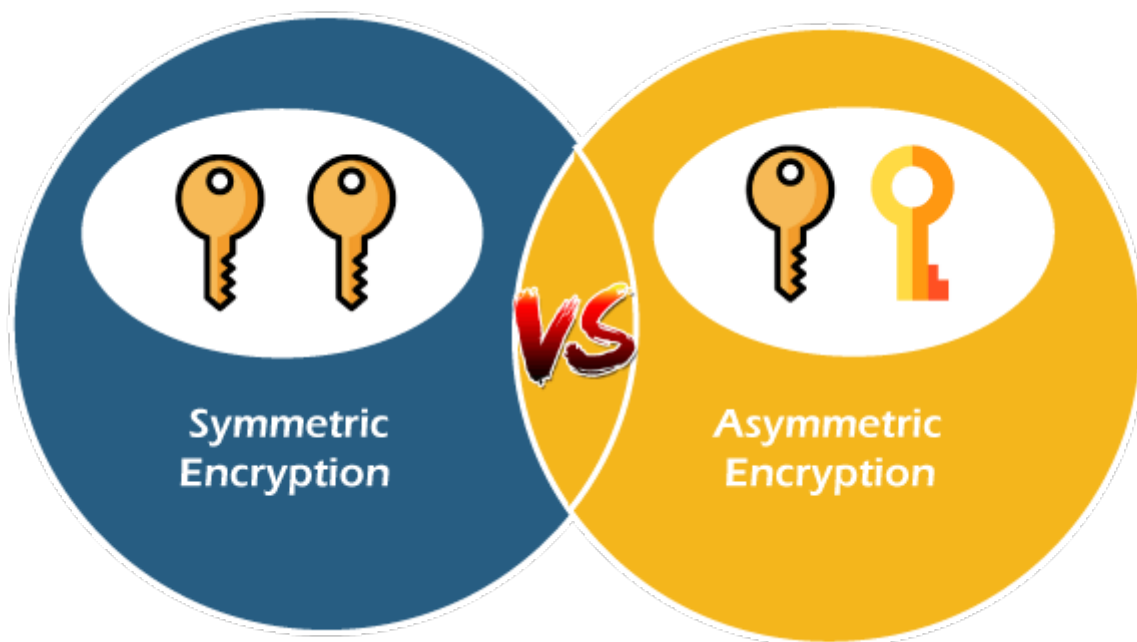


[Fondamentaux] Chiffrement symétrique / asymétrique

Introduction

Cette page va décrire les fonctionnements des deux grands types de chiffrement que sont chiffrement **symétrique** et **asymétrique**.



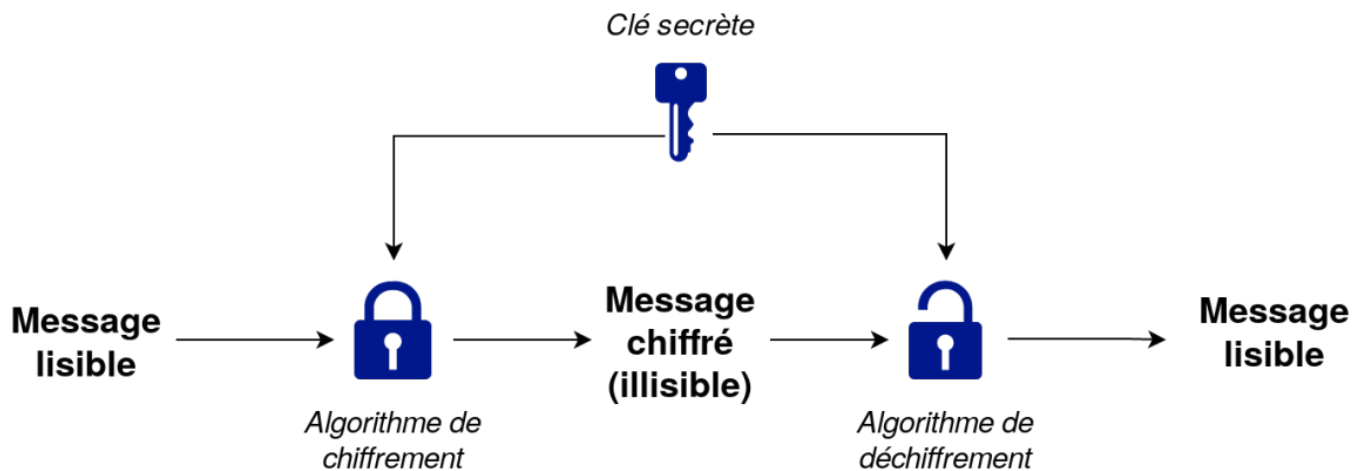
Chiffrement symétrique

Il est le type de chiffrement le **moins sécurisé** mais est encore utilisé notamment pour sa **consommation de ressource qui est moindre** que celle du chiffrement asymétrique.

