

Chapitre 21 : Cryptographie et infrastructure à clé publique

BENJAMIN
DESROSIERS-BOSSÉ
2023

Chapitre 21 – Sections et objectifs



La cryptographie

Utiliser des outils pour chiffrer et déchiffrer des données.

- Utiliser la cryptographie pour sécuriser les communications.
- Expliquer le rôle de la cryptographie pour garantir l'intégrité et l'authenticité des données.
- Expliquer les méthodes cryptographiques d'amélioration de la confidentialité des données.

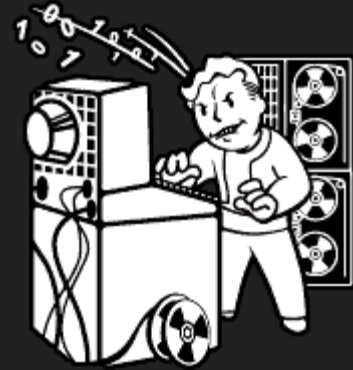


Cryptographie à clé publique

Expliquer comment l'infrastructure à clé publique (PKI) assure la sécurité du réseau.

- Expliquer la cryptographie à clé publique.
- Expliquer comment l'infrastructure à clé publique fonctionne.
- Expliquer comment l'utilisation de la cryptographie a un impact sur les opérations de cybersécurité.

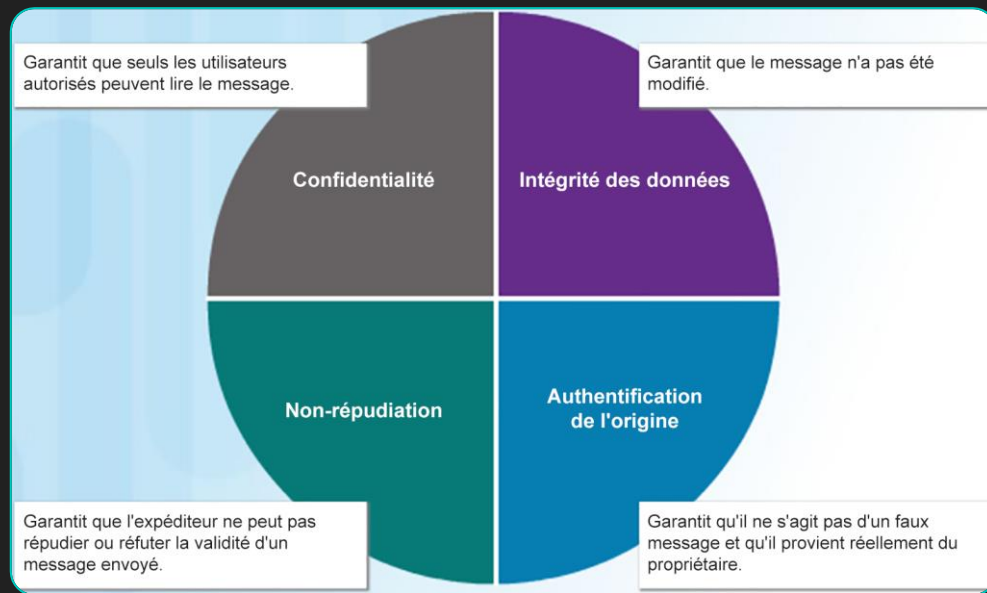
Cryptographie



Qu'est-ce que la cryptographie ?

Sécurisation des communications

- La sécurité de l'information consiste à protéger les appareils de l'infrastructure de réseau et les données qui transitent sur le réseau.
- La cryptographie permet d'atteindre quatre objectifs en matière de sécurité de l'information :
 - **Confidentialité des données** : seuls les utilisateurs autorisés peuvent consulter les données.
 - **Intégrité des données** : les données ne peuvent pas être modifiées par des personnes non autorisées.
 - **Authentification de l'origine** : les données proviennent d'une source prévisible.
 - **Non-répudiation** : l'expéditeur peut prouver de manière irréfutable l'intégrité du message.



Qu'est-ce que la cryptographie ?

Cryptologie

- La cryptologie est la science de la création et du déchiffrement des codes secrets. Il existe deux disciplines :
 - **La cryptographie** : correspond au développement et à l'utilisation des codes utilisés pour communiquer en privé. Concrètement, il s'agit de la pratique et de l'étude des techniques de sécurisation des communications.
 - **Cryptanalyse** : correspond au déchiffrement de ces codes. Concrètement, il s'agit de la pratique et de l'étude de la détermination et de l'exploitation des faiblesses des techniques cryptographiques.

Quel genre de personne est spécialisé en cryptographie?



Cryptographie – Chiffrement

- Vous trouverez ci-dessous les types de chiffres utilisés au fil des ans :
 - Chiffrement par substitution : les chiffres par substitution conservent la fréquence des lettres du message original.
 - Chiffrement par transposition : avec le chiffrement par transposition, les lettres ne sont pas remplacées, mais réorganisées.
 - Chiffrements polyalphabétiques : les chiffrements polyalphabétiques sont fondés sur un mécanisme de substitution utilisant plusieurs alphabets.

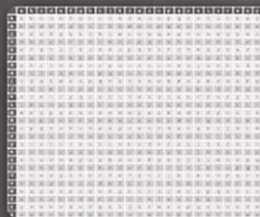
Méthodes de chiffrement



Scytale

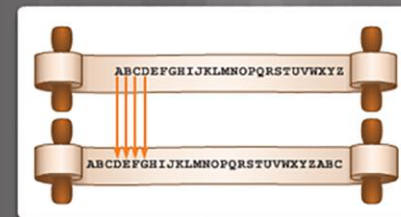


Machine allemande Enigma



	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

Table de Vigenère



Chiffre de César

Démo

○ <https://cryptii.com/pipes/caesar-cipher>

Qu'est-ce que la cryptographie ?

Cryptanalyse – Déchiffrement du code

- Il existe de nombreuses méthodes de déchiffrement des codes (cryptanalyse), telles que la force brute, le texte chiffré et le texte clair connu, entre autres.
- La cryptanalyse repose sur plusieurs méthodes :
 - Force brute : le cryptanalyste essaie chaque clé possible en sachant que l'une d'entre elles sera la bonne.
 - Texte chiffré seul : le cryptanalyste dispose du texte chiffré de plusieurs messages chiffrés, mais ne connaît pas le texte clair correspondant.
 - Texte clair connu : le cryptanalyste dispose du texte chiffré de plusieurs messages et des parties du texte clair correspondant au texte chiffré.
 - Texte clair choisi : le cryptanalyste choisit les données que l'appareil de chiffrement doit chiffrer et observe le texte chiffré généré.
 - Texte chiffré choisi : le cryptanalyste peut choisir différents textes chiffrés à déchiffrer et dispose du texte clair déchiffré.
 - Méthode du juste milieu : le cryptanalyste connaît une partie du texte clair et son équivalent en texte chiffré.

