LARRE Jean-Christophe
BOUKHOUROU Sophiane

License Informatique 2003-2004

LA CRYPTOGRAPHIE

Encadrement : Sandrine Julia

I INTRODUCTION

Depuis Les débuts de l'écriture et des grandes civilisations, la cryptographie a été nécessaire, particulièrement en temps de guerre, pour faire passer un message d'un front à un autre, en gardant le secret, bien évidemment.

Le mot « Cryptographie » désigne l'ensemble des techniques permettant de chiffrer des messages et de les rendre inintelligibles.

La cryptographie est donc traditionnellement utilisée pour dissimuler des messages aux yeux de certaines personnes. Cet interet est aujourd'hui d'autant plus grand que les ordinateurs et le réseau Internet se sont considérablement développés.

Elle est désormais indispensable pour préserver la sécurité et la confidentialité des données, mais aussi leur intégrité et leur authenticité (nous verrons tout de suite après les définitions), particulièrement dans un point de vue économique avec la multiplication des entreprises sur Internet, avec par exemple le commerce électronique où la cryptographie joue un rôle plus que considérable avec la gestion des paiements, on pense surtout aux paiements par carte bancaire.

Nous verrons donc diverses techniques de cryptages, depuis l'Antiquité jusqu'à nos jours, et surtout où retrouve-t-on la cryptographie dans l'informatique contemporaine.

SOMMAIRE

I Introduction

II Cryptographie Par Substitution

1) Substitution Monoalphabétique

- Le Chiffre de Cesar

2) Substitution Polyalphabétique

- Le Chiffre de Vigenere

III Cryptographie Par Transposition

La Technique Assyrienne

IV Cryptographie Moderne

1) Cryptographie à Clé Privée

- DES
- AES

2) Cryptographie à Clé Publique

- RSA

V Applications de la Cryptographie

1) Sécuriser le Réseau Internet

- Problématique
- Notion de Certificats
- Les protocoles de Sécurité
    - Le Protocole **SSL**
    - Le Protocole **S-http**
    - Le Protocole **SET**

2) Sécuriser un Shell à Distance : SSH

- Présentation de SSH
- Fonctionnement de SSH

VI Conclusion

VII Bibliographie

II/ Cryptographie par Substitution

1) Substitution Monoalphabétique

Intro :

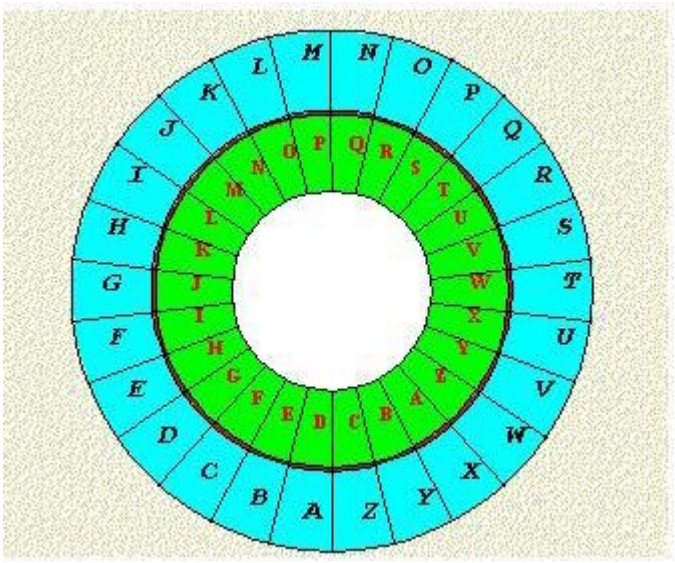
Le codage par substitution monoalphabétique, malgrès son nom quelque peu repoussant, est en réalité le plus simple a réaliser. Il s'agit de remplacer chaque lettre par une lettre différente. Rien de bien compliquer donc !

LE CHIFFRE DE CESAR

(Asterix par Goscinny et Uderzo)

Le chiffrement de César consiste simplement a effectuer une rotation d'un ou plusieurs crans, vers la gauche ou vers la droite, des lettres de l'alphabet.

Lorsque l'ajout d'une valeur donne une lettre dépassant la lettre Z, il suffit de continuer en repartant depuis la lettre A, ce qui revient donc a effectuer un modulo 26.



Par exemple, en décalant le message CRYPTOGRAPHIE de 3 crans, on obtient FUBSWRJUDSKLH.

On appelle « clé » le caractere correspondant à la valeur que l'on ajoute au message, par exemple, pour un décalage de 3, la clé est : C.

Curiosité amusante, en chiffrant le mot OUI avec un décalage de 10, on obtient YES.

MAIS …

Ce système de cryptage est donc très simple à mettre en oeuvre, ce qui lui vaut du même coup d'être assez peu sûr. En effet, le nombre de possibilités reste très faible, puisqu'il est égal au nombre de lettres de l'alphabet, c'est à dire que l'on a seulement 26 possibilités.

On peut donc facilement décrypter le message en effectuant successivement des soustractions de 1 à 26, jusqu'à ce que le message soit compréhensible.

Une autre méthode consiste à chercher les lettres qui réapparaissent le plus souvent. En effet, chaque langue a des lettres qui reviennent plus souvent que d'autre, par exemple en français, la lettre E a la plus grande fréquence. Ainsi, plus le message est long, plus il est facile de repérer cette lettre, et ainsi, on trouve la clé immédiatement.

ROT. 13

Le ROT. 13 désigne tout simplement le chiffrement de César, pour lequel on a effectué une rotation de 13 lettres. La clé est donc la lettre N. Il n'a pa été choisit pour cacher des informations, mais plutot pour pouvoir crypter et décrypter facilement des messages.

