Sécurité des échanges sur les réseaux :

Définition : un réseau de communication peut être défini comme l'ensemble des ressources matériels et logiciels liées à la transmission et l'échange d'information entre différentes entités.
Suivant leur organisation, ou architecture, les distances, les vitesses de transmission et la nature des informations, transmises, les réseaux font l'objet d'un certain nombre de spécifications des normes.

Enjeux : La garantie de l'intégrité et de l'inviolabilité des données conservées et échangées est essentielle au développement d'une économie internationalisée fondée sur les technologies de l'information.
Nous devons sécurisée nos données pour éviter toute perte dans une entreprise.
(80% des entreprises ayant perdu leurs données informatiques font faillite dans les 12 mois)

Pour protéger les particuliers ou les entreprises le système d'information « sécurisé » se doit d'utiliser trois principaux critères :

- Confidentialité
  Lors d'un échange de message, par celui-là ne doit être lue que par son ou ses destinataires.
- Intégrité
  Le message reçu est bien celui qui a été envoyé. Il n'a en aucune manière pu être modifié en cours de transfert.
- Authenticité
  Les interlocuteurs, émetteur et récepteur(s) doivent pouvoir être identifiés sans qu'il puisse exister le moindre doute sur leur identité.

- **Risques liés aux réseaux** :

  Interception de messages
  - Prise de connaissance des mots de passe
  - Vol d'information
  - Perte d'intégrité du système et du réseau
- Intrusion des systèmes
  - Vol ou compromission des informations
  - Destruction des informations
  - Virus
  - Détournement de biens
- Perte d'accessibilité au système ou au réseau
- Faux clients, marchands escrocs

Comment sécuriser nos échanges sur les réseaux ?

Il existe des solutions technologiques pour garantir des communications avec un niveau de sécurité acceptable : le chiffrement des données par clés asymétriques, les certificats d'authenticité et les signatures…

Recommandations : Dans une entreprise

- Conserver la sauvegarde dans un bâtiment séparé
- Contrôler régulièrement que les données sauvegardées sont exploitables
- Mesurer la durée d'interruption d'activité que l'entreprise peut supporter et estimer cette perte d'activité journalière
- Définir un plan de continuité
- Procéder à une sauvegarde journalière

Objectifs :

Pour sécuriser des échanges sur les réseaux on doit mettre en place un système de confidentialité d'Authentification sur les serveurs ou ordinateurs clients, un contrôle d'intégrité ainsi qu'un moyen efficace pour identifier l'auteur d'une transaction soit « non répudiation ».

L'authentification est une phase qui permet à l'utilisateur d'apporter la preuve de son identité. Elle intervient après la phase dite d'identification. Elle permet de répondre à la question : "Êtes-vous réellement cette personne ?". L'utilisateur utilise un authentifiant ou "code secret" que lui seul connait.

Le code secret d'un utilisateur est **une information personnelle qui ne doit en aucun cas être divulgués**. Il est aussi communément nommé "mot de passe".

Le mot de passet ne permet pas de donner un droit d'accès, il **permet uniquement d'assurer l'imputabilité** dans l'usage de ces droits d'accès.

La **confidentialité** consiste à rendre l'information inintelligible à d'autres personnes que les seuls acteurs de la transaction

La **non-répudiation** de l'information est la garantie qu'aucun des correspondants ne pourra nier la transaction.

Contrôle d'**intégrité** des données consiste à déterminer si les données n'ont pas été altérées durant la communication (de manière fortuite ou intentionnelle).

Moyen efficace de protéger et sécurisée des échanges sur les réseaux.

Pour sécuriser des échanges de données telle que des mots de passes, données sensible, messagerie sécurisée, site web,

Nous pouvons utiliser des logiciels permettant de chiffrer ces données personnelles, grâce un système de chiffrement et de déchiffrement qui utilise des algorithmes crée à partir de fonction mathématique.

Le **chiffrement** ou **cryptage** est un procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de (dé)chiffrement.

Ils existent plusieurs types de cryptages : Le chiffrement chiffrement symétrique quand il utilise la même clé pour chiffrer et déchiffrer.

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.

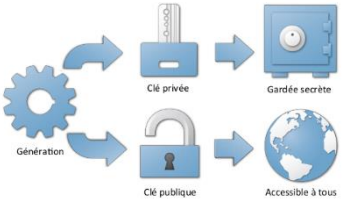
Les méthodes les plus connues sont le DES, le Triple DES et l'AES pour le chiffrement symétrique, et le RSA pour le chiffrement asymétrique, aussi appelé chiffrement à clé publique.

Exemple de logiciel permettant le chiffrement de donnée : AxCrypt permet de crypter des fichiers stockés sur son Windows ou bien WinScp un client SFTP permettant de stocker, télécharger et partager des fichiers.

