3.1 Introduction

Un crypto système, est un terme utilisé en cryptographie pour désigner un ensemble composé d'algorithmes cryptographiques et de tous les textes en clairs, textes chiffrés et clés possibles (définition de Bruce Schneier). Cette dénomination est toutefois confuse car très souvent associée à la cryptographie asymétrique avec l'utilisation d'une clé publique pour les opérations de chiffrement. **[7][A]**

Nous allons exposer les différentes méthodes de cryptographie utilisée actuellement les principes qui y sont sous-jacents.

1. Les systèmes à clefs secrètes, dont le plus connu est le système DES.
2. Et le système de cryptage à clefs publiques dont la méthode la plus employée est le système RSA.

Nous avons fait une comparaison de ces méthodes de cryptage.

En fait de telles méthodes sont souvent mixées pour donner des méthodes mixtes ce qui permet de conjuguer les avantages des deux méthodes.

A coté de ces méthodes classiques, pour lesquelles des méthodes de cryptanalyse se développent depuis des dizaines d'années, apparaissent des méthodes nouvelles plus originales, plus lentes aussi (donc pas opérationnelles pour des transferts de très gros fichiers), mais pas moins efficaces.

3.2. Description de systèmes cryptographiques classiques

3.2.1. *Algorithme de substitution*

Le chiffrement par substitution, consiste à remplacer dans un message une ou plusieurs entités (généralement des lettres) par une ou plusieurs autres entités.

- ***Substitution monoalphabétiques :*** Consiste à remplacer chaque lettre du message par une autre lettre de l'alphabet.
- ***Substitution polyalphabétique :*** consiste à utiliser une suite de chiffres monoalphabétiques réutilisée périodiquement.
- ***Substitution homophonique :*** permet de faire correspondre à chaque lettre du message en clair un ensemble possible d'autres caractères.

- ***Substitution de polygrammes :*** consiste à substituer un groupe de caractères (polygramme) dans le message par un autre groupe de caractères.

3.2.2. *Le chiffre de césar*

Ce code est l'un des plus anciens, utilisé par Jules César. Le principe de codage repose sur l'ajout d'une valeur constante à l'ensemble des caractères du message, ou plus exactement à leur code ASCII.

Il consiste en une substitution mono-alphabétique : chaque lettre est remplacée ("substitution") par une *seule* autre ("mono-alphabétique"), selon un certain décalage dans l'alphabet ou de façon arbitraire. D'après Suétone, César avait coutume d'utiliser un décalage de 3 lettres : A devient D, B devient E, C devient F, etc. Il écrivait donc son message normalement, puis remplaçait chaque lettre par celle qui lui correspondait. Lorsque l'ajout de la valeur donne une lettre dépassant la lettre Z, il suffit de continuer en partant de A, ce qui revient à effectuer un modulo 26.

CLAIR	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
-> décalage = 3																										
CODE	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

Tableau 3.1 : le principe de César

On appelle clé le caractère correspondant à la valeur que l'on ajoute au message pour effectuer le cryptage. Dans notre cas la clé est C, car c'est la 3éme lettre de l'alphabet.

Ce système de cryptage est certes simple à mettre en œuvre, mais il a pour inconvénient d'être totalement symétrique, cela signifie qu'il suffit de faire une soustraction pour connaitre le message initial. Une méthode primaire peut consister à une bête soustraction des nombres 1 à 26 pour voir si l'un de ces nombres donne un message compréhensible.

Une méthode plus évoluée consiste à calculer les fréquences d'apparition des lettres dans le message codé (cela est d'autant plus facile à faire que le message est long). Effectivement, selon la langue, certaines lettres reviennent plus couramment que d'autre (en français, par exemple, la lettre la plus utilisée est la lettre E), ainsi la lettre apparaissant le plus souvent dans un texte crypté par le chiffrage de César correspondra vraisemblablement à la lettre E, une simple soustraction donne alors la clé de cryptage. **[6][8][B]**

3.2.3. *Le chiffre de VIGENERE ou de BEAUFORT*

Fonctionnement

Le chiffre de vigenere est un système de chiffrement, élaboré par Blaise de vigenere (1523-1596), diplomate français du XVI° siècle.