En conclusion, le chiffrement de César était intéressant dans l'Antiquité, il misait aussi beaucoup sur l'effet de « surprise », du point de vue que les ennemis ne connaissaient pas le « truc », mais aujourd'hui il reste vraiement basique et facile à « casser ».

2) Substitution Polyalphabétique

Intro :

L'exemple le plus connu est celui du « Carré de Vigenere » ou « Chiffre de Vigenere », qui porte le nom de Blaise de Vigenere (bien qu'il s'appuya sur les bases de Bellaso, Alberti, Porta et Trithème) en l'honneur de celui qui lui donna sa forme finale, lors de la publication de son œuvre : *Traicté des chiffres ou Secrètes manières d'écrire.*

Principe :

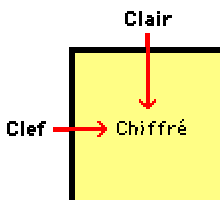
Il s'agit en réalité d'une amélioration du « Chiffre de César ». L'idée est d'utiliser la même méthode, mais en changeant le décalage de lettre en lettre. On n'utilise donc pas un, mais 26 alphabets, écrits en carré, et en décalant d'une lettre à chaque fois.

	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

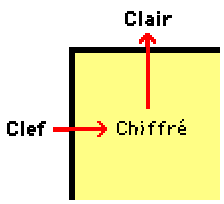
(Le Carré de Vigenere)

Pour coder un message, on choisit donc une clé de longueur arbitraire, en la répétant suivant la longueur du message à coder. On l'écrit ensuite au dessus du message à coder, par exemple de la façon suivante en prenant « CRYPTO » comme clé et en voulant coder « MESSAGE » :

C	R	Y	P	T	O	C
M	E	S	S	A	G	E



Chiffrer



Déchiffrer

Ici par exemple, pour la premiere lettre, le M, la clef sera la lettre C, on prend C dans la premiere colonne, et la lettre M dans la premiere ligne, la lettre codée se trouve a l'intersection de cette ligne et de cette colonne :

	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

(Codage de M avec C comme clé)

La lettre codée est le O. On obtient donc après avoir coder tout le message :

OVQHTUG

Pour déchiffrer un message, il suffit de faire la même operation en sens inverse, c'est à dire que sur la ligne de la lettre de la clé on recherche la lettre du message codé, la véritable lettre se trouve alors au sommet de la colonne correspondante.

Les points forts :

Il est facile d'utilisation, pour coder et décoder, et son plus grand interet est que la même lettre sera codée de différentes manieres. Ici par exemple, on voit que la lettre E a été codée respectivement V et G. Cela rend impossible l'analyse des fréquences d'apparition des lettres, comme on le disait précédement.

Les point faibles :

Bien plus sûr que le chiffrement de Cesar, ce chiffrement n'est pa pour autant « incassable ».

En effet, dans les cas ou le message est bien plus long que la longueur de la clé, il est possible de repérer cette longueur dans le message. Ainsi par exemple, pour une clé de longueur 3, on c que la premiere lettre du message est codée avec la premiere de la clé, la deuxieme avec la deuxieme, la troisieme avec la troisieme, et on revient, la quatrième avec la premiere…

Il suffit alors d'appliquer la recherche des frequences d'apparition des lettres pour déterminer un à un les caractères de la clef.

Une solution est donc de prendre une clé se rapprochant le plus possible de la longueur du message, mais cela devient très vite difficile a coder, et augmente les chances de commettre une erreur, ce qui rendrait alors le message indéchiffrable.

II/ Cryptographie par Transposition

Intro :

La cryptographie par transposition consiste simplement à réorganiser l'arrangement des lettres, et non pas à les transformer. Il s'agit de les transformer géométriquement, afin de les rendre visiblement non exploitables.

La Technique Assyrienne

Sans doute une des premières preuves de l'utilisation de la cryptographie chez les grecs, dès 600 Av JC pour dissimuler des messages écrits sur des papyrus.

La technique est simple :

- enrouler une bande de papyrus sur un cylindre appelé **scytale**
- écrire le texte longitudinalement sur la bandelette ainsi enroulée

Le message une fois déroulé n'est plus comprehensible, et pour le retrouver il faut avoir un cylindre de meme diametre ! Il est evident qu'il est très simple de casser ce cryptage.

III/ Cryptographie Moderne

Intro :

Avec le développement des ordinateurs, les techniques de cryptographie ont nettement évolué, jetant du même coup aux oubliettes les techniques de cryptage à la main. On distingue alors deux catégories de cryptographie. La cryptographie à clé privée, et la cryptographie à clé publique. Pour cette derniere, cela permet de s'échanger la clé publiquement, avec le message, tandis qu'avec la privée nécessite un partage de la clé en privé. (par exemple les valises diplomatiques pour les chefs d'Etats)

1) Clef Privée

DES (Data Encryption Standard)

Intro :

En 1973 le NIST *(National Institute of Standards and Technology*) fait un appel d'offres public pour un algorithme:

- Niveau de securité élevé
- Complètement spécifié et compréehensible
- Securité liée á la clef
- Disponible à tous les utilisateurs
- Adaptable à diverses applications
- Réalisé de façon économique
- Efficace
- Possible d'être validé
- Exportable

IBM propose Lucifer, qui aprés modification par la NSA, devient alors DES *(Data Encryption Standard)*

L'algorithme consiste à faire des combinaisons, des substitutions et des permutations entre le texte à chiffrer et la clé, en faisant en sorte que les opérations puissent se faire dans les deux sens (pour le déchiffrement). On appelle **code produit** la combinaison entre substitutions et permutations. La clé est codée sur 64 bits et formée de 16 blocs de 4 bits, généralement notés k_1 à k_{16}. Etant donné que "seulement" 56 bits servent réellement à chiffrer, il y a 2^{56} (soit $7.2*10^{16}$) possibilités de clés différentes !