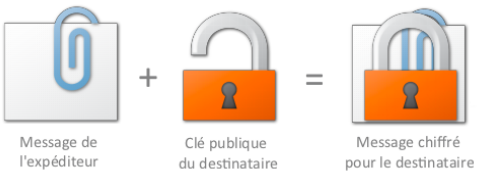
Chiffrement d'un message.

Déchiffrement d'un message

Chiffrement Asymétrique : Principe en image :



Chiffrement Symétrique : Principe en image



Asymétrique vs Symétrique :

Le chiffrement symétrique utilise une clé unique partagée entre les 2 interlocuteurs. On encode et on décode le message avec la même clé.

Le problème de ce chiffrement est qu'il faut trouver un moyen de transmettre la clé unique entre les 2 interlocuteurs.

Par contre le chiffrement asymétrique est le fait d'avoir 2 clés (que l'on fabrique soi-même) :

- Quand on encode avec la première clé, on peut décoder avec la 2e clé
- Quand on encode avec la 2e clé, on peut décoder avec la 1ère clé

Par convention, on appelle une des 2 clés la clé privée et l'autre la clé publique.

La clé privée n'est jamais transmise à personne

La clé publique est en revanche diffusée publiquement sans problème.

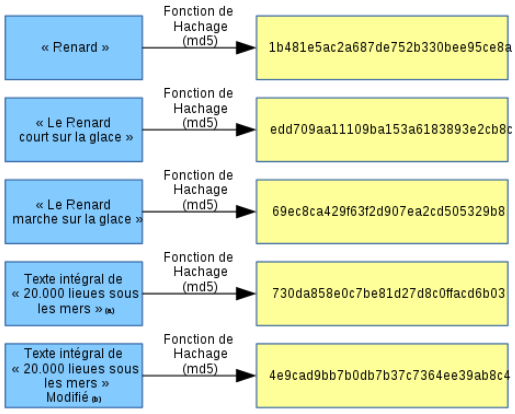
Dans une transmission simple, ce système permet 2 choses essentielles :

- Assurer la confidentialité d'un message transmis : personne ne peut le lire sauf le destinataire
- Signer un message : le destinataire est certain que le message vient bien du bon interlocuteur

Fonction de Hachage :

On nomme **fonction de hachage**, de l'anglais *hash function* (*hash* : pagaille, désordre, recouper et mélanger) par analogie avec la cuisine, une fonction particulière qui, à partir d'une donnée fournie en entrée, calcule une *empreinte* servant à identifier rapidement, bien qu'incomplètement, la donnée initiale. Les fonctions de hachage sont utilisées en informatique et en cryptographie.

Cette fonction va prendre le texte du mot de passe et le « mouliner » pour obtenir une signature (cette signature est aussi appelée « empreinte »). L'ordinateur ne va pas envoyer le mot de passe au serveur, mais une signature du mot de passe. Le serveur ne va enregistrer le mot de passe mais enregistrera cette signature. Lorsque l'utilisateur se connectera, le serveur ne va pas vérifier si le mot de passe est identique, mais il va vérifier que la signature du mot de passe saisi est bien la même que la signature du mot de passe enregistré.



RSA : Le premier système à clé publique solide à avoir été inventé, et le plus utilisé actuellement, est le système RSA. Publié en 1977 par Ron **R**ivest, Adi **S**hamir et Leonard **A**dleman de l'Institut de technologie du Massachusetts (MIT), le RSA est fondé sur la difficulté de factoriser des grands nombres, et la fonction à sens unique utilisée est une fonction "puissance".

RSA, du nom de ces inventeurs, est un algorithme de chiffrement appartenant à la grande famille "Cryptographie asymétrique".

RSA peut être utilisé pour assurer :

- La confidentialité : seul le propriétaire de la clé privée pourra lire le message chiffré avec la clé publique correspondante.
- La non-altération et la non-répudiation : seul le propriétaire de la clé privée peut signer un message (avec la clé privée). Une signature déchiffrée avec la clé publique prouvera donc l'authenticité du message

Mise en œuvre du RSA Exemple :

Alice et Bob

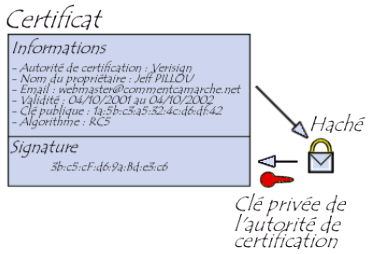
- Bob possède un message confidentiel qu'il souhaite transmettre à Alice.
- Alice construit deux clés :
  - Une clé de chiffrement publique qu'elle transmet à Bob.
  - Une clé de déchiffrement privée qu'elle conserve soigneusement.
- Bob utilise la clé publique pour chiffrer le message, et le transmets à Alice.
- Alice utilise la clé privée pour déchiffrer le message reçu.

