La cryptographie

I) Définition, But et Histoire

Etymologie:
La cryptographie vient du grec *kruptos* qui veut dire caché et de *graphein* qui signifie écrire.
La cryptographie est donc un ensemble des techniques permettant de protéger une communication au moyen d'un code graphique secret.
Etant donné qu'une lettre ou une communication téléphonique peuvent êtres interceptées par un individu mal intentionné, il est prudent de rendre le message incompréhensible à l'aide de la cryptographie.
Depuis Jules César, qui a été sans doute le premier a l'utiliser pour communiquer avec ses troupes, jusqu'à l'armée allemande qui s'est servie de machines électromécaniques lors de la deuxième guerre mondiale, la cryptographie a fait d'énormes progrès avec l'arrivée de l'informatique.
Car la cryptographie se sert de la puissance des ordinateurs et des progrès mathématiques pour rendre tout message incompréhensible par un tiers.

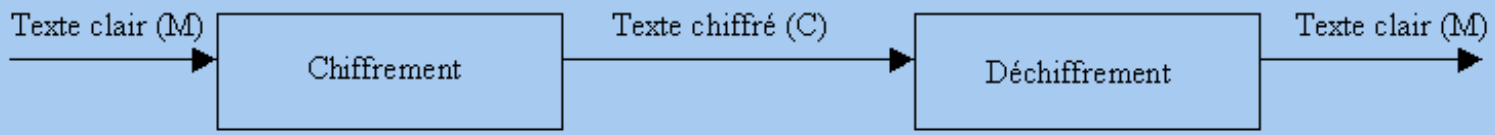
La cryptographie répond à différents besoins :

- La confidentialité : qui consiste à rendre l'information inintelligible à tous ceux qui pourraient intercepter le message.
- Le contrôle d'accès : qui permet de limiter l'accès aux données, serveurs aux personnes autorisées (mot de passe Unix, par exemple).
- L'intégrité des données : qui consiste à vérifier que cette donnée n'a pas été altérée frauduleusement.
- L'identification : qui permet d'assurer de l'authentification des partenaires et de l'origine des message.
- La non répudiation : pour que les partenaires ne puisse nier le contenu des informations.

La cryptographie sert aujourd'hui lors des transactions bancaires, et par exemple, sur Internet pour les paiements à distances et aussi pour l'envoi d'émail sécurisé ou bien encore lors des conversations avec téléphone cellulaires.

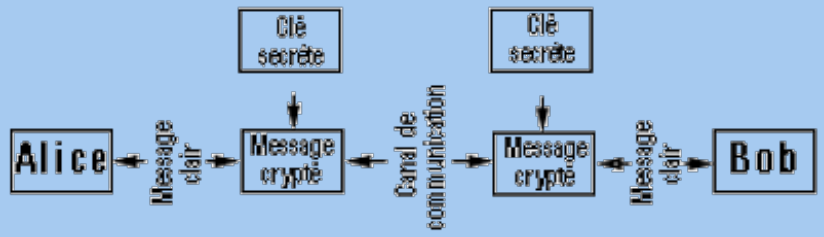
II) Les différents algorithmes

Tout système de cryptage est composé d'un algorithme de codage plus ou moins compliqué utilisant ou non une ou plusieurs clés de sécurité et il est, en principe, conçu de manière à être inviolable.
La cryptographie nécessite deux fonctions :
Le message M en clair est crypté par une fonction d'encryptage E(M)=C et le cryptogramme C est décrypté par le destinataire par une fonction de décryptage D(C)=M, d'où ***D(E(M))=M***.