Voici maintenant les grandes lignes de l'algorithme

1/ Après avoir été convertit en bits, le message est découpé par blocs de 64 bits.

2/ On calcule ensuite une permutation pour chaque bloc de 64 bits $y=P(x)$, avec $y=G_0D_0$, G_0 étant les 32 bits de gauche et D_0 les 32 bits de droite, c'est la permutation initiale.

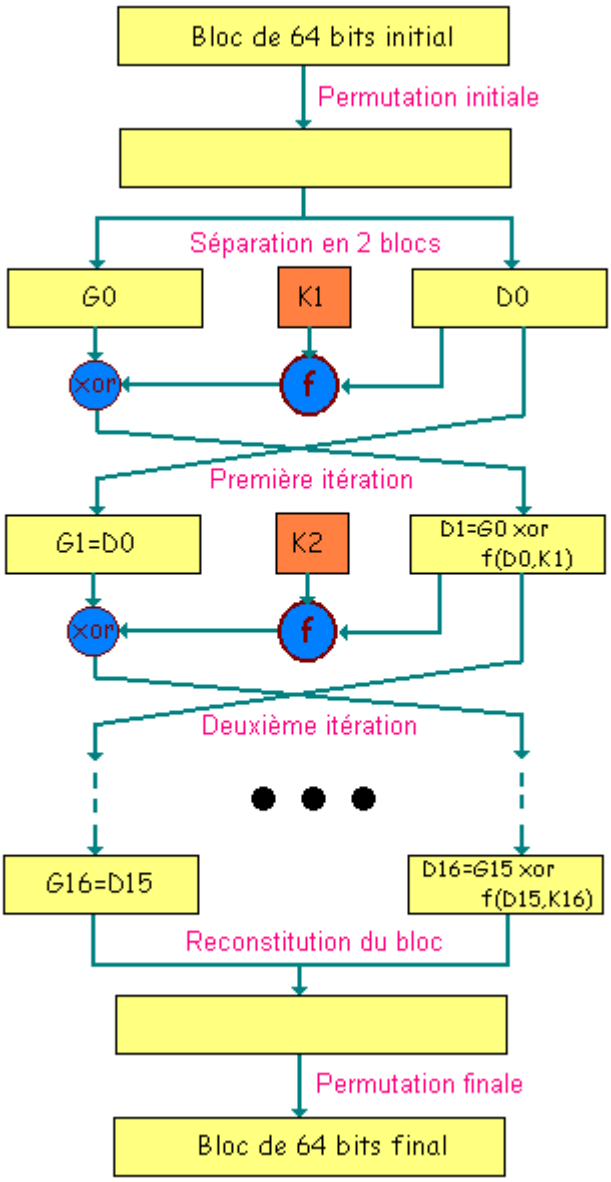
3/ On applique ensuite 16 rondes d'une même fonction sur $G_{i-1}D_{i-1}$ (i de 1 à 16). On calcule G_iD_i en posant :

$G_i = D_{i-1}$

$D_{i-1} = G_{i-1}$ XOR $f(D_{i-1}, K_i)$

Avec XOR le ou exclusif et f une fonction destinée à mélanger tout, c'est une suite de substitution et de permutations.

4/ On fait une ultime permutation, qui est en réalité la même permutation que la permutation initiale, mais en sens inverse.



Régulièrement, le DES a fait l'objet de polémiques. Toute sa sécurité repose sur la fonction de confusion f, et en particulier à l'intérieur de celle-ci sur des boîtes S, tableau 4x16 d'entiers compris entre 0 et 15, aux valeurs mystérieuses. Certains ont affirmé que la NSA, qui a finalisé l'algorithme, a placé dans ces boîtes S des trappes qui lui permettaient de tout décrypter, tout en affirmant que l'algorithme est sûr. Toutefois, rien n'a objectivement étayé cela. En particulier, le DES a toujours résisté aux travaux des cryptanalystes non basés sur la force brute.
Ce qui a définitivement tué le DES, n'est rien d'autre que l'extraordinaire progression de l'informatique, plus particulierement de la puissance des ordinateurs. Le 17 juin 1997, DES est cassé en 3 semaines par un groupe de petites machines sur Internet.

La solution a été dans un premier temps l'adoption du triple DES, trois applications de DES à la suite avec 2 clés différentes (d'où une clé de 112 bits) :

Le triple DES est suffisement efficace, cependant, il a très logiquement le défaut d'être trois fois plus lent que le DES. C'est pourquoi en 1997 le NIST lance à nouveau un appel d'offre pour trouver un remplaçant. L'algorithme choisit sera celui de deux belges : Vincent Rijmen et Joan Daemen, qui le baptiseront **RIJNDAEL** (prononcer Raindal).
Ce nouvel algorithme portera également le nom de AES *(Advance Encryption Standard)*

AES (Advanced Encryption Standard)

Intro :

L'AES *(Advanced Encryption Standard)* fut créé dans le but de remplacer DES, devenu trop faible au regard des attaques actuelles, et avec le développement de l'informatique. Il fut adopté dans les mêmes conditions que DES, à la suite d'un appel d'offre de la NIST, qui comportait les points suivants :

- évidemment, une grande sécurité.
- une large portabibilité : l'algorithme devant remplacer le DES, il est destiné à servir aussi bien dans les cartes à puces, aux processeurs 8 bits peu puissants, que dans des processeurs spécialisés pour chiffrer des miliers de télécommunications à la volée.
- la rapidité.
- une lecture facile de l'algorithme, puisqu'il est destiné à être rendu public.
- techniquement, le chiffrement doit se faire par blocs de 128 bits, les clés comportant 128,192 ou 256 bits.

L'alogrithme choisit est en réalité l'algorithme de **Rijndael**.

Pour comparaison, les clés DES ont une taille de 56 bits (64 en réalité, mais 8 bits servent pour les controles de parité), on a donc à peu près $7.2x10^{16}$ clés possibles. Avec l'AES on aura 10^{21} fois plus de clés 128 bits, que de clés 56 bits pour le DES.

