1-Introduction :

De nos jours, il y a de plus en plus d'informations qui circulent sur le Web et donc doivent rester secrètes ou confidentielles. En effet, les informations échangées par les banques ou un mot de passe ne doivent pas être divulgués et personne ne doit pouvoir y avoir accès. C'est pourquoi ce genre d'informations est crypté.

2-Qu'est-ce que la cryptologie ?

La cryptologie est un ensemble de techniques qui permettent de protéger des informations grâce à un code secret. Elle étudie notamment les outils servant à sécuriser ces informations face à des menaces intentionnelles. [6]

2-1-Les branches de la cryptologie :

La **cryptologie** est la science qui englobe la cryptographie et la cryptanalyse.

3-Qu'est-ce que la cryptographie?

Discipline incluant les principes, les moyens et les méthodes de transformation des données, dans le but de masquer leur contenu, empêcher leur modification ou leur utilisation illégale, ainsi que les opérations inverses, pour rendre le document à nouveau intelligible.

3-1-Objectif de la cryptographie :

L'objectif fondamental de la cryptographie est de permettre à deux personnes, appelées traditionnellement Amel et Réda de communiquer par l'intermédiaire d'un canal de transmission **public** (une ligne de téléphone, ou un réseau par exemple tous deux réputés peu sûr), sans qu'un espion éventuel appelé Omar en comprenne le sens.

3-2-Principe :

Le message de départ qu'Amel envoie à Réda noté x, peut être un simple texte dans une langue naturelle, une image, une musique, ou tout autre forme de données numériques. Amel transforme le message de départ x par un procédé de chiffrement (ou **codage**) noté K en un message y, et l'envoie alors à Réda. Omar qui espionne le canal de transmission ne peut pas comprendre le message car il ne connaît pas la façon de procéder pour le déchiffrer (ou **décoder**). Ce n'est pas le cas de Réda, qui peut appliquer le procédé inverse à celui d'Amel, et transformer le message chiffré y pour qu'il soit identique au message x d'origine.
Le message est couramment appelé **texte en clair**. Le processus de transformation d'un message de telle manière à le rendre incompréhensible est appelé **chiffrement** (ou **encryption**). Le résultat de ce processus de chiffrement est appelé texte chiffré (ou encore **cryptogramme**). Le processus de reconstruction du texte en clair à partir du texte chiffré est appelé **déchiffrement** (ou **décryptage**).

3 -3- L' emploi de la cryptographie dans l'informatique :

A l'origine la cryptographie était principalement utilisée par l'armée et les instances gouvernementales, afin de garantir la confidentialité de leurs informations. puis avec le développement de l'informatique, des techniques de communication et des réseaux, l'utilisation de la cryptographie s'est fortement démocratisée. En effet, le flux croissant de données transitant dans les réseaux internationaux impose de crypter les informations pour en assurer l'intégrité et la confidentialité.
De nos jours, le cryptage d'information est très utilisé par les banques et institutions financières (avec les cartes de crédit par exemple) ainsi que dans les entreprises.
De plus en plus, on le voit apparaître dans notre vie quotidienne par l'intermédiaire du courrier électronique mais aussi au travers de l'Internet pour des paiements sécurisés par exemple. [9]

3-4-Les fonctions de la cryptographie :

-La confidentialité :
La confidentialité consiste à rendre l'information inintelligible à d'autres personnes que les acteurs de la transaction.

-L'intégrité :
Vérifier l'intégrité des données consiste à déterminer si les données n'ont pas été altérées durant la communication (de manière fortuite ou intentionnelle).

-L'authentification :
L'authentification consiste à assurer l'identité d'un utilisateur, c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être. Un contrôle d'accès peut permettre (par exemple par le moyen d'un mot de passe qui devra être crypte) l'accès à des ressources uniquement aux personnes autorisées.

-La non-répudiation :
La non-répudiation de l'information est la garantie qu'aucun des correspondants ne pourra nier la transaction.