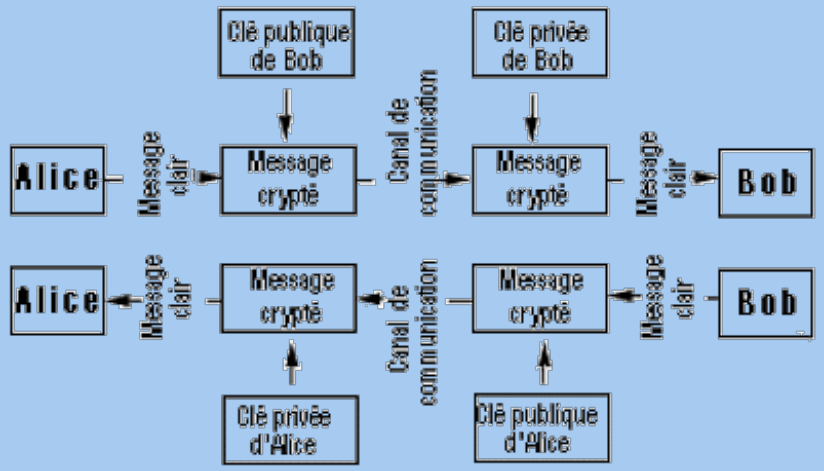


PDF created on http://www.htm2pdf.co.uk via the HTML to PDF API

La notion de clef :
Il existe deux grands types de cryptographie :
- La cryptographie symétrique ou a *clef secrète* : la même clé (le code secret) est utilisée pour encrypter et décrypter l'information. Le problème de cette méthode est qu'il faut trouver le moyen de transmettre de manière sécurisée la clé à son correspondant.



- La cryptographie asymétrique ou a *clef publique* : ce n'est pas la même clé qui crypte et qui décrypte les messages. L'utilisateur possède une clé privée et une clé publique. Il distribue sa clé publique et garde secrète sa clé privée. Dans ce type d'application, tout le monde peut lui écrire en utilisant la clé publique, mais seul l'utilisateur destinataire pourra décrypter et donc lire le message avec sa clé privée.



Application : Le système des mots de passe sous Unix est géré grâce à une fonction de codage à sens unique : le mot de passe est codé puis comparé avec le mot de passe préalablement codé qui est dans la base de donnée. Avec un tel système, il est possible de faire une attaque par dictionnaire : tous les mots d'un dictionnaire sont essayés les uns après les autres. Il est ainsi possible de trouver avec un ordinateur individuel 20% des mots de passe en une semaine.

Voici les algorithmes simples :
La substitution où l'on change les lettre suivant une règle précise.
C'est le procédé qu'utilisait Jules César : Il remplaçait chaque lettre du texte par celle qui se trouve trois places plus loin dans l'alphabet mis en cercle : A devient D, B devient E etc. il suffisait de supprimer les espaces entre les mots pour qu'il forme une suite de lettre incompréhensible. Dans ce codage, la clef était 3.

PDF created on http://www.htm2pdf.co.uk via the HTML to PDF API

L'ennui d'un tel procédé est qu'un cryptanalyste peut retrouver le texte de départ en étudiant la statistique du texte crypté et ainsi retrouver le texte de départ.
Ce type de codage peut être cassé en quelques secondes par un ordinateur actuel.
La transposition où la position des caractères est modifiée.
Pour encrypter un message, on l'écrit en colonne de taille fixes et on lit les colonnes dans un ordre déterminé :
Dans l'exemple ci-dessous, la clef de codage et de décodage est "briques"

B	R	I	Q	U	E	S
1	5	3	4	7	2	6
t	r	a	n	s	f	é
r	e	z	u	n	m	i
l	l	i	a	r	d	d
e	f	r	a	n	c	s
à	m	o	n	c	o	m
p	t	e	s	u	i	s
s	e	n	u	m	é	r
o	t	é	z	é	r	o
z	é	r	o	s	e	p
t	a	b	c	d	e	f

texte en clair

tranférezunmilliarddefrancsàmon
comptesuissenumérotézérozérosept

texte chiffré

TRLEAPSOZTFMDCOIEREEAZIROENERB
NUAANSUZOCRELFMTETEAEIDSMSROPF
SNRNCUMESD

Le bloc jetable (carré de *Vigenère*) : il faut une clef aussi longue que le message a chiffrer. On additionne le rang des lettres du texte à chiffrer avec le rang des lettres de la clef. La clef qui est aussi appelée masque, est jetée dès que le codage est effectué par l'expéditeur et après le décodage par le destinataire.

Ce chiffrement est incassable : par exemple, le message **urzgmk** donne **pommes** avec la clef **ekethr** et **cerise** avec la clef **ruzxtf**.