Ce chiffrement introduit la notion de clé (elle se représente sous la forme d'un mot ou d'une phrase).

		Lettre en clair																										
		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**	
Clé Utilisée	**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	**Lettre chiffrée**
	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	

Tableau 3.2 : table de vigenere

Il consiste à remplacer une lettre par une autre qui n'est pas toujours la même. L'outil indispensable de ce chiffrement est la table de « **vigenere »;** table de 26 alphabets de substitution.

Caractère de la clé K : nombre de décalage dans l'i_éme alphabet.

Voici la table de vigenere. C'est un code très difficile à « casser » si on ne connait pas la clé, donc très sur. Le codage/décodage est par contre un peu long… **[15][8][B]**

Pour coder ton message, pour chaque lettre du message en clair tu sélectionne la colonne correspondante et pour une lettre de la clé tu sélectionne la ligne adéquate, puis au croisement de la ligne et de la colonne on trouve la lettre de chiffrement. Si ton message est plus long que ta clé, réécris la première lettre de la clé.par exemple si tu veux coder « BONJOUR » avec la clé « SCOUT », ça donne « TQBDHMT », comme dans le tableau si dessous.

Message	clé	code
B	S	T
O	C	Q
N	O	B
J	U	D
O	T	H
U	S	M
R	C	T

Pour décoder il faut que tu connaisses la clé. Dans la colonne correspondant à la première lettre de la clé, trouve la première lettre du code. Tu peux donc retrouver la première du message au bout de la ligne. Poursuis ensuite avec les lettres suivantes. Là encore, si ton message codé est plus long que la clé, repars à la première lettre de la clé **[7][8].**

Principe mathématique

Mathématiquement, on considère que les lettres de l'alphabet sont numérotées de 0 à 25 (A=0, B=1…). La transformation lettre par lettre se formalise simplement par :

- Chiffre= (texte + clé) modulo 26

(Texte+ clé) modulo 26 correspond au « reste de la division entière de (Texte+clé) par 26 », les ordinateurs le font très bien ! En fait il suffit d'effectuer l'addition des deux caractères puis de trouver le numéro correspondant à la lettre chiffrée, notre alphabet étant circulaire (après Z on A), le modulo nous assure que notre résultat sera compris entre 0 et 25.

Remarquez que si l'on utilise la clé avec un texte rempli uniquement avec des A on retrouve assez facilement la clé.

- « A » + Lettre Inconnue = Lettre Inconnue, soit du point de vue mathématique : 0 +x = x.

3.2.4. Le chiffre de transposition

Les méthodes de chiffrement par transposition consistent à réarranger les données à crypter de telle façon à les rendre incompréhensibles. Il s'agit généralement de réarranger géométriquement les données pour les rendre visuellement inexploitable.[6][8][C]

La technique assyrienne

Cette technique de cryptage est vraisemblablement la première preuve de l'utilisation de moyens de chiffrement en Grèce dès 600 avant Jésus Christ pour dissimuler des messages écrits sur des bandes de papyrus.

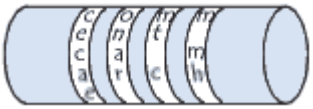

Figure 3.1 : la technique assyrienne **[D]**

La technique consistait à :

- Enrouler une bande de papyrus sur un cylindre appelé **scytale.**
- Ecrire le texte longitudinalement sur la bandelette ainsi enroulée (le message dans l'exemple si dessus est « comment ça marche »).

Le message une fois déroulé n'est plus compréhensible (« cecaeonar mt c m mh »). Il suffit au destinataire d'avoir un cylindre de même rayon pour pouvoir déchiffrer le message. En réalité un casseur peut déchiffrer le message en essayant des cylindres de diamètre successifs différents, ce qui revient à dire que la méthode peut être cassée statiquement (il suffit de prendre les caractères un à un, éloignés d'une certaine distance).

