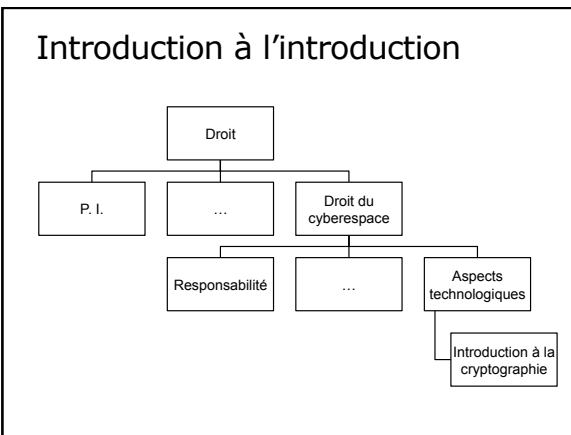


Daniel Poulin
DRT 3808 - 2009
**INTRODUCTION À LA
CRYPTOGRAPHIE**



Introduction à la cryptographie

- Intérêt juridique
 - Signature
 - Intégrité des documents
 - Preuve
 - Paiement et commerce électronique
 - Propriété intellectuelle
 - Sécurité
 - Vie privée

Dans cette introduction

- Notions
- Cryptographie à clé secrète
- Cryptographie à clé publique
- Les systèmes hybrides
- Les fonctions de hachage
- La signature électronique
- Les certificats, les infrastructure à clé publique, ...
- Le protocole SSL

La cryptographie

- Définition
 - L'ensemble des principes, méthodes et techniques dont l'application assure le chiffrement et le déchiffrement des données afin d'en préserver la confidentialité et l'authenticité (GDT)
- Intérêt
 - Assurer une sécurité des échanges indépendante du canal d'information
- L'alternative : l'utilisation de canaux que l'on contrôle

Cryptographie et Internet

- L'utilisation d'Internet à des fins médicales, bancaires, commerciales et autres exige la sécurité des communications
- Les ordinateurs en réseau ont aussi besoin d'être protégés

Trois facettes de la sécurité

- Confidentialité
 - Caractère des données dont l'accès doit être restreint aux seules personnes ou entités autorisées
- Intégrité
 - Propriété des données qui, lors de leur traitement ou de leur transmission, ne subissent aucune altération volontaire ou accidentelle et conservent un format permettant leur utilisation
 - Voir [aussi art. 6, Loi québécoise LCJI](#)
- Authenticité
 - Caractère d'une information dont l'origine et l'intégrité sont garanties
 - Au sens juridique, selon H. Reid : « qualité conférée à un acte passé devant un officiel public compétent suivant certaines formalités prescrites par la loi »
- Note : l'intégrité et l'authenticité sont essentielles l'un à l'autre

Notions

- L'information peut être cachée
 - Usage d'une encre sympathique ou encore en tatouant le crâne d'un esclave
 - Par le recours à une convention
- L'information peut être codée ou « chiffrée »
 - Table de chiffrement de César (Ici, la clé est « 3 »)

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
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

- Ainsi, "erqmrxu" signifie. Voir : http://www.simon Singh.net/The_Black_Chamber/caesar.html
- Sur un support numérique, l'information est manipulée mathématiquement afin d'être codée

La fréquence des lettres

- Comme le chiffrement de César n'offre que 25 clés, il est facile à décrypter
- La fréquence des lettres peut être analysée, par exemple, en anglais
- Illustration, voir le site de Simon Singh
 - http://www.simon Singh.net/The_Black_Chamber/frequencyanalysis.html

•Lettre	•Fréquence
E	131.05
T	104.68
A	81.51
O	79.95
N	70.98
R	68.32
I	63.45
S	61.01
H	52.59
D	37.88
L	33.89
F	29.24
C	27.58
M	25.36
U	24.59
G	19.94
Y	19.82

Le Code Morse

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

La cryptographie d'aujourd'hui

- Bases
 - L'information est encodée numériquement
 - Les algorithmes de chiffrement sont généralement connus
 - Le secret repose sur la connaissance de la clé
- **Chiffre** (ou cryptage) : Transformer un message en texte clair en un cryptogramme inintelligible par des opérations mathématiques indépendantes du contenu (l'opération inverse est le **déchiffre**)
- Le but de la cryptographie est de rendre le **décriptage**, c'est-à-dire, le passage du message chiffré au message en clair sans la connaissance de la clé, impraticable sinon impossible.