Le fonctionnement est assez simple : la donnée d'entrée va être chiffrée avec une **clé** par un **algorithme de chiffrement** pour obtenir une donnée incompréhensible en sortie qui pourra transiter sans risque de **confidentialité**.

Ensuite, le récepteur va récupérer la donnée chiffrée qu'il va pouvoir décoder avec la **même clé** qui a servi à chiffrer cette donnée et avec le même algorithme de chiffrement.

Exemple : Le chiffrement **César** qui prend une phrase en entrée et qui va décaler chaque lettre d'un certains nombre.



Chiffrement asymétrique

Réputé pour son **niveau de sécurité plus robuste**, il est utilisé dans la plupart des protocoles et applications sécurisées.

Il est cependant plus lent et gourmand en ressource.

Voici son fonctionnement :

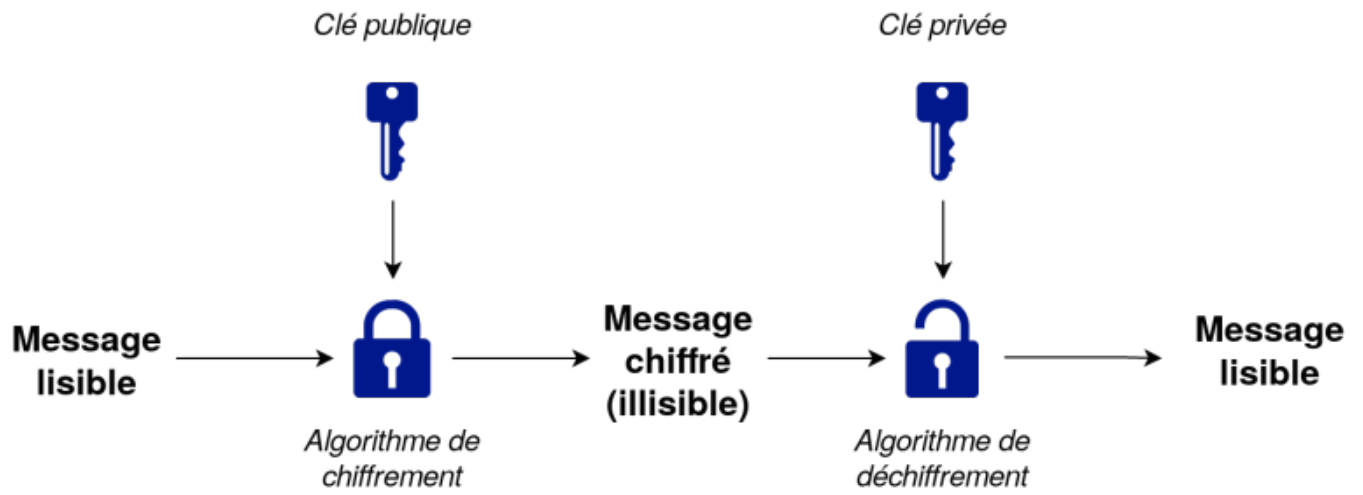
Une paire de clé va être générée avant l'échange de donnée totalisant :

- Une **clé privé** (présente sur le serveur uniquement).
- Une **clé publique** (qui pourra être partagée aux hôtes sans risque).

L'hôte va pouvoir envoyer une donnée de manière confidentielle en chiffrant la donnée à l'aide sa clé publique et de l'algorithme de chiffrement.

Cette donnée chiffrée ne pourra être décodée qu'à l'aide de la clé privé présente sur le serveur et du même algorithme de chiffrement.

Ainsi, pour déchiffrer les échanges dans les deux sens il faudra se munir des deux clés, de l'algorithme de chiffrement et du message chiffrée, ce qui rend la tâche complexe à un pirate pour récupérer la donnée brute initiale.



Revision #1

Created 28 September 2023 19:34:42 by Elieroc

Updated 28 September 2023 20:00:07 by Elieroc