Exemple écriture en dents scie :

Le texte clair : LA TRANSPOSITION PERMET EN THEORIE D'AVOIR UN HAUT DEGRE DE SECURITE

L	R	S	S	I	P	M	E	H	R	D	O	U	A	D	R	E	C	I
A	A	P	I	O	E	E	N	E	I	A	I	N	U	E	E	S	U	T

T	N	O	T	N	R	T	T	O	E	V	R	H	T	G	D	E	R	E

Tableau 3.3 : écriture en dents scie

Le texte chiffré :

LRSSIPMEHRDOUADRECIAAPIOEENEIAINUEESUTTNOTNRTTOEVRHTGDE

3.2.5. Le OU exclusif

Tous les électroniciens connaissent la table de vérité du ou exclusif, que nous nous rappelons tout de même en tableau suivant :

A	B	C=A⊕B
0	0	0
0	1	1
1	0	1
1	1	0

Tableau 3.4 : table de vérité du OU exclusif

Le OU exclusif peut être utilisé comme chiffre cryptographiques au moyen d'une clé, et en applique alors les relations :

C=M(+) K pour le chiffrement

M=C(+) K pour le déchiffrement

Il est évident que cette relation n'est appliquée bit à bit, c'est-à-dire avec une clé de un bit, mais qu'elle travaille au contraire sur des blocs, de tailles identiques à la taille de la clé. Même avec une clé très longue, il faut tout de même savoir que le OU exclusif n'arrête pas un bon cryptographe plus de quelques minutes.[6][8][E]

3.3. Système cryptographiques modernes

3.3.1. Systèmes symétriques à clé secrètes

La cryptographie à algorithmes symétriques utilise la même clé pour les processus de codage et de décodage ; cette clé est le plus souvent appelée « secrète ». le chiffrement consiste à appliquer une opération (algorithme) sur les données à chiffrer à l'aide de la clé privée, afin de les rendre inintelligibles. Ainsi, le moindre algorithme peut rendre le système quasiment inviolable (la sécurité absolue n'existant pas). **[4]**

Toutefois dans les années 40 Claude Shannon démontra qu'être totalement sûre, les systèmes à clefs privées doivent utiliser des clefs d'une longueur au moins égale à celle du message à chiffrer. **[12] [1] [7][F]**

Principe de base

Un expéditeur et un destinataire souhaitant communiquer de manière sécurisée à l'aide du cryptage conventionnel doivent convenir d'une clé et ne pas la divulguer. Dans la majorité des systèmes de cryptages symétrique la clé de chiffrement et la clé de déchiffrement sont identiques.

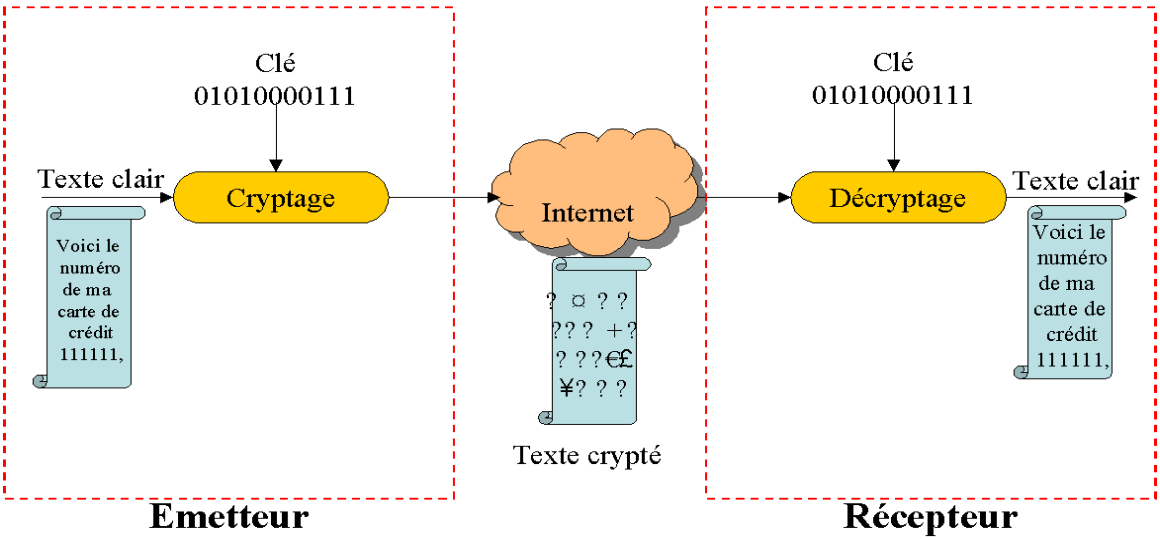

Figure 3.2 : cryptographie symétrique

Quelques algorithmes de chiffrement symétriques très utilisés :