- Le sigle **PKI** *(Public key infrastructure)* désigne une infrastructure à clé publique, qui est constituée d'un ensemble de services, éventuellement externalisés, basés sur le concept de certificat numérique. Ce dernier, qui est un document électronique garantissant l'identité d'un individu ou d'une entité technique, est lui-même fondé sur le concept de chiffrement asymétrique. L'infrastructure PKI représente un cadre global pour la gestion de la sécurité, associée à l'ensemble des utilisateurs et des applications d'un réseau, privé ou public.

Ils existent de nombreux certificats électroniques qui permet d'associer une clé publique à une entité (une personne, une machine, ...) afin d'en assurer la validité. Le certificat est en quelque sorte la carte d'identité de la clé publique, délivré par un organisme appelé *autorité de certification* (souvent notée CA pour *Certification Autorithy*).

Exemple : pour le site https://kevin-breant.com le certificat signé est vérifié par COMODO CA Limited en tant que connexion sécurisé et chiffré.

L'autorité de certification est chargée de délivrer les certificats, de leur assigner une date de validité (équivalent à la date limite de péremption des produits alimentaires), ainsi que de révoquer éventuellement des certificats avant cette date en cas de compromission de la clé (ou du propriétaire).



Les certificats sont des petits fichiers divisés en deux parties :

- La partie contenant les informations
- La partie contenant la signature de l'autorité de certification

La structure des certificats est normalisée par le standard **X.509** de l'UIT (plus exactement X.509v3), qui définit les informations contenues dans le certificat :

- La version de X.509 à laquelle le certificat correspond ;
- Le numéro de série du certificat ;
- L'algorithme de chiffrement utilisé pour signer le certificat ;
- Le nom (DN, pour *Distinguished Name*) de l'autorité de certification émettrice ;
- La date de début de validité du certificat ;
- La date de fin de validité du certificat ;
- L'objet de l'utilisation de la clé publique ;
- La clé publique du propriétaire du certificat ;
- La signature de l'émetteur du certificat (*thumbprint*).

L'ensemble de ces informations (informations + clé publique du demandeur) est signé par l'autorité de certification, cela signifie qu'une fonction de hachage crée une empreinte de ces informations, puis ce condensé est chiffré à l'aide de la clé privée de l'autorité de certification; la clé publique ayant été préalablement largement diffusée afin de permettre aux utilisateurs de vérifier la signature avec la clé publique de l'*autorité de certification*.

Signatures de certificats

On distingue différents types de certificats selon le niveau de signature :

- Les **certificats auto-signés** sont des certificats à usage interne.

Signés par un serveur local, ce type de certificat permet de garantir la confidentialité des échanges au sein d'une organisation, par exemple pour le besoin d'un intranet. Il est ainsi possible d'effectuer une authentification des utilisateurs grâce à des certificats auto-signés.

- Les **certificats signés par un organisme de certification** sont

Nécessaires lorsqu'il s'agit d'assurer la sécurité des échanges avec des utilisateurs anonymes, par exemple dans le cas d'un site web sécurisé accessible au grand public. Le certificateur tiers permet d'assurer à l'utilisateur que le certificat appartient bien à l'organisation à laquelle il est déclaré appartenir.

Types d'usages

Les certificats servent principalement dans trois types de contextes :

- Le **certificat client**, stocké sur le poste de travail de l'utilisateur

Ou embarqué dans un conteneur tel qu'une carte à puce, permet d'identifier un utilisateur et de lui associer des droits. Dans la plupart des scénarios il est transmis au serveur lors d'une connexion, qui affecte des droits en fonction de l'accréditation de l'utilisateur. Il s'agit d'une véritable carte d'identité numérique utilisant une paire de clé asymétrique d'une longueur de 512 à 1024 bits.

- Le **certificat serveur** installé sur un serveur web permet d'assurer le lien

Entre le service et le propriétaire du service. Dans le cas d'un site web, il permet de garantir que l'URL et en particulier le domaine de la page web appartiennent bien à telle ou telle entreprise. Par ailleurs il permet de sécuriser les transactions avec les utilisateurs grâce au protocole SSL.

- Le **certificat VPN** est un type de certificat installé dans les équipements

Réseaux, permettant de chiffrer les flux de communication de bout en bout entre deux points (par exemple deux sites d'une entreprise). Dans ce type de scénario, les utilisateurs possèdent un certificat client, les serveurs mettent en œuvre un certificat serveur et les équipements de communication utilisent un certificat particulier (généralement un certificat IPSec.