3-5- Comment la cryptographie assure ses fonctions ?

a)La confidentialité :

La confidentialité est historiquement le premier problème posé à la cryptographie. Il se résout par la notion de *chiffrement* : un *message clair* est préalablement chiffré par une fonction de chiffrement **C** à l'aide d'une *clef chiffrante*. Un *déchiffrement* semblable s'opère au moyen d'une clef qui peut être différente et d'une fonction de déchiffrement **D**.

b)L'intégrité :

Le problème de l'intégrité des données intervient dans différentes situations :

1. lorsque l'on partage des ressources de mémoires sur des ordinateurs : si l'on laisse des données sur une mémoire, on aimerait pouvoir être sûr qu'elles n'ont pas été volontairement modifiées quand on y accède à nouveau.
2. lorsque l'on communique avec une autre personne au travers d'un canal peu sûr on aimerait que le destinataire soit convaincu que le message n'a pas été altéré volontairement
3. lorsque dans un protocole, on doit choisir une donnée sans la révéler et s'engager à ne pas la modifier (par exemple, si plusieurs participants doivent choisir simultanément une valeur sans que le choix des uns ne dépende de celui des autres).

En cryptographie, on fait appel aux fonctions de hachage qui résolvent ces situations.

Une *fonction de hachage* est une fonction qui réduit une liste de données de taille arbitraire en une donnée de taille fixe. Dans la situation 1, on peut noter le résultat *haché* des données en mémoire sur un support sécurisé (son propre agenda par exemple). Dans la situation 2, si l'on dispose d'un canal sécurisé (mais plus coûteux) en parallèle, on peut communiquer le résultat haché par l'intermédiaire de ce canal. Dans la situation 3, on met en gage résultat haché de la donnée choisie.

c)L'authenticité :

1-Un vieux problème posé par l'écriture de documents est celui de l'authenticité. Il est plus ou moins résolu par des procédés de signature, de sceaux ou autre empreinte difficilement reproductible comme les dernières inventions de la banque de France utilisées dans le billet Antoine de Saint-Exupéry. L'ordinateur étant capable de reproduire aussi fidèlement que possible des données numériques, une notion de *signature électronique* est nécessaire.

2-L'authentification de message, effectué par la signature électronique, ne traite pas tout les problèmes d'authenticité. L'authentification des personnes est également nécessaire. Lorsque deux personnes (ou deux processus) communiquent au travers d'un réseau, elles ont besoin d'être convaincues qu'elles parlent bien avec la personne avec laquelle elles croient parler. Pour ce faire, chacune d'elles prouve, protocole interactif, qu'elle connaît un secret en rapport avec son identité, et ce, sans révéler la moindre information sur ce secret. De tels protocoles sont dits *0-knowledge*.

3-6-Techniques de la cryptographie:

On peut classer ces méthodes en 3 grandes classes, comme nous le montre le schéma qui suit :

