La Cryptographie et ses principaux systèmes de références

Adda ALI PACHA - Naima HADJ-SAID
Laboratoire des Techniques du Codage et de la Cryptographie
dans le Domaine de la Transmission des Données
Université des Sciences et de la Technologie d' Or an
*USTO- **BP 1505 ElM'Naouer Oran 31036 ALGERIE** :*
E-mail : AlipachaCdryahoo.com

1) Introduction

La cryptographie est un moyen de sauvegarder le caractère confidentiel des informations. Elle ne protège pas les communications en tant que telles mais plutôt leur contenu.

Avec la venue de l'Internet , des réseaux téléinformatiques (les réseaux locaux, métropolitains et les réseaux à grande distance) et l'emploi des liaisons satellites, la nouvelle révolution industrielle en informatique et dans les télécommunications a abouti au stockage et à la transmission de grande quantités de données confidentielles et à un souci croissant d'en protéger l'accès (vue que ces données sont disponibles pour n'importe quelle personne). Donc le cryptage (Chiffrage) est nécessaire pour que les données soit non-intelligibles sauf à l'auditoire voulu.

Les méthodes de chiffrage destinées à garder le secret des messages à caractère politique, militaire ou religieux sont connues depuis des milliers d'années. Mais le premier qui a fournit à ces méthodes de chiffrage un fondement mathématique solide fut C.E.Shannon.

Bien que les systèmes de chiffrage soient nombreux, dans ce qui suit nous allons présenter seulement le système de chiffrage des informations organisées sous forme de séquences car c'est celui le plus en faveur actuellement; et introduire deux systèmes cryptographiques qui pourraient servir de référence l'algorithme RSA, le standard de codage des données américains DES (Data Encryption Standard), l'algorithme de la signature électronique DSA et l'algorithme à clé mixte PGP (Pretty Good Privacy).

2) Définitions et Terminologies de la cryptographie

La cryptographie (sécurité des données) est l'ensemble des processus de verrouillage visant à protéger l'accès à certaines données afin de les rendre incompréhensible aux personnes non autorisées [2,4,5], autrement dit garantir la confidentialité, l'intégrité de ces informations, ainsi

que leur imputabilité. L'émetteur d'une information doit être certain de l'identité du destinataire et inversement.

- L'opération par laquelle le message est rendu méconnaissable (déguisé) s'appelle ***CHIFFRAGE.***

Le texte en clair est noté M, c'est le message [1] à chiffrer. Il peut être une suite de bits, un fichier de texte, un enregistrement de voix numérisé, ou une image vidéo numérique. De toute façon M n'est rien d'autre que de l'information binaire, comme il peut être transmis ou stocké.

- Le message chiffré s'appelle ***CRYPTOGRAMME.***

Le texte chiffré est noté C. C'est aussi de l'information binaire, parfois de la même taille que M, parfois plus grand.

- Opération inverse, à savoir revenir de l'espace des cryptogrammes à l'espace des messages ; cette opération s'appelle ***DECHIFFRAGE.***

Les deux fonctions de chiffrement et déchiffrement sont notées respectivement E (pour Coder) et D (pour Décoder). La fonction de chiffrement E transforme M en C, ce qui sera noté mathématiquement :

$$E(M)=C$$

La fonction inverse, de déchiffrement, D, transforme C en M, ce qui sera noté par:

$$D(C)=M$$

Le but principal est de retrouver le message en clair à partir de la version chiffrée de ce même message, il faut que
l'identité suivante soit vérifiée :

$$D(E(M))=M$$

- La technique des systèmes de chiffrage s'appelle ***CRYPTOGRAPHIE.***
- Les algorithmes de chiffrement moderne dépendent de certains paramètres que l'on appelle *CLE,* notée K. C'est l'information la plus secrète et la plus importante échangée entre l'expéditeur et le destinataire. L'ensemble de valeurs possibles que peut prendre une clé est appelé espace des clés.

Il existe deux classes de système de cryptographie à base de clé :

1. Les Systèmes Symétriques ou à Clé Secrète :

La même clé K est utilisée pour le chiffrement et le déchiffrement, cela est illustré par la figure N°I.

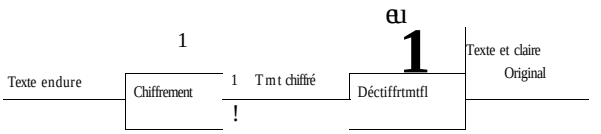


Figure 1 : Chiffrement et déchiffrement avec une clé

Donc si le processus de chiffrement et déchiffrement est fait à l'aide d'une clé K, alors les deux fonctions E et D vont avoir deux paramètres, et les formules de chiffrage et déchiffrage respectivement sont les suivantes :

$$E(M, K)=C \quad \text{et} \quad D(C, K)=M$$

Et l'identité qui doit être vérifiée est :

$$D(E(M,K),K)=M$$

2. Les Systèmes Asymétriques ou à Clé Publique :

Les algorithmes à base de ce système ont une clé de chiffrement notée K tout à fait différente de la clé de déchiffrement notée K'. On peut illustrer cela par la figure N°2. Dans ce cas les fonctions de codage et décodage sont les suivantes :

$$E(M, K)=C \quad \text{et} \quad D(C, K')=M$$

Ainsi que l'identité qui doit être vérifiée est :

$$D(E(M, K),K')=M$$

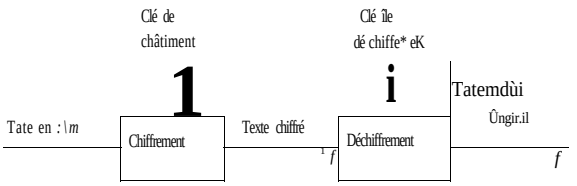


Figure 2: Chiffrement et déchiffrement avec les 2 clés

- Le procédé par lequel on déduit le message du cryptogramme lorsque la dé n'est pas connue s'appelle ***CRYPIANALYSE.***
- La ***CRYPTOLOGIE*** couvre en même temps la cryptographie et la cryptanalyste.