Qu'est-ce que la cryptographie ?

Clés

- Avec la technologie moderne, la sécurité du chiffrement dépend de la confidentialité des clés, et non de l'algorithme.

Deux termes sont utilisés pour décrire les clés :

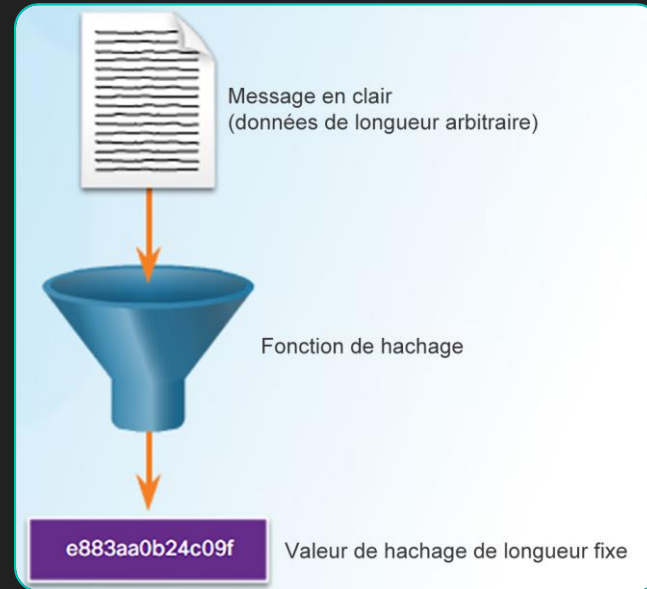
- **Longueur de clé** : mesure de la clé, exprimée en bits (également connue comme la taille de clé). Dans ce cours, nous utiliserons le terme « longueur de clé ».
- **Espace de clés** : désigne le nombre de possibilités pouvant être générées par une longueur de clé spécifique.
- L'espace de clés augmente exponentiellement au fur et à mesure que la longueur de clé s'accroît.

Clé DES	Espace de clé	Nombre de clés possibles
56 bits	2^{56} 111111 111111 111111 111111 111111 111111 111111	72 000 000 000 000 000
57 bits	2^{57} 111111 111111 111111 111111 111111 111111 111111 1	144 000 000 000 000 000
58 bits	2^{58} 111111 111111 111111 111111 111111 111111 111111 11	288 000 000 000 000 000
59 bits	2^{59} 111111 111111 111111 111111 111111 111111 111111 111	576 000 000 000 000 000
60 bits	2^{60} 111111 111111 111111 111111 111111 111111 111111 1111	1 152 000 000 000 000 000

Intégrité et authenticité

Fonctions de hachage cryptographique

- Les hashes cryptographiques permettent de contrôler et d'assurer l'intégrité des données.
- Le hash est une fonction mathématique unidirectionnelle relativement simple à calculer, mais extrêmement difficile à inverser.
- La fonction de hachage cryptographique permet également de vérifier l'authentification.
- Une fonction de hachage prend un bloc variable de données binaires (le message) et produit une représentation condensée de longueur fixe (le hash).
- Le hash qui en résulte est parfois appelé le condensé de message, le condensé ou l'empreinte numérique.
- Avec les fonctions de hachage, deux ensembles de données différents ne peuvent pas générer de hashes identiques sur le plan informatique.
- Chaque fois que les données sont modifiées ou altérées, la valeur de hash change également.

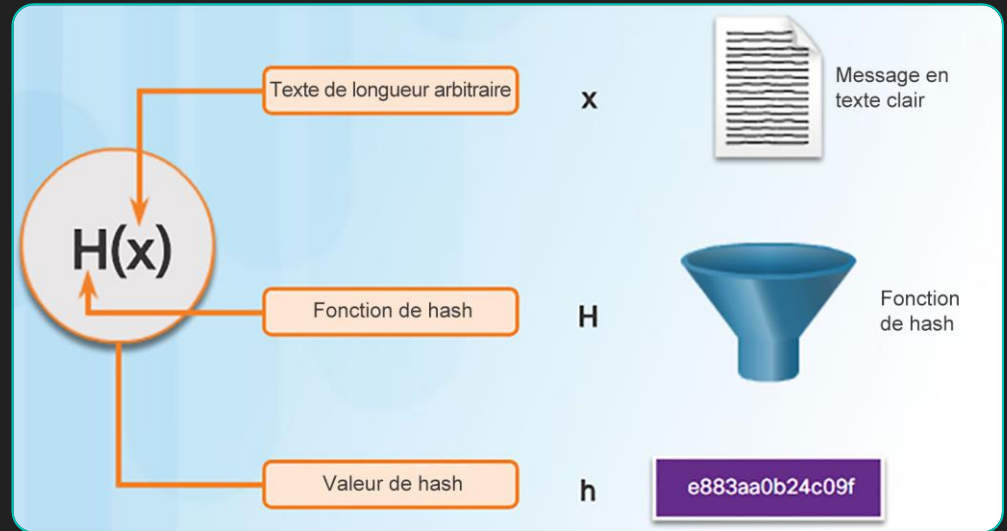


C'est quoi la différence entre chiffrement et hachage?

Intégrité et authenticité

Fonctions de hachage cryptographique

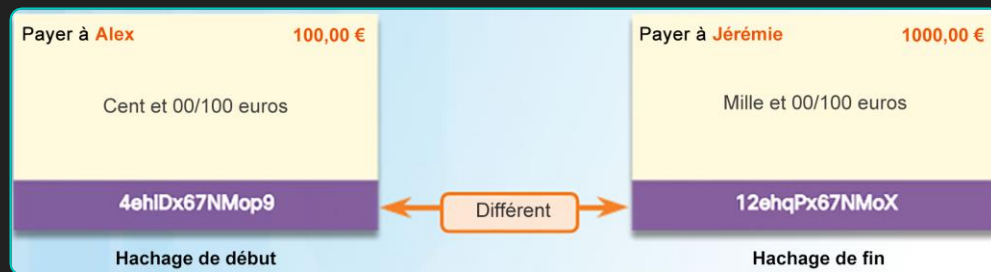
- Mathématiquement, l'équation $h = H(x)$ sert à expliquer comment fonctionne un algorithme de hachage.
- Une fonction de hash cryptographique doit posséder les propriétés suivantes :
 - Il n'y a pas de limite de longueur pour le texte saisi.
 - La longueur du résultat est fixe.
 - $H(x)$ est relativement facile à calculer pour toute valeur x .
 - $H(x)$ est unidirectionnel et irréversible.
 - $H(x)$ est libre de toute collision : deux valeurs d'entrée distinctes génèrent des valeurs de hachage différentes.