PDF created on http://www.htm2pdf.co.uk via the HTML to PDF API

Certains messages des espions soviétiques lors de la guerre froide, n'ont jamais été, et ne seront jamais déchiffrés!. Le gros défaut de ce codage est qu'il faut faire parvenir le masque au destinataire et donc, qu'il peut être intercepter par l'ennemi potentiel.

Les machines à tambour : ces machines mécaniques sont utilisées depuis la première guerre mais ont connu un grand développement durant la seconde guerre mondiale. La plus connue est la machine allemande **ENIGMA** qui a été "cassée" par l'équipe d'Alan Turing (l'inventeur du premier ordinateur).

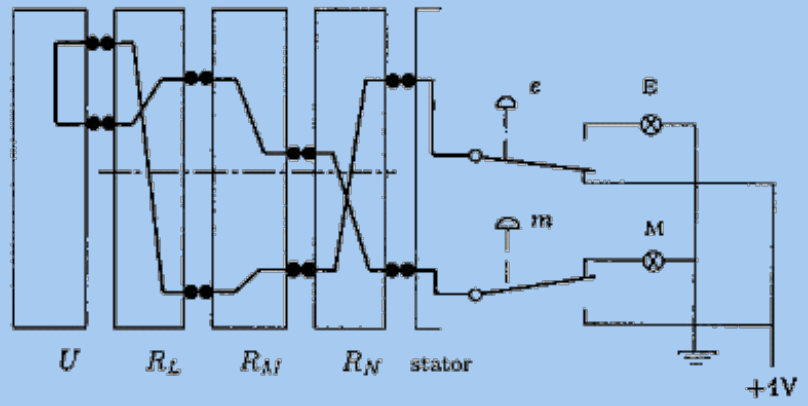
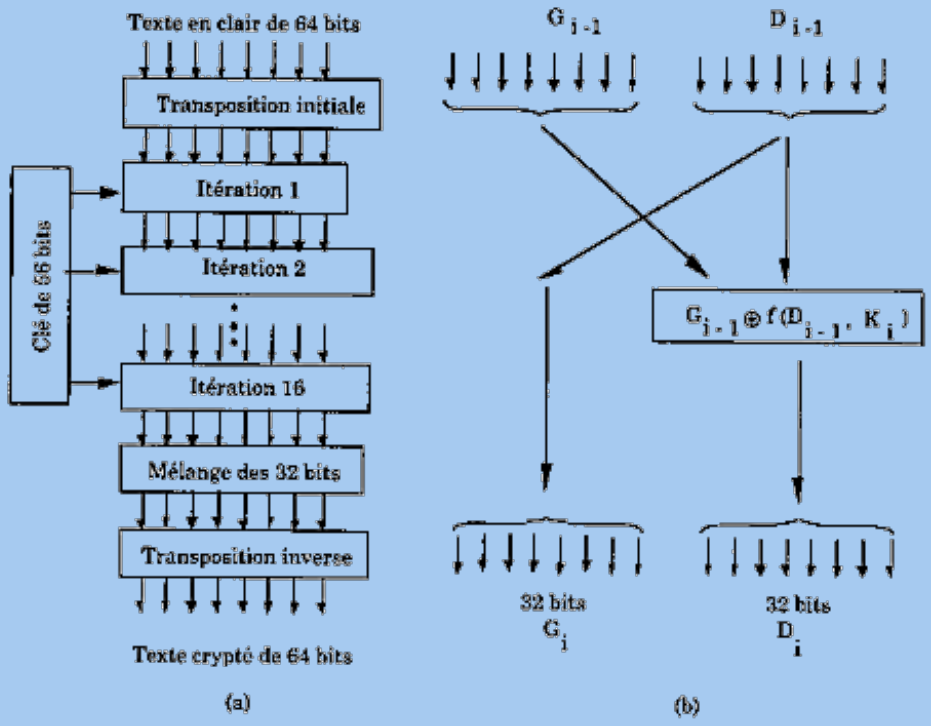


Schéma électrique d'une machine ENIGMA (bouton e et lampe M)

Elles fonctionnaient en utilisant une combinaison du carré de Vigenère avec des substitutions.
Ces machines étaient équipées d'un clavier sur lequel on tapait le message et le code sortaient automatiquement.
Pour décoder, il fallait utiliser la même machine en connaissant la position des roulettes qui avaient codés.