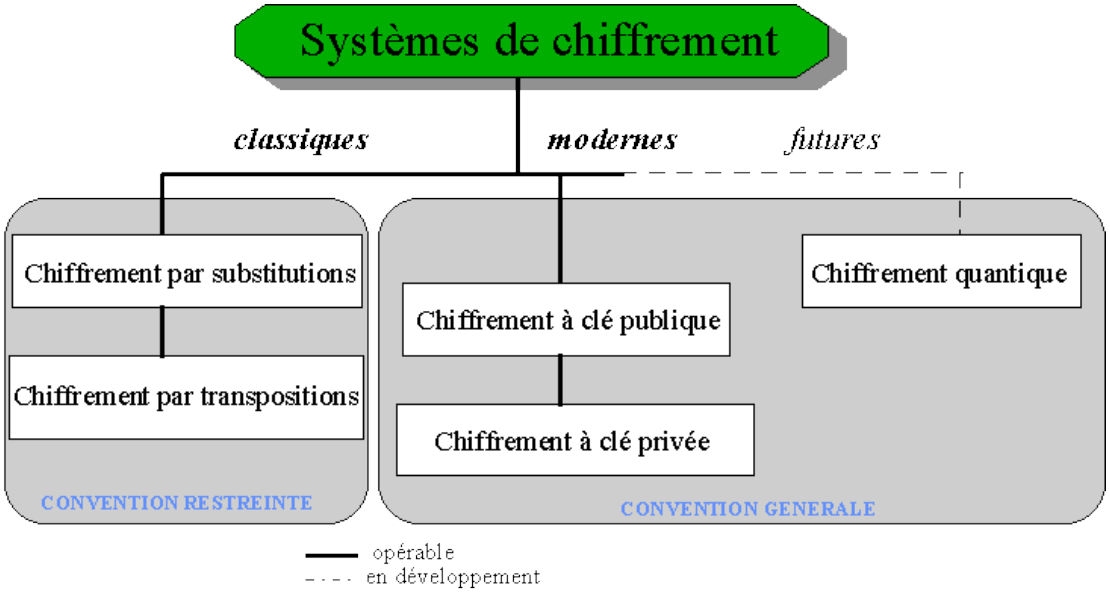


fig 1.1 Principales techniques en cryptographie

La cryptographie **classique** décrit la période avant les ordinateurs. Elle traite des systèmes reposant sur les lettres et les caractères d'une langue naturelle (allemand, anglais, français, etc.). Les principaux outils utilisés remplacent des caractères par des autres et les transposent dans des ordres différents. Les meilleurs systèmes (de cette classe d'algorithmes) répètent ces deux opérations de base plusieurs fois. Cela suppose que les procédures (de chiffrement ou déchiffrement) soient gardées **secrètes** ; et sans cela comme nous l'avons déjà dit le système est complètement inefficace (n'importe qui peut déchiffrer le message codé). On appelle généralement cette classe de méthodes : le chiffrement à usage **restreint**.

Les méthodes utilisées de nos jours sont plus complexes, cependant la philosophie reste la même. La différence fondamentale est que les méthodes **modernes** (les algorithmes, puisque l'on utilise maintenant des ordinateurs) manipulent directement des bits (liés à l'implantation sur les machines) contrairement aux anciennes méthodes qui opéraient sur des caractères alphabétiques. Ce n'est donc qu'un changement de taille (ou de représentation), puisque l'on utilise plus que deux éléments au lieu des 26 lettres de l'alphabet. La plupart des bons systèmes de cette catégorie combinent toujours des substitutions et des transpositions, et les règles sont connues de tous, c'est pourquoi on appelle cette classe : le chiffrement à usage **général**. La sécurité de ces méthodes reposent maintenant sur un nouveau concept clé : les **clés** (pour faire un mauvais jeu de mot). [12]

3-6-1-Le chiffrement classique :

a) Substitution :
La substitution consiste a effectuer des dérivations pour que chaque caractère du message chiffré soit différent des caractères du message en clair. Le destinataire légitime du message applique la dérivée inverse au texte chiffré pour recouvrer le message initial.
On distingue couramment 2 types de substitutions différentes :

Exemple : texte en clair = «NON JE NE SUIS PAS FOU»
texte chiffré(***avec 5 divisions***) = «ABAWR ARFHV FCNFS BH»

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
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

dictionnaire ROT13

1)Substitution simple ou substitution monoalphabétique : chaque caractère du texte en clair est remplacé par un caractère correspondant dans le texte chiffré. Les exemples les plus célèbres sont les algorithmes de *César, Rot13*, et bien évidemment le code morse. Ils sont encore utilisés aujourd'hui pour cacher le sens de certains messages (par exemple la solution de certains jeux dans des journaux), mais bien sûr elles sont très peu sûrs. [12]
2)Substitution polyalphabétique : le principe consiste à remplacer chaque lettre du message en clair par une nouvelle lettre prise dans un ou plusieurs alphabets aléatoires associés. Par exemple, on pourra utiliser n substitutions monoalphabétiques ; celle qui est utilisée dépend de la position du caractère à chiffrer dans le texte en clair. On choisit une clé qui sert d'entrée dans la grille polyalphabétique incluant autant de symboles qu'il y a de lettres différentes à chiffrer. Chaque caractère de la clé désigne une lettre particulière dans la grille de codage. Pour coder un caractère, on doit lire le caractère correspondant du texte en clair en utilisant la grille polyalphabétique et le mot clé associé dans l'ordre séquentiel (on répète la clé si la longueur de celle-ci est inférieure à celle du texte de départ). L'exemple le plus célèbre est l'algorithme de *VIGENERE* .(la description de cet algorithme est dans le chapitre suivant).

