Chapitre 3

Sécurisation des communications

3.1 Cryptographie

La cryptographie est une discipline visant à assurer la **confidentialité**, l'**authenticité** et l'**intégrité** des données stockées ou échangées par une ou plusieurs entités (humains, organisations, machines, etc). On peut résumer ces trois notions de la façon suivante.

Confidentialité : fait que l'information ne soit accessible qu'aux entités autorisées.

Authenticité : assurance de la légitimité d'une demande d'accès à des informations faite par une entité.

Intégrité : état des données lors de leur traitement, transfert ou conservation ; celles-ci ne doivent pas subir de destruction (volontaire ou non), être altérées et rester dans un format exploitable.

La protection de ces données repose souvent sur des méthodes de **chiffrement** ; le chiffrement est une méthode consistant à prendre des données en clair, ou brutes, et à les transformer en données incompréhensibles pour une entité n'étant pas autorisée à y accéder.

Exemple : la phrase « Il y a un serpent dans ma botte », en clair, peut être chiffrée sous la forme

Hk x z tm rdqodms czmr lz anssd,

laquelle est moins compréhensible.

Le chiffrement repose la plupart du temps sur des **clés**. Les clés sont des paramètres des fonctions de chiffrement, elles déterminent la façon dont les données vont être chiffrées et déchiffrées.

Exemple : Le message de l'exemple précédent a été chiffré par la méthode du chiffre de César, il s'agit d'un simple décalage dans l'ordre des lettres. La clé de cette méthode réside dans les deux lettres qui définissent ce décalage. Dans l'exemple précédent, la clé est b→a, autrement dit, on a un décalage de -1 ou de 1 vers la gauche dans l'alphabet. Pour déchiffrer le message, il suffit d'effectuer le décalage inverse.

Le chiffre de César est ainsi nommé car il fut utilisé par Jules César dans ses correspondances. Les méthodes de chiffrement étaient ainsi utilisées dès l'Antiquité. Elles ont connu un essor

rapide lors du XX^{e} siècle avec celui de l'informatique et les progrès en mathématiques, aussi bien en termes de méthodes de chiffrement que de déchiffrement, passant alors de l'état d'art à celui de science. On peut notamment penser aux machines Enigma et de Lorenz utilisées par l'Allemagne nazie durant la seconde guerre mondiale afin de chiffrer ses communications et dont les déchiffrements ont eu une influence très importante sur le cours de la guerre.

Aujourd'hui, le chiffrement des données tend à se généraliser et est utilisé sans que l'on s'en rende compte ou que l'on ait quoi que ce soit à faire. On pensera au stockage des données avec la possibilité de chiffrer des ordinateurs ou des serveurs cloud (de plus en plus en option par défaut) ; aux communications avec la possibilité de chiffrer ses mails ou ses messages (grâce à des services comme WhatsApp, Signal, Proton, etc) et à la navigation sur le Web grâce à des protocoles comme HTTPS.

Il existe et a toujours existé une forme de course entre les moyens de chiffrer et d'attaquer les chiffrements. Actuellement, nous disposons de systèmes de sécurisation des données et communications performants. L'enjeu est dans l'accessibilité des méthodes et la compréhension de l'intérêt de le faire : l'immense majorité des mails, des ordinateurs et téléphones n'est pas chiffrée par méconnaissance et incompréhension. De l'autre côté, il existe de nombreux moyens de s'attaquer à la sécurisation des données, on peut notamment citer :

— les attaques par force brute : on essaye toutes les combinaisons possibles, cela fonctionne bien sur des messages chiffrés avec le chiffre de César ou des mots de passe faibles mais est inefficace contre des moyens de chiffrement élaborés ;

— les analyses mathématiques (notamment fréquentielle) et de rétro-ingénierie ; ce sont par exemple elles qui ont permis aux Alliés de déchiffrer les messages de la machine de Lorenz sans jamais en avoir vu une seule ;

— les analyses et attaques psychologiques, sociologiques et linguistiques ;

— les attaques du type l'homme du milieu, etc.

Le déchiffrement d'Enigma résulte d'un mélange de plusieurs types d'attaques : analyses mathématiques, sociologiques, linguistiques, force brute...

Deux aspects sont actuellement considérés comme essentiels en matière de cryptographie :

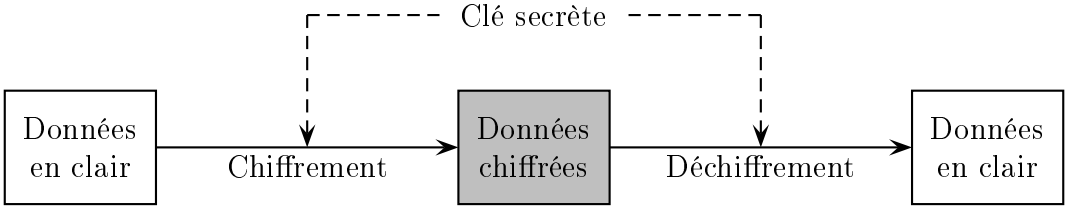
— la sécurité calculatoire : la clé doit avoir suffisamment de valeurs possibles pour qu'une attaque par force brute puisse être menée en temps raisonnable ;

— le non secret de l'algorithme de chiffrement, voire son accès libre : le chiffrement ne doit pas pouvoir être défait par la simple connaissance de l'algorithme qui l'a crée ; cela joue en faveur d'algorithmes de chiffrement libres, qui sont connus de tous et peuvent être ainsi éprouvés ; au contraire, un algorithme de chiffrement fermé ou secret ne garantit pas sa fonctionnalité (ou uniquement celle-ci) et comporte des faiblesses face à l'espionnage ou la trahison.