Algorithmes informatiques : la cryptographie moderne repose sur des algorithmes standard dont en voici quelques un:
Le **DES** (Data Encryption Standard) inventé en 1975 par une équipe d'IBM. C'est l'algorithme le plus populaire. C'est le standard de chiffrement du gouvernement américain et il a l'aval de l'armée. Le DES est un algorithme à clef secrète : la même clef sert au chiffrement et au déchiffrement. Il sert par exemple pour les transactions bancaires. Ce standard cessera d'être utilisé en 1998.
Chaque utilisateur choisit sa propre clé, mais il doit, pour permettre le décodage, communiquer celle-ci aux divers destinataires de ses messages; là réside le point faible du DES, car un secret partagé par plusieurs personnes n'est plus un secret.

PDF created on http://www.htm2pdf.co.uk via the HTML to PDF API



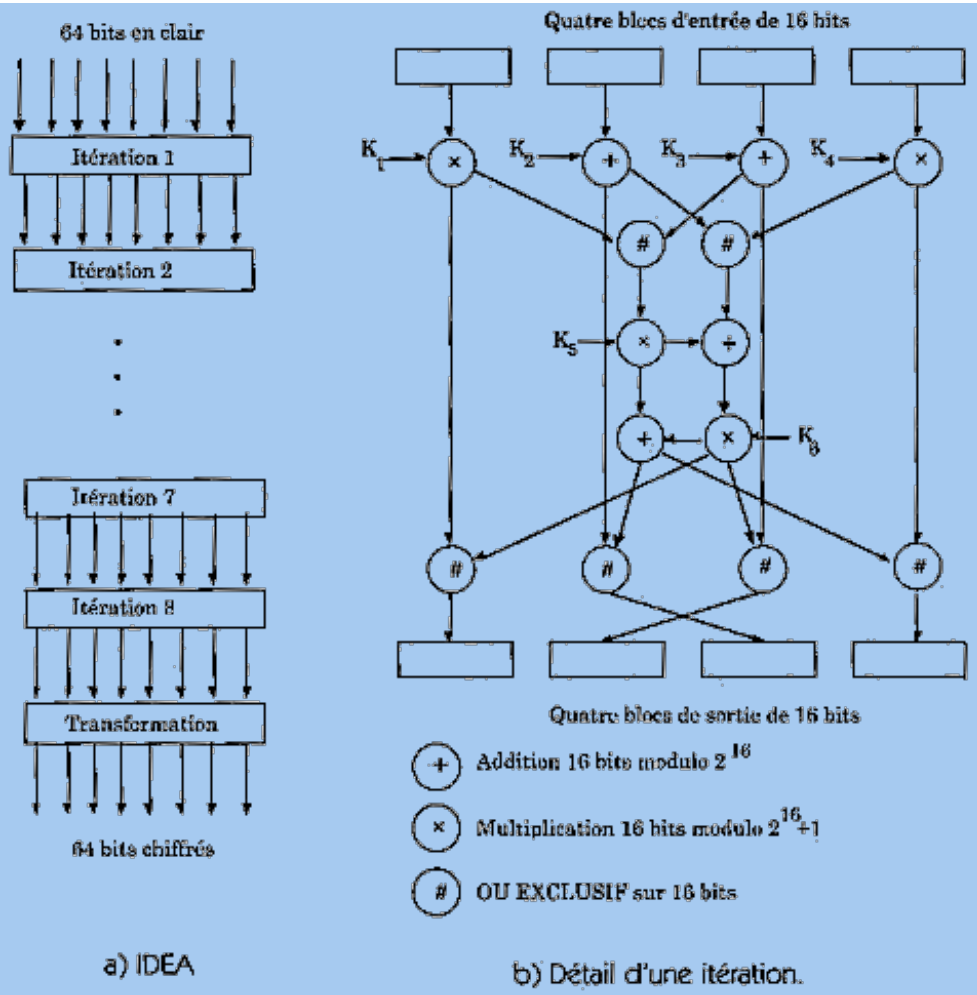
Il chiffre le texte par bloc de 64 bits avec une clef de 56 bits. Il utilise la diffusion et la confusion : Une substitution suivie d'une permutation appliquée au texte, basée sur la clef K. Il effectue 16 rondes où les blocs de 64 bits sont séparés en blocs Gauche et Droit.