La figure N°3 représente le schéma de principe de chiffrage où S [3] est une source binaire (Laquelle peut être la sortie d'un convertisseur analogique - numérique).

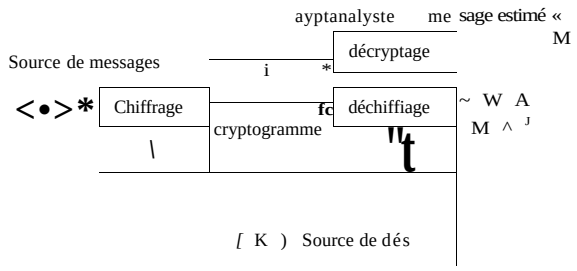


Figure 3: Système de chiffrage

3) Exemple de chiffrage

L'expéditeur et le destinataire se mettent d'accord sur une **Edition** particulière d'un **Livre** particulier.

Pour coder un message l'expéditeur cherche chaque mot du message dans le livre et écrit :

- la page,
- la ligne et
- la position ou il se trouve.

Les nombres de référence constituent le code. Pour décoder on consulte simplement chaque référence pour obtenir le texte clair. C'est l'une des méthodes générales les plus anciennes [2], parfois encore utilisée. La **clé** est le livre utilisé.

- Comme avantage, il est difficile pour un adversaire de deviner la clé (le livre).
- Les inconvénients majeurs sont le temps et les efforts qu'il faut déployer pour chercher dans un ouvrage parfois long le mot désiré pour le codage et la possibilité réelle qu'un mot nécessaire ne soit pas dans le livre.

De nos jours, la protection des données contre les interceptions non autorisées trouve de larges applications aussi bien dans :

- La transmission entre les ordinateurs: Les banquiers et les services commerciaux ont besoin de disposer de protocole de signatures, avant d'accepter un ordre de virement ou une commande (il est impensable d'accepter une commande téléphonique sur le simple énoncé d'un numéro de carte bancaire).

- Les transmissions téléphoniques ou télévision : système de décodage *MediaGard* pour Canal Plus et Canal Satellite ainsi que, le système de décodage *Viaccess* pour le TPS.

4) Principaux systèmes cryptographiques

Dans l'état actuel des choses, il existe deux systèmes cryptographiques [3] qui pourraient servir de références. Ils sont à base de clés.

- Les algorithmes à clé publique, et
- Les algorithmes à clé secrète.

Ces algorithmes servent à coder des informations qui seront ensuite décodées avec la clé appropriée . En utilisant des algorithmes, on verrouille les données, c'est-à-dire qu'on les transforme, les mélange ou les échange en les attachant à d'autres données.

Il existe une autre catégorie d'algorithmes en cycle de recherche, et qui ne sont pas utilisable. Ce sont des algorithmes à base de la cryptographie quantique. Ils sont fondées sur la mécanique quantique et les propriétés très particulière de la matière dans ce domaine. Ils utilisent comme véhicule de transmission un canal quantique. Grossièrement, chaque bit du message serait codé avec un photon.

4.1 Algorithmes à Clé Publique

La sécurité de ce système, qui est représenté principalement par le code dit RSA conçu au MIT (Massachussets Institue of Technology) et l'algorithme de signature électronique DSA, repose sur l'impossibilité d'effectuer la factorisation d'un grand nombre de quelques centaines de chiffres en un temps raisonnable.

Car la cryptographie moderne est orientée vers la manipulation des bits (chiffres en binaires), et utilise avec abondance des résultats des fonctions de l'arithmétique, et repose sur l'emploi de formules mathématiques souvent complexes.

4.1.1. Notions Mathématiques

La théorie des nombres est devenue depuis une vingtaines d'années un vivier dans lequel la science de la cryptologie est venue puiser [5].

a) Nombres Premiers

Un nombre p est premier s'il admet exactement deux diviseurs, 1 et lui même (1 n'est pas premier). Il est facile de vérifier de tête que 7, 13 ou 31 sont des nombres premiers.

- Mais *quelle méthode adopter pour montrer que 4999 est premier ?*

Essayer toutes les divisions de '4^99 pdr D allant clé 2 à 4996. Si •aucune division ne tombé ^usté, dlors on peut affirmer que '4999 est premier.

a *Comment créer une liste des nombres premiers ?*

La méthode proposée par Eratosthène donne une solution **(Crible Eratosthène**).

Ecrire tous les nombres cfè 2 'a 'lOOO. 2 est "premier, on ïè souligne et on raie tous les multiple de 2. Le premier nombre non raye *{êst* 3. Il est "donc premier, on le souligne et on raie tous ses multiples. Etc. Arrivé fà 32, qui supérieur à la racine carrée de 1000, on a terminé.

Tous les nombres qui n'ont pas été rayés sont premiers.