b) Transposition :
Avec le principe de la transposition toutes les lettres du message sont présentes, mais dans un ordre différent. Il utilise le principe mathématique des **permutations**. Plusieurs types différents de transpositions existent :
1)Transposition simple par colonnes : on écrit le message horizontalement dans une matrice prédéfinie, et on trouve le texte à chiffrer en lisant la grille verticalement (cf. la figure ci-dessous). Le destinataire légal pour décrypter le message réalise le procédé inverse. L'algorithme allemand ADFGFX est fondé sur ce principe et fut utilisé pendant la première guerre mondiale. Il fut cassé par une jeune étudiante française.

Texte à chiffrer : **La sécurité est importante**
On utilise une matrice de [6,4]

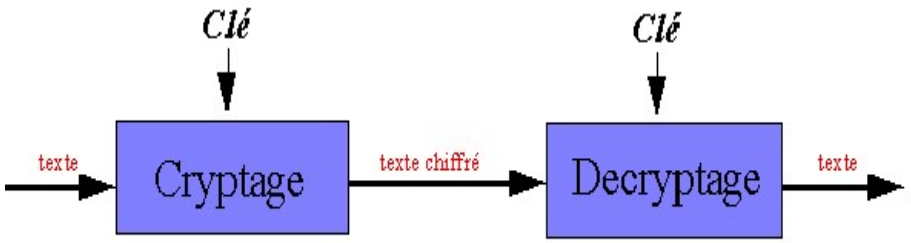
l	**a**	**s**	**e**
c	**u**	**r**	**i**
t	**e**	**e**	**s**
t	**i**	**m**	**p**
o	**r**	**t**	**a**
n	**t**	**e**	

Transposition simple par colonnes:
Le texte chiffré :
lctto nauei rtsre mteei spa

3-6-2-Le chiffrement moderne :

3-6-2-1-Chiffrement symétrique :

Les systèmes symétriques sont synonymes de systèmes à clés secrètes. Une même clé est utilisé pour le chiffrement et le déchiffrement, d'ou l'obligation que celle-ci reste



Chiffrement Symétrique

confidentielle, sous peine de rendre le système inefficient. [12]

Théorie :

L'émetteur (Amel) et le destinataire (Réda) doivent se mettre d'accord préalablement sur la clé (k) à utiliser, pour ceci ils ne doivent pas utiliser le réseau de communication standard qui est susceptible d'être espionné (par Omar). Chaque fois qu'Amel veux transmettre un message (m) à Réda, elle utilise sa clé secrète pour chiffrer (c=Ek(m)), et elle envoie le résultat de ce chiffrement par l'intermédiaire du même canal. Réda utilise à son tour la même clé secrète et le même algorithme public pour déchiffrer le message codé qu'il a reçu. [12]

Algorithme D.E.S :

D.E.S., pour Data Encryption Standard ("standard de cryptage de données"), est un algorithme très répandu à clé privée crée à l'origine par IBM en 1977. Il sert à la cryptographie et l'authentification de données.

DES a été pensé par les chercheurs d'IBM pour satisfaire la demande des banques. Il a été conçu pour être implémenté directement en machine. En effet puisque les étapes de l'algorithme étaient simples, mais nombreuses, il était possible à IBM de créer des processeurs dédiés, capables de crypter et de décrypter rapidement des données avec l'algorithme DES.

Cet algorithme a donc été étudié intensivement depuis les 15 dernières années et est devenu l'algorithme le mieux connu et le plus utilisé dans le monde à ce jour.