L'utilisation de clés: la table de Blaise de Vigenère (1523 - 1596)

- Un des premiers systèmes à mot de passe (ou clé)
- La table est connue, c'est le mot de passe qui est secret
- Si la clé est « coco » et le message « montreal »
- La clé est répétée pour être de même longueur que le message 'cocococo'

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Source: Wikipedia/Vigenère cipher

Notions

- Le chiffrage et le déchiffrage sont définis par des algorithmes – généralement connus
- Algorithme
 - Une méthode systématique susceptible d'être mécanisée pour exécuter une tâche

Les algorithmes de chiffrage

- Fonction : « une relation qui associe un nombre d'un ensemble de départ à un autre d'un ensemble d'arrivée»
- Fonction aisément réversible
 - On associe à un 'x', une valeur 'y', $f(x) = 3x + 1 = y$
 - Il existe une fonction inverse $g(y)$, telles que $g(y) = (y - 1) / 3 = x$
 - Exemple : la température centigrade : $f(tf) = (tf - 32) * 5/9 = tc$
- Certaines fonctions sont moins aisément inversées
 - (Non) Chercher le numéro associé à un nom dans un bottin téléphonique
 - (Non) $f(x) = x^2$; par exemple, si $f(x) = 343$ ou 2197 (13)
- Fonctions à sens unique (non réversibles)
 - « many look and smell like it » (Schneier, p. 29)
 - On ne peut jamais être certains

Factorisation des grands nombres

- Nombre premier : un nombre qui ne se divise que par lui-même et par 1
 - Exemple: 1, 3, 5, 7, ...
- Factorisation : décomposer un nombre en ses facteurs
 - Exemples
 - Pour le nombre 6 les facteurs sont 6, 3, 2 et 1
 - Pour le nombre 7 : 7 et 1, donc 7 est un nombre premier

Factorisation des grands nombres

- Exemple
 - $43 \times 41 = 2021$
- Qu'en est-il de 2023?
 - $289 \times 7 = 2023$
- Qu'en est-il de 289?
 - $17 \times 17 = 289$
- Qu'en est-il de 7871 ou 7873 (premier)
- Les mathématiciens ne connaissent pas de façon simple de factoriser les nombres
- En 1999, une équipe est parvenue à factoriser un nombre de 512 bits (soit 155 chiffres décimaux) en 4 mois avec 300 ordinateurs (RSA)

Les systèmes cryptographiques



- Les systèmes à clé secrète (symétrique)
- Les systèmes à clé publique (asymétriques)
- Les systèmes hybrides
- Le hachage et la signature

Les systèmes cryptographiques à clé secrète

- Systèmes où la même clé sert au chiffage et au déchiffage des messages

Cryptographie à clé secrète



[http://i.msdn.microsoft.com/Aa480570.ch2_dataconf_f01\(en-us.MSDN.10\).gif](http://i.msdn.microsoft.com/Aa480570.ch2_dataconf_f01(en-us.MSDN.10).gif)

Le plus connu des systèmes à clé secrète : DES

- Le déploiement de la cryptographie exige des normes et des standards
 - Pour l'interopérabilité
 - Parce que la qualité est difficile à mesurer
- Le Data Encryption Standard (DES)
 - Développé par IBM pour le gouvernement US au milieu des années 70
 - À partir de 2001, DES a été remplacé par son successeur, l'Advanced Encryption Standard (AES)
- Utilisation
 - Pour les transferts de fonds dans le monde bancaire
 - Pour la protection des mots de passe dans les ordinateurs
 - Pour le chiffrement en temps réel des conversations téléphoniques

DES a toujours été controversé

- Le gouvernement cherchait quelque chose de solide, mais pas trop
 - IBM avait proposé un clé de 128 bits
 - La longueur retenue fut de 56 bits, offrant 72 057 594 037 927 936 clés possibles
 - Certains soupçonnaient l'existence d'une porte arrière
- Longueur de clé : retour sur César et Vigenère
- DES, bien que décrit dans les publications scientifiques, ne pouvait être exporté jusque dans les années 90 (sauf en pays amis)
- Vers la fin des années 90, l'EFF parvenait à trouver une clé en 56 heures; puis, en 1999, en 22 heures
 - Ce qui soulève la question de la durée requise du secret