La méthode devient inefficaces avec des nombres très grands (par exemple pour une table des nombres premiers jusqu'à 10 000 000).

a *'Existe-t-il des grands nombres premiers ?*

La réponse a été fournie par Euclide qui affirme qu'un nombre est soit prernïe'r, soit qd'me't 'un 'diviseur premier. S"il 'dctrVfèt *'un* cWiseùV p'rèYïiësr, "on effectue la 'division et on recommence avec le quotient obtenu (**critère de Lén'mer** 'qui permet de savoir si 'un entier fN 'èsst 'pre'mtèï lorsque l'on 'db'hn'dît 'là aecomposïfïôh en facteur premiers de N-l).

En effet, si on suppose que cet ensemble est infini, il est composé de n nombrespi,p2 …,p_n alors N=pi*p2*...*Pn+l est premier.

b) Cortgruences

Chdcun sait c|ue s'il est 3 heures, dans 2 heures il sera -5 heures. Normal puisque 3+2=5. De même, s'il est 11 heures, dans 2 heures il sera 1 heure. Normalpuisque 11+2=1.

Comrrlënt'atrive-t-on à ce résultat surprenant ?

En faitlèrreste'd'élà tïîvïstôrVae ï3p!aï ?2*è^t:1 •:
les calculs d:he!ofe%erfon1t rrtôdùlo ï^.''On'devrait:ëh fait'écrire !1 '1+2=1 'môà (12).

a et b sont congrus modulo n s'ils ont un même reste par la division par n.

c) Petit Théorème de Fermât

Si ***p** pférfiïer Eet "p ne ilrvise 'pas rà ('C'-é^t à dire a et p dernier entré eux').
'Xiôrs QP-^{1} =:l^{2}ft>].
4i :p TÎfëmfer et 'a 'èntfér aioïs %*> =:a [ffI.

d) Fonctions à Sens Unique

La théorie de la calculabilité et de la complexité algorithmiques introduit une classe de fonctions dites à sens unique, dont l'existence est toujours une conjecture.
La notion de sens unique signifie que tout algorithme de calcul de l'inverse donne un résultat au bout d'un temps extrêmement long (la complexité de l'algorithme est exponentielle).

La rapidité ne dépend pas de la puissance du processeur qu'on utilise.

/ à sens unique ⇔ r— Vx y=/(x) est calculable rapidement
-<
L_ x^-^{1} (y) se calcule en temps très long

C'est cette disproportion du temps de calcul de / et /-' qui va être mise à profit pour faire bénéficier de la rapidité des processeurs de calculs les cryptographes, au détriment légitime des cryptanalystes.

e) Fonctions de Hachage à Sens Unique :
le Hachage d'un message consiste en l'application d'une fonction mathématique qui permet d'en crée un condensé. Donc, la fonction de hachage H est la transformation d'un bloc d'informations m de taille variable en un bloc d'informations de taille fixe h qui est la valeur de hachage, on a h = H(m).

- H(X) doit être rapidement calculable pour tout X,
- H(X) ne doit pas être facilement inversible, Il est impossible de trouver le message qui a généré un résumé donné; en fait on ne doit pas pouvoir obtenir la moindre information utile sur le message, même pas un simple bit.
- H(X) doit être sans collisions : c'est à dire quelque que soit le message X, on ne peut pas trouver un message Y différent de X vérifiant H(X)=H(Y).

L'utilisation de l'algorithme de hachage sécurisé [1,5] SHS (Secure Hasch Algorithm) développé par Ronald Rivest en 1990, est requis pour toutes les opérations de signature digitale basées sur le standard DSA. Etant donné un message de langueur inférieure à 2^{64} bits, l'algorithme SHA produit un compressé de 160 bits de ce message, appelé condensé. Ce condensé est utilisé à la fois dans l'opération de signature électronique du message et dans le processus de vérification de cette signature.

f) Exponentielle Modulaire - Algorithme Discret

La fonction aP mod n de la variable p, est appelée exponentielle modulaire. L'algorithme de cette fonction se programme d'une manière récursive, en effectuant les deux opérations en même temps :

$$\begin{cases} 1 & \text{si } p=0 \\ (a^{p/2} \bmod n)^2 \bmod n & \text{si p est pair} \\ (a(a^{p'''} \bmod n)) \bmod n & \text{si p est impair} \end{cases}$$

Le calcul d'une exponentielle modulaire se fait en temps logarithmique par rapport aux données , c'est à dire très rapidement. Leurs inverses, qui sont difficilement calculables, portent le nom de **logarithmes discret.**

4.1.2 Le Système à Clé Public R.S.A :

Le système R.S.A [1,5] est un système de cryptage à clé public, il a été développé en 1977 par Ronald Rivest, Adi Shamir et Léonard Adelman (dont les initiales forment RSA). Il est fondé sur l'utilisation de l'exponentiation modulaire, réputée être une fonction trappe. Donc il utilise une fonction à sens unique permettant l'inversion de la fonction par celui connaissant la gâche secrète, donnant lieu à deux applications essentielles.

1. L'envoi de messages confidentiels à une personne.
2. L'authentification par toute personne du message envoyé par individu: Signature électronique

4.1.2.1 Protocole d'Encryption :

Le système RSA [9] est basé sur la difficulté de factoriser un nombre qui est le produit de deux grands nombres premiers.

a) Création des clés.