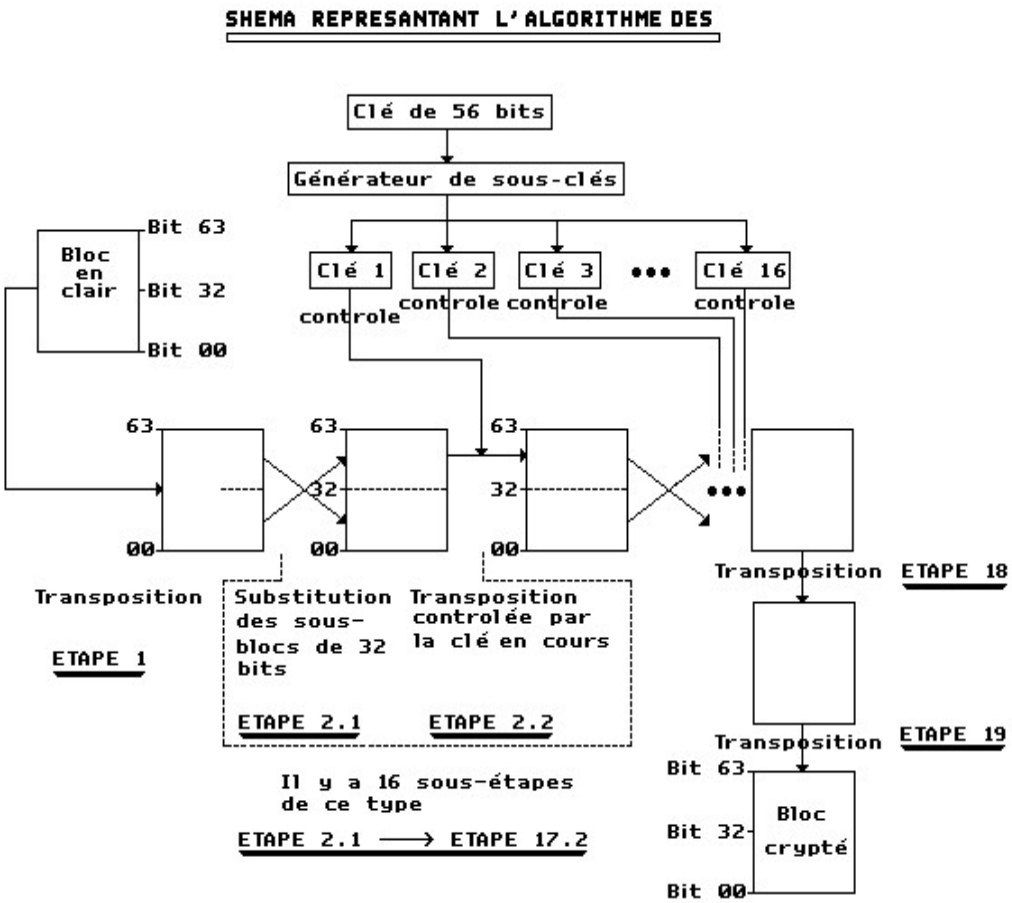
Description de l'algorithme DES :

L'algorithme DES est un algorithme de cryptographie en bloc. En pratique, il sert à crypter une série de blocs de 64 bits (8 octets).

Le cryptage :

DES utilise une clé secrète de 56 bits, qu'il transforme en 16 "sous-clés" de 48 bits chacune. Le cryptage se déroule sur 19 étapes.

1ère étape:
La première étape est une transposition fixe (standard) des 64 bits à crypter.
16 étapes suivantes:
Les 16 étapes suivantes peuvent être divisées en 2 "sous-étapes" chacune. Dans un premier temps, Le bloc de 64 bits est découpé en 2x32 bits, et une substitution est effectuée entre ces deux blocs, en fait, ces deux blocs seront tout simplement échangés l'un avec l'autre. Dans un second temps, le bloc de 32 bits ayant le poids le plus fort (le bloc qui va du bit n°32 au bit n°63) subira une transposition contrôlée par la sous-clé correspondant à l'étape en cours
Etape 18 et 19:
Les deux dernières étapes sont deux transpositions.

