La Cryptographie déchiffrée

De Aumasson, Jean-Philippe

Table des matières

Chiffrement

Le chiffrement est la fonction principale de la cryptographie. Cette technique a pour but de rendre les informations illisibles afin de protéger leur confidentialité. Un système de chiffrement, connu sous le terme anglais "cipher", repose sur une donnée secrète appelée clé. Sans cette clé, il est impossible de restaurer le contenu d'un message chiffré ou d'y accéder.

À noter : le verbe « chiffrer » sera préféré à l'anglicisme « crypter ». On fait distinction entre « déchiffrer » (permettre de récupérer le message original à partir du message chiffré avec la clé) et « décrypter » (essayer de récupérer le message sans posséder la clé, souvent en utilisant des méthodes d'analyse de données pour exploiter des faiblesses dans le système). En parlant de « chiffre » (ou cipher), on désigne un système de chiffrement ou "cryptosystème".

Les fondamentaux

Lors de la chiffrage d'un message, on parle de plaintext pour désigner le texte clair et de ciphertext pour le texte chiffré. Un système de chiffrement se compose principalement de deux étapes : le chiffrement, qui convertit le plaintext en ciphertext, et le déchiffrement, qui convertit le ciphertext en plaintext. Par exemple, si l'on note l'opération de chiffrement par E, alors le chiffrement d'un message P avec une clé K donne en résultat C. Cette relation se décrit par C = E(K, P). De même, pour le déchiffrement, on peut noter D(K, C).

Systèmes de chiffrement classiques

Avant l'ère numérique, les systèmes de chiffrement traditionnels utilisaient des lettres plutôt que des bits pour créer des messages secrets. Ces anciens cryptosystèmes sont beaucoup plus simples que les systèmes modernes tels que DES. Par exemple, au cours de l'Antiquité romaine ou même pendant la Première Guerre mondiale, le chiffrement devait être réalisable uniquement avec un simple crayon et du papier. Parmi les méthodes célèbres, deux se distinguent : celle de César et celle de Vigenère.

Le chiffre de César

Le chiffre de César porte le nom du célèbre chef romain Jules César. Cette méthode consiste à décaler chaque lettre d'un message d'un certain nombre de positions dans l'alphabet ; par exemple, un décalage de trois signifie que A devient D, B devient E, et ainsi de suite. Par conséquent, "CAESAR" devient "FDHDVU". Ce chiffrement est particulièrement facile à déchiffrer, car il suffit de ramener les lettres trois positions en arrière.

Bien qu'il ait pu protéger des communications à des époques passées, ce chiffrement est désormais considéré comme trop simple. En effet, en 2006, la police italienne a pu déchiffrer des messages de la mafia sicilienne utilisant une variante du chiffre de César.

Pour renforcer la sécurité, une variante pourrait impliquer un décalage secret plutôt que de demeurer constant, mais cela reste peu efficace, car un attaquant pourrait simplement essayer toutes les options possibles, soit 25 décalages au total.

Le chiffre de Vigenère

Il a fallu environ 1500 ans pour que le chiffre de Vigenère émerge, introduit par Giovan Battista Bellaso au XVIe siècle. Ce chiffre est plus complexe que celui de César, car il utilise une clé constituée de lettres qui déterminent des décalages différents pour chaque lettre du texte à crypter. Par exemple, si la clé est "DIJH", chaque lettre du texte est décalée de 3, 8, 9, et 7 positions respectivement.

Bien que plus résistant que le chiffre de César, Vigenère reste vulnérable. Pour le casser, un analyste cherche d'abord à déterminer la longueur de la clé, puis utilise l'analyse de fréquence pour déduire les lettres chiffrées les plus communes. Cela nécessite souvent que le texte soit un peu plus long que quelques phrases.

Comment le chiffrement fonctionne-t-il ?

Le chiffrement se base sur deux éléments essentiels : les permutations et les modes opératoires. Une permutation est une méthode qui remplace les lettres d'un message par d'autres, de manière à ce que chaque lettre ait une correspondance unique. Par exemple, un décalage est une forme de permutation où chaque lettre est déplacée d'un nombre fixe de rangs.

Un mode opératoire utilise différentes permutations pour traiter des messages de toutes les tailles. Dans le chiffre de César, chaque lettre subit la même opération, mais le chiffre de Vigenère applique des permutations différentes en fonction de la position des lettres.

