Haute école d'ingénierie et d'architecture Fribourg
Hochschule für Technik und Architektur Freiburg

Hes·so

Téléinformatique – Ch. 20

Sécurité

Vincent Magnin
vincent.magnin@hefr.ch

Objectifs

- Connaître les critères de sécurité et les facteurs d'authentification.
- Connaître les menaces et types d'attaques les plus courantes et les moyens de protection.
- Connaître la différence entre le codage et le chiffrement.
- Savoir expliquer la notion de chiffrement, clés symétriques, asymétriques, et de signature numérique.
- Savoir expliquer ce qu'est le hachage.
- Connaitre les différents éléments d'une infrastructure informatique qui permettent d'augmenter la sécurité.

Définition

La sécurité des systèmes d'information (SSI) est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, rétablir et garantir la sécurité du système d'information. (Wikipédia)

En anglais, le terme sécurité peut avoir 2 significations :

- Safety : Protection de systèmes informatiques contre les accidents dus à l'environnement, les défauts du système, etc.
- Security : Protection des systèmes informatiques contre les actions malveillantes intentionnelles.

Critères de sécurité (CIA)

En (télé)informatique, on distingue 3 critères de sécurité principaux.

1. La confidentialité garantit que les données transmises ne sont pas dévoilées à une tierce personne.

2. L'intégrité assure que les données n'ont pas été modifiées entre l'émission et la réception.

3. L'authentification :
   - (*personne*) assure que la personne est identifiée et est bien celle qu'elle prétend être.
   - (*message*) assure que le message provient bien de la bonne origine.

Facteurs d'authentification

On distingue plusieurs facteurs d'authentification, dont au moins 2 sont requis pour qualifier une authentification forte.

- Ce que l'authentifié sait : secret partagé, information mémorisée...
- Ce que l'authentifié possède : carte à puce, clé USB, certificat numérique, RFID...
- Ce que l'authentifié est : empreinte digitale, pupille, élément biométrique...
- Ce que l'authentifié sait faire : comportement, démarche, signature manuscrite...

Les systèmes informatiques doivent posséder une authentification forte pour réduire le risque d'intrusion.

Les différentes menaces

- Les utilisateurs : Insouciant ou mal informé, un utilisateur peut créer de graves failles de sécurité (mot de passe faible, brancher un AP sur le réseau, …).
- Une personne malveillante (« pirate ») : Utilise différentes techniques pour entrer sur un réseau et dérober, modifier, détruire des informations; peut être par « fun », espionnage industriel…
- Un programme malveillant : Un logiciel destiné à nuire ou à abuser des ressources du système est installé (par mégarde ou par malveillance) sur la machine, crée des failles de sécurité et donne, par exemple accès à un pirate.
- Un sinistre (vol, incendie, dégât des eaux) : Une mauvaise manipulation ou une malveillance entrainant une perte de matériel et/ou de données.

Conclusion : Besoin de sécurité sur plusieurs niveaux : information aux utilisateurs, sécurité de l'information, du réseau et physique.

Les différentes attaques

- Interceptions de communications
  - Usurpation d'identité
  - Vol de session (session hijacking)
  - Vol, altération des messages
- Intrusions
  - Vol de données
  - Destruction
  - Modification
- Dénis de service (DoS)
  - Variante DDoS
  - Paquet mal formatés (traitement plus long)
  - Flooding / surcharge
- Social engineering
  - Vol d'informations
  - Phishing
- Accès physique
  - Détérioration du matériel
  - Coupure de courant
  - Ecoute du trafic
  - Installation de malware
- « Ennuis »
  - Spam
  - Désinformation

Logiciels malveillants

Les logiciels malveillants sont souvent appelés malware (malicious software). Ils sont classés dans 3 catégories :

- Mécanisme de propagation
- Mécanisme de déclenchement
- Charge utile

Il existe différents types de malwares :

- Virus
- Ver (worm)
- Cheval de Troie (trojan)
- Rançongiel (ransomware)
- …
- Keylogger
- Reverse shell
- Rootkit
- Botnet

Moyens de protection

En sécurité informatique, le risque 0 n'existe pas. Il est nécessaire de protéger les systèmes avec différents moyens, et de constamment mettre à jour les systèmes de sécurité.