Limites de la cryptographie à clé secrète

- Ces systèmes peuvent offrir une excellente sécurité
- Le principal problème a trait à la distribution des clés
 - Si la même clé est utilisée par plus de 2 personnes
 - Elle doit être abandonnée lorsqu'une copie est compromise
 - Elle ne peut authentifier, ni permettre la « non-répudiation »
 - L'approche conduit à l'utilisation de nombreuses clés, un clé pour chaque paire d'intervenants
- Sur Internet ou dans une grande organisation le nombre de clés peut devenir très grand ($N = n*(n-1)/2$)

Nombre de clés pour la cryptographie à clé secrète



$n=2, N=1$

$n=5, N=10$



$n=3, N=3$

$n=6, N=15$



$n=4, N=6$

$n=7, N=21$

$n=10, N=45$

$n=1000, N=499\,500$

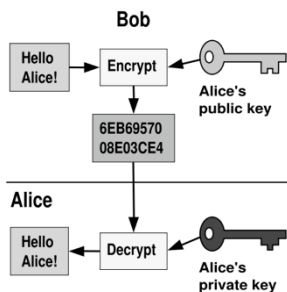
$$N = n(n-1) / 2$$

Les systèmes cryptographiques à clé publique

- Ces systèmes utilisent deux clés
 - Une clé privée et secrète
 - Une clé publique et accessible (dans les messages électroniques, dans les répertoires)
 - Sur Google : "BEGIN PGP PUBLIC KEY BLOCK"
- Les deux clés sont complémentaires
 - Ce qui est chiffré avec une, peut être déchiffré avec l'autre, et vice-versa
 - Ces systèmes sont particulièrement utiles pour échanger une clé secrète

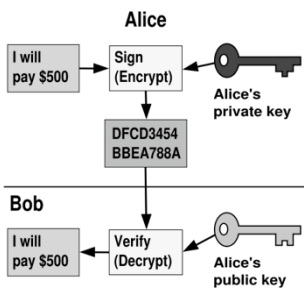
Cryptographie à clé publique - le cryptage

- Chaque participant possède 2 clés
- Celles-ci sont utilisées afin de permettre tant le chiffrage que la signature



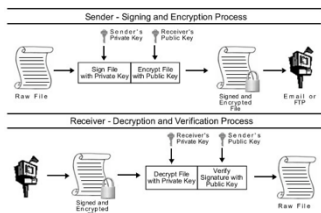
<http://www.consultants-online.co.za>

Cryptographie à clé publique - La signature électronique



<http://www.consultants-online.co.za>

Cryptographie à clé publique - Chiffrement d'un message signé



<http://blogs.microsoft.co.il/blogs/kim/archive/2009/01/23/pgp-zip-encrypted-files-with-c.aspx>

Les systèmes hybrides

- La cryptographie à clé publique est utilisée pour établir **une clé secrète de session**
- La clé de session permet de chiffrer les messages échangés au cours de la session
- La clé de session est oubliée à la fin de la session
- Intérêt : le chiffage avec clé secrète est 1000 fois plus rapide!

Les codes vérificateurs

- Permette de vérifier l'intégrité des documents
- Il est souvent difficile de déceler les erreurs, particulièrement dans les messages inintelligibles
- Les numéro de greffe au Québec comportent un code vérificateur: 200-10-001808-059
- Autre exemple, les codes ISBN à 10 chiffres
 - 2-89451-022-5 ou 1-56592-428-2
- Vérification d'intégrité

2	8	9	4	5	1	0	2	2	5
---	---	---	---	---	---	---	---	---	---

10	9	8	7	6	5	4	3	2	1
----	---	---	---	---	---	---	---	---	---

20	72	72	28	30	5	0	6	4	5	242
----	----	----	----	----	---	---	---	---	---	-----

$242/11 = 0$, donc c'est valide

Fonction de hachage

- Il est souvent possible de produire un résumé d'un message
 - Le résumé aura, par exemple, 16 ou 32 octets (pour nos fins un octet équivaut à un caractère)
- Notion de fonction de hachage
 - Une fonction mathématique qui transforme une chaîne de caractère de longueur variable en une chaîne de longueur fixe, c'est-à-dire, une valeur de hachage ou un résumé