Intégrité et authenticité

MD5 et SHA

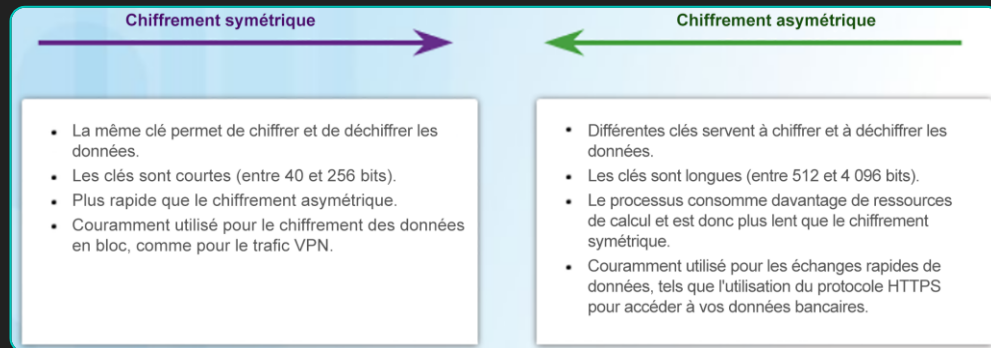
- Les fonctions de hachage sont utilisées pour garantir l'intégrité d'un message. Elles assurent que les données n'ont pas été accidentellement ou intentionnellement modifiées.
- Il existe trois algorithmes de hash bien connus : MD5 128 bits, SHA-1 et SHA-2.
 - **MD5 avec un condensé de 128 bits** : fonction unidirectionnelle qui génère un message haché de 128 bits. MD5 est considéré comme étant un algorithme ancien. Il est plutôt recommandé d'utiliser la fonction SHA-2.
 - **SHA-1** : très similaire aux fonctions de hachage MD5. Elle se décline en plusieurs versions. La fonction SHA-1 génère un message de 160 bits hachés et se révèle légèrement plus lent que la fonction MD5. Elle présente des défauts et apparaît comme un algorithme obsolète.
 - **SHA-2** : algorithme nouvelle génération qu'il convient d'utiliser chaque fois que possible.
- Bien que le hachage permette de détecter des modifications accidentelles, il ne peut être utilisé pour se prémunir contre les modifications intentionnelles. La procédure de hash ne comporte aucune information d'identification unique provenant de l'expéditeur.



Confidentialité Chiffrement

Ces deux classes se distinguent par leur mode d'utilisation des clés :

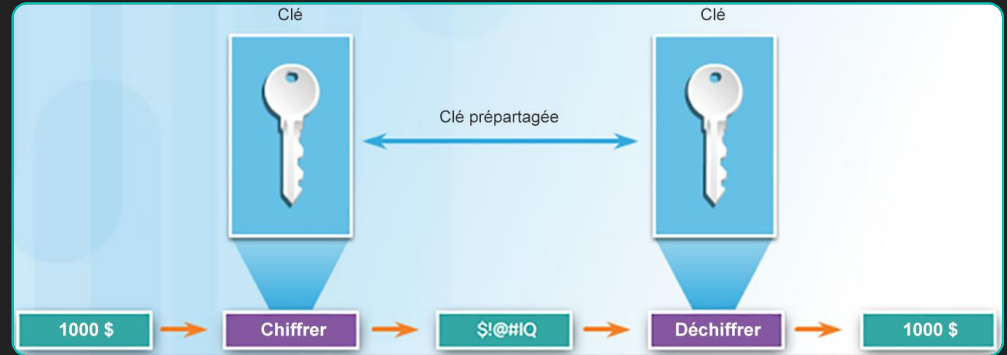
- **Algorithmes de chiffrement symétrique** : ces algorithmes de chiffrement utilisent la même clé pour chiffrer et déchiffrer les données. Ils partent du principe que chacune des parties engagées dans la communication connaît la clé prépartagée.
- **Algorithmes de chiffrement asymétrique** : ces algorithmes de chiffrement utilisent des clés différentes pour chiffrer et pour déchiffrer les données. Ils partent du principe que les deux parties engagées dans la communication n'ont pas encore partagé de secret et doivent mettre en place une méthode sécurisée pour ce faire. Ces algorithmes consomment énormément de ressources et leur exécution est plus lente.



Confidentialité

Chiffrement symétrique

- Les algorithmes de chiffrement symétrique utilisent la même clé prépartagée pour chiffrer et déchiffrer les données.
- Aujourd'hui, les algorithmes de chiffrement symétrique sont couramment utilisés avec le trafic VPN. En effet, les algorithmes de chiffrement symétrique sollicitent moins l'UC que les algorithmes de chiffrement asymétrique.
- Lorsque vous utilisez un algorithme de chiffrement symétrique, et comme avec les autres types de chiffrement, plus la clé est longue, plus le temps nécessaire pour la découvrir est important.
- La plupart des clés de chiffrement comprennent entre 112 et 256 bits. Utilisez une clé plus longue pour des communications plus sécurisées.

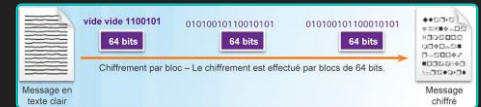


Confidentialité

Algorithmes de chiffrement symétrique

Les algorithmes de chiffrement sont souvent classés comme suit :

- **Chiffrement par blocs** : transforme un bloc de longueur fixe de texte clair en un bloc commun de texte chiffré de 64 ou 128 bits.
- **Chiffrement de flux** : chiffre un texte en clair, à raison d'un bit/octetet à la fois.



Les algorithmes de chiffrement symétrique courants incluent : **Data Encryption Standard (DES)**, **3DES (Triple DES)**, **Advanced Encryption Standard (AES)**, **Software-Optimized Encryption Algorithm (SEAL)**, **chiffrement Rivest (RC)**

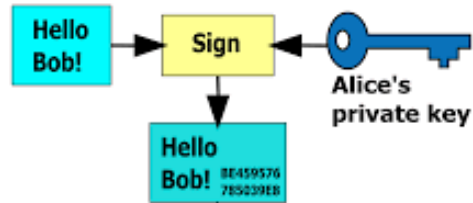
Confidentialité

Algorithmes de chiffrement asymétrique

- Les algorithmes asymétriques (ou « algorithmes à clé publique ») sont conçus de sorte que la clé utilisée pour le chiffement diffère de la clé utilisée pour le déchiffement.
- La clé de déchiffement ne peut être déduite de la clé de chiffement dans un délai raisonnable, et inversement.
- Les algorithmes asymétriques utilisent une clé publique et une clé privée.
- Les deux clés permettent le processus de chiffement, mais la clé associée complémentaire est requise pour le déchiffement.
- Le processus est également réversible puisqu'une clé privée doit être utilisée pour déchiffrer les données chiffrées avec la clé publique.
- Ce processus permet aux algorithmes asymétriques de garantir la confidentialité, l'authentification et l'intégrité.