Certaines techniques de sécurisation sont les suivantes :

- Antivirus
- Firewall
- IDS / IPS
- VPN
- SSL / TLS
- Formations humaines

Firewall

Un Firewall est un logiciel et/ou un matériel dont le but est de faire respecter la politique de sécurité. Il en existe 3 types :

1. Firewall stateless (sans état) : regarde chaque paquet indépendamment des autres et le compare à une liste de règles préconfigurées.

2. Firewall stateful (avec état) : vérifie la conformité des paquets par rapport à une connexion en cours. S'utilise sur les protocoles dits « à états » comme TCP qui introduisent une notion de connexion.

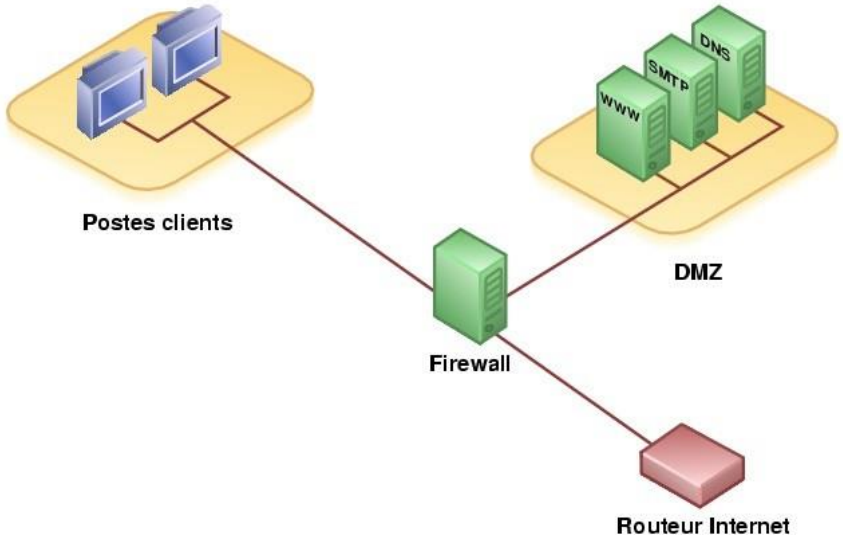
3. Firewall application : inspecte le contenu des paquets.

Firewall (2)

Le firewall contrôle le trafic entre les différentes zones. On distingue les zones de confiance, les zones de confiance nulle, et les DMZ (demilitarized zone).

Les critères de filtrage d'un firewall peuvent être :

- IP source / destination
- Numéro de port source / destination
- Type de protocole
- Contenu du paquet
- …

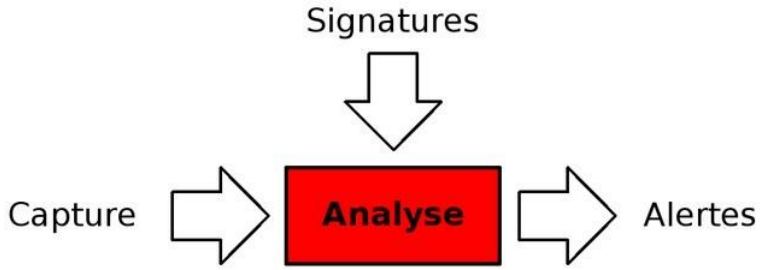


IDS / IPS

Un IDS (Intrusion Detection System) est un mécanisme destiné à détecter des activités anormales ou suspectes sur un réseau ou un hôte. Il permet ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions.

L'IDS possède 3 éléments principaux :

- La capture
- Une bibliothèque de signatures
- Des alertes

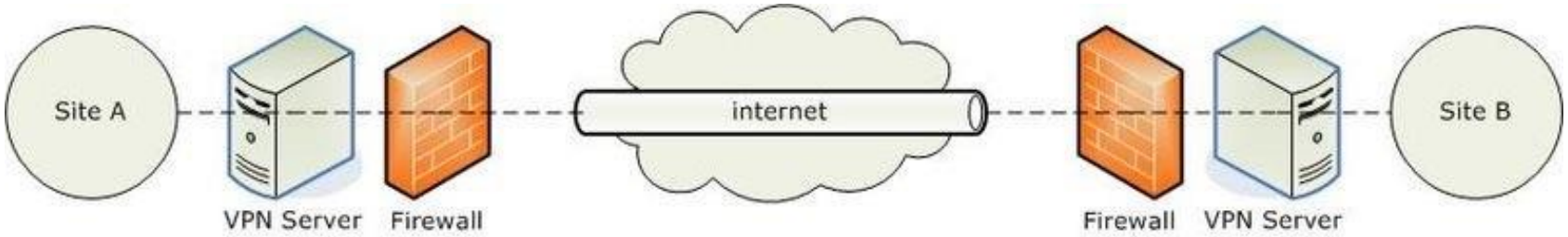


Un IPS (Intrusion Prevention System) est un IDS actif qui peut prendre des mesures, comme bloquer un port spécifique.