Destinataire construit un quadruplet de nombres (p, q, e, d)

- L'utilisateur choisit deux grands nombres **p** et q premiers et les multiplie pour obtenir **n** = **p** * q
- Il choisit un nombre grand **e** premier avec (p-l)(q-1)
- On calcul **d** inverse de **e** , tel que **(ed** - 1) est un multiple de (p - 1)(q - 1), c'est-à-dire tel que **ed=l mod** (p-l)(q-1). Celle-ci peut être résolue grâce à une version étendue de l'algorithme d'Euclide.
- Si A est un entier quelconque, alors: A^{ed} = A **(mod** n), et c'est cette identité qui va tout faire fonctionner.

b) Publication la clet publique.

Destinataire rend publics (n, e), qui constituent la clé publique. Il la publie dans un annuaire ou la communique à *Emetteur,* qui la lui demande. Il ne communique surtout pas p, q ou d. Les nombres p et q peuvent être oubliés, car ils ne serviront plus à personne. Le nombre (n, d) constitue la clé secrète de *Destinataire.*

c) Transmission d'information.

Emetteur, qui veut transmettre une information secrète au *Destinataire,* transforme son information en un nombre entier A, inférieur à n (ou en plusieurs si nécessaire), en utilisant des conventions connues de tous comme par exemple le code ASCII. C'est à dire une personne voulant envoyer le message A au propriétaire des paramètres (n, e) va décomposer A en blocs ai de taille connue ;

d) Chiffrage de l'information.

Emetteur calcule, grâce à la méthode d'exponentiation rapide :

- Calculer pour tout i : $bi = ai^e$ **Mod** n
- Former le message B en regroupant les blocs bi, et $B = A^e \pmod n$, envoie B à *Destinataire* par un canal qui n'a pas besoin d'être protégé (par exemple, le courrier électronique).

d) Déchiffrage de l'information.

Destinataire, pour décoder B, calcule $B^d \pmod n$, ce qui lui redonne A, car, d'après le théorème du RSA, on a :

$$Bd = A^{ed} = A \pmod n.$$

4.1.2.2 Exemple de Cryptage

Si p = 47 et q = 71 alors N= p.q = 3337

La clé de chiffrement **e** ne doit pas avoir de facteurs communs avec

$$(p-l).(q-l) = 46.70 = 3220$$

On choisi **e** (aléatoirement) égal à 79. Dans ce cas

$$d = 79\text{-}i \bmod 3220 = 1019$$

Ce nombre a été calculer on utilisant l'algorithme d'Euclide étendu. On publie **e** et on garde **d** secret. On jette **p** et q .

Pour chiffrer le message : m = 6882326879666683

Divisant le en petit blocs. Des blocs de trois chiffres conviendrons dans ce cas ci. Le message est divisé en six blocs mi tels que :

mi = 688 ; m_2 = 232 ; m3 • 687; rru = 966 ; m_5 = 668 ; m* = 3

Le premier bloc est chiffré par: $688^{79} \bmod 3337 = 1570 = Ci$

En effectuant la même opération pour tous les blocs , on obtient le message chiffré :

C = 1570 2756 2091 2276 2423 158

Pour déchiffrer le message, il faut effectuer les mêmes exponentiation mais en utilisant le clé de déchiffrement 1019. Donc :

$$1570^{'\circ 19} \bmod 3337 - 688 = m,$$

Le reste du message est obtenu de la même manière.

4.1.3 Signature Numérique d'un document

Pour signer le message que vous expédiez, il suffit en effet de leur appliquer une fonction mathématique (appelée fonction de hachage) qui produit un résumé du message. Le résumé obtenu est propre à chaque message, à l'instar d'une empreinte digitale qui permet également d'identifier l'émetteur et de certifier le document. Elle peut ensuite être chiffré à l'aide de votre clé privée et annexée à votre message. C'est ce code qui constitue la **signature numérique** [8,9]. Cette empreinte digitale (code haché) peut être séparer du document permettant ainsi de générer une base de données qui s'appuie sur le stockage des empreintes des fichiers et en associant une date a chaque empreinte interdisant ainsi l'accès aux fichiers.

Le destinataire du message peut ensuite vérifier que vous en êtes bien l'expéditeur en déchiffrant la signature numérique, au moyen de votre clé publique, pour obtenir le code haché. Le destinataire applique ensuite la même fonction de hachage au message reçu ; si les deux codes sont identiques, vous êtes bien l'expéditeur du message (non - répudiation) et le message n'a pas été altéré (intégrité).

Il y a deux méthodes utilisées pour la signature de l'empreinte:

- **A l'aide de chiffrement**

C'est l'oeuvre de plusieurs algorithmes cryptographiques [1, 3, 4], elle s'obtient en associant une opération de hachage et une opération de chiffrement , c'est à dire:

1. Création par l'émetteur d'un condensé du message par une opération de hachage.

2. Chiffrement asymétrique du condensé par la clé privée de l'émetteur. Ceci constitue la signature.
3. Envoi des deux informations (message et signature) au destinataire.

Le destinataire qui reçoit ces deux informations doit, pour vérifier la signature, procéder ainsi :

1. Calcul à nouveau du condensé du message par le même algorithme que celui utilisé par l'émetteur.
2. Déchiffrement de la signature en utilisant la clé publique de l'émetteur. Cela permet de reconstituer le condensé crée par l'émetteur.
3. Comparaison des deux informations condensées ainsi obtenues. Si elles sont identiques, seul l'émetteur (le processeur de la clé privée) a pu envoyer ce message.