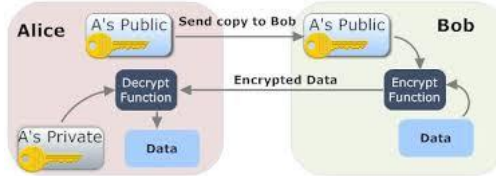
Alice



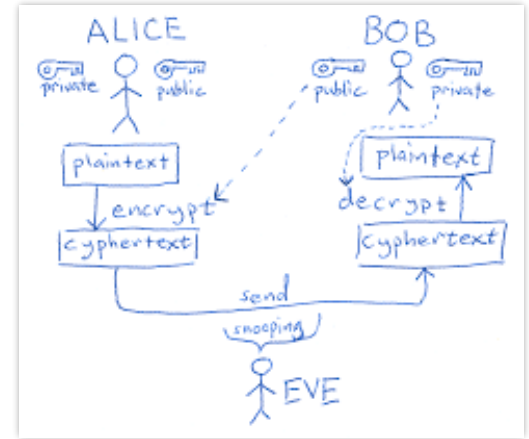
Bob



Signature



Chiffrement



Chiffrement+Signature

Démo

Confidentialité

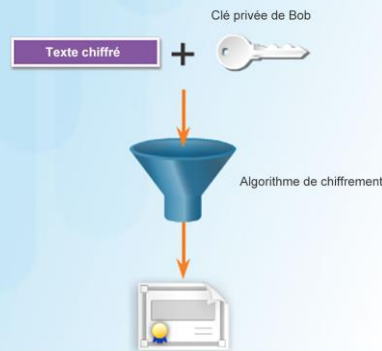
Chiffrement asymétrique – Confidentialité

- Les algorithmes asymétriques assurent la confidentialité sans partager de mot de passe au préalable.
- La confidentialité des algorithmes asymétriques est garantie quand vous lancez le processus de chiffrement avec la clé publique.

Le processus peut être récapitulé à l'aide de la formule : **clé publique (chiffrer) + clé privée (déchiffrement) = confidentialité**

- Là où la clé publique sert à chiffrer les données, la clé privée doit être utilisée pour les déchiffrer.
- Un seul hôte a la clé privée.

Bob déchiffre le message à l'aide de sa clé privée



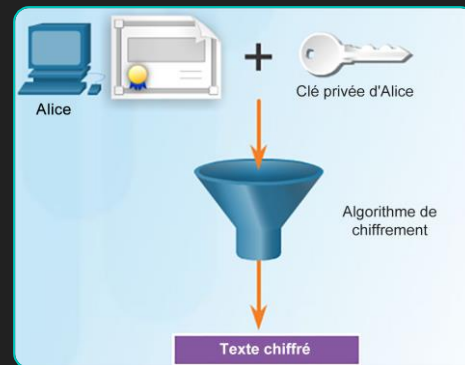
Confidentialité

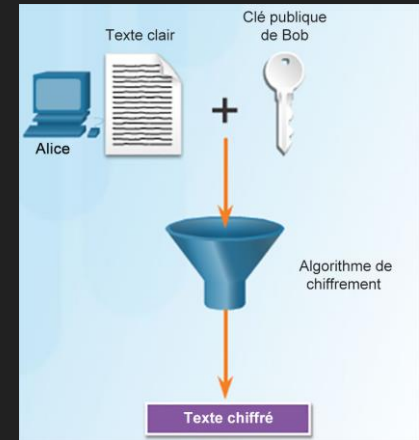
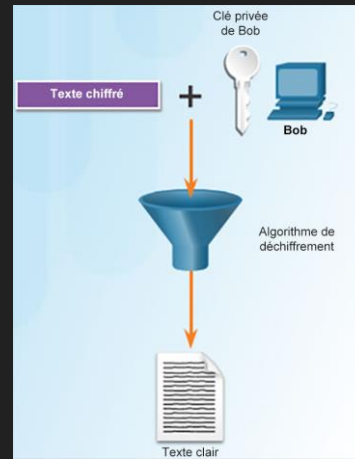
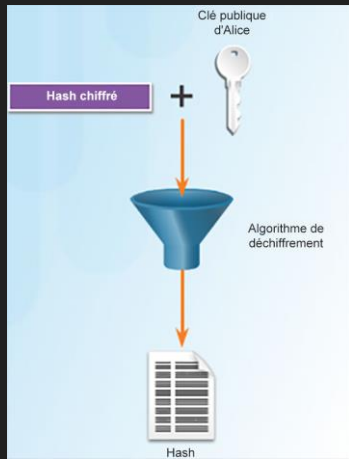
Chiffrement asymétrique – Authentification

- L'authentification des algorithmes asymétriques est réalisée quand vous lancez le processus de chiffrement avec la clé privée.

Le processus peut être résumé à l'aide de cette formule :

- **Clé privée (chiffrer) + clé publique (déchiffrer) = Authentification**
- Là où la clé privée sert à chiffrer les données, la clé publique correspondante doit être utilisée pour les déchiffrer.
- Un seul hôte possède la clé privée ; par conséquent, seul cet hôte peut avoir chiffré le message, authentifiant ainsi l'expéditeur.
- Si un hôte déchiffre avec succès un message à l'aide d'une clé publique, c'est que celui-ci a bien été chiffré avec la clé privée ; l'identité de l'expéditeur est vérifiée.