VPN

Un VPN (Virtual Private Network) est un tunnel virtuel créé au travers d'un réseau non fiable, dans lequel transite du trafic sécurisé. Il permet de relier plusieurs terminaux ou réseaux locaux ensemble à distance.

Un VPN apporte la confidentialité, l'authentification et l'intégrité des données par le chiffrement offert par le tunnel.

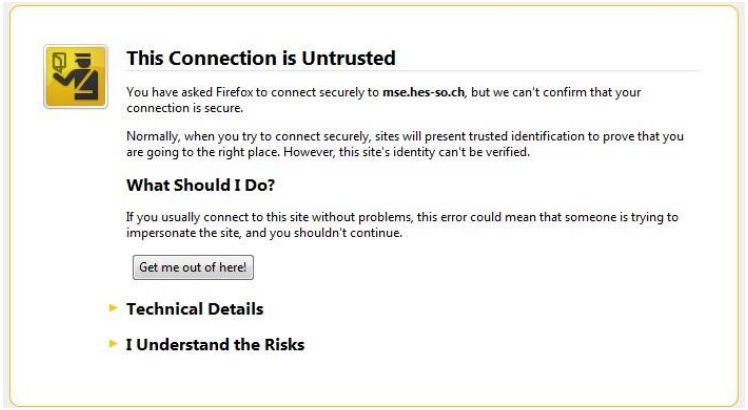


SSL / TLS

Le protocole TLS (Transport Layer Security) permet de sécuriser une communication. HTTPS est une utilisation typique du protocole TLS.

TLS utilise généralement un système de certificats numériques servant à prouver l'origine du serveur. Il créé alors un tunnel virtuel (VPN) entre le client et le serveur pour échanger les données.

C'est notamment ce protocole qui a permis de développer le commerce sur Internet.



Codage de l'information

Le codage, ou l'encodage de l'information est le principe de passer d'une représentation d'une donnée vers une autre. On ne sécurise pas l'information en l'encodant.

Quelques exemples de codage de l'information :

- Base64
- ROT13
- uuencode
- xxencode

Exemple :

- Message original : `Bonjour à tous`
- Encodé en Base64 : `Qm9uam91ciDDoCB0b3Vz`
- Encodé en uuencode : `/0F]N:F]U<B##H"!T;W5S`

Terminologie de la cryptographie

On distingue 2 grands thèmes dans la cryptographie :

La cryptographie est un ensemble de techniques mathématiques et physiques dont les buts sont de résoudre divers problèmes reliés à la sécurité de l'information.

La cryptanalyse est l'activité consistant à mesurer ou à casser la sécurité d'un procédé cryptographique.

La cryptologie est une science récente englobant à la fois la cryptographie et la cryptanalyse.

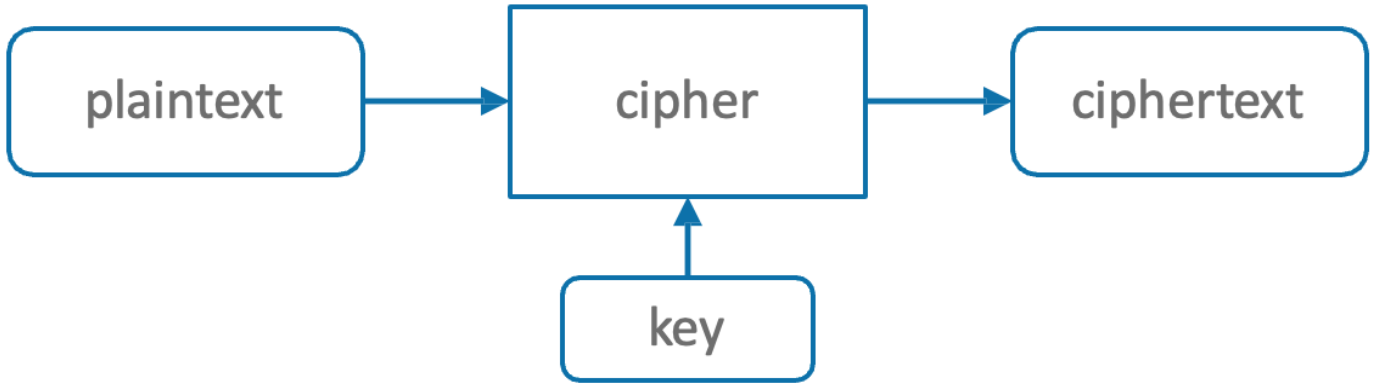
Terminologie de la cryptographie (2)

