Chapitre 3
Cryptographie

1. Introduction

Les techniques cryptographiques font partie des éléments de base du fonctionnement d'une PKI (*Public Key Infrastructure* ou infrastructure de clé publique). Ce sont ces technologies qui seront concrètement utilisées pour fournir :

– La confidentialité, qui correspond au chiffrement des données de façon à ce qu'elles soient illisibles.
– L'authentification de l'utilisateur ou de l'ordinateur.
– L'intégrité des données qui assure que les données resteront non modifiées durant leur transit.

L'objectif de ce chapitre est de fournir les bases essentielles qui vous permettront de comprendre clairement le rôle de la cryptographie dans une infrastructure de PKI, et particulièrement son lien avec l'autorité de certification et les services/applicatifs utilisant des certificats.

Les ateliers de ce chapitre de mise en place du système EFS (*Encrypting File System*) dans un environnement de groupe de travail (Workgroup), illustreront les techniques de chiffrement.

2. Chiffrement des données (confidentialité)

Le chiffrement des données repose sur l'utilisation d'algorithmes mathématiques et des certificats. Deux types de chiffrement peuvent être utilisés, le chiffrement symétrique et le chiffrement asymétrique.

Remarque

Certaines documentations utilisent également le terme de cryptage symétrique ou cryptage asymétrique. Afin de ne pas prêter à confusion, nous utilisons uniquement dans ce livre le terme équivalent de chiffrement (cipher en anglais).

2.1 Chiffrement symétrique

Le chiffrement symétrique utilise des algorithmes mathématiques (tels que Des, 3Des ou Aes…) pour chiffrer les données.

Étant donné que ces algorithmes mathématiques sont publiquement connus, un attaquant pourrait, en renversant l'algorithme, retrouver les données en clair. C'est pour cela qu'un élément aléatoire doit être introduit dans le calcul mathématique, une valeur, généralement codée sur 128 ou 256 bits, qui permet de rendre le résultat aléatoire et donc très difficilement réversible. Pour retrouver le texte en clair il faudrait essayer l'algorithme mathématique avec toutes les combinaisons possibles de clés aléatoires. Pour une clé codée sur 256 bits qui représente la norme actuelle, les temps de calcul seraient trop importants et humainement impraticables.

Cette clé, tirée aléatoirement avant chaque chiffrement, est appelée clé symétrique. Le terme symétrique vient du fait que c'est la même clé qui, associée à l'algorithme mathématique, permet aussi bien le chiffrement que le déchiffrement des données.

Prenons un exemple…

Nous souhaitons envoyer un fichier chiffré à l'utilisateur Bob (un mail ou tout autre ensemble de données…).

Imaginons un algorithme mathématique simple qui pour chiffrer un texte décalerait les lettres de trois positions dans l'ordre alphabétique. On décale alors la lettre B de trois positions selon l'ordre alphabétique pour obtenir la lettre E, puis on décale alors la lettre suivante, o, de trois positions selon l'ordre alphabétique pour obtenir la lettre r, puis on décale à nouveau la lettre suivante n de trois positions selon l'ordre alphabétique, pour obtenir la lettre q et ainsi de suite…

Le mot Bonjour après chiffrement devient alors le mot Erqmrxu.

Dans notre exemple, l'algorithme mathématique est un décalage de lettre dans l'ordre alphabétique et la clé symétrique aléatoire qui fait varier le résultat est la valeur 3. Lors d'une prochaine utilisation, on pourrait choisir une clé aléatoire symétrique différente, 8 par exemple, pour décaler d'un nombre de positions différent dans l'ordre alphabétique.

Nous pouvons ensuite envoyer le texte chiffré à Bob avec la clé de chiffrement symétrique. Bob utilisera cette même clé (3), pour décaler en sens inverse chaque lettre de trois positions dans l'ordre alphabétique. Il pourra ainsi déchiffrer le texte.

L'algorithme de chiffrement décale les lettres dans l'ordre alphabétique d'un nombre de positions fixé par la clé de chiffrement symétrique (ici 3).