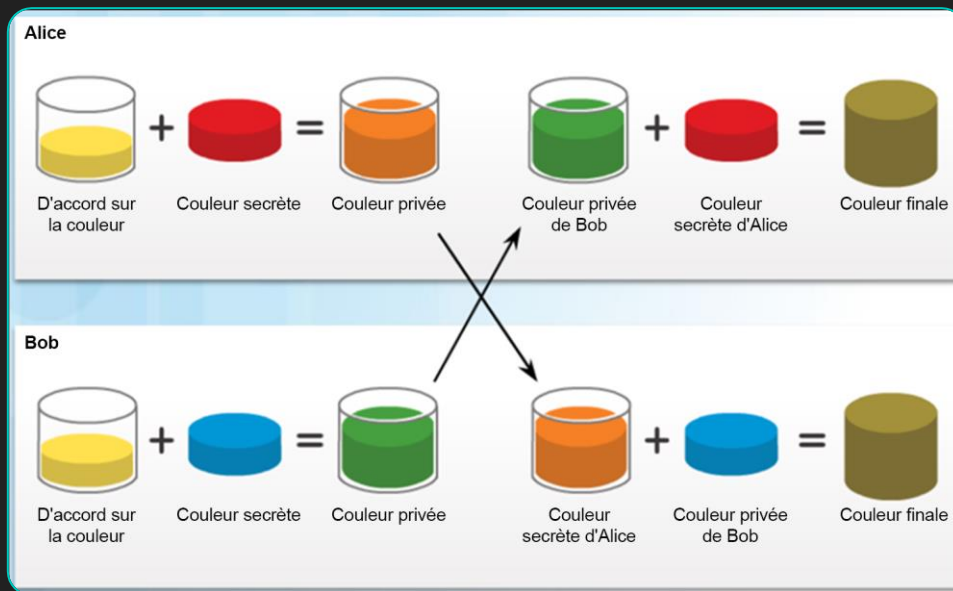
Confidentialité Chiffrement asymétrique – Intégrité

- En combinant les deux processus de chiffrement asymétrique, vous assurez l'intégrité, l'authentification et la confidentialité de vos messages.

Confidentialité

Diffie-Hellman

- L'échange de clé DH (Diffie-Hellman) est un algorithme mathématique asymétrique qui permet à deux ordinateurs de générer un secret partagé identique sans avoir communiqué auparavant.
- En réalité, la nouvelle clé partagée n'est pas véritablement échangée entre l'émetteur et le récepteur.
- Comme les deux parties connaissent la clé, elle peut cependant être utilisée par un algorithme de chiffrement pour chiffrer le trafic entre les deux systèmes.
- La sécurité de l'algorithme DH repose sur l'utilisation de nombres extrêmement grands dans ses calculs.
- Malheureusement, les systèmes à clé asymétrique sont extrêmement lents, quel que soit le mode de chiffrement par bloc. C'est pourquoi il est courant de chiffrer l'ensemble du trafic à l'aide d'un algorithme symétrique.





L'infrastructure à clé publique

La cryptographie à clé publique

Utilisation des signatures numériques

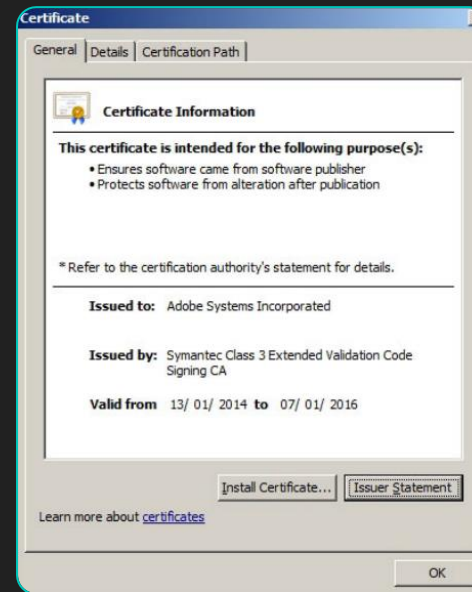
- La signature numérique est une technique mathématique utilisée pour assurer l'authenticité, l'intégrité et la non-répudiation sous la forme de certificats numériques et de signature de code.
- Les signatures numériques sont couramment utilisées dans les deux situations suivantes :
 - Signature de code : permet de vérifier l'intégrité des fichiers exécutables téléchargés à partir du site web d'un fournisseur.
 - Certificats numériques : utilisés pour authentifier l'identité d'un système et échanger des informations confidentielles.
- Trois algorithmes DSS (Digital Signature Standard) sont utilisés pour générer et vérifier les signatures numériques :
 - Algorithme DSA (Digital Signature Algorithm)
 - Algorithme RSA (Rivest-Shamir Adelman Algorithm)
 - Algorithme ECDSA (Elliptic Curve Digital Signature Algorithm)



La cryptographie à clé publique

Signatures numériques de signature de code

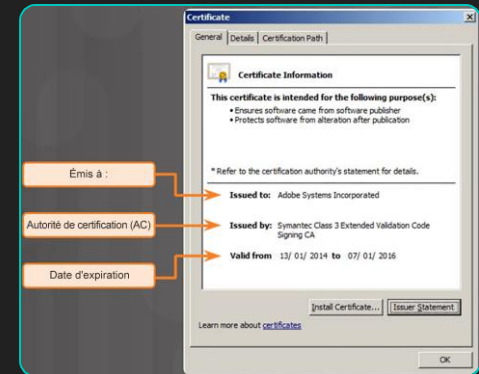
- Les signatures numériques sont couramment utilisées pour garantir l'authenticité et l'intégrité du code logiciel.
- Les fichiers exécutables sont encapsulés dans une enveloppe signée numériquement, ce qui permet à l'utilisateur final de vérifier la signature avant d'installer le logiciel.
- La signature numérique du code offre plusieurs garanties sur le code :
 - Le code est authentique et provient de l'éditeur.
 - Le code n'a pas été modifié depuis qu'il a quitté l'éditeur de logiciels.
 - C'est indéniablement l'éditeur qui a publié le code. Cela assure la non-répudiation de l'acte de publication.



La cryptographie à clé publique

Signatures numériques de certificat numérique

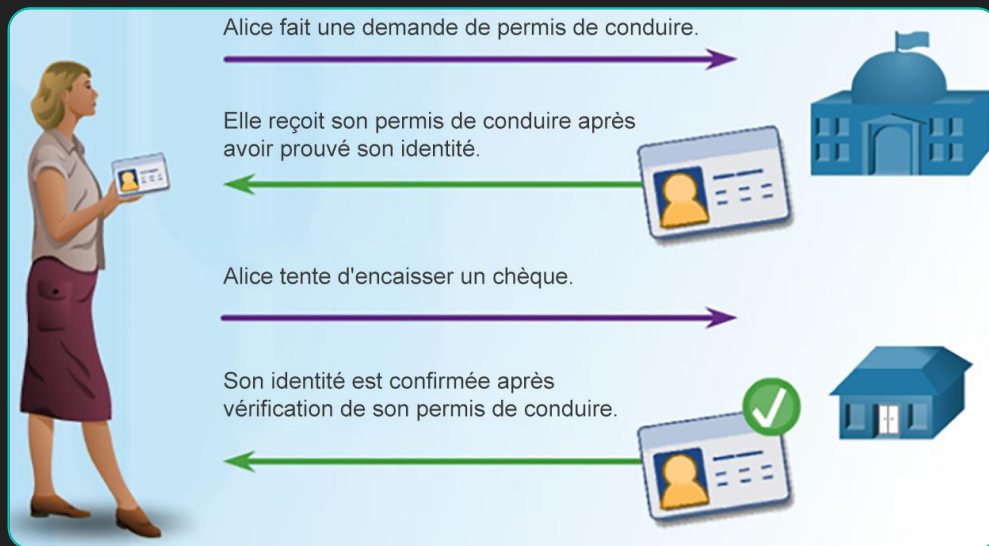
- Les certificats numériques permettent aux utilisateurs, aux hôtes et aux entreprises d'échanger des informations sur Internet de manière sécurisée.
- Concrètement, un certificat numérique permet d'authentifier et de vérifier que l'expéditeur d'un message est bien celui qu'il prétend être.
- Les certificats numériques permettent également de garantir la confidentialité du destinataire en lui permettant de chiffrer sa réponse.