Fonction de hachage

- Dans une bonne fonction de hachage, tous les bits du résumé (image) sont influencés par tous les bits de la chaîne reçue (pré-image)
 - Si un bit est changé, au moins 50% des bits du résumé change
 - Étant donné une chaîne reçue et son résumé, il n'est pas réalisable informatiquement de produire une autre chaîne d'entrée produisant la même valeur de hachage, i.e. le même résumé
- Illustration: <http://www.dynamicguru.com/tools/md5.php>

Utilisation des fonctions de hachage

- Pour les signatures électroniques
- Pour l'intégrité
- Pour la certification
 - Un tiers, neutre, prépare le résumé d'un document, par exemple, une pièce d'identité électronique et le signe numériquement
 - Il pourrait même, ne par voir l'objet signée et ne signer que le résumé et produire ainsi une signature aveugle

Scénario de signature électronique

- Étapes pour le signataire
 - Produire un résumé du message
 - Chiffrer ce résumé avec la clé privée
 - Envoyer le message, éventuellement en clair, accompagné du résumé chiffré, i.e., de la signature
- Étapes pour le destinataire
 - Déchiffre la signature à l'aide de la clé publique
 - Produit un nouveau résumé du message
 - Compare le résumé résultant du déchiffrage avec celui qu'il a lui-même préparé
 - S'ils sont identiques, le message est intègre et il vient bien du signataire

La signature numérique

- **L.R.Q. c. C-1.1, art 39.** Quel que soit le support du document, **la signature d'une personne peut servir à l'établissement d'un lien entre elle et un document.** La signature peut être apposée au document au moyen de **tout procédé qui permet de satisfaire aux exigences de l'article 2827 du Code civil.**
- **C.c.Q, art. 2827.** La signature consiste dans l'apposition qu'une personne fait à un acte **de son nom** ou d'une **marque qui lui est personnelle** et qu'elle **utilise de façon courante**, pour manifester son **consentement.**

Apposition d'une marque personnelle

- En principe et en pratique, on peut apposer une marque personnelle dans un environnement numérique de plusieurs façons
 - En écrivant ses initiales au bas d'un message électronique
 - En collant une image de sa signature manuscrite
 - En utilisant la cryptographie à clé secrète
 - En utilisant la cryptographie asymétrique
 - Par une combinaison d'identificateur et de mot de passe

d.p.



Bibliographie

- De nombreuses encyclopédies offrent de bons articles introductifs sur la cryptographie
 - Comment ça marche (CCM), <http://www.commentcamarche.net>
 - Answers.com, <http://www.answers.com>
- Livres
 - Schneier Bruce, Secrets and Lies: Digital Security in a Networked World, 2004, John Wiley & Sons Canada, Ltd. ; ISBN: 0471453803



INTRODUCTION À LA CRYPTOGRAPHIE (SUITE)

Révision

- Cryptographie symétrique
- Cryptographie asymétrique

- L'une et l'autre peuvent servir à signer
- ... mais que vaut la signature d'Alice?

Identification et authentification

- Qui êtes-vous et pouvez-vous le prouver?
- Trois types d'approches sont disponibles. Elles se basent sur
 - Quelque chose que vous connaissez
 - Quelque chose que vous êtes
 - Quelque chose que vous avez
- Souvent les systèmes combinent ces éléments, par exemple, les guichets automatiques exigent la présentation d'une carte et la connaissance d'un mot de passe

Le certificat numérique

- Une réponse à ce besoin d'identification et d'authentification en contexte de réseau
 - Un document officiel attestant d'une chose
 - En pratique, le certificat atteste notre identité dans un monde numérique
- Le certificat est émis par un prestataire de service de certificats (autorité de certification)
- Dans le contexte actuel
 - Un certificat numérique atteste le plus souvent la relation entre une clé publique et un site web

La certification selon la *Loi concernant le cadre juridique des technologies de l'information* (L.R.Q., chapitre C-1.1)