Avec les opérations suivantes : $G_i=L_{i-1}$ et $R_i=L_{i-1}\oplus f(R_{i-1},K_i)$

Le décryptage étant réalise avec les mêmes opérations.

L'**IDEA** (International Data Encryption Algorithm) inventé en 1992, c'est le plus sûr des algorithmes à clef privée. Il effectue des opérations du même genre que celle du **DES** avec des blocs de 64 bits et une clef de 128 bits. Le texte est sépare en 4 sous blocs et il effectue 8 rondes qui combinent des ou exclusifs, des additions modulo $2^{\wedge 16}$ et des multiplications modulo $2^{\wedge 16+1}$. A chaque ronde, les données initiales sont combinées avec la clef, d'où il en sort donc un mélange inextricable.

PDF created on http://www.htm2pdf.co.uk via the HTML to PDF API



a) IDEA

b) Détail d'une itération.

Pour casser l'**IDEA**, il faudrait effectuer $2^{\wedge 128}=10^{\wedge 38}$ combinaisons. En calculant un million de combinaisons par seconde, un super ordinateur de type CRAY1 mettrait $10^{\wedge 25}$ années, soit, un million de milliard de fois l'âge de l'univers !

Le **RSA** (Rivest, Shamir et Adleman) inventé en 1978. Il porte le nom de ses inventeurs ; c'est l'algorithme a clef publique le plus populaire. Il peut aussi bien être utilisé pour le chiffrement des communications, que pour la signature numérique, c'est-à-dire une méthode d'authentification de l'expéditeur du message (on imagine l'importance de l'authentification de l'expéditeur d'un message chez les militaires ou les banquiers).
Il a le désavantage d'être 1500 fois plus lents que le **DES**. Il fonctionne grâce au fait mathématique, qu'il est très difficile de décomposer en nombres premier un grand nombre de plus de 100 chiffres.

Le **DSA** (Data Signature Algorithm) inventé en 1994, cet algorithme est spécifiquement conçu pour authentifier une information par une signature électronique. Il appartient au standard de signature électronique **DSS** reconnu par le gouvernement américain.

PDF created on http://www.htm2pdf.co.uk via the HTML to PDF API

III) Exemple : le RSA

1. Choisir deux nombres premiers, p et q, chacun plus grand que 10^{100}.
2. Calculer n = p.q et z = (p-l).(q-l).
3. Choisir e aléatoire tel que e et z soient premier entre eux.
4. Chercher d tel que e.d ≡ 1 mod(z)

Le couple (n,e) forme la clef publique d'encryptage et le couple (n,d) forme la clef privée de décryptage.
Ces différents paramètres sont calculés à l'avance. Nous sommes prêts à effectuer l'opération de chiffrement. Découpons le texte en clair (considéré comme une suite de bits) en une suite de blocs

Pour chiffrer un message M, on calcule la fonction de chiffrement : $C=M^e \bmod(n)$

Pour déchiffrer C, on calcule la fonction de déchiffrement : $M=C^d \bmod(n)$
La sécurité de cette méthode réside dans la difficulté à décomposer de très grands nombres en facteurs premiers. Comme les mathématiques n'ont guère progressé, depuis 300 ans, dans la recherche des facteurs premiers de très grands nombres, il est impossible a un cryptanalyste de factoriser le nombre public n et donc de trouver d et e.
D'après Rivest, la décomposition d'un nombre de deux cents chiffres nécessite 4 milliards d'années de calculs sur ordinateur, celle d'un nombre de cinq cents chiffres plus de 1025 années!.