Le Rijndael procède par blocs de 128 bits. Chaque blocs subit une séquence de 5 transformations répétées 10 fois :

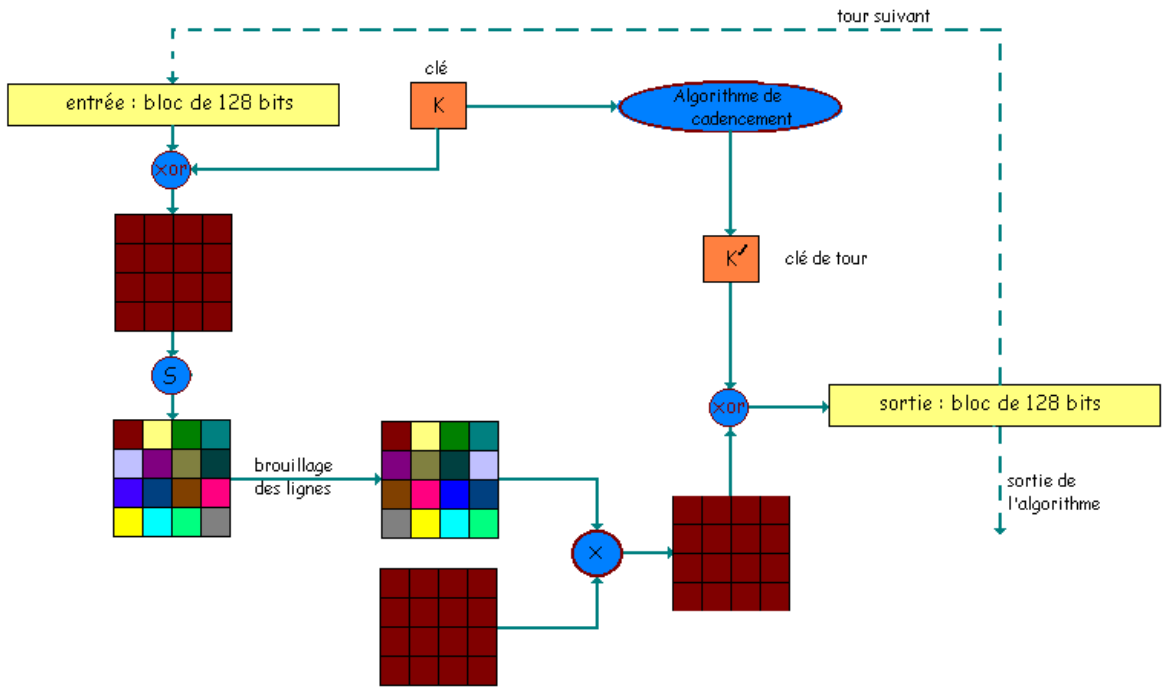
1/ **<u>Entrée</u>** : soit M le message (128 bits), et K la clé (également 128 bits), on ajoute K à M par le biais d'un OU EXCLUSIF : M⊕K

2/ **<u>Transformation non linéaire</u>** : on répartit les 128 bits en 16 blocs de 8 bits, dispatchés dans un tableau de 4x4, chaque octet est ensuite transformé par une fonction non linéaire S.

3/ **<u>Décalage de ligne</u>** : la ligne j (pour j de 1 à 4) est décalée circulairement de j-1 cases dans le tableau.

4/ **<u>Brouillage de colonne</u>** : Chaque colonne est transformée par combinaisons linéaires des différents éléments de la colonne (ce qui revient à multiplier la matrice 4×4 par une autre matrice 4×4). Les calculs sur les octets de 8 bits sont réalisés dans le corps à 2^8 éléments.

5/ **<u>Addition de la clé de tour</u>** : A chaque tour, une clé de tour est générée à partir de la clé secrète par un sous-algorithme (dit de cadencement). Cette clé de tour est ajoutée par un ou exclusif au dernier bloc obtenu.



En conclusion, l'AES est plus sûr que le 3DES car il présente, entre autres, une plus grande résistance aux attaques par dictionnaires de clés. Les autres attaques ne sont pas appliquables dans son cas.

2) Clef publique

Intro :

D'une façon imagée, voici comment on peut voir la cryptographie à clé publique : supposez qu'un ami doive vous envoyer quelque chose de très important par la poste, mais que vous n'ayez pas confiance en votre facteur. Vous envoyez alors, dans un premier temps, à votre ami, un cadenas en position ouverte. Votre ami le reçois, met ce qu'il devait vous envoyer dans une boite fermée avec le cadenas en question. Il n'a pa la clé de ce cadenas, le facteur non plus, et quand vous recevez la boite, vous etes le seul à pouvoir l'ouvrir.

Cette méthode de cryptographie à clé publique est apparu en 1976, avec la publication d'un ouvragesur la cryptographie par *Whitfield Diffie* et *Martin Hellman*.

La cryptographie à clé publique repose exactement sur ce principe. On dispose d'une fonction P sur les entiers, qui possède un inverse S. On suppose qu'on peut fabriquer un tel couple (P,S), mais que connaissant uniquement P, il est impossible (ou au moins très difficile) de retrouver S.

- P est la clé publique, que vous pouvez révéler à quiconque. Si Louis veut vous envoyer un message, il vous transmet P(message).
- S est la clé secrète, elle reste en votre seul possession. Vous décodez le message en calculant S(P(message))=message.
- La connaissance de P par un tiers ne compormet pas la sécurité de l'envoi des messages codés, puisqu'elle ne permet pas de retrouver S. Il est possible de donner librement P, qui mérite bien son nom de clé publique

Bien sûr, il reste une difficulté : comment trouver de telles fonctions P et S. Diffie et Hellman n'ont pas eux-même proposé de fonctions satisfaisantes, mais dès 1977, D.Rivest, A.Shamir et L.Adleman trouvent une solution possible, la meilleure et la plus utilisée à ce jour, la cryptographie RSA. Le RSA repose sur la dichotomie suivante :

- il est facile de fabriquer de grands nombres premiers p et q (pour fixer les idées, 100 chiffres).
- étant donné un nombre entier n=pq produit de 2 grands nombres premiers, il est très difficile de retrouver les facteurs p et q.

