qualités d'un système cryptographique sont résumées par les mots clés suivants :

- Confidentialité : seules les personnes habilitées ont accès au contenu du message.
- Intégrité des données : le message ne peut pas être falsifié sans qu'on s'en aperçoive.
- Authentification : s'assurer de l'identité l'émetteur/ destinataire.
- Non-répudiation qui se décompose en trois :
  - Non-répudiation d'origine : l'émetteur ne peut nier avoir écrit le message.
  - Non-répudiation de réception : le receveur ne peut nier avoir reçu le message.
  - Non-répudiation de transmission : l'émetteur du message ne peut nier avoir envoyé le message.

1.7 Différentes notions de sécurité d'un cryptosystème

-La sécurité inconditionnelle qui ne préjuge pas de la puissance de calcul du cryptanalyste qui peut être illimitée.

-La sécurité calculatoire qui repose sur l'impossibilité de faire en un temps raisonnable, compte tenu de la puissance de calcul disponible, les calculs nécessaires pour décrypter un message. Cette notion dépend de l'état de la technique à un instant donné.

-La sécurité prouvée qui réduit la sécurité du cryptosystème à un problème bien connu réputé difficile, par exemple on pourrait prouver un théorème disant qu'un système cryptographique est sûr si un entier donné n ne peut pas être factorisé.

-La confidentialité parfaite qualité des codes pour lesquels un couple (message clair, message chiffré) ne donne aucune information sur la clé.

1.8 Cryptanalyse " attaques sur un chiffrement"

La cryptanalyse est l'ensembles des procédés d'attaque d'un cryptosystème. Elle est indispensable pour l'étude de la sécurité des procédés de chiffrement utilisés en cryptographie. Son but ultime est de trouver un algorithme de déchiffrement des messages. Le plus souvent on essaye de reconstituer la clé secrète de déchiffrement.

On suppose, en vertu des principes de Kerckhoffs, pour toutes les évaluations de sécurité d'un cryptosystème que l'attaquant connait le système cryptographique utilisé, la seule partie secrète du cryptosystème est la clé. On doit distinguer entre les types d'attaques d'un adversaires et les buts des attaques d'un adversaire. Les principaux types d'attaques :

- Attaque à texte chiffré connu : l'opposant ne connait que le message chiffré y.
- Attaque à texte clair connu : l'opposant dispose d'un texte clair x et du message chiffré correspondant y.
- Attaque à texte clair choisi : l'opposant a accès à une machine chiffrante. Il peut choisir un texte clair et obtenir le texte chiffré correspondant y, mais il ne connait pas la clé de chiffrement.
- Attaque à texte chiffré choisi : l'opposant a accès à une machine déchiffrante. Il peut choisir un texte chiffré, y et obtenir le texte clair correspondant x, mais il ne connait pas la clé de déchiffrement.

1.9 Quelles mathématiques pour la cryptographie

Actuellement tous les cryptosystèmes utilisent des mathématiques. Elles sont utilisées aussi pour définir et tester la sécurité des cryptosystèmes. Parmi les disciplines mathématiques utilisées pour la cryptographie on a :

- Logique : théorie de la complexité.
- Probabilités pour la théorie de l'information.
- Analyse harmonique pour la théorie du signal.
- Combinatoire (théorie de graphes) : construction de cryptosystèmes asymétriques, preuves sans apport d'information, partage de secret à seuil.
- Algèbre : théorie des corps finis, des polynômes sur un corps fini, ..., pour les codes symétriques.

- Théorie des nombres (arithmétique modulaire, théorie algébrique des nombres) : construction de cryptosystèmes asymétriques (RSA, ElGamal), générateurs de nombres aléatoires.
- Géométrie algébrique sur un corps fini : construction de cryptosystèmes basés sur les courbes elliptiques sur un corps finis, cryptosystèmes basés sur les codes correcteurs d'erreurs.
- Algorithmique (algèbre, théorie des nombres et géométrie effective) : mesure de la complexité algorithmique, réalisation pratique d'algorithmes performants, évaluation de la sécurité des cryptosystèmes.

1.10 Quelques utilisations de la cryptographie

Les mécanismes de cryptographie peuvent être appliqués :

- Les cartes bancaires : Les banques font partie des premiers utilisateurs de systèmes cryptographies. Les cartes bancaires possèdent trois niveaux de sécurité : Le code confidentiel, la signature et L'authentification.
- Les navigateurs Web : Les navigateurs, ou broswers, tels que Mozilla Firefox ou Internet Explorer, utilisent le protocole de sécurité SSL (Secure Sockets Layers).
- Internet (achat, identification, . . .).
- Téléphones portables, clés électroniques (e.g voitures).
- Carte d'identités électroniques, carte de santé, …
- Chiffrement des fichiers : EFS, TrueCrypt.
- Au niveau des documents et données à protéger : PGP, S/MIME, signature XML.

1.11 Cryptographie vs Stéganographie

La stéganographie (du grec **steganos**, couvert et **graphein**, écriture) est l'art de cacher un message secret au sein d'un autre message porteur (texte, image, son, vidéo...) de caractère anodin, de sorte que l'existence même du secret en soit dissimulée. Alors qu'avec la cryptographie, la sécurité repose sur le fait que le message chiffré soit incompréhensible pour les personnes non autorisées, avec la stéganographie, la sécurité repose sur le fait que la présence même d'un message secret ne sera sans doute pas soupçonné et détecté.

La stéganographie peut être utilisée sur n'importe quel support tel que le texte, l'audio, la vidéo et l'image, tandis que la cryptographie est implémentée uniquement dans un fichier texte. En stéganographie, la structure principale du message n'est pas modifiée alors que la cryptographie impose un changement sur le message secret avant de le transférer sur le réseau.

La stéganographie ne fournit que la confidentialité et l'authentification. Au contraire, les principes de sécurité fournis par la cryptographie sont la confidentialité, l'intégrité, l'authentification et la non-répudiation. L'ingénierie inverse utilisée pour décoder le message en cryptographie est connue sous le nom de cryptanalyse. Par contre, la technique utilisée pour détecter la présence de la stéganographie est connue sous le nom de stéganalyse. Lorsqu'elles sont combinées, la stéganographie et la cryptographie peuvent fournir deux niveaux de sécurité. Il existe des programmes informatiques qui cryptent un message en utilisant la cryptographie et cachent le cryptage dans une image en utilisant la stéganographie.