Les systèmes de chiffrement classiques sont généralement vulnérables face aux ordinateurs modernes, car ils reposent sur des opérations simples. Ces méthodes, bien qu'utiles autrefois, ne peuvent pas résister à la puissance de calcul actuelle, ce qui rend leur décryptage rapide et facile.

Le chiffre parfait : le "one-time pad"

Le "one-time pad", ou masque jetable, est une méthode théoriquement infaillible. Elle repose sur l'utilisation d'une clé aussi longue que le message, utilisée une seule fois. Cela permet d'atteindre une sécurité parfaite, car même avec une capacité de calcul illimitée, il est impossible pour un attaquant de découvrir des informations sur le message en clair en se basant uniquement sur le texte chiffré.

Le chiffrement asymétrique

Contrairement au chiffrement symétrique, où deux parties partagent la même clé, le chiffrement asymétrique utilise deux clés : une publique pour le chiffrement et une secrète pour le déchiffrement. Cette méthode permet à quiconque d'envoyer des messages chiffrés sans avoir besoin de partager une clé secrète. Ce modèle fait appel à des opérations mathématiques qui sont faciles à effectuer dans une direction (chiffrer avec la clé publique) mais incroyablement difficiles dans l'autre (déchiffrer sans la clé secrète).

Cas d'utilisation d'une clé asymétrique

L’utilisation d’une clé asymétrique est particulièrement adaptée dans les contextes où la distribution sécurisée des clés est complexe, ou lorsque plusieurs personnes ou entités doivent communiquer de manière sécurisée sans qu’elles se connaissent à l’avance. Voici quelques cas concrets et exemples illustrant l'utilité des clés asymétriques :

1. Transmission sécurisée de données

L'un des principaux usages des clés asymétriques est de permettre la transmission sécurisée de données sur des réseaux non sûrs, comme Internet.

- **Exemple :** Alice veut envoyer un message confidentiel à Bob. Elle utilise la clé publique de Bob pour chiffrer le message. Une fois chiffré, seul Bob, qui dispose de la clé privée correspondante, peut le déchiffrer. Ainsi, même si le message est intercepté en chemin, il reste illisible pour quiconque ne possède pas la clé privée de Bob.

2. Authentification et signatures numériques

Le chiffrement asymétrique permet également de garantir l’authenticité d’un message ou d’une transaction via des signatures numériques.

- **Exemple :** Lorsqu’elle envoie un document, Alice peut utiliser sa clé privée pour signer numériquement le fichier. Toute personne possédant la clé publique d’Alice peut vérifier la signature et confirmer que le document provient bien d’elle et n’a pas été altéré.

- **Applications concrètes :** Les signatures numériques sont couramment utilisées dans les transactions bancaires en ligne, l’authentification des courriers électroniques et la validation des logiciels ou des documents PDF.

3. Protocole SSL/TLS et navigation web sécurisée

Le chiffrement asymétrique joue un rôle fondamental dans les protocoles de sécurisation des communications sur le web, notamment SSL/TLS.

- **Exemple :** Lorsque vous accédez à un site web sécurisé (HTTPS), votre navigateur utilise la clé publique du serveur pour échanger une clé de session temporaire. Une fois cet échange terminé, les communications ultérieures se font en utilisant un chiffrement symétrique, plus rapide.
- **Pourquoi utiliser l'asymétrie ?** L’asymétrie garantit que seul le serveur, avec sa clé privée, peut lire les informations envoyées par le navigateur.

4. Partage sécurisé de clés symétriques

Bien que le chiffrement asymétrique soit plus lent et coûteux en termes de ressources, il est souvent utilisé pour échanger des clés symétriques de manière sécurisée.

- **Exemple :** Lors d'une session chiffrée, Alice et Bob peuvent utiliser un chiffrement asymétrique pour échanger une clé symétrique temporaire. Une fois la clé symétrique partagée, elle sert au chiffrement et au déchiffrement rapide des données.

- **Applications concrètes :** Ce mécanisme est la base de nombreux protocoles de communication sécurisés, comme SSH (Secure Shell).

5. Gestion des identités et certificats

Dans les infrastructures à clé publique (PKI), les clés asymétriques sont utilisées pour établir la confiance entre différentes entités.