- Chiffrer (encrypt) : rendre une information confidentielle.
- Clé (key) : secret utilisé pour chiffrer une information.
- Déchiffrer (decrypt) : recouvrer légitimement une information à partir de sa version chiffrée.
- Décrypter : recouvrer une information à partir de sa version chiffrée, mais sans posséder la clef correspondante.
- Texte clair (plaintext) : information non protégée par un procédé cryptographique quelconque.
- Texte chiffré (ciphertext) : information rendue confidentielle au moyen de cryptographie.

Source : Alexandre Duc (HEIG-VD) / Cryptographie / MSE 2017-2018

Chiffrement

Le chiffrement 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).



Chiffrement à clé symétrique

Le chiffrement à clé symétrique est très simple. La même clé sert à chiffrer et déchiffrer l'information. Il est fondamental que seules les personnes concernées possèdent la clé.

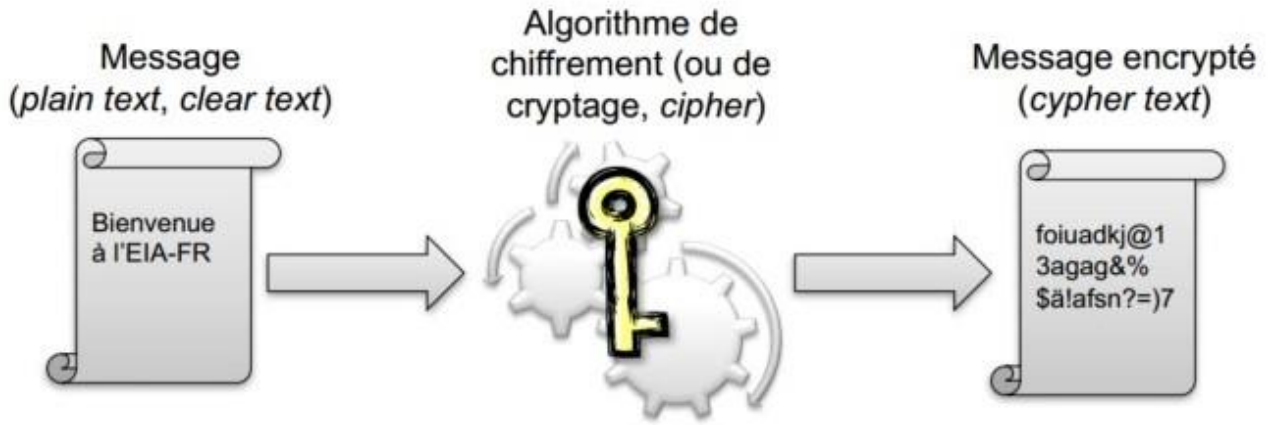
Dans une situation où tous les clients d'un ensemble doivent pouvoir communiquer individuellement de manière sécurisée, le nombre de clé est égal à :

$$N_{Clés} = \frac{C * (C-1)}{2}$$ avec C le nombre de clients.

L'avantage de ce chiffrement est sa grande rapidité. En revanche, il est nécessaire de sécuriser l'échange des clés. De plus, le nombre de clés augmente de manière exponentielle avec le nombre de clients (pour 20 personnes, il faut déjà 190 clés !).

Chiffrement à clé symétrique (2)

Il existe de nombreux algorithmes de chiffrement à clé symétrique. En voici certains : César, Vigenère, RC4, DES, 3DES, IDEA, AES, ChaCha, SalSa20...



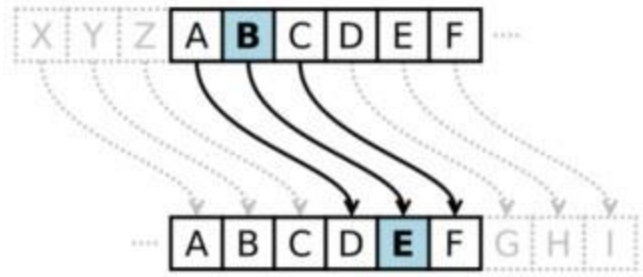
Chiffrement à clé symétrique (3)

L'algorithme de César est la plus ancienne méthode cryptographique connue. Il était utilisé par l'armée romaine pour transmettre des informations de manière chiffrée.

