I/ Introduction

La cryptographie est essentielle à la sécurité des systèmes d'information. Sans elle, un attaquant peut écouter vos communications électroniques, par exemple en interceptant des requêtes HTTP. Il peut aussi lire les fichiers du disque dur de votre ordinateur sans avoir votre mot de passe. De même, il pourrait retirer de l'argent avec votre carte de crédit ou encore ouvrir votre voiture et même la démarrer sans avoir la clé.

II/ Définitions

Le chiffrement

Le chiffrement est la transformation d'une information en clair en une information chiffrée, incompréhensible, mais que l'on peut déchiffrer avec une clé pour obtenir l'information en clair originale.

Un système de chiffrement (ou *crypto-système,* ou encore *chiffre*) est composé d'algorithmes de chiffrement et déchiffrement et d'une clé de chiffrement.

Un message en clair

Un message en clair (ou *texte clair*) est une information non protégée et compréhensible par tout le monde.

Un texte chiffré

Un texte chiffré est une information incompréhensible pour qui ne possède pas la clé de déchiffrement, mais qu'on peut déchiffrer, retransformer en texte clair, si on possède la clé.

Un texte chiffré contient donc toutes les informations contenues dans le texte clair pour celui qui possède la clé, mais aucune de ces informations pour celui qui ne la possède pas. C'est ce que l'on appelle la confidentialité d'une information chiffrée.

Un algorithme de chiffrement

Un algorithme de chiffrement est une fonction qui prend en entrée le texte clair et la clé de chiffrement, transforme le texte par des opérations, et fournit en sortie un texte chiffré.

L'algorithme de déchiffrement est la fonction inverse, qui prend en entrée le texte chiffré et la clé de déchiffrement, transforme ce texte par des opérations, et fournit en sortie le texte clair d'origine.

Une clé de chiffrement

La clé de chiffrement (ou *crypto-variable*) est l'information qui permet de transformer un texte clair en texte chiffré en utilisant un algorithme de chiffrement. De même, la clé de déchiffrement est l'information qui permet de transformer un texte chiffré en son texte clair d'origine. L'espace de clé est l'ensemble des valeurs possibles de la clé, c'est une notion importante pour la sécurité d'un algorithme.

Si la clé de chiffrement et la clé de déchiffrement sont identiques, on parle de clé secrète et de chiffrement symétrique. C'est ce type de chiffrement que nous allons étudier dans cette 1e partie du cours.

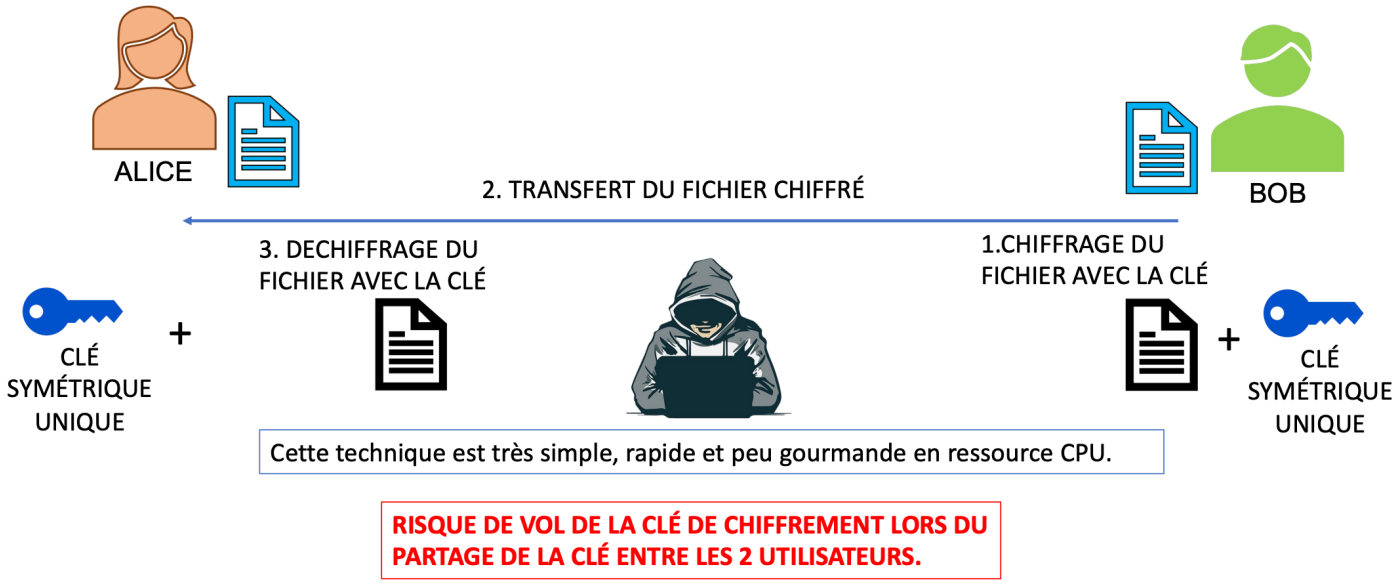
III/ Type de chiffrement

Un système de chiffrement est dit :

- à chiffrement symétrique quand il utilise la même clé pour chiffrer et déchiffrer ;
- à chiffrement asymétrique quand il utilise des clés différentes : une paire composée d'une *clé publique*, servant au chiffrement, et d'une *clé privée*, servant à déchiffrer.

IV/ Chiffrement symétrique

Le chiffrement symétrique permet à la fois de chiffrer et de déchiffrer des messages à l'aide d'un même mot clé.



Cette technique est très simple, rapide et peu gourmande en ressource CPU.