- **Exemple :** Une autorité de certification (CA) émet des certificats numériques contenant la clé publique d'une organisation ou d'un individu. Ces certificats permettent à d'autres parties de vérifier leur identité. Cela est essentiel pour des applications comme le commerce électronique, où les utilisateurs doivent faire confiance aux sites qu'ils visitent.

6. Cryptomonnaies et blockchain

Le chiffrement asymétrique est au cœur des technologies blockchain et des cryptomonnaies comme Bitcoin et Ethereum.

- **Exemple :** Chaque utilisateur possède une paire de clés asymétriques : une clé publique pour recevoir des fonds et une clé privée pour signer les transactions. Cela garantit que seules les personnes disposant de la clé privée peuvent autoriser des transferts depuis leur portefeuille.

Avantages et limitations

- **Avantages :**
    - Aucune nécessité de partager une clé secrète de manière physique ou préalable.
    - Permet des fonctions supplémentaires comme les signatures numériques et l'authentification.
- **Limitations :**
    - Plus lent que le chiffrement symétrique.

- Nécessite une infrastructure robuste pour gérer les clés publiques (certificats, revocation, etc.).

Mécanisme de création de la clé symétrique dans SSL/TLS

Le protocole SSL/TLS est essentiel pour sécuriser les communications sur Internet, permettant aux utilisateurs et aux serveurs d'échanger des informations en toute sécurité. L'un des aspects cruciaux de ce protocole est la création d'une clé symétrique temporaire, nommée clé de session, qui est utilisée pour chiffrer les données échangées pendant la session. Le processus de création de cette clé symétrique peut être décomposé en plusieurs étapes détaillées :

1. Négociation initiale

Lorsque le client (par exemple, un navigateur web) souhaite établir une connexion sécurisée avec un serveur, il initie une phase de négociation appelée "Handshake" (poignée de main). À ce stade, le client envoie une requête de connexion au serveur. En réponse, le serveur fournit son certificat numérique, qui contient sa clé publique. Ce certificat est signé par une autorité de certification (CA) reconnue, ce qui garantit l'authenticité du serveur.

Objectif : S'assurer que le client communique avec le bon serveur et non un imposteur.

2. Génération de la clé de session

Après avoir vérifié le certificat du serveur et établi une connexion, le client génère une clé symétrique aléatoire, souvent de 128 ou 256 bits. Cette clé de session est temporaire et sera utilisée exclusivement pour chiffrer les données durant cette session.

Importance de l'aléatoire : La sécurité de cette clé dépend de son caractère aléatoire, évitant ainsi que des attaquants ne puissent prédire ou déduire la clé en observant les communications précédentes.

3. Chiffrement de la clé de session

Une fois la clé de session générée, le client utilise la clé publique du serveur pour chiffrer cette clé de session. Il s'agit d'une étape cruciale, car elle garantit que seule la personne possédant la clé privée correspondante (c'est-à-dire le serveur) pourra déchiffrer la clé symétrique.

Principe de sécurité : Le chiffrement de la clé de session avec la clé publique du serveur utilise des algorithmes asymétriques, ce qui rend pratiquement impossible pour un attaquant de déchiffrer la clé de session sans posséder la clé privée.

4. Transmission au serveur

Après avoir chiffré la clé de session, le client envoie cette clé symétrique chiffrée au serveur dans le cadre du message de "Handshake". Cela peut impliquer d'autres informations de contrôle nécessaires à l'établissement de la connexion sécurisée, mais l'aspect crucial est la transmission sécurisée de la clé de session.

Sécurisation des données : Même si un attaquant intercepte ce message, sans la clé privée du serveur, il ne pourra pas accéder à la clé de session, garantissant ainsi la confidentialité de l'échange.

5. Déchiffrement par le serveur

Dès que le serveur reçoit la clé symétrique chiffrée, il utilise sa clé privée pour déchiffrer celle-ci. Une fois le déchiffrement effectué, les deux parties (client et serveur) disposent alors de la même clé de session, permettant des communications sécurisées.

Alignement des clés : À ce stade, le client et le serveur utilisent la clé de session pour chiffrer et déchiffrer tous les messages échangés durant cette session. Cela garantit que la connexion est rapidement sécurisée grâce au chiffrement symétrique, qui est beaucoup moins exigeant en termes de ressources que le chiffrement asymétrique.