Le principe est simple : on procède à une substitution monoalphabétique par décalage des lettres de l'alphabet d'un nombre N (N étant la clé de chiffrement).

Par exemple, si la clé est égale à 3 :

- Plaintext = `SECRET`
- Ciphretext = `VHFUHW`



Chiffrement à clé symétrique (3)

L'algorithme de Vigenère est une version améliorée de l'algorithme de César. Il procède à une substitution polyalphabétique en utilisant la clé de (dé)chiffrement et en s'aidant de la table de Vigenère.

La clé est juxtaposée au message en clair, et chaque lettre du message en clair est chiffrée en fonction de la lettre de la clé correspondante. Si la clé est moins longue que le message en clair, alors elle est répliquée autant de fois que nécessaire.

Exemple avec la clé `MAISON` et le texte `VIVE LES RESEAUX IP` :

Plaintext: `VIVE LES RESEAUX IP`

Key: `MAIS ONM AISONMA IS`

Ciphertext: `HIDW ZRE RMKSNGX QH`

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Chiffrement à clé symétrique (4)

Il existe différentes attaques qui permettent de casser un algorithme de chiffrement à clé symétrique. Les principales sont les suivantes :

Attaque par brute force : tenter toutes les combinaisons possibles de clé jusqu'à trouver un message cohérent.

Attaque par analyse fréquentielle : rechercher la fréquence d'apparition des lettres pour faire les correspondances entre le texte clair et le texte chiffré.

Attaque spécifique à l'algorithme :

- Side-channel attack
- Related-key attack
- …

Chiffrement à clé asymétrique

Dans un processus de chiffrement à clé asymétrique, chaque personne dispose d'une paire de clés ayant des propriétés mathématiques spécifiques :

- Clé privée : conne uniquement par son propriétaire.
- Clé publique : distribuée ou publiée sur Internet pour tout le monde.

Le chiffrement à clé asymétrique permet de réduire considérablement le nombre de clés nécessaires, mais le processus est presque 1000 fois plus lent que le chiffrement symétrique ! Un exemple très connu d'algorithme à clé asymétrique est RSA.

Chiffrement à clé asymétrique (2)

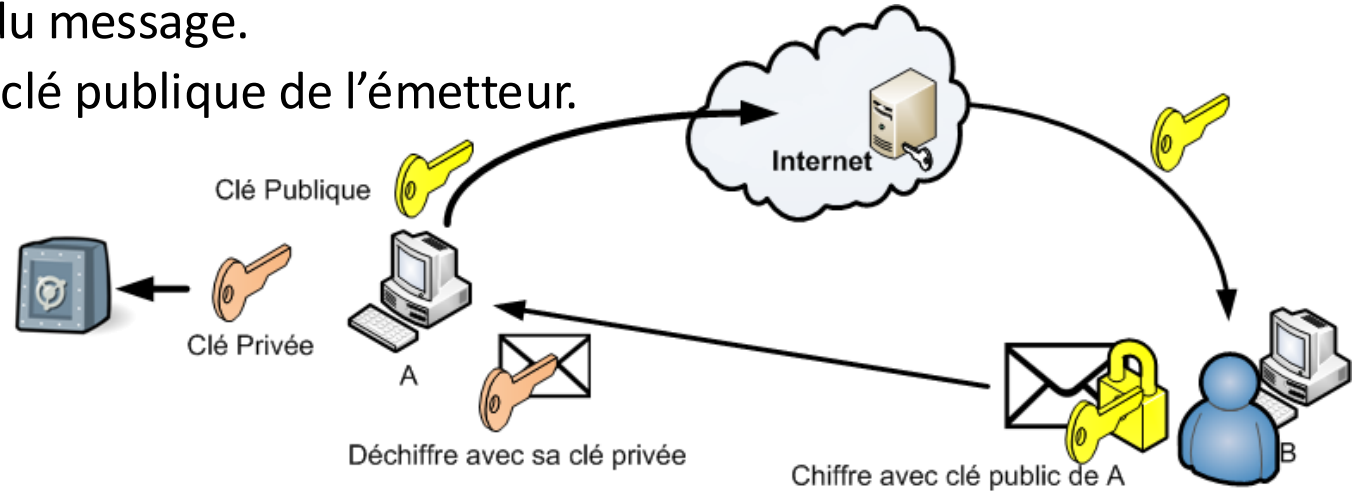
Le processus de chiffrement à clé asymétrique est applicable de 2 manières :

Chiffrer avec la clé publique du destinataire :

- Permet de garantir la confidentialité du message.
- Seul le destinataire peut déchiffrer avec sa clé privée.