- **Sans l'aide de chiffrement**

C'est une nouvelle technique créer pour que la signature soit propre sans avoir procédé à faire le chiffrement de l'empreinte. On utilise l'empreinte du document et la clé privée de l'émetteur pour faire un traitement mathématique. Le résultat de ce traitement (valeur numérique) sera la signature numérique du document. L'émetteur A calcul l'empreinte du document avec la fonction de hachage et signe, à l'aide de l'algorithme de la signature, l'empreinte avec sa clé secrète (Ks). Cette signature est associée au document original.

Le destinataire recevra le document avec sa signature, il calcul avec la fonction de hachage uniquement l'empreinte du document et vérifié, à l'aide de l'algorithme de la signature, l'empreinte avec la clé publique de A (Kp). Le résultat de ce traitement sera comparé avec la signature envoyé et s'ils sont égaux donc la signature est valide.

L'algorithme DSA (Digital Signature Algorithm) est un exemple de ce type de signature.

4.1.3.1 Standard de Signature Digitale DSA

Le DSA [1,3,5] utilise les paramètres suivants:

- P = un nombre premier de L bits de long, où L est compris entre 512 et 1024 et est un multiple de 64. Dans le standard original, la longueur de P était fixée à 512 bits.
- Q = un facteur premier de P-1 long de 160 bits.
- **G** = $h(^{p}\text{-}')/^{Q}$ mod P, où h est n'importe quel nombre inférieur à P-1 tel que

h(P-u/Q mod P soit plus grand que 1.

- X = un nombre de 160 bits inférieur à Q
- $Y = G^x \bmod P$.
- K est un entier choisi aléatoirement dans l'intervalle]0,Q[.

Les trois premiers paramètres P, Q et G forment la clé publique et peuvent être communs à un réseau d'utilisateurs. Chaque utilisateur possède une clé privée X et une clé publique Y, valables durant une période de temps limitée.

Dans l'algorithme DSA les paramètres X et K sont utilisés uniquement lors de la génération de signatures, et le nombre K doit être régénéré à chaque signature. Le protocole de signature associé à l'algorithme DSA peut alors être décrit comme suit :

4.1.3.2 Génération de Signature

Si l'utilisateur A souhaite envoyer le message M à l'utilisateur B, alors A calcule deux quantités entières R et S obtenues comme suit :

R = **(G« mod P) mod Q**

S =(K^ (SHA(M)+X*R)) mod Q

Ici K^{-1} désigne l'inverse multiplicatif de K (mod Q), c'est-à-dire l'unique entier de l'intervalle]0,Q[tel que $K^{-1} * K = 1 \pmod Q$. La valeur SHA(M) est le résultat de l'application de la fonction de hachage sécurisée sur le message M produisant une chaîne de 160 bits, qui est à son tour convertie en un entier. Les nombres entiers R et S constituent la signature digitale associée au message M, et sont envoyés au destinataire B avec le message M.

4.1.3.3 Vérification de la Signature

Le destinataire B du message M et des entiers R et S reçoit ces quantités (par exemple via un réseau) sous la forme M', R', S'. Il dispose également de l'identité A de l'émetteur et de sa clé publique Y. Pour vérifier la signature du message transmis on a :

0<R'<Q et 0<S*<Q *

B effectue successivement les opérations suivantes :

- Si l'une des deux inégalités (*) n'est pas satisfaite, alors la signature est invalide.
- Si les deux inégalités (*) sont satisfaites, alors B calcul les quantités suivantes :

W = (S')-i **mod** Q

Ul = (SHA(M')*W) **mod** Q

U2 = (R'*W) **mod** Q

V=(((G^XY"^{2})) **mod** P) **mod** Q

Si V=R', on conclu que R' reçu est le R émis (de même pour M' et S') alors la signature est vérifiée, et le vérificateur peut acquérir une quasi-certitude que le message adressé a bien été envoyé par le possesseur de la clé Y générée par la clé secrète X.

Si, au contraire, V ' R', alors les possibilités suivantes sont envisageables :

1. le message M été modifié.
2. le message M été signé de manière incorrecte par l'émetteur.
3. le message M a été signé par un contrefacteur.

Bien entendu, dans chacun des cas 1, 2 et 3 ci-dessus, le message M doit être considéré comme invalide.

4.2 Algorithmes à Clé Secrète

Ce système combine simultanément des méthodes cryptographiques traditionnelles [2, 3, 4] comme par exemple la substitution et la transposition qui, séparées sont des méthodes de cryptographie peu sûres, mais dont le mixage permet d'atteindre un degré de sécurité largement plus élevé.
La méthode de la substitution préserve l'ordre des symboles (message) mais les déguisent. Par contre, la méthode de la transposition les réordonnent mais ne les déguisent pas.