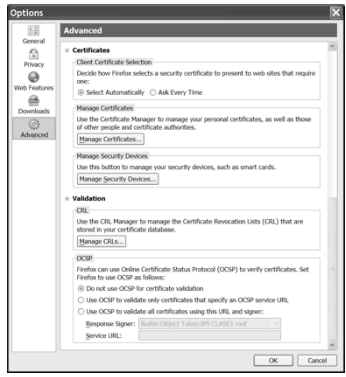
- Chapitre III : L'établissement d'un lien avec un document technologique
 - Section III : La certification
- Ainsi, en droit québécois, la question est abordée comme étant celle de l'établissement d'un lien entre une personne ou une organisation et un document technologique

La certification selon la *Loi concernant le cadre juridique des technologies de l'information* (L.R.Q., chapitre C-1.1)

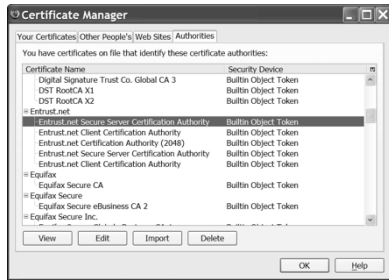
- Certificat.

47. Un certificat peut servir à établir un ou plusieurs faits dont la confirmation de l'identité d'une personne, de l'identification d'une société, d'une association ou de l'État, de **l'exactitude d'un identifiant d'un document ou d'un autre objet**, de l'existence de certains attributs d'une personne, d'un document ou d'un autre objet ou encore du lien entre eux et un dispositif d'identification ou de localisation tangible ou logique.

Exemple de certificat



Exemple de certificat



Exemple de certificat

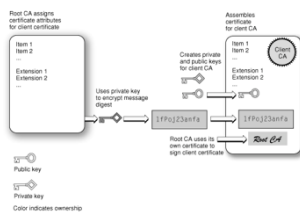


Exemple de certificat



La préparation d'un certificat

- L'utilisateur fournit
 - Son nom
 - Sa clé publique
- L'utilisateur établit la fiabilité des renseignements demandés selon les exigences de l'autorité de certification
- L'autorité de certification prépare un certificat de durée limitée



Source de l'illustration : http://developer.apple.com/documentation/Security/Conceptual/Security_Overview

Demande d'un certificat pour un serveur

- La préparation d'un « Certificate Signing Request » (CSR)
- Inscription de la demande auprès d'un organisme de certification
 - Exemple : Entrust
- Vérifications par l'autorité de certification des informations reçues et le cas échéant préparation du certificat

Inscription de la demande auprès d'une autorité de certification

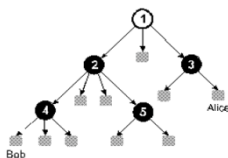
- Autres informations requises
 - La durée du certificat
 - Choisir un mot de passe
 - Le type de logiciel où le certificat sera installé
- Identification des personnes ressources
 - L'individu qui autorise
 - Le contact technique
 - L'individu devant recevoir la facturation
- Le nom d'entreprise doit être le même que celui apparaissant dans le CSR (O)

Vérifications qui sont menées par l'autorité de certification

- À titre d'exemple, les vérifications menées par Entrust ont trait
 - Au droit de faire affaires sous la raison sociale inscrite dans la demande
 - À la propriété du nom de domaine, le nom de l'entité propriétaire du nom de domaine doit être le même que celui fournit dans le CSR
 - La validité des informations du CSR
- Entrust procède également à la vérification de la demande de certificat auprès de l'organisation elle-même

Les infrastructure à clé publique (ICP)

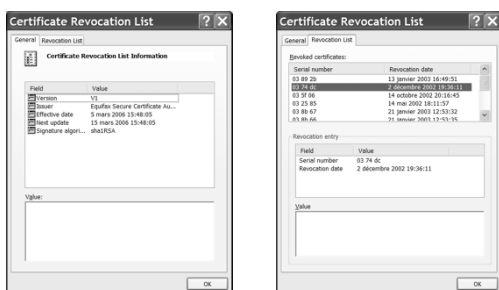
- En anglais, Public Key Infrastructure (PKI)
- Comment Alice vérifie le certificat de Bob si l'autorité de certification (1) est reconnue par Alice?