À méditer : une chaîne est aussi forte que le plus faible de ses maillons.

3.2 Chiffrement symétrique

Le chiffrement symétrique ou chiffrement par clé secrète est une méthode de chiffrement dans laquelle la clé permet à la fois de chiffrer et de déchiffrer les données.



Un chiffrement symétrique a pour avantage d'être généralement rapide et convient donc bien à des échanges d'importantes quantités de données. Il peut aussi être très sûr comme par exemple le masque jetable ; lequel est inviolable et a notamment été utilisé pour le fonctionnement du téléphone rouge entre le Kremlin et la Maison Blanche.

Le chiffrement symétrique présente toutefois des inconvénients. Le premier étant que la clé doit être échangée par un autre canal que celui qui servira à communiquer pour des raisons évidentes de sécurité. Ainsi, encore dans les années 1970, des coursiers parcouraient la planète, parfois sous escorte, afin d'apporter les clés à intervalles réguliers aux entités souhaitant communiquer. Cela posait des problèmes évidents de confiance dans les personnes choisies et de logistique face à l'augmentation des entités devant chiffrer leurs communications.

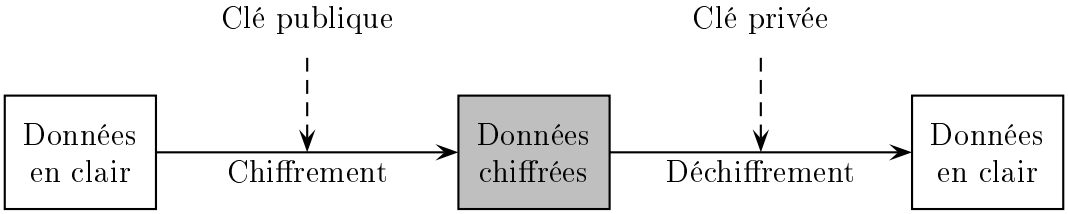
Exemples : de méthodes de chiffrement symétrique.

- Chiffre de César.
- Chiffrement par substitution.
- AES.
- Masque Jetable.
- Chiffre de Vigenère.

3.3 Chiffrement asymétrique

3.3.1 Chiffrement de données

Le chiffrement asymétrique ou chiffrement par clés publique et privée est une méthode de chiffrement dans laquelle la clé publique permet de chiffrer les données la clé privée permet de les déchiffrer.



Le concept a été inventé dans les années 1970 de façon indépendante par des chercheurs américains et des chercheurs travaillant pour le renseignement britannique ; cependant, le caractère secret des recherches de ces derniers fit que leurs travaux ne furent rendu publique que des années plus tard.

Il repose sur l'idée de fonction à sens unique et de fonction à portes dérobées. Les fonctions à sens unique sont des fonctions pour lesquelles il est aisé de calculer une image mais pour lesquelles la recherche d'antécédent est difficile voire impossible. Les fonctions à portes dérobées sont des fonctions à sens unique pour lesquelles la recherche d'antécédent est facile connaissant certains paramètres. Ces fonctions à sens unique servent à constituer la clé publique et donc à chiffrer, elles assurent que le chiffrement soit difficile à défaire. Les portes dérobées, autrement dit les paramètres et fonctions qui facilitent l'inversion, et donc le déchiffrement, constituent la clé privée.

Ainsi, comme son nom l'indique, la clé publique peut et doit être connue de tous. Elle sert à chiffrer des données que seul le destinataire pourra déchiffrer à l'aide de sa clé privée, laquelle doit bien évidemment rester secrète. Cette méthode de chiffrement a pour immense avantage de permettre la transmission de la clé publique par le canal de communication qui sert à transmettre les données contrairement au chiffrement symétrique. Elle a donc été massivement adoptée depuis son invention dans les années 1970. Elle a toutefois pour inconvénients d'être lente, ne convenant pas à d'important échanges de données, et n'est pas invulnérable non plus. Elle est notamment vulnérable à l'attaque de l'homme du milieu, ce qui pose le problème de l'authentification.

Exemples : de méthodes et logiciels de chiffrement asymétrique.

- RSA.
- Cryptographie sur les courbes elliptiques.
- Logiciel GPG.
- Logiciel OpenSSL.