4.2.1 Substitution :

La substitution sert à rendre inintelligible le texte en clair pour toute autre personne que son destinataire légitime. Ce dernier applique la substitution inverse au texte chiffré pour retrouver le texte en clair. La substitution correspond à remplacer chaque lettre du message clair par une autre lettre ou un autre caractère. Un chiffre à substitution est un chiffre dans lequel chaque caractère du texte en clair est remplacé par un autre caractère dans le texte chiffré.
Comme Jules César qui utilisait ce système pour communiquer secrètement : chaque lettre de l'alphabet était décalée de 3 unités, a donnait e. . . . .x donnait a, y donnait b et z donnait c. Ajoutons à l'alphabet quelques caractères de ponctuation : 'espace', 'virgule', 'point', '?', et ':' pour disposer d'un alphabet de 31 caractères (31 est premier).
Avec ces 31 caractères a devient d

z devient '.'
'espace' devient '?'
',' devient ':'
'.' devient a
'?' devient b

On reconnaît là une congruence modulo 31 : on commence par remplacer a par 1, b par 2 ..., z par 26, 'espace' par 27 , 'virgule' par 28, 'point' par 29, '?' par 30, et ':' par 31. Cette convention permet alors d'effectuer des calculs sur le texte.

4.2.2 Transposition :

Un chiffre à transposition est un chiffre dans lequel les caractères du texte en clair demeurent inchangés mais dont les positions respectives sont modifiées, pour appliquer la transposition simple en colonnes, on écrit le texte en clair horizontalement sur un morceau de papier quadrillé de largeur fixe et l'on relève le texte chiffré verticalement.

Exemple : Texte en clair : " L'assassin est le docteur MATRIX, regardez derrière l'horloge. "

L	**A**	**S**	**S**	**A**	**S**	**S**	**I**	**N**
E	**S**	**T**	**L**	**E**	**D**	**O**	**C**	**T**
E	**u**	**R**	**M**	**A**	**T**	**R**	**I**	**X**
R	**E**	**G**	**A**	**R**	**D**	**E**	**Z**	**D**
E	**R**	**R**	**I**	**E**	**R**	**E**	**L**	**H**
O	**R**	**L**	**O**	**G**	**E**			_

Text chiffré: " LEERE OASUE RRSTR GRLSL MAIOA EAREG SDTDR ESORE EICIZ LNTXD H ".

Pour déchiffrer le cryptogramme il suffit d'écrire verticalement celui ci sur un morceau de papier quadrillé de la même largeur et de lire horizontalement le texte en clair.

4.2.3 Data Encryption Standard DES

Le standard de codage des données américains DES (Data Encryption Standard) est un code produit, dont l'idée vient de Shannon : il combine simultanément transposition et substitution à la séquence de bits (0 ou 1) représentant l'information à crypter.

Les transpositions sont les relations par ou *exclusif* dans l'algorithme du DES qui sont linéaires par contre la substitution principale du DES est non linéaire (connue généralement sous le nom de *fonction de sélection)* afin de produire un texte codé si complexe qu'une cryptanalyse mathématique [10,11] est impossible.

Ce système est actuellement par basé sur l'algorithme LUCIFER [5] et conçu par la firme IBM en 1977, repose entièrement sur la clé personnelle de l'utilisateur, car toutes ces opérations (les procédures) sont fixes et publics (connues de tous). Et la même clé est utilisée pour coder et décoder des données.

4.2.3.1.L'algorithme LUCIFER

a) Pour commencer le texte clair est divisé en un nombre de blocs comportant chacun 2n bits, un bloc est noté par M=(U, Ro), L pour Left et R pour Right, soit la moitié gauche et la moitié droite du message. Dans le cas du DES, 2n = 64 bits (8 octets ou caractères).

L'algorithme va être appliqué à chacun de ces bloc jusqu'à ce que le texte soit entièrement transformé en un texte codé .

b) La clé K de longueur k permet par un procédé à préciser, de fabriquer d sous clés ki, k2. . . . .kd. Dans le cas du DES la clé K est constituée de 56 bits. Cette clé, choisie au hasard par l'utilisateur, est divulguée aux personnes concernées, qui doivent aussi s'en servir pour lire les données protégées. Sachant qu'il y a plus de 70 milliards de millions de combinaisons de 56 bits possibles (2^{S6} clés possibles), les chances de découvrir une clé au hasard s'avèrent infimes. En fait, le décodage de ce type de message demeure toujours possible à l'aide d'un puissant ordinateur, mais le temps requis serait alors de plusieurs centaines d'années. Par exemple avec un ordinateur réalisant 100 millions d'essais à la seconde, il faudrait 23 ans pour trouver une clé DES.

c) Le message subit un certain nombre de " rondes " . Dans le cas du DES, le nombre de rondes est de 16.

d) On dispose d'une fonction f, dont le choix est essentiel car elle doit être non linéaire et elle doit bien " brouiller les cartes ". il n'y a pas en principe d'autre condition à respecter pour le choix de la fonction f.

On utilise cette fonction de la façon suivante : Si N est un vecteur de longueur n de $(Z/2Z)^n$. f(N, k) est vecteur de $(Z/2Z)^n$, où k est la clé utilisée,:

Entrée : **(Lo , Ro)**

1er Ronde **(Li=R_0 , Ri=Lo Âf(R_0, ki))**

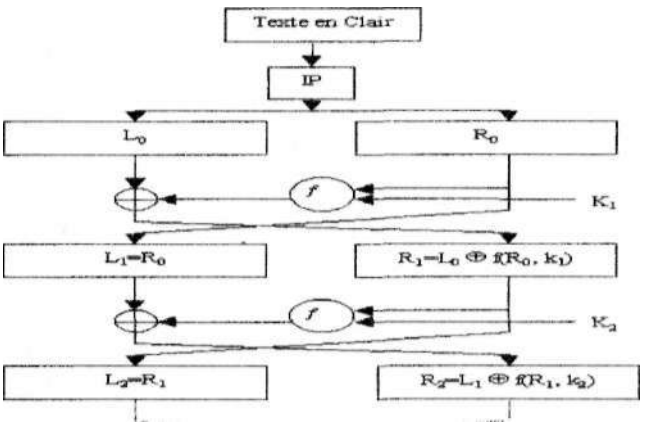
2« Ronde **(L_2=R,** , R_2=*U* **Âf(R,, k_2))**

le Ronde (Li=Ri-i , RFLO Â f(Rii, ki))

de Ronde **(Ld-Rd-i** , Rd=L_d-i Âf(R_d-i, kd))

Ceci signifie qu'après chaque ronde, la partie droite est placée à gauche, tandis que la partie gauche est additionnée modulo avec le résultat de la fonction f appliquée à la partie droite, le résultat étant placé à droite.