La donnée de n est la clé publique : elle suffit pour chiffrer. Pour décrypter, il faut connaitre p et q, qui constituent la clé privée.

RSA (Rivest – Shamir – Adleman)

Intro :

RSA est toujours aujourd'hui la méthode de cryptographie la plus utilisée et reste encore très sûre, bien que l'on sache comment casser le code (factorisation de grands entiers), mais cela prendrait tellement de temps qu'il n'y a aucun interet. Le record avec les meilleurs algorithmes, et le meilleur materiel mis a disposition est la factorisation d'un entier à 155 chiffres, soit l'equivalent d'une clé de 512 bits ($2^{512} \approx 10^{155}$). Il faut donc, pour garantir une bonne sécurité, choisir des clés bien plus grande. Les experts recommandent des clés de 768 bits pour un usage privé, et de 1024 ou 2048 bits pour des sujets plus sensibles. Si on suppose que la puissance des ordinateurs double tous les 18 mois (Loi de Moore), alors une clé de 2048 bits tiendrait jusqu'en 2079 !

Il est intéressant de remarquer que son invention est fortuite : au départ, Rivest, Shamir et Adleman voulaient prouver que tout système à clé publique possède une faille.

Algo :

1. **Création des clés** : Bob crée 4 nombres p,q, e et d :
   - p et q sont deux grands nombres premiers distincts.
   - e est un entier premier avec le produit (p-1)(q-1).
   - d est tel que ed=1 modulo (p-1)(q-1). Autrement dit, ed-1 est un multiple de (p-1)(q-1). On peut fabriquer d à partir de e, p et q, en se servant de l'algorithme d'Euclide.
2. **Distribution des clés :** Le couple (n,e) constitue la clé publique de Bob. Il la rend disponible par exemple en la mettant dans un annuaire. Le couple (n,d) constitue sa clé privée. Il la garde secrète. (Voir certificats et signatures plus loin)
3. **Envoi du message codé :** Alice veut envoyer un message codé à Bob. Elle le représente sous la forme d'un ou plusieurs entiers M compris entre 0 et n-1. Alice possède la clé publique (n,e) de Bob. Elle calcule $C=M^e \bmod n$. C'est ce dernier nombre qu'elle envoie à Bob.
4. **Réception du message codé** : Bob reçoit C, et il calcule grâce à sa clé privée $D=C^d \pmod n$. D'après un théorème du mathématicien Euler, $D=M^{de}=M \pmod n$. Il a donc reconstitué le message initial.

Faiblesse :

La cryptographie RSA est unanimement considérée comme un système très sûr. Mais, mal utilisée, elle peut être aussi catastrophique. Supposons par exemple que Bob souhaite envoyer le même message M à 3 correspondants. Ces derniers ont pour clés publiques RSA : (n_1,e_1); (n_2,e_2); (n_3,e_3). Souvent, afin de simplifier les calculs, on choisit l'exposant e le plus petit possible, c'est-à-dire 3 (c'est par exemple l'exposant utilisé dans le système des cartes bleues). Nous supposons donc que $e_1=e_2=e_3=3$.

Bob envoie à ses 3 correspondants $C_1=M^3 \bmod n_1$, $C_2=M^3 \bmod n_2$, et $C_3=M^3 \bmod n_3$. Si Alice écoute la conversation, elle intercepte les 3 nombres C_1, C_2 et C_3. En utilisant le théorème des restes chinois, elle peut trouver très facilement, et très rapidement, un entier C tel que $C=M^3 \bmod (n_1n_2n_3)$. Maintenant, on sait que $M<n_1$, $M<n_2$, $M<n_3$. On a donc $M^3<n_1n_2n_3$. Le calcul de la racine cubique $C^{1/3}$ n'est plus un calcul de logarithme discret, mais simplement la prise de la racine cubique usuelle (très rapide!). En calculant $C^{1/3}$, Alice retrouve le message initial M sans le moindre effort!

La parade est très simple pour Bob : il suffit qu'il envoie aux 3 destinataires un message différent, en introduisant aléatoirement des espaces par exemple.

Conclusion

L'algorithme RSA, reste le meilleur moyen du moment, mais tout comme les autres algorithmes de cryptographie a clé publique, est très lent.

V Applications de la Cryptographie

1) Sécuriser Le Réseau Internet

a) PROBLEMATIQUE

Souvent on envoie des donnes confidentielles avec Internet, ces échanges doivent être cryptés pour garantir la confidentialité. La cryptographie est aujourd'hui un outil indispensable pour naviguer sur le Web en toute sécurité. Peut-être vous avez déjà commandé sur un site marchand, vous avez fournit votre numéro de carte bancaire, tous ces échanges doivent être confidentiels et sécurisés, il ne faudrait pas qu'une personne malveillante puisse récupéré ce numéro en usurpant de l'identité du site marchand.

Ainsi, des protocoles de sécurité ont été définit. Ces protocoles sont très utilisés dans le domaine du commerce électronique. Il existe plusieurs protocoles mais le plus populaire et le plus utilisé est le protocole SSL. Ces protocoles utilisent pour la plupart des certificats électroniques.

b) LA NOTION DE CERTIFICATS

RSA comme tout autre algorithme de chiffrement asymétrique repose sur le partage d'une clé publique.