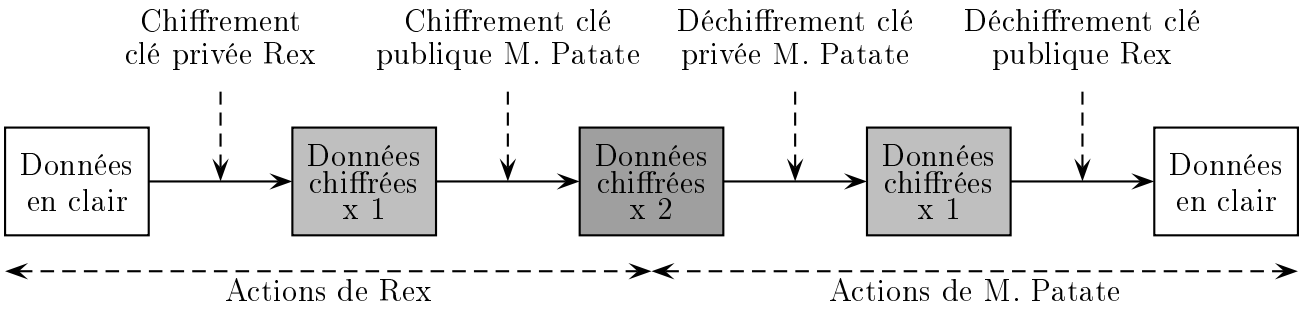
3.3.2 Authentification

L'authentification repose sur une spécificité des paire de clés publiques privées. Si la clé publique chiffre et la privée déchiffre, l'inverse est aussi vrai : si on chiffre en utilisant la clé privée, alors on peut déchiffrer en utilisant la clé publique.

Considérons deux entités souhaitant communiquer : appelons-les Monsieur Patate et Rex. Rex souhaite communiquer de façon chiffrée avec Monsieur Patate, il chiffre les données qu'il veut envoyer à Monsieur Patate avec la clé publique de ce dernier ; seul Monsieur Patate peut donc les déchiffrer. Mais comment Monsieur Patate peut-il être sûr que les données qu'il reçoit ont été envoyées par Rex et non par un imposteur ?

Pour assurer Monsieur Patate que c'est bien lui qui lui a envoyé les données, Rex peut les signer numériquement (à ne pas confondre avec la signature électronique manuscrite) à l'aide de sa clé privée. Il s'agit en réalité d'une opération de chiffrement supplémentaire, les données sont chiffrées à l'aide de la clé privée et déchiffrées grâce à la clé publique, ce qui garantit l'identité de leur auteur : seul celui-ci possède sa clé privée (excepté un éventuel vol). On a ainsi la procédure suivante.

1. Rex chiffre une première fois les données avec sa clé privée.
2. Rex chiffre une seconde fois les données avec la clé publique de Monsieur Patate et lui envoie.
3. Monsieur Patate reçoit les données et les déchiffre à l'aide sa clé privée, opération qu'il est le seul à pouvoir effectuer. Toutefois, les données qu'il obtient restent chiffrées à cause du premier chiffrement.
4. Monsieur Patate déchiffre une seconde fois les données, cette fois-ci à l'aide de la clé publique de Rex, ce qui garantit que ce dernier est bien l'expéditeur de ces données.



3.4 Protocole HTTPS

Le protocole HTTPS est la version chiffrée du protocole HTTP, généralement à l'aide du protocole TLS (Transport Layer Security qui succède au SSL). Il a pour but de répondre à deux problématiques :

— la sécurisation des données transmises sur les sites Web comme celles des formulaires, des mails (attention, cela ne chiffre pas le contenu des mails), etc ;

— l'authentification du serveur et éventuellement du client (n'importe quel client ne peut accéder à n'importe quelles données).

L'authentification du serveur est primordiale. En effet, sans elle, rien ne garantit que l'on n'est pas en train de subir une attaque de l'homme du milieu. C'est d'ailleurs la base des attaques par phishing (hameçonnage) : un site en usurpant un autre récupère des données personnelles. Il est ainsi capital de s'assurer de l'identité du site.

L'authentification est assurée par des certificats électroniques. Ceux-ci sont délivrés par des autorités de certification qui sont généralement en contact direct avec les systèmes d'exploitation et les navigateurs. Le certificat est construit à partir de trois données :

— la clé publique du site à authentifier et qui permettra aux utilisateurs de d'assurer de son identité ;

— des informations permettant d'identifier le site ;

— la clé privée de l'autorité de certification.

Le protocole HTTPS combine les deux chiffrements : asymétrique dans un premier temps afin de s'assurer des identités des entités en présence grâce aux certificats et de mettre en place le deuxième chiffrement, symétrique cette fois-ci, afin d'échanger d'important volumes de données. Il se déroule selon les étapes suivantes.

1. Le client envoie sa version de TLS utilisée.
2. Le serveur répond en renvoyant son certificat prouvant son identité, ainsi que sa clé publique.
3. Le client interroge l'autorité de certification pour valider le fait que le certificat est bien valide et que le serveur est bien celui qu'il prétend être. Cette vérification est faite grâce au chiffrement asymétrique.
4. Une fois vérifiée l'authenticité du serveur et que son certificat est valide, une clé de chiffrement symétrique est créée à partir des informations échangées à l'aide du chiffrement symétrique. Cette clé est appelée AES.

Une fois le chiffrement symétrique établi, les données permettant la navigation sur le site peuvent être échangées.