Le message crypté est C=e\M,K^= *[la , R<0\,* obtenu après d " rondes " , et on obtient le schéma de la figure N°4.



Ru-L» «î CR.M. ku) :J

èr / y^

R-w—I-is œ' SJ*13. kM>

IP-l

HZ

Texte Oliffi-4

Figure 4: Algorithme LUCIFER : DES

On remarquera que :

1. Il a été introduit une permutation notée IP avant les 16 rondes, ainsi que sa permutation inverse notée IP-' après les 16 rondes.

Celles-ci n'ont aucun intérêt cryptographique.

2. A la dernière ronde les parties gauche et droite on été inversé.

Quel est l'intérêt de l'algorithme LUCIFER ?

4.2.3.2.Décodage du DES

Puisque le DES est un processus symétrique, le décodage est identique au codage. Pour décrypter un cryptogramme on effectue les mêmes opérations que pour le cryptage sauf que les 16 itérations de la clé K sont utilisées dans l'ordre inverse, de KM à Ki et l'algorithme agit comme son propre inverse

(même tables et procédures).

Pour le comprendre, regardons comment déchiffrer le message reçu C : il suffit d'appliquer les mêmes opérations, mais dans l'ordre inverse.

En effet, on a C= (Ld , M avec

RcFLd-i Â f(R_d i, kd)= Ld-i Â **f(Ld,** k_d) Û Ld-i = **RdÀ** f(L_d, k_d)

(Addition et la Soustraction modulo 2 sont identiques)

Bref, connaissant Ld, Rd et kd on retrouve Ld-i et ainsi de suite en appliquant l'algorithme LUCIFER dans l'ordre inverse.

La conséquence est que le même processeur, la même carte ou le même logiciel sert à chiffrer et à déchiffrer.

Le DES, qui est aujourd'hui majoritairement utilisé dans l'industrie du logiciel [1,5] et des cartes à puces. Il est 1000 fois plus rapide que le RSA.

On peut dire aussi, que le système DES est le résultat d'un travail d'amélioration d'algorithmes de codage conventionnels, et en tant que tel s'inscrit directement dans une tradition historique.

4.3. Algorithmes à Clés Mixtes :

Quel est le meilleur système cryptographique : système à clé secrète ou système à clé publique ?

cryptosystème	**Avantages**	**Inconvénients**
Clé secrète	- Rapide, - Peut être facilement réalisée sur une puce.	- Difficulté de distribuer les clés, - Ne permet pas la signature électronique.
Clé publique	- Utilise deux clés différentes, - Fournit des garanties d'intégrité et de non répudiation par signature électronique.	- Lent et demande beaucoup de calcul.

Les deux systèmes cryptographiques de base à clé secrète et à clé publique souffrent de problèmes complémentaires et chacun a ses spécificités. La force des algorithmes à clés publiques réside dans la distribution des clés alors que les algorithmes à clés secrètes sont très performants en vitesse de chiffrement.

Ainsi, l'intérêt pour augmenter la sécurité des systèmes de cryptage passe certainement par l'utilisation combinée de ces deux techniques, ce que l'on

nomme la cryptographie mixte. L'algorithme PGP [7] (Pretty Good Privacy) est un système cryptographique à clé mixte.

4.4. le système PGP :

Le PGP de Phil Zimmermann utilise deux algorithmes distincts pour crypter et décrypter les données dans un réseau de téléinformatique, l'un est à clé publique et l'autre à clé secrète. L'opération de cryptage se fait donc en trois étapes principales:

1. PGP crée une clé secrète de manière aléatoire sur la base de la clé de l'utilisateur (pour l'algorithme à clé secrète), et crypte les données du texte en clair.
2. Il crypte cette clé secrète précédemment crée au moyen de la clé publique (de l'algorithme à clé publique) du destinataire.
3. Transmission de (1) et (2), c'est à dire du texte chiffré par la clé secrète et de la clé secrète crypte par la clé publique au destinataire.

PGP offre aussi une méthode d'utilisation des signatures numériques. Celles-ci permettent au destinataire de vérifier leur authenticité, leur origine, mais également de s'assurer qu'elles sont intactes. Elles fournissent également une fonctionnalité de non répudiation, afin d'éviter que l'expéditeur ne prétend qu'il n'a pas envoyé les informations. Donc, Il applique au texte clair une fonction de hachage évoluée, qui génère un élément de données à longueur définie, appelé résumé de message ensuite il utilise ce résumé et la clé privée pour créer la signature.
Le texte clair avec sa signature peut être enfin crypter par le PGP.

On conclut que le système PGP utilise la signature électronique et les algorithmes à clé public et à clé secrète. Donc, il est la synthèse des algorithmes de base que nous avons étudier.