Les autorités et le système d'infrastructure à clé publique

Gestion des clés publiques

- Lorsqu'ils établissent une connexion asymétrique entre deux hôtes, les hôtes échangent leurs informations de clé publique.
- Des tiers de confiance sur Internet valident l'authenticité de ces clés publiques à l'aide de certificats numériques. Le tiers émet des informations d'identification qui sont particulièrement difficiles à falsifier.
- À partir de ce moment-là, toutes les personnes qui font confiance au tiers acceptent simplement les informations d'identification qu'il émet.



Les autorités et le système d'infrastructure à clé publique

L'infrastructure à clé publique

- L'infrastructure PKI est nécessaire pour soutenir une distribution de grande envergure et l'identification des clés de chiffrement publiques.
- Le cadre PKI favorise une relation de confiance hautement évolutive.
- Il regroupe le matériel, les logiciels, les personnes, les politiques et les procédures nécessaires pour créer, gérer, stocker, distribuer et révoquer des certificats numériques.
- Les certificats PKI ne sont pas tous directement envoyés par l'autorité de certification. Une autorité d'enregistrement (RA) est une autorité de certification subordonnée certifiée par une autorité de certification racine pour la délivrance de certificats à des fins spécifiques.

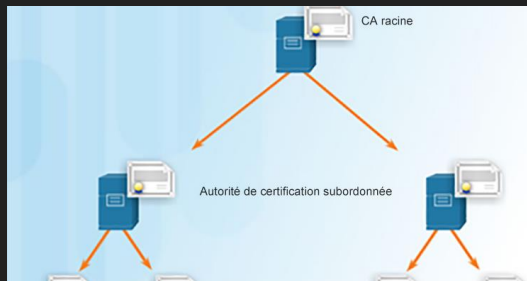


Les autorités et le système d'infrastructure à clé publique

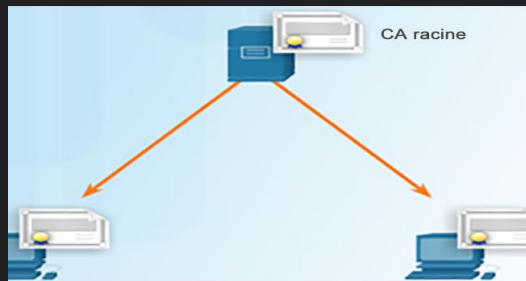
Le système d'autorités PKI

- De nombreux fournisseurs proposent leurs serveurs CA sous la forme d'un service managé ou d'un produit pour utilisateur final.
- Les entreprises peuvent également implémenter une infrastructure PKI privée à l'aide de Microsoft Server ou d'Open SSL.
- Les autorités de certification délivrent des certificats par classes qui déterminent le degré de confiance d'un certificat.
- Le numéro de classe est déterminé par le degré de rigueur de la procédure à l'heure de vérifier l'identité du titulaire lors de l'émission du certificat.
- Plus le numéro de classe est élevé, plus le certificat est fiable.
- Les clés publiques de certaines autorités de certifications sont préchargées, à l'instar de celles indiquées par les navigateurs web.
- Une entreprise peut également implémenter une infrastructure PKI pour un usage interne.

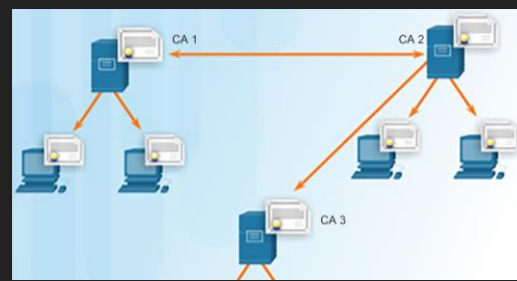
Classe	Description
0	Destinée à des fins de test sans aucune vérification.
1	Destinée aux particuliers et est axée sur la vérification des e-mails.
2	Destinée aux entreprises exigeant la preuve de l'identité.
3	Destinée aux serveurs et logiciels pour lesquels une vérification indépendante de l'identité et de l'autorité est effectuée par l'autorité de certification les ayant publiés.
4	Destinée aux transactions commerciales en ligne entre entreprises.
5	Destinée aux entreprises privées ou à la sécurité des administrations



Autorité de certification
hiérarchique



PKI à racine unique



Autorité de
certification croisée

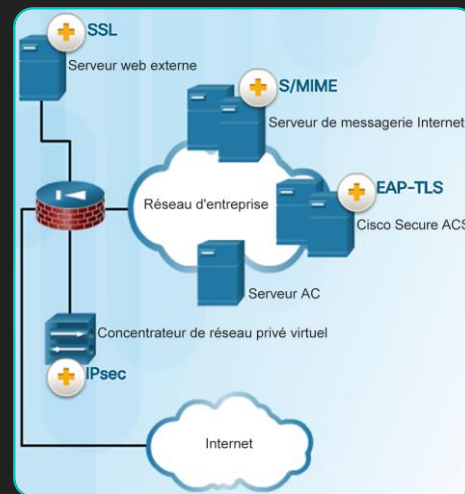
Les autorités et le système d'infrastructure à clé publique Le système de confiance PKI

- Les infrastructures PKI peuvent présenter différentes topologies de confiance. La topologie PKI à racine unique est la plus simple.
- Sur les réseaux d'envergure, les autorités de certification de l'infrastructure PKI peuvent être réunies à l'aide de deux architectures de base :
 - **Topologies CA cocertifiées** : il s'agit d'un modèle peer-to-peer dans lequel chaque autorité de certification établit des relations de confiance avec les autres autorités de certification au travers de certificats CA transversaux.
 - **Topologies CA hiérarchiques** : l'autorité de certification racine a le niveau le plus élevé. Celle-ci peut délivrer des certificats aux utilisateurs finaux et aux autorités de certification subordonnées.