Il ne s'agit bien sûr que d'un exemple pédagogique, dans la réalité les algorithmes de chiffrement (Des, 3DES et AES) sont bien plus robustes et complexes.

2.2 Chiffrement asymétrique

Dans le chiffrement asymétrique, deux clés sont utilisées (et non plus une seule comme dans le chiffrement symétrique) : la clé publique et la clé privée.

Où sont stockées ces clés ?

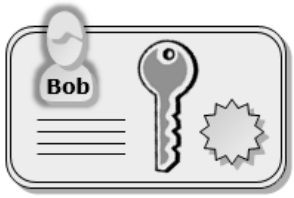
La clé publique est liée au certificat, elle est incluse dans le certificat. En donnant mon certificat, je donne aussi ma clé publique. La clé privée, elle, est stockée à l'extérieur du certificat, dans un emplacement protégé de l'ordinateur.

La taille standard de clés privées/publiques est actuellement de 1024, 2048 ou 4096 bits.

Qu'est-ce qu'un certificat ?

Un certificat est un fichier binaire qui contient (entre autres) :

– La clé publique !
– Des informations en clair sur le propriétaire des clés, leur durée de vie, les utilisations possibles…



Clé Publique de Bob

Le point capital à comprendre ici est que, ces deux clés, publique et privée, sont liées par un rapport mathématique de 1 à 1. Ce qui veut dire en clair que ce qui est chiffré avec l'une des deux clés ne peut être déchiffré que par l'autre clé correspondante. Nous n'allons pas démontrer ce point, il nous faudrait rentrer dans des mathématiques pures (les deux clés sont, pour vulgariser à l'extrême, le résultat de la factorisation de deux nombres premiers). Nous n'avons heureusement aucun besoin de démontrer ce lien mathématique de 1 à 1. C'est un fait, admettons le comme tel.

Mathématiquement, une clé publique ne correspond qu'à une (et une seule) clé privée, et inversement.

Avec laquelle des deux clés va-t-on chiffrer ?

Quelqu'un va souhaiter chiffrer un document pour vous l'envoyer. Il doit utiliser l'une de vos deux clés. Par convention il utilisera la clé dite publique. Comme son nom l'indique, elle peut être fournie à tout service/applicatif extérieur en charge du chiffrement.

Avec quelle clé va-t-on déchiffrer ?

Vous utiliserez votre clé dite privée. Comme son nom l'indique, vous conserverez cette clé de façon privée et vous serez la seule personne à l'utiliser pour déchiffrer le document.

■Remarque

Comme les clés privées/publiques sont liées par un rapport mathématique d'une à une, seule votre clé privée (correspondant à votre clé publique) pourra déchiffrer les données chiffrées !

Prenons un exemple…

Nous voulons envoyer des données chiffrées à Bob. Nous allons utiliser sa clé publique (celle de Bob) pour chiffrer les données. Une fois les données reçues par Bob, lui seul pourra déchiffrer les données avec sa clé privée (à cause du lien mathématique d'un à un entre les clés privée et publique).

On utilise la clé publique du destinataire pour chiffrer, le destinataire utilise sa clé privée pour déchiffrer.

2.3 Comparatif chiffrement symétrique et asymétrique

Nous avons vu qu'il existait deux types de chiffrement (symétrique et asymétrique). Quel est le plus couramment utilisé dans la pratique cryptographique ?

Effectuons une comparaison entre les deux types de chiffrement…

– Le chiffrement symétrique : il n'utilise qu'une seule clé pour chiffrer et déchiffrer. La clé étant de petite taille (256 bits par exemple), il est donc beaucoup plus rapide (100 fois ou plus) que le chiffrement asymétrique qui utilise deux clés de taille plus conséquente (2 048 bits par exemple).

L'inconvénient majeur du chiffrement symétrique est que les deux parties doivent déjà disposer d'un moyen sécurisé pour échanger la clé symétrique utilisée pour le chiffrement. De plus, avec quelques siècles, et en testant toutes les combinaisons clés symétriques, il serait possible … théoriquement … de déchiffrer les données.