5. Cryptanalyse :

Le but de la cryptographie est de préserver les données confidentielles [1,5,10,11] de l'indiscrétion des attaquants (adversaires, espions intercepteurs, intrus, opposants, oreilles indiscrètes, cryptanalystes, décrypteurs, ou ennemis).

Une cryptanalyse réussite peut fournir soit le texte en clair, soit la clé. Une tentative de cryptanalyse est appelée attaque, et une attaque réussite est appelée méthode.

Forcer un code consiste à essayer de repérer des régularités au sein des données apparemment obscures. Plus le contenu d'un message est brouillé, plus il est difficile de parvenir à découvrir comment le concepteur du cryptage s'y est pris pour le coder.

Il existe six types génériques d'attaques cryptanalytiques Chacune repose sur le fait que le cryptanalyste connaît les détails de l'algorithme de chiffrement. Tout dépend du type de l'algorithme. Si l'algorithme est utilisé dans un programme de sécurité alors c'est une question de temps et d'argent pour casser le programme et retrouver la méthode. Si l'algorithme est utilisé dans un système militaire de communication, alors c'est aussi une question de temps et d'argent pour acheter (ou voler) l'équipement et la reconstitution de la méthode. Selon le degré de sécurité requis, on utilise des algorithmes plus ou moins performants. Il existe quatre possibilités d'attaques d'un crypto système à clés secrètes :

1. L'attaque gloutonne : consiste à essayer toutes les clés, si l'algorithme E est connu de l'espion.
2. L'attaque à textes chiffrés : consiste à découvrir tout ou partie de la clé à partir de messages cryptés.
3. L'attaque à textes chiffrés et clairs : par un moyen rusé, l'espion possède des textes chiffrés pour lesquels il connaît le texte clair correspondant.
4. L'attaque à texte clair choisi : la plus pernicieuse, elle consiste à choisir les textes clairs pour obtenir en retour les textes cryptés correspondants.

Les codes DES et RSA représentent une sorte de ramification parmi toute les façons d'aborder la cryptologie. Tous deux découlent du postulat de base que tous les codes adaptés au communications de masse peuvent être en définitive forcés [5], mais que l'on peut parvenir à une sécurité suffisante en rendant totalement irréaliste la quantité de travail qu'il faudrait fournir pour les forcer.

- Le DES (Lucifer 1970, et le DES 1976) a été casser en Juin 1998. il s'est révélé résistant à la cryptanalyse différentielle dont les principes ne seront redécouverts par des universitaires (non tenus au secret) que bien après la création du DES.
- Par contre, le RSA-155 a été casser en Août 1999. néanmoins le RSA reste solide avec des clés plus longues que 155 chiffres.

6) Conclusion

L'application la plus évidente de la cryptographie est la protection de la confidentialité d'une information, qu'elle soit stockée localement sur une machine ou transmise sur un réseau.
Le besoin de confidentialité n'est pas l'apanage des militaires ou de certains gros industriels. Tous les individus, toutes les organisations ont, à des degrés divers, un tel besoin :

- Confidentialité des transactions bancaires,
- Protection de secrets industriels ou commerciaux,
- Protection des sessions de télé-travail,
- Protection du secret médical,
- Protection des systèmes informatiques contre les intrusions,
- Protection de la confidentialité des communications dans le cadre d'une association, d'un parti politique, d'un syndicat...
- Protection de la vie privée,
- Jeux

Mais la cryptographie propose d'autres fonctions par le biais de la signature électronique :

- l'Authentification des correspondants
- La non-répudiation des transactions
- l'Intégrité des documents

Ces fonctions sont très attendues par tous ceux qui voudraient sécuriser des transactions sur l'Internet ou protéger les données ou les oeuvres intellectuelles transférées [6].

7). Bibliographies

[I] B.SCHNEIER :"Cryptographie appliquée", John Wiley & Sons, Inc., 1994.

[2] Beckett Brian :" Introduction aux méthodes de la cryptologie", Editions Masson, 1990.

[3] Marsault Xavier :" Compression et cryptage des données multimédias", 2e édition revue et augmentée, Editions Hermès, 1992.

[4] Alexandru Spâtaru :" Fondements de la théorie de la transmission de l'information", Pesses Polytechniques romandes, 1987.

[5] J.DUBERTET, Initiation à la cryptographie, 2eme Edition VEBERT, Avril 2000.

[6] Lionel Thoumyre," Les enjeux de la cryptologie", LIONEL@JURISCOM.NET, directeur de juriscom.net, 1998.

[7] Jean Luc Montagnier, " Pratiques des réseaux d'entreprise ", Eyrolles 1996, 1998.

[8] R.RIVEST, A.SHAMIR et LADELMAN"A Method for Obtainning Digital Signatures and Public Key crypto Systems ^Communications of the ACM, Vol.21,ppl20-126, Février 1978.

[9] R.RIVEST, A.SHAMIR et L.ADELMAN"On Digital Signatures and Public Key crypto Systems ",MIT Laboratory for Computer Science, 1979.

[10] E. BIHAM et A. SHAMIR' "Differential Cryptanalysis of DES-Like Cryptosystems", Journal of Cryptology, VOL.4, N°l, pp.3-72, 1991.

[II] M. MATSUI , "Linear Cryptanalysis Method for DES Cipher", Springer-Verlag, Berlin, 1994.