Les autorités et le système d'infrastructure à clé publique

Interopérabilité des différents fournisseurs d'infrastructure PKI

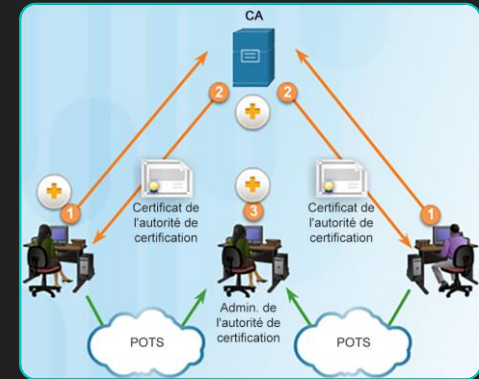
- L'interopérabilité entre une infrastructure PKI et ses services d'assistance revêt une importance particulière, car de nombreux fournisseurs CA ont préféré proposer et implémenter des solutions propriétaires plutôt que d'attendre la publication de normes.
- Pour résoudre ce problème d'interopérabilité, l'IETF a publié une politique sur les certificats des infrastructures à clé publique Internet X.509 et instauré un cadre sur les pratiques de certification (RFC 2527).
- Le standard X.509 version 3 (X.509v3) définit le format d'un certificat numérique.



Les autorités et le système d'infrastructure à clé publique

Inscription, authentification et révocation de certificats

- Tous les systèmes qui tirent parti d'une infrastructure à clé publique doivent posséder la clé publique de l'autorité de certification, appelée certificat autosigné.
- La clé publique de l'autorité de certification vérifie tous les certificats émis par l'autorité de certification et est essentielle au bon fonctionnement de l'infrastructure à clé publique.
- Le processus d'inscription de certificats début lorsque les certificats CA sont récupérés intrabande via un réseau et que l'authentification s'effectue hors bande (OOB) à l'aide d'un téléphone.
- Le système qui s'inscrit sur une infrastructure PKI contacte une autorité de certification afin de demander et d'obtenir un certificat d'identité numérique pour lui-même, et récupérer le certificat auto-signé de l'autorité de certification.
- L'étape finale consiste à vérifier que le certificat CA est authentique ; elle repose sur une méthode OOB (ancien système de téléphone simple, POTS, p. ex.), afin d'obtenir l'empreinte du certificat d'identité CA valide.
- Un certificat numérique peut être révoqué si sa clé est compromise ou qu'elle n'est plus nécessaire.



Les utilisations et les effets de la cryptographie

Applications PKI

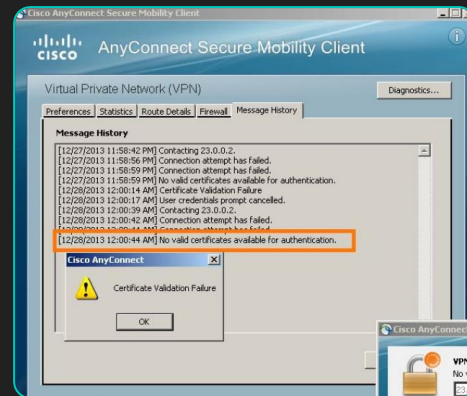
- Voici certaines utilisations des infrastructures à clé publique :
 - Authentification des homologues basée sur des certificats SSL/TLS
 - Trafic réseau sécurisé à l'aide de VPN IPsec
 - Trafic web HTTPS
 - Contrôler l'accès au réseau via une authentification 802.1x ;
 - Sécurisation des e-mails via le protocole S/MIME ;
 - Sécurisation des messages instantanés ;
 - Approbation et autorisation d'applications avec la signature de code ;
 - Protection des données utilisateur avec le système EFS (Encryption File System) ;
 - Implémentation d'une authentification à deux facteurs avec carte à puce ;
 - Sécurisation des appareils de stockage USB ;



Les utilisations et les effets de la cryptographie

Chiffrement des transactions réseau

- Les cybercriminels peuvent utiliser le protocole SSL/TLS pour compromettre le respect des réglementations, ou introduire un virus, un programme malveillant, une perte de données ou une tentative d'intrusion dans un réseau.
- Les autres problèmes rattachés au protocole SSL/TLS peuvent porter sur la validation du certificat d'un serveur web. Lequel cas, les navigateurs web affichent un avertissement de sécurité. Les problèmes d'infrastructure PKI associés aux avertissements de sécurité comprennent :
 - **Plage de validité** : les certificats X.509v3 spécifient les dates limites (« après le » et « avant le »). Si la date du jour se trouve en dehors de la plage, le navigateur web affiche un message.
 - **Erreur de validation de signature** : si un navigateur ne peut pas valider la signature du certificat, rien ne garantit que la clé publique du certificat soit authentique.



Les utilisations et les effets de la cryptographie

Chiffrement et surveillance de la sécurité

- Lorsque les paquets sont chiffrés, la surveillance réseau pose de nouveaux enjeux.
- Comme le protocole HTTPS implique un trafic HTTP chiffré de bout en bout (par protocole TLS/SSL), l'examen du trafic des utilisateurs n'est pas un jeu d'enfant.
- Voici une liste des tâches que pourrait réaliser un analyste en charge de la sécurité :
 - Configurer des règles pour distinguer le trafic SSL du trafic non-SSL ou le trafic SSL HTTPS du trafic SSL non-HTTPS.
 - Renforcer la sécurité par une validation de certificat de serveur à l'aide de listes CRL et OCSP.
 - Mettre en œuvre une protection antimalware et le filtrage des URL du contenu HTTPS.
 - Déployer une appliance SSL Cisco pour déchiffrer le trafic SSL et l'envoyer aux appliances du système de prévention des intrusions afin d'identifier les risques normalement dissimulés par SSL.



Récapitulatif

Récapitulatif

- La sécurisation des communications se compose de quatre éléments :
 - La confidentialité des données qui garantit que seuls les utilisateurs autorisés peuvent consulter les données.
 - L'intégrité des données qui garantit que le message n'a pas été modifié.
 - L'authentification de l'origine qui garantit qu'il ne s'agit pas d'un faux message et qu'il provient réellement du propriétaire.
 - La non-répudiation des données qui garantit que l'expéditeur ne peut pas répudier ni réfuter la validité d'un message envoyé.
- La cryptologie est la science de la création et du déchiffrement des codes secrets. Deux disciplines se distinguent : la cryptographie et la cryptanalyse (ou analyse cryptographique).
- Un chiffrement est un algorithme composé d'une série d'étapes bien définies que vous pouvez suivre pour chiffrer et déchiffrer des messages.
- Il existe de nombreuses méthodes de déchiffrement des codes (cryptanalyse), telles que la force brute, le texte chiffré et le texte clair connu, entre autres.
- Avec la technologie moderne, la sécurité du chiffrement dépend de la confidentialité des clés, et non de l'algorithme. Plus précisément la longueur de clé et l'espace de clé.