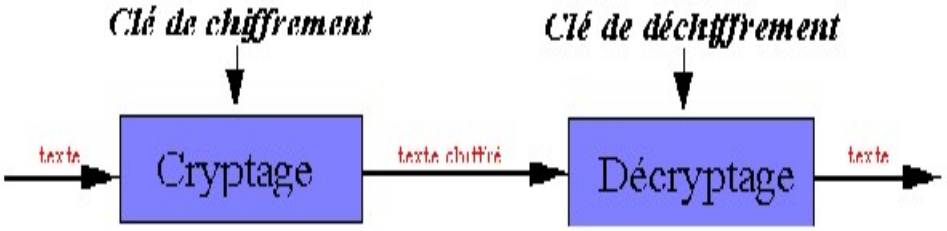


Le décryptage :

Pour décrypter un document auparavant crypté avec DES, il suffit d'effectuer l'algorithme à l'envers avec la bonne clé. En effet, il n'est pas nécessaire d'utiliser un algorithme différent ou une clé différente puisque DES est comme nous l'avons vu un algorithme symétrique. Il est donc totalement et facilement réversible, si l'on possède la clé secrète.

3-6-2-2-Chiffrement asymétrique :

Ces algorithmes sont aussi synonymes d'algorithmes à clés publiques. Une clé différente est utilisée à la fois pour chiffrer et déchiffrer, et il est impossible de générer une clé à partir de l'autre. Il a été inventé en 1975 par deux ingénieurs en électronique : Whitfield Diffe et Martin Hellman de l'Université de Stanford.



Chiffrement Asymétrique

Théorie

Une des difficultés principales de la méthode ci-dessus est que chaque couple potentiel d'utilisateurs doit posséder sa propre clé secrète, et se l'échanger par un moyen sécurisé avant leur premier échange d'informations, ce qui peut s'avérer difficile à réaliser dans la pratique. Le but d'un système à clé publique est de résoudre ce problème.

La clé publique est généralement publiée dans un répertoire. L'avantage est donc qu'Amel peut envoyer un message à Réda sans communication privée préalable (elle choisit sa clé privée, et la clé publique de Réda). Réda est la seule personne à pouvoir déchiffrer le message en appliquant sa clé secrète et personnelle, et la clé publique d'Amel. On dit généralement que chaque clé déverrouille le code produit par l'autre. Une remarque intéressante à faire est qu'avec ce système, même Amel qui a chiffré un message pour Réda, ne pourra déchiffrer le message ainsi codé. C'est un des systèmes les plus évolués que l'on peut actuellement trouver.

La première application à ce principe fut le chiffrement RSA. Depuis, plusieurs systèmes ont été proposés. Leur sécurité repose sur divers problèmes calculatoires, et notamment la théorie des grands nombres.

Algorithme R.S.A :

R.S.A. signifie Rivest-Shamir-Adleman, en l'honneur de ses inventeurs : Ron Rivest, Adi Shamir et Leonard Adleman qui l'ont inventé en 1977.

C'est l'algorithme à clé publique le plus commode qui existe. Comme pour le D.E.S. Sa sécurité repose sur l'utilisation de clés suffisamment longue (512 bits n'est pas assez, 768 est modérément sûr, et 1024 bits est une bonne clé). C'est la difficulté que l'on a à factoriser les entiers premiers (le problème des logarithmes discrets est souvent considérés comme insurmontable) qui font que l'on ne peut que difficilement casser cet algorithme.

Cependant de larges avancées en matière de factorisation des entiers larges, ou une augmentation considérable de la puissance de nos super-calculateurs rendront RSA très vulnérable.

Description de l'algorithme RSA :

Soit *n* un entier tel que *n=pq*

1. Génération des clés:

- Clé publique:

- Choisir deux nombres premiers *p* et *q* très grands (de l'ordre de 100 chiffres). Il existe pour cela des algorithmes de génération aléatoire de nombres premiers. On pose *n=pq*.

- Trouver un entier *e* entre 2 et φ(n)=(p-1)*(q-1) (fonction indicatrice d'Euler, c'est en fait le nombre d'entiers inférieurs à *n* qui sont premiers avec lui) tel que *e* et φ(n) soient premiers entre eux.