RISQUE DE VOL DE LA CLÉ DE CHIFFREMENT LORS DU PARTAGE DE LA CLÉ ENTRE LES 2 UTILISATEURS.

V/ Chiffrement asymétrique

1) Principe

Chaque interlocuteur possède une paire de clés composée d'une clé publique (Public Key) et d'une clé privée (Private Key). Comme pour des clés physiques, ces clés sont liées comme dans un trousseau. Dans ce crypto-système, les deux clés sont étroitement liées à l'aide d'un algorithme mathématique : les données qui sont chiffrées grâce à la clé publique peuvent uniquement être déchiffrées par la clé privée. Pour garantir la protection des données et le fonctionnement sans entrave du chiffrement asymétrique, il est indispensable que la clé privée reste privée et ne soit connue de personne, pas même des autres interlocuteurs.

En pratique, l'expéditeur de données à besoin de la clé publique du destinataire. La clé publique fonctionne à sens unique dans ce procédé : elle peut chiffrer les données, mais pas les déchiffrer, le déchiffrement n'est réalisable que par la clé privée du destinataire. La clé publique ne sert pas uniquement au chiffrement, elle permet également de vérifier une signature numérique et de vérifier les interlocuteurs.

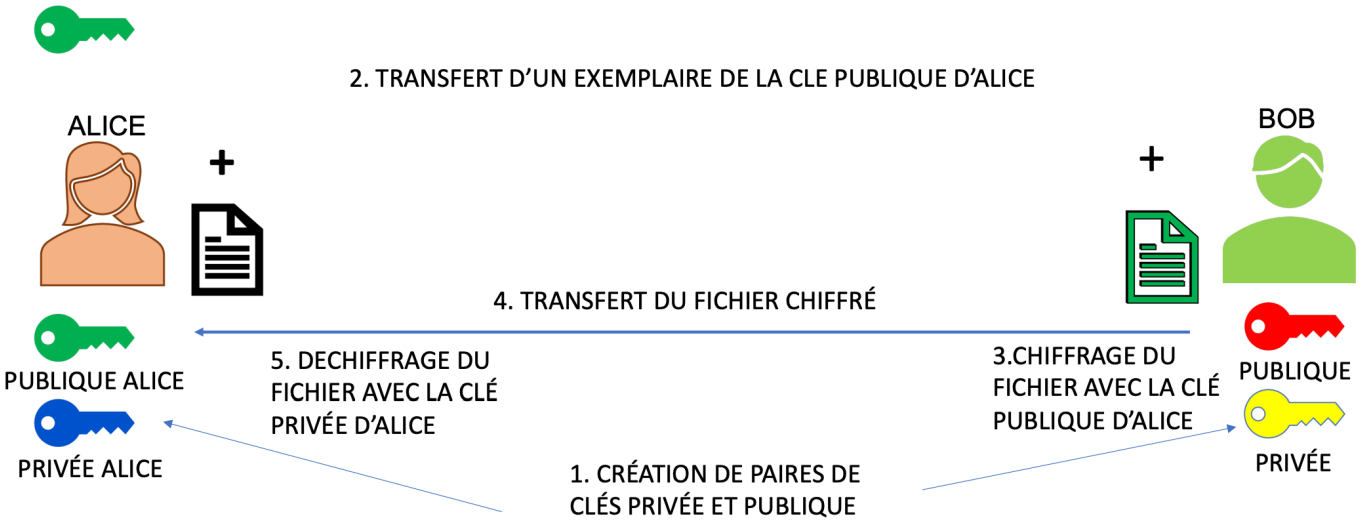
La transmission de clés se fait lors du premier contact. Dans le même temps, la clé privée crée une signature numérique et peut ainsi être identifiée par les autres interlocuteurs. En d'autres termes, le chiffrement asymétrique permet que chaque participant puisse accéder à la clé publique, mais ne puisse déchiffrer les messages qu'avec la clé privée. Cela permet un échange de donnée hautement sécurisé.

2) Fonctionnement

Pour débuter le chiffrement asymétrique, le destinataire crée sa paire de clés. Il conserve la clé privée et permet à son ou ses interlocuteurs d'accéder à sa clé publique. Cela peut se faire par un simple transport, par une autorité de certification ou par des « Key Server » (c'est-à-dire des serveurs de clés) sur lesquels la clé peut être stockée. L'expéditeur utilise cette clé publique pour encoder son message et peut l'envoyer au destinataire sous forme de « texte chiffré ».

À ce stade, le chiffrement du message n'est plus déchiffrable que par la clé privée du destinataire. C'est pour cette raison que le choix du canal de communication est en principe libre : si le message chiffré est intercepté, la personne qui récupère le message ne pourra pas accéder à son contenu.

C'est sur ce fonctionnement à sens unique que repose le système de chiffrement asymétrique. Lorsqu'il connait la clé publique, un pirate ne peut pas en déduire d'information sur la clé privée. Pour cela, les clés publiques fonctionnent selon des facteurs premiers clairement définis qui sont multipliés pour obtenir un résultat unique.


2. TRANSFERT D'UN EXEMPLAIRE DE LA CLE PUBLIQUE D'ALICE
ALICE
BOB
+
+
4. TRANSFERT DU FICHIER CHIFFRÉ
PUBLIQUE ALICE
PRIVÉE ALICE
5. DECHIFFRAGE DU FICHIER AVEC LA CLÉ PRIVÉE D'ALICE
3.CHIFFRAGE DU FICHIER AVEC LA CLÉ PUBLIQUE D'ALICE
PUBLIQUE
PRIVÉE
1. CRÉATION DE PAIRES DE CLÉS PRIVÉE ET PUBLIQUE