La révocation des certificats

- Les certificats comportent une durée de vie : validity not before, not after, par exemple:
 - Le certificat d'un professeur : 5 ans, celui d'un étudiant : 1 ans
- Il faut parfois annuler ou révoquer les certificats
 - Si le professeur est congédié, s'il change d'emploi, si sa clé a été compromise
- Voir : <http://www.geotrust.com/resources/crls/index.asp>

Exemple de liste de certificats révoqués



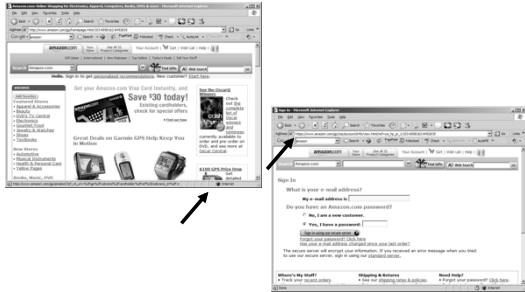
Chiffage et signature

- Doit-on utiliser plus d'une paire de clés?
- Certains systèmes utilisent deux paires de clés
 - Une paire de clés pour la signature
 - Une paire pour le chiffage

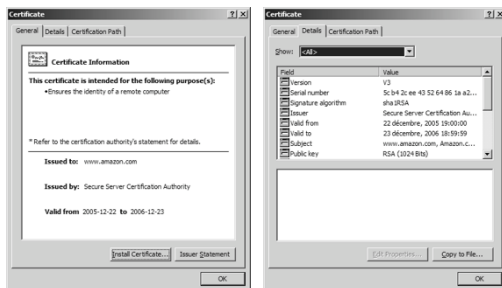
Secure Sockets Layer (SSL)

- Un protocole permettant des échanges protégés entre un serveur authentifié et un client qui ne l'est pas
- SSL, ou TLS (Transport Layer Security), est devenu la norme de facto en matière de transactions sécurisées sur le Web
- SSL assure la confidentialité, l'intégrité et l'authentification par la mise en œuvre de
 - Chiffrement (symétrique et asymétrique)
 - Signature numérique (chaque message est signé)
 - Certificat numérique (obligatoire pour le serveur)

Exemple d'utilisation de SSL



Exemple d'utilisation de SSL



Fonctionnement de SSL

1. Le client envoie une requête pour une connexion avec sécurité (https://...) comprenant :
 - La liste des algorithmes de chiffrement et de compression ainsi que la version la plus avancée du protocole SSL qu'il reconnaît;
2. Le serveur envoie son certificat et son choix de paramètres
3. Le client vérifie si le certificat provient d'une autorité de certification de confiance
 - En pratique, les certificats préinstallés dans le navigateur jouent ici un grand rôle
 - Le client vérifie le certificat et compare l'information avec celle qu'il reçoit du site: nom de domaine, clé publique
4. Si OK, le client génère une clé de session, une clé de cryptographique symétrique, et la retourne en la chiffrant avec la clé publique du serveur
5. Le serveur reçoit le message contenant la clé de session, le déchiffre et s'authentifie auprès du client en lui retournant un message chiffré avec la clé reçue
6. Le serveur et le client utilisent ensuite la clé de session dans leurs échanges
7. À la fin de la session, la clé est abandonnée

Récapitulation

- Cryptographie symétrique
- Cryptographie asymétrique
- Préparation de résumés et fonction de hachage

Fonction de hachage

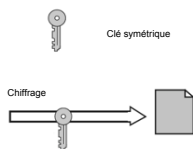
- Procédé cryptographique permettant de préparer un résumé de hachage ou empreinte d'un document
- Ce que l'on résume est de taille quelconque et le résultat de hachage est de taille prédéterminée et relativement petite
- Les fonctions de hachage sont des fonctions à sens unique, il est extrêmement difficile de modifier un message sans modifier le résumé de hachage

Les fonctions de hachage



Cryptographie symétrique

- Procédé cryptographique selon lequel une même clé est utilisée pour chiffrer et déchiffrer le message
- Ces systèmes posent généralement le problème de la distribution des clés
- Les systèmes cryptographiques symétriques chiffrent et déchiffrant 1 000 fois plus rapidement que leur alternative asymétrique



Cryptographie asymétrique

- Procédé cryptographique selon lequel une paire de clés complémentaire est utilisée
- Ce qui est chiffré avec une ne peut être déchiffré qu'avec l'autre
- L'une de ces clés est privée, l'autre publique
- Les systèmes sur le marché offrent souvent deux paires de clés
 - Les clés d'échange ou de chiffrement, privée et publique