Exemple concret avec des petits nombres :

- Si p=3 et q=11, on a donc n=p.q=33
- Ainsi, z=(p-1).(q-1)=2.10=20
- On choisit aléatoirement e=3, qui n'a pas de facteur commun avec 20
- On cherche $d=e^{-1} \bmod(20)$, soit d=7.
- On publie e et n, on garde d secret.

La figure suivante montre le chiffrement du texte "SUZANNE" en codant chaque lettre avec sont numéro alphabétique :

PDF created on http://www.htm2pdf.co.uk via the HTML to PDF API

Texte en clair (P)		Texte chiffré (C)			Après déchiffrement	
Caractère	Valeur	P^3	P^3 (mod 33)	C^7	C^7 (mod 33)	Caractère
S	19	6859	28	13492928512	19	S
U	21	9261	21	1801088541	21	U
Z	26	17576	20	1280000000	26	Z
A	01	1	1	1	1	A
N	14	2744	5	78125	14	N
N	14	2744	5	78125	14	N
E	05	125	26	8031810176	5	E
Calculs de l'émetteur				Calculs du récepteur		

Le PGP (Pretty Good Privacy) :
PGP est un système de chiffrement à clé publique qui combine les avantages d'un IDEA performant et d'un RSA robuste : IDEA est 1000 fois plus rapide que RSA et il est pratiquement impossible de percer la clé secrète RSA.
Il a été créé dans un but précis par Philip Zimmermann, un programmeur américain, passionné de cryptographie.
La première version PGP 1.0 a été créé en 1992 et diffusée sur des BBS aux USA, mais a finit par être amélioré en dehors des USA, à cause des lois sur l'exportation et des lois sur la cryptographie.
Voici ce qui se passera, lorsque vous utilisez PGP pour chiffrer un message e-mail :

- PGP génère d'abord une clé aléatoire de session pour le message.
- Il utilise l'algorithme IDEA pour chiffrer le message avec la clé de session.
- Il emploie ensuite l'algorithme RSA pour chiffrer la clé de session avec la clé publique du destinataire.
- Il prépare enfin le tout, la clé de session chiffrée et le message chiffré, pour l'envoi par e-mail.

Le processus inverse, le déchiffrement, se déroulera comme suit :

- PGP utilise IDEA pour déchiffrer la clé secrète sur disque du destinataire avec comme clé le mot (phrase) de passe fourni au clavier par le destinataire.

PDF created on http://www.htm2pdf.co.uk via the HTML to PDF API

- Il emploie RSA pour déchiffrer la clé de session avec la clé secrète du destinataire.
- Il utilise de nouveau IDEA pour déchiffrer enfin le message avec la clé de session.

De plus, les cryptogrammes sont compressés avec le système zip de façon a prendre moins de place.

Pour exemple voici ma clef publique :

```
Type Bits/KeyID    Date       User ID
pub  1024/A6A42A85 1997/11/01 Thomas Vivet <vivett@chez.com>

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3i

mQCNAzRbK9kAAAEEAMG0FjmXE1AuCxhlyUMgWIWvAoh5XktwpFIGk/FnEumWiz85
Mbs/zvtyiFiR6Q61shrrLudoG7bBlpr+x8I/k6yNEnpZRDM2vZQfXspn1a/Io5a1
7my2prJrdTVT95axJEfQysGwdpIs1dzXy/ZeZNtNLNzK7RjyOtT7BUumpCqFAAUR
tB5UaG9tYXMgVml2ZXQgPHZpdmV0dEBjaGV6LmNvbT6JAJUDBRA0WyvZ1PsFS6ak
KoUBAbDGBACfg9/Cgs1So0pk7BgNr2GjzPI/Hdd+DysT5PG9QHQVp3oL/2BVjZ8g
FIiIaJktuf+VMyyC1iJ4HKHKud+TVrmKPNB2OFrhve3eQLvWO+aNVx2txZ1sqrsE
RtpAMndMJmIdCoqP13a/7mpwp7uaxnodRrLSEYTiDFM74eQzv4S71g==
=Ieoc
-----END PGP PUBLIC KEY BLOCK-----
```

IV) Législation et cadre juridique

Depuis toujours, l'utilisation de la cryptographie a toujours été utilisée par les gouvernements, l'armés et les services de renseignement. La première utilisation démilitarisée de DES remonte à 1977, année considérée comme fondatrice de la cryptologie moderne.