Les nombres *n* et *e* forment la clé publique avec laquelle n'importe qui pourra crypter un message. On la notera (*n*,*e*).

-Clé privée :

Il nous faut maintenant calculer le nombre *d* qui sera nécessaire au déchiffrement. Selon la théorie de RSA, nous devons avoir *d* tel que *e**d-1 soit divisible par φ(n) (i.e ∃k tel que

e*d-1=k*φ(n)), soit :
Trouver d et k ∈z tel que e*d+k*φ(n)=1

Or, comme *e* et *φ(n) sont premiers entre eux, le théorème de Bezout prouve l'existence de *d* et *k* dans *Z*. Ceci signifie donc que $d=e^{-1} \bmod \varphi(n)$.

Nous voilà prêts à décrypter. Le nombre *d* est notre clé privée. Nous pouvons à présent divulguer la clé publique (*n*,*e*) et garder la clé privée. Quant aux nombres *p*, *q*, et φ(n) , on doit soit les conserver secrets, soit les détruire car ils ne serviront plus.

2-Chiffrement du message :

soit *m* un message, son chiffré *c* est obtenu par $c=m^e \bmod n$.

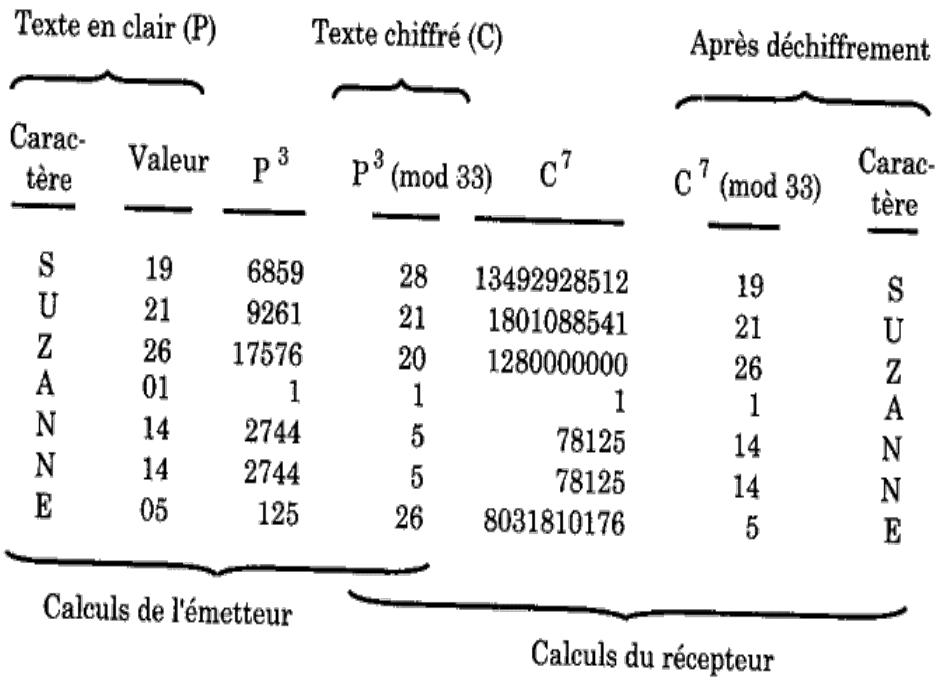
3-Déchiffrement du message codé :

m est retrouvé à l'aide de la clé secrète par $m=c^d \bmod n$.

4-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 : [15]



3-6-2-3- Chiffrement mixte

Les algorithmes à clé publique sont assez lents. La méthode généralement utilisée pour envoyer un message, est de tirer au hasard une clé secrète, chiffrer le message avec un algorithme à clé privée en utilisant cette clé, puis chiffrer cette clé aléatoire elle-même avec la clé publique du destinataire. Ceci permet d'avoir la sécurité des systèmes à clé publique, avec la performance des systèmes à clé privée. Il existe un logiciel qui effectue toutes ces opérations de manière transparente, et qui est gratuit et téléchargeable à partir de dizaines de sites par le monde : le célèbre **PGP** de **Phil Zimmermann**. (Il y a d'autres logiciels aussi performants, mais PGP est sûrement le plus connu.). Correctement utilisé, il est sûr, même contre les meilleurs cryptanalystes du monde.