Récapitulatif (suite)

- Les hashes cryptographiques permettent de contrôler et d'assurer l'intégrité des données.
- Avec les fonctions de hachage, deux ensembles de données différents ne peuvent pas générer de hashes identiques sur le plan informatique.
- Mathématiquement, l'équation $h = H(x)$ sert à expliquer comment fonctionne un algorithme de hachage.
- Les trois fonctions de hachage les plus connues sont :
 - La fonction MD5 avec un condensé de 128 bits
 - SHA-1
 - La fonction SHA-2
- Pour assurer l'authentification et l'intégrité des messages, vous devez ajouter un code HMAC comme entrée d'une fonction de hachage. Si les deux parties partagent une clé secrète et utilisent les fonctions HMAC pour l'authentification, un condensé HMAC correctement constitué d'un message qu'une partie a reçu indique que l'autre partie est l'auteur du message.
- La confidentialité des données est assurée par un chiffrement symétrique ou asymétrique.

Récapitulatif (suite)

- La confidentialité des données est assurée par un chiffrement symétrique ou asymétrique.
- Les algorithmes de chiffrement symétrique utilisent la même clé prépartagée pour chiffrer et déchiffrer les données.
- Les algorithmes de chiffrement symétrique sont souvent classés dans l'une des catégories suivantes : **chiffrement par bloc** ou **le chiffrement par flux**.
- Les algorithmes asymétriques (ou « algorithmes à clé publique ») sont conçus de sorte que la clé utilisée pour le chiffrement diffère de la clé utilisée pour le déchiffrement.
- Les algorithmes asymétriques assurent la confidentialité sans partager de mot de passe au préalable. La confidentialité des algorithmes asymétriques est garantie quand vous lancez le processus de chiffrement avec la clé publique.
- L'authentification des algorithmes asymétriques est réalisée quand vous lancez le processus de chiffrement avec la clé privée. Utilisez la formule : **clé privée (chiffrer) + clé publique (déchiffrement) = authentification**.
- En combinant les deux processus de chiffrement asymétrique, vous assurez l'intégrité, l'authentification et la confidentialité de vos messages.
- L'échange de clé DH (Diffie-Hellman) est un algorithme mathématique asymétrique qui permet à deux ordinateurs de générer un secret partagé identique sans avoir communiqué auparavant.

Récapitulatif (suite)

- La signature numérique est une technique mathématique utilisée pour assurer l'authenticité, l'intégrité et la non-répudiation sous la forme de certificats numériques et de signature de code.
- Les signatures numériques sont couramment utilisées pour garantir l'authenticité et l'intégrité du code logiciel.
- Les certificats numériques permettent aux utilisateurs, aux hôtes et aux entreprises d'échanger des informations sur Internet de manière sécurisée.
- L'infrastructure de clé publique (PKI) constitue un exemple de système tiers de confiance appelé « autorité de certification » (CA).
- L'infrastructure PKI est nécessaire pour soutenir une distribution de grande envergure et l'identification des clés de chiffrement publiques.
- De nombreux fournisseurs proposent leurs serveurs CA sous la forme d'un service managé ou d'un produit pour utilisateur final. Les entreprises peuvent également implémenter une infrastructure PKI privée à l'aide de Microsoft Server ou d'Open SSL. Les autorités de certification délivrent des certificats par classes qui déterminent le degré de confiance d'un certificat.
- Les infrastructures PKI peuvent présenter différentes topologies de confiance. La topologie PKI à racine unique est la plus simple. Sur les réseaux de grande taille, les autorités de certification PKI peuvent être associées à l'aide de deux architectures de base : les topologies CA croisées et les topologies CA hiérarchiques.

Récapitulatif (suite)

- L'interopérabilité entre une infrastructure PKI et ses services d'assistance revêt une importance particulière, car de nombreux fournisseurs CA ont préféré proposer et implémenter des solutions propriétaires plutôt que d'attendre la publication de normes. Pour résoudre ce problème d'interopérabilité, l'IETF a publié une politique sur les certificats des infrastructures à clé publique Internet X.509 et instauré un cadre sur les pratiques de certification (RFC 2527). Le standard X.509 version 3 (X.509v3) définit le format d'un certificat numérique.
- Tous les systèmes qui tirent parti d'une infrastructure à clé publique doivent posséder la clé publique de l'autorité de certification, appelée certificat autosigné. La clé publique de l'autorité de certification vérifie tous les certificats émis par l'autorité de certification et est essentielle au bon fonctionnement de l'infrastructure à clé publique.
- Il existe de nombreuses utilisations possibles des infrastructures PKI.
- Les cybercriminels peuvent utiliser le protocole SSL/TLS pour compromettre le respect des réglementations, ou introduire un virus, un programme malveillant, une perte de données ou une tentative d'intrusion dans un réseau.
- Lorsque les paquets sont chiffrés, la surveillance réseau pose de nouveaux enjeux. Comme le protocole HTTPS implique un trafic HTTP chiffré de bout en bout (par protocole TLS/SSL), l'examen du trafic des utilisateurs n'est pas un jeu d'enfant. Voici une liste des tâches que pourrait réaliser un analyste en charge de la sécurité :
 - Configurer des règles pour distinguer le trafic SSL du trafic non-SSL ou le trafic SSL HTTPS du trafic SSL non-HTTPS.
 - Renforcer la sécurité par une validation de certificat de serveur à l'aide de listes CRL et OCSP.
 - Mettre en œuvre une protection antimalware et le filtrage des URL du contenu HTTPS.
 - Déployer une appliance SSL Cisco pour déchiffrer le trafic SSL et l'envoyer aux appliances du système de prévention des intrusions afin d'identifier les risques normalement dissimulés par SSL.

Chapitre 21

Nouveaux termes et nouvelles commandes

- 3DES (Triple DES)
 - AES
 - chiffrement asymétrique
 - Chiffrement par bloc
 - Chiffrement
 - Cryptanalyse
 - cryptographie
 - cryptologie
 - Algorithme DES (Data Encryption Standard)
 - Diffie-Hellman (DH)
 - Algorithme DSA (Digital Signature Algorithm)
 - DSS (Digital Signature Standard)
 - ElGamal
 - Elliptical Curve
 - hash
 - HMAC (Hash Message Authentication Code)
 - MD5 (Message Digest 5)
 - Infrastructure de clé publique (PKI)
 - Chiffrement Rivest
 - RSA
 - SHA-1 (Secure Hash Algorithm 1)
 - SHA-2 (Secure Hash Algorithm 2)
 - Algorithmes SEAL (Software-Optimized Encryption Algorithm)
 - Chiffrement de flux
 - Chiffrement symétrique
-