La législation internationale :
Diverses organisations internationales participent aux débats sur la cryptologie.
L'OCDE : Elle donne les lignes directrices régissant la politique de cryptographie (27 mars 1997). Ces lignes directrices prônent la libéralisation des moyens cryptographiques pour favoriser l'éclosion du commerce électronique.
La "Global Internet Liberty Campaign". La Campagne Internationale pour Liberté sur Internet, lancée en 1996, regroupe 16 organisations citoyennes internationales. Sa vocation est de défendre les libertés individuelles sur Internet, gravement menacées par les gouvernements et les organisations comme le G7.

La législation française :
La Loi française définit la cryptologie comme "toute prestation visant à transformer à l'aide de conventions secrètes des informations ou signaux clairs en informations ou signaux inintelligibles pour des tiers, ou à réaliser l'opération inverse, grâce à des moyens conçus à cet effet". Les moyens de cryptologie sont définis comme "les matériels ou logiciels qui permettent de réaliser ces prestations".
Les décrets d'application de la loi du 26 juillet 1996 de réglementation des télécommunications ne sont toujours pas passés.
Mais, une fois les décrets publiés, la liberté sera totale d'utiliser des moyens cryptographiques pour garantir l'identification et l'intégrité de l'information, tant que le message reste en clair. La liberté de crypter le message sera totale pour peu que les moyens cryptographiques employés soient gérés par un tiers de confiance. L'utilisateur passe un contrat avec le tiers de confiance qui lui fournit les clés pour chiffrer ses informations. Le tiers de confiance est susceptible de fournir les

PDF created on http://www.htm2pdf.co.uk via the HTML to PDF API

clés à une autorité reconnue légalement.

La législation américaine :
Les lois actuellement en vigueur aux Etats-Unis autorisent un usage sans restriction des moyens cryptologiques sur le territoire national. En revanche, tout produit cryptographique destiné à l'exportation est sérieusement restreint : le codage des clés de cryptage est limité à 40 bits, une taille insuffisante pour garantir la confidentialité des messages.
Car, aux Etats-Unis, les moyens cryptographiques sont associés à du matériel de guerre. Or toute exportation de matériel de guerre est interdite. Donc l'exportation de moyens cryptographiques est interdite.
L'administration Clinton lutte avec le Congrès depuis plusieurs années pour instaurer un système de tiers de confiance. Différents lobbies - défense des libertés individuelles, industries high-tech, multinationales, etc. - soutiennent les initiatives des membres du
Congrès visant à libéraliser totalement les moyens cryptologiques (y compris à l'exportation).
À l'heure actuelle, différentes initiatives jouent en faveur de la libéralisation. Le projet de loi SAFE est en bonne posture pour être adopté sauf veto présidentiel.
Des industriels trouvent des astuces pour commercialiser hors des Etats-Unis des applications cryptographiques sûres.
Enfin, tous les logiciels freeware développés aux Etats-Unis sont disponibles sur des serveurs hébergés par des pays libéraux (Australie, Finlande, etc.).
L'administration américaine le 1er octobre, a annoncée une libéralisation partielle du chiffrement à l'exportation, mais avec l'obligation de dépôt de clefs.

Il y a donc trois possibilités face à l'interdiction d'utilisation des moyens de cryptage : soit ne pas protéger son informatique, ne pas faire de commerce électronique et ne pas authentifier ses correspondants soit être hors la loi ou soit changer de pays!

V) Applications

Voiçi quelques applications de la cryptographie : étant donné que 80% du temps un ordinateur individuel ne sert à rien, il est possible d'imaginer un *virus* inoffensif distribué au travers des réseaux informatiques. Ce virus ferait une recherche exhaustive des codes de cryptage d'un code qu'on lui enverait. Ainsi, au bout de quelques jours, sur le parc informatique mondial, un virus aura bien réussit a trouver le bon code et l'enverait à son commanditaire!!. Cette méthode peut couteuse est tout à fait envisagable dans un avenir proche.