4-Qu'est-ce que la Cryptanalyse ?

La Cryptanalyse est tout simplement l'art de rendre clair un texte crypté sans avoir connaissance de la clef utilisée. Dans la Cryptanalyse, on part du principe que l'homme est faible, et facilement soudable. Ainsi, on considère que la force d'un système de cryptographie ne doit pas reposer sur la non connaissance d'un algorithme mais sur la force du principe utilisé. Dans le jargon de la cryptographie, on appel **attaque** une tentative de déchiffrement. Les méthodes de Cryptanalyse sont bien sûr très nombreuses et dépendent en grande partie du type d'algorithme auquel on est confronté des clefs pour chiffrer les textes. l'intérêt est très limité car, à partir du moment ou vous possédez les clefs il ne reste plus grand chose à faire.

5- Les protocoles utilisant la cryptographie :

Les protocoles cryptographiques sont connus pour établir la confiance lors des transactions électroniques. Ils reposent sur des primitives cryptographiques visant à assurer l'intégrité des données, l'authentification ou l'anonymat des participants, la confidentialité des transactions, …etc.

5-1- Protocole SSL :

SSL (Secure Sockets Layers, que l'on pourrait traduire par couche de sockets sécurisée) est un procédé de sécurisation des transactions effectuées via Internet mis au point par Netscape, en collaboration avec Mastercard, Bank of America, MCI et Silicon Graphics. Il repose sur un procédé de cryptographie par clef publique afin de garantir la sécurité de la transmission de données sur Internet.
Le système SSL est indépendant du protocole utilisé, ce qui signifie qu'il peut aussi bien sécuriser des transactions faites sur le Web par le protocole HTTP que des liaisons via le protocole FTP ou Telnet.

En effet, SSL agit telle une couche, permettant d'assurer la sécurité des données, et située entre les sockets (l'implémentation logicielle, c'est-à-dire les lignes d'un programme orienté Internet, permettant à l'ordinateur d'envoyer des informations via une ligne de transmission) et un protocole de la suite TCP/IP.

De cette manière, SSL est transparent pour l'utilisateur (entendez par là qu'il peut ignorer qu'il utilise SSL). Par exemple un utilisateur utilisant un navigateur Internet pour se connecter à un site de commerce électronique sécurisé par SSL enverra des données cryptées sans s'en préoccuper.

La globalité des navigateurs supporte désormais les Secure Sockets Layers. Netscape Navigator affiche par exemple un cadenas verrouillé pour indiquer la connexion à un site sécurisé par SSL et un cadenas ouvert dans le cas contraire, tandis que Microsoft Internet Explorer affiche un cadenas uniquement lors de la connexion à un site sécurisé par SSL. Un serveur sécurisé par SSL possède une URL commençant par https://, où la "s" signifie bien évidemment secured (sécurisé).

6-Conclusion :

Explorer les méthodes cryptographiques sur les informations peut essentiellement apporter un meilleur niveau de sécurité à votre système et à ses données. Cependant, la mise en place d'une bonne surveillance du codage et d'une formation des utilisateurs est indispensable si vous souhaitez assurer une protection efficace de vos données, même codée.
Cependant, même si la cryptographie apparaît comme étant un système le plus répandu pour garantir la transmission et la confidentialité de ses données circulant sur les réseaux, la cryptographie demeure constamment communicative pour concevoir des nouvelles méthodes cryptographiques, ce qui permet aux internautes d'aller plus loin dans la protection de leur données personnelles.
Mais comme, les méchants existent : il s'agisse de terroristes, de mafieux, d'espions, les possibilités données à ces gens là pour communiquer secrètement est une arme trop dangereuse et il est indispensable que les autorités aient une possibilité de les combattre efficacement.