La distribution de la clé n'est pas sans risque: Comment s'assurer de l'identité du propriétaire de la clé? Comment garantir que la clé est bien celle de l'utilisateur à qui elle est associée? Un individu pourrait modifier ou carrément la remplacer par sa clé publique. Il pourra ensuite déchiffrer tous les messages chiffrés avec cette clé. C'est pour résoudre cette usurpation d'identité qu'on a conçu le certificat.

Certificats numériques:

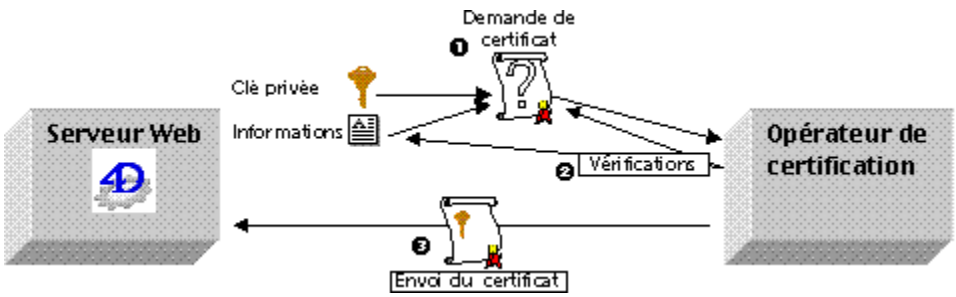
Le certificat est un petit fichier électronique confirmant qu'une clé publique appartient bien à une entité. Il a le même rôle qu'une pièce d'identité. Il contient quelques informations parmi lesquelles:

- le nom de l'autorité de certification
- la validité du certificat
- le nom du propriétaire du certificat
- l'algorithme de chiffrement utilise
- la clé publique du propriétaire

Il est délivré par l'autorité de certification.

Autorité de certificats

C'est l'organisme qui délivre le certificat électronique. Des règles strictes permettent d'établir avec certitude l'identité d'un serveur par exemple. Elle a la même fonction qu'une préfecture qui délivre une pièce d'identité.



c) LES PROTOCOLES DE SECURITE

Le Protocole SSL

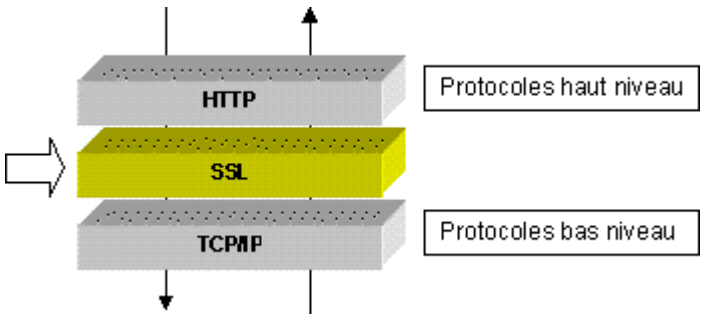
Présentation de SSL

Il a été mis au point par la société Netscape en 1994 en collaboration avec Mastercard, Bank of America, MCI et Silicon Graphics pour la transmission de données confidentielles. Aujourd'hui il est présent dans la plupart des navigateurs Web comme Microsoft Explorer et Mozilla. Il est à l'origine d'une volonté de sécuriser les transactions électroniques. Il est très utilise dans le commerce électronique.

SSL utilise la cryptographie à clé publique RSA.

Fonctionnement de SSL

Au niveau de l'architecture, c'est une couche intermédiaire. Elle n'est pas liée à une application en particulier ce qui lui permet d'être compatible avec http, ftp, telnet, etc. Ssl sécurise les protocoles existants de façon transparente.



Les trois principaux objectifs de SSL sont :

- **authentification**: l'assurance de l'identité de l'entité

Cela permet un utilisateur d'avoir une confirmation de l'identité d'un serveur.
En effet un programme client SSL utilise des méthodes de chiffrement à clé publique pour vérifier si le certificat et l'identité publique fournis par le serveur sont valides et ont été fournis par un fournisseur de certificat présent dans la liste de ceux connus du client.

Cette fonctionnalité est importante dans la mesure où le client doit envoyer des données confidentielles comme son numéro de carte bleue. Elle se réalise en utilisant l'algorithme asymétrique.

- l**a confidentialité** des échanges

Toutes les données issues de l'entité émettrice sont chiffrées et déchiffrées par l'entité réceptrice, ce qui permet de garantir la confidentialité des données.

- **l'intégrité** des données

Le transport du message inclut un message de vérification d'intégrité.

Comment garantir l'intégrité des données transmises ?

MAC - Message Authentification Code :

Cette méthode consiste à utiliser un algorithme de chiffrement par blocs en mode chaîné. On peut par exemple chiffrer les données à l'aide d'un DES en mode CBC puis considérer le dernier bloc comme étant le MAC. Le destinataire ne pourra vérifier l'intégrité des données que s'il possède la clé symétrique ayant servi à la génération du MAC. Contrairement à la signature digitale, seul un destinataire particulier sera en mesure de faire cette opération.

L'utilisation de MAC (monde bancaire) n'assure pas vraiment la non répudiation (l'émetteur des données ne peut pas nier être à l'origine du message) : les destinataires possèdent en effet la même clé symétrique que l'expéditeur. Ce dernier peut donc légitimement nier avoir signé telles données en générant un MAC, arguant du fait qu'il n'est pas le seul à pouvoir le faire. Il faut s'assurer d'un canal sûr pour transmettre la clé symétrique.

HMAC - Hashed Message Authentification Code :

On peut aussi joindre aux données à signer une chaîne aléatoire de bits, puis passer le tout au travers d'une fonction de hachage pour obtenir le HMAC, ou « keyed-MAC ». Le destinataire recalcule un HMAC à l'aide du code qu'il partage avec l'expéditeur. Si les deux MACs sont égaux, il est assuré de l'intégrité des données et de l'authenticité de la signature (encore faut-il que chaque code soit associé de façon non équivoque à deux identités). L'utilisation de HMAC n'assure pas non plus la non répudiation, et l'échange sécurisé des codes est aussi à gérer.