La loterie chinoise est une autre application de la cryptographie : en supposant que chaque chinois a une télévision dans la quelle, il y a une puce spéciale **DES**, permettant de réaliser un million de chiffrement par seconde. En supposant que les 1,5 milliard de chinois ont la télévision, il suffit au gouvernement qui veut casser un message codé de diffuser ce message sur le signal de la télévision. En moins de 60 secondes, on aura trouvé la clef et un message avertira l'heureux possesseur de la télévision d'appeler un numéro de téléphone pour toucher la cagnotte en échange de la clef qui sera affichée sur son téléviseur.

Enfin, une voie de recherche, et qui pourrait paraître comme sortie de la science fiction est la *cryptographie quantique*. Cette nouvelle voie sur laquelle se lancent de grandes sociétés comme IBM à beaucoup d'avenir.
Elle se sert des propriétés de la physique quantique pour transmettre des photons polarisés. Le fait est que si jamais un intrus essaye de lire les données transitant à travers une fibre optique, le message est irrémédiablement changé. Actuellement, il est ainsi possible de transmettre quelques photons polarisés sur un distance de quelques mètres.

VI) Conclusions

Il faut que la cryptographie avance comme le boulet et la cuirasse, c'est à dire qu'il faut toujours chercher de nouveaux algorithmes plus puissants même si ceux utilisés aujourd'hui sont fiables. En l'an 200, une machine étant capable de décrypter en un an, un message codé sur 64 bits coûtera 4 millions de dollars.
Aujourd'hui, le cryptage des messages est devenu un problème légal, voire un problème de société de nature à la fois technique, éthique et politique. Car la

PDF created on http://www.htm2pdf.co.uk via the HTML to PDF API

généralisation des communications numériques (courrier électronique, téléphonie cellulaire, réseaux informatiques, etc...) rend nécessaire l'utilisation d'outils sûrs, en particulier pour le commerce électronique et la protection de la vie privée.
D'un côté, les gouvernements craignent que la libéralisation de l'usage de la cryptographie ne soit mise à profit par les hors-la-loi pour nuire à la société. Tandis que la libéralisation des moyens cryptographiques, est la condition indispensable pour garantir la protection de la vie privée et assurer la réussite du commerce électronique.
Mais comme, les méchants existent, qu'il s'agisse de terroristes, de mafieux, de pédophiles ou d'espions, la possibilité donnée à ces gens là de communiquer secrètement est une arme trop dangereuse, et il est indispensable que les autorités aient une possibilité de les combattre efficacement.
Or le problème français des écoutes téléphoniques à l'Elysée pose bien le problème du tiers de confiance désigné dans le décret de juillet 1996.

Car, le PGP ayant beau être le moyen actuel le plus sûr pour crypter ses communications, il est interdit à toute personne privée ou publique, de s'en servir pour communiquer!.
Comme le dit Phil Zimmermann, "*Si la confidentialité est mise hors la loi, seul les hors la loi profiteront de la confidentialité*"

Annexe : L'article de loi de juillet 1996 relatif à la cryptographie

VII) Bibliographie :

- Littérature :
  Science et vie n°953
  Réseaux (Tanenbaum)
  Cryptographie appliquée (Bruce Scheiner)
  Cryptologie contemporaine (G. Brassard)
  Decrypted secrets (F.L. Bauer)
- Sur le web :
  L'excellent site de TechnoSphere :
  Une introduction à la cryptographie
  Planète Internet : Article
  Un site sur le PGP (canada)
  PGP, une cryptographie pour tous (canada)
  Site ftp pour télécharger PGP
  Autre ftp avec PGP
  Autre ftp avec PGP
  Textes sur la conférence du 25 septembre 1997 à Paris
  Lois françaises sur la cryptographie
  Texte de l'OECD sur la cryptographie
  Textes de lois sur la crytographie (GB)

©1997 Thomas Vivet

PDF created on http://www.htm2pdf.co.uk via the HTML to PDF API

Email: p9603@bigiup.univ-lemans.fr

PDF created on http://www.htm2pdf.co.uk via the HTML to PDF API