Qu'est-ce qu'un KMS (Key Management Service) ?

Un KMS, ou **Key Management Service**, est un service de gestion des clés qui permet de créer, gérer, stocker, et utiliser des clés cryptographiques de manière sécurisée. Ces services sont essentiels dans le domaine de la cybersécurité, car ils facilitent la gestion de la cryptographie et la protection des données sensibles. Les KMS peuvent être fournis sous une forme autonomisée, intégrée à des solutions de sécurité de données, ou encore comme partie d'un environnement cloud.

En quoi un KMS est-il utile ?

1. **Gestion centralisée des clés** : Un KMS propose une plateforme centralisée pour gérer toutes les clés cryptographiques d’une organisation. Cela comprend les clés utilisées pour le chiffrement des données, les signatures numériques, et plus encore. Une gestion centralisée simplifie les opérations et réduit le risque d'erreurs humaines.

2. **Sécurité renforcée** : Le KMS offre des mécanismes de sécurité avancés pour protéger les clés. Cela peut comprendre le chiffrement au repos, le contrôle d’accès basé sur les rôles (RBAC), et des audits réguliers. Ainsi, seul le personnel autorisé peut accéder à certaines clés ou opérations, ce qui contribue à la sécurité globale des systèmes.

3. **Conformité aux réglementations** : De nombreuses organisations sont soumises à des exigences légales et réglementaires concernant la protection des données, comme le GDPR

en Europe ou la HIPAA aux États-Unis. Un KMS facilite la conformité en fournissant des outils pour la gestion des clés, incluant la traçabilité des accès et des usages, ce qui est essentiel lors de la réponse à des audits de conformité.

4. **Facilitation du chiffrement des données** : Avec un KMS, les développeurs et les administrateurs peuvent facilement intégrer des fonctionnalités de chiffrement et de déchiffrement dans leurs applications, sans avoir à gérer la complexité de la cryptographie sous-jacente. Cela permet d'implémenter des pratiques de sécurité robustes avec une efficacité accrue.

5. **Scalabilité et flexibilité** : Les KMS sont généralement conçus pour être évolutifs. Que ce soit pour une petite entreprise ou une grande organisation, ils permettent d'élargir facilement les capacités de gestion des clés en fonction des besoins. Dans le cas des solutions basées sur le cloud, les utilisateurs peuvent également ajuster facilement les ressources pour s'adapter à leur charge de travail.

6. **Automatisation** : La plupart des KMS modernes supportent l'automatisation des tâches de gestion des clés. Cela inclut la rotation automatique des clés, l'expiration et le renouvellement des clés, ce qui réduit la charge opérationnelle et améliore la sécurité en minimisant la durée d'exposition des clés.

7. **Intégration avec d'autres services** : Les KMS s'intègrent facilement avec d'autres solutions de sécurité et outils de l'écosystème informatique d'une organisation, tels que des bases de données sécurisées, des systèmes de sauvegarde, ou des services d'infrastructure en tant que service (IaaS). Cette intégration renforce la sécurité des données tout en simplifiant la gestion globale.

Quand et pourquoi utiliser un KMS ?

Un KMS est particulièrement bénéfique dans plusieurs situations :

- **Gestion de données sensibles** : Toute organisation qui traite des données sensibles, telles que des informations personnelles, des données financières ou des informations commerciales stratégiques, devrait envisager d'utiliser un KMS pour sécuriser ces informations.

- **Déploiement sur le cloud** : Lorsque des ressources et applications sont basées sur le cloud, un KMS peut simplifier la gestion des clés de chiffrement utilisées pour protéger les données à chaque niveau de l'infrastructure.

- **Conformité réglementaire** : Les entreprises qui doivent se conformer à des normes de sécurité spécifiques ou des réglementations de protection des données trouveront qu'un KMS peut les aider à respecter les exigences en matière de cryptage et de contrôle d'accès.

- **Environnements multi-applications** : Dans des environnements complexes avec plusieurs applications et systèmes, un KMS est crucial pour maintenir la cohérence de la gestion des clés, garantissant que les bonnes clés sont utilisées de manière appropriée dans chaque application.

- **Protection des données en transit** : Un KMS est essentiel pour les organisations qui transmettent régulièrement des données sensibles sur des réseaux non sécurisés, car il permet de s'assurer que les données sont correctement chiffrées avant la transmission.