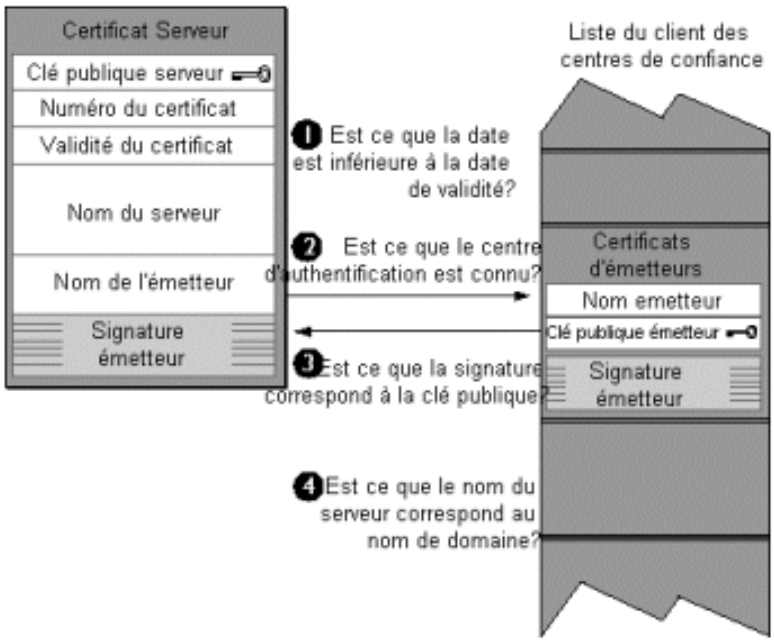
Deux phases constituent l’étape d’authentification :

Première phase : authentification du serveur

Suite à la requête d'un client, le serveur envoie au client son certificat et lui liste les algorithmes qu'il peut utiliser. Le client vérifie la validité du certificat (à l'aide de la clé publique du CA contenue dans son navigateur, des dates de validité et, éventuellement, en consultant une signature (rarement dans la pratique), puis, si le certificat est valide, génère une clé maître (symétrique), la chiffre à l'aide de la clé publique du serveur et la lui envoie. Les données échangées par la suite entre le client et le serveur sont chiffrées et authentifiées à l'aide de clés dérivées de la clé maître.

Deuxième phase : authentification du client

Le serveur envoie au client un challenge (une petite série de bits) que le client doit signer, à l'aide de sa clé privée correspondant à son certificat, et le renvoyer au serveur pour s'authentifier. Il lui envoie de même son certificat, que le serveur vérifiera avant de poursuivre les transactions.



SSL présente toute de même quelques inconvénients il n'évite pas la non répudiation, et l'entité réceptrice obtient les informations confidentielles.

Non répudiation :

Il s'agit de garantir l'authenticité de l'acte. L'émetteur ou le récepteur ne peut pas nier le dépôt ou la remise de l'information, ni le contenu de cette information.

Les protocoles qui sont présentés dans la suite peuvent résoudre ce problème.

Le protocole S-HTTP

S-HTTP permet de sécuriser les transactions du protocole http, c'est simplement une extension du protocole http. S-HTTP a été conçu par EIT (Enterprise Integration Technologies) mais n'est pas aussi populaire que SSL. Il est supporté par très peu de navigateurs parmi lesquels Mosaic.

A l'oppose de SSL qui permet de sécuriser la connexion entre le client et le serveur, S-HTTP assure le chiffrement de chaque message séparément, au niveau applicatif. Il n'est pas indépendant de l'application. L'entête de chaque message envoyé contient les préférences cryptographiques du destinataire et de l'expéditeur ce qui permettra à expéditeur de déchiffrer le message.

En plus de la confidentialité et de l'authentification, la non répudiation est garantit à la différence de SSL.

SSL et S-HTTP ne sont pas concurrents car ils agissent à deux niveaux protocolaires différents. SSL sécurise la connexion Internet tandis que S-http les transactions http. Certaines compagnies ont utilisé cette complémentarité pour développer des applications pour la sécurité intégrant les deux protocoles.

Le protocole SET

Le protocole SET (Secure Electronic Transactions) créé par MasterCard et Visa a été développé pour sécuriser les transactions électroniques (paiements par carte bancaire).

La sécurité des échanges se fait non seulement avec le commerçant et l'acheteur mais aussi avec leurs banques respectives. Pendant la transaction, le client n'envoie pas les données confidentielles au marchand mais seulement la commande. Le numéro de la carte bancaire est envoyé à la banque du commerçant qui vérifie en temps réel les coordonnées bancaires en contactant la banque du client.

L'avantage principal est que le vendeur n'a pas accès à des informations telles que le numéro de carte bancaire du client contrairement à ssl.