Chiffrer avec la clé privée :

- Permet de garantir l'authentification du message.
- Tout le monde peut déchiffrer avec la clé publique de l'émetteur.



Fonction de hachage

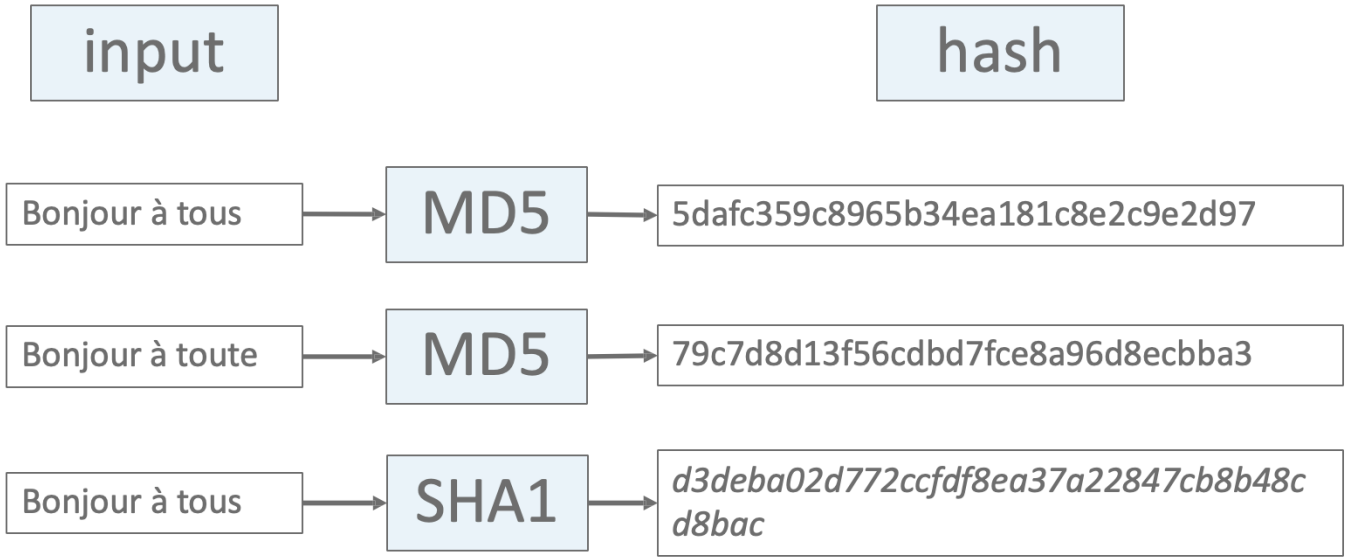
Une fonction de hachage produit une empreinte unique à partir d'une donnée. C'est une opération à sens unique très rapide dont le résultat aura toujours la même taille. L'empreinte, également appelée le hash, peut être utilisé dans le cadre des signatures numériques pour vérifier l'intégrité d'un message.

Quelques exemples d'algorithmes de hachage :

- MD5
- SHA1
- SHA2 (SHA-256, SHA-512)
- SHA3
- …

Fonction de hachage (2)

Dès lors que l'input de la fonction de hachage est modifié, le hash de sorti sera complètement différent.



Les fonctions de hachage peuvent également être sujettes à des attaques, comme du brute force, ou encore des collisions (deux messages générant le même hash).

Ethical Hacking

"An ethical hacker is a computer and networking expert who systematically attempts to penetrate a computer system or network on behalf of its owners for the purpose of finding security vulnerabilities that a malicious hacker could potentially exploit."

http://searchsecurity.techtarget.com/

Références

- Ancien cours « Téléinformatique » (G. Waeber, S. Paccard, Q. Vaucher, N. Wirth).
- Ancien cours « Téléinformatique » (M. Roch-Neirey).