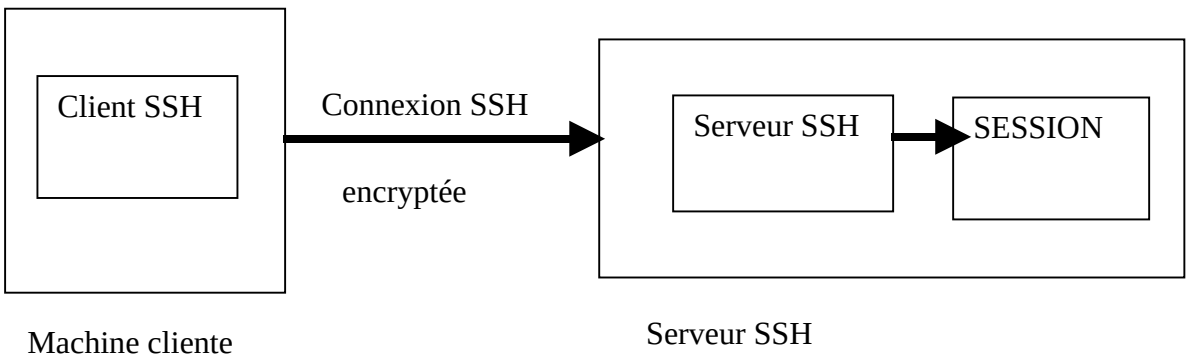
2) SECURISER UN SHEEL A DISTANCE : SSH

a) Présentation de SSH

Les méthodes permettant de se connecter à un autre système à distance sont très nombreuses : telnet, rlogin ou rsh mais elles ne sont pas sécurisés. SSH (ou *S*ecure *SH*ell) est un protocole servant à créer une connexion sécurisée entre deux systèmes. SSH permet de réduire les risques de sécurité pour votre système et le système distant.

Il existe deux versions de SSH, SSH1 présente une faille, un pirate peut très bien introduire des données dans le flux chiffré. SSH2 est sorti en 1997 pour corriger cette faille.

SSH étant un service fonctionnant au niveau applicatif, son utilisation n est pas transparente pour l utilisateur, il nécessite l installation du logiciel SSH (ou SSF) sur le poste utilisateur.



b) Le fonctionnement de SSH

Le fonctionnement de SSH se décompose en deux étapes :

- Mise en place du canal sécurise
- Authentification du client

On détermine tout d'abord l'algorithme asymétrique et symétrique utilisée en s'échangeant les algorithmes supportés par le client et le serveur. Pour le chiffrement asymétrique on a le choix entre RSA et DSA.

Ensuite le serveur envoie la clé publique du serveur et hote(la machine), le client crée alors une clé de session, il la chiffre grâce aux 2 clés publiques (serveur et hote) puis l'envoie au serveur. Le serveur est capable de déchiffrer grâce à ses clés privées. Le serveur alors répond au client par un message de confirmation crypté.

Lors d'une première connexion à la machine, un message demandant l'enregistrement de la clé hote du serveur apparaît :

Host key not found from the list of known hosts.
Are you sure you want to continue connecting (yes/no)?

Ainsi la clé publique du serveur est enregistrée dans le fichier known_host et lors des prochaines sessions la connexion se fera automatiquement.

La communication est cryptée par la clé de session partagée par le client et le serveur ce qui garantit la confidentialité des échanges Tous les échanges sont désormais chiffrées par l'algorithme symétrique choisit.

Une fois le canal sécurise etablit on peut commencer l'authentification du client.
SSH autorise deux types d'authentification :

- Par mot de passe
- Par couple de clé (algorithme asymétrique)

La première méthode est la plus utilisée, le client donne son login et son mot de passe, puis le serveur vérifie que le client existe et a accès à la machine distante, ensuite le client peut se connecter à cette machine.

Au lieu de se connecter par mot de passe on a la possibilité de se connecter en utilisant un couple de clés publiques/privées. Ce couple de clé est généré, la clé privée est stockée dans ~/.ssh/id_dsa et la clé publique dans ~/.ssh/id_dsa.pub.
Pour crypter cette clé privée un passphrase est demande permettant de crypter le fichier contenant la clé privée utilisée Ssh-agent est un mécanisme permettant de ne pas répéter cette étape, la passphrase est conservée.

Quelque ce soit la méthode utilisée ssh présente de nombreux avantages si l'on compare aux autres protocole d'accès à distance :

- Authentification des machine par couple de clé publique/privée, ce qui est plus efficace que l'utilisation de nom et adresse de machine que propose telnet par exemple.
- Les données ne circulent pas sur le réseau en clair mais sont chiffrés en utilisant une clé partagée ce qui diminue le risque de lire les données en clair.
- Il existe plusieurs niveaux d'identification de l'utilisateur.

VI CONCLUSION

La cryptographie a fait ces débuts avec l'empire romain, ensuite c'est l'armée et les services de renseignements qui l'ont intégré. Depuis Internet, le besoin de confidentialité et de sécuriser les échanges n'a cesser de progresser et la cryptographie s'est imposée dans la société. Le domaine d'application de la cryptographie s'est agrandit, divers secteurs l'ont adopté :

La télévision pour crypter les chaînes payantes (Canal +,CanalSatelllite, …)
Les cartes bancaires pour chiffrer le code accès
Les communications par réseau (on utilise des protocoles de sécurité)
Le commerce électronique…

Même si RSA et les algorithmes utilisés actuellement sont difficilement attaquable. Toutefois tous les systèmes de cryptographie vus jusqu'à présent ne sont pas infaillibles à long terme. Les progrès de la cryptanalyse conduisent sans cesse à corriger ou modifier les algorithmes de chiffrement symétriques et asymétriques.

Le problème réside dans le fait que les deux techniques de cryptographie public ou privée ne permettent pas de savoir si le message crypté émis a été intercepté par un individu autre que le destinataire prévu. Par contre avec la cryptographie quantique, un individu autre que le destinataire serait immédiatement intercepté. Ce système est une véritable révolution, il rendrait inviolable les messages cryptés.

Malheureusement, ce n'est que de la théorie les ordinateurs quantiques ne sont pas prévus pour demain et les algorithmes de chiffrement doivent faire face au perfectionnement des techniques de cryptanalyse.

VII BIBLIOGRAPHIE

http://www.commentcamarche.net/crypto/crypto.php3

http://www.bibmath.net/crypto/plan.php3

http://www.uqtr.ca/~delisle/Crypto

http://people.via.ecp.fr/~alexis/formation-linux/ssh.html

http://www.dockpacks.tchom.ch/data/Cryptographie/