- Chiffre de Vernam (le seul offrant une sécurité théorique absolue, à condition que la clé ait au moins la même longueur que le message, qu'elle ne soit utilisée qu'une seule fois à chiffrer et qu'elle soit totalement aléatoire)

- DES
- 3DES
- AES

- RC5

3.3.2. Génération du DES

Le *Data Encription Standard* (standard de chiffrement de données a été publié en 1977, et fut ainsi le premier algorithme cryptographie à petite clé secrète (56 bits) à avoir été rendu public. Le DES consiste en un réseau de Feistel de 16 tours : le message à chiffrer est découpé en blocs de 64 bits, chacun d'eux étant séparé en deux sous-blocs de 32 bits.

Le cahier des charges était le suivant :

- L'algorithme repose sur une clé relativement petite, qui sert à la fois au chiffrement et au déchiffrement.
- L'algorithme doit être facile à implémenter, logiciellement et matériellement, et doit être très rapide.
- Le chiffrement doit avoir un haut niveau de sûreté, uniquement lié à la clé, et non à la confidentialité de l'algorithme**. [7][14][G]**

Principe du DES

Le DES n'est qu'un code produit dont l'idée vient de Shanon : il combine simultanément diffusion et confusion qui sont des méthodes peu sure quant on les utilise séparément. Néanmoins, leur combinaison permet d'attendre un niveau de sécurité assez considérable. Nul ne pourrait démontrer l'inviolabilité d'un tel produit, mais l'aspect aléatoire du produit des bits chiffrés rendait la tache très difficile à tout cryptanalyse. La diffusion utilise ici des permutations dont le but est d'éclater dans le fichier crypté la redondance présente dans le fichier clair.

La confusion qui a pour but de compliquer la liaison entre le fichier crypté et les clés secrètes, utilise ici des substitutions, non linéaires, de façon à produire un système cryptographique qui résiste à toute cryptanalyse mathématique.

Notons que à l'origine, le DES est un code à blocs de 64 bits. Le fichier clair est donc découpé en plusieurs blocs de 64 bits. La transformation d'un bloc comporte 16 itérations d'un processus de codage, qui effectue respectivement une étape de confusion, puis une étape de diffusion. **[7] [14].**

En effet, la sécurité des données cryptées repose sur une clé secrète de 64 bits (succession de 0 et de 1), mais en fait seuls 56 bits servent réellement à définir la clé. Les bits 8, 16, 24, 32, 40, 48, 56, 64 sont des bits de parité (=bits de détection d'erreur). Le 8éme bit est fait en sorte

que sur les 8 premiers bits, il y ait un nombre impair de 1. Par exemple, si les 7 premiers bits sont 1010001, le 8éme bits est 0. Ceci permet d'éviter les erreurs de transmission. **[7]**

Les grandes lignes de l'algorithme sont les suivantes

Phase1 : préparation- diversification de la clé :

Le texte est découpé en blocs de 64 bits. On diversifie aussi la clé K, c'est-à-dire qu'on fabrique à partir de K 16 sous-clés K1,……, K16 à 48 bits. Les Ki sont composés de 48 bits de K, pris dans un certain ordre.

Phase2 : permutation initiale :

Pour chaque bloc de 64 bits x du texte, on calcule une permutation finie y=P(x). y est représenté sous la forme y=G0D0, G0 étant les 32 bits à gauche de y, D0 les 32 bits à droite.

Phase3 : Itération :

On applique 16 rondes d'une même fonction. A partir de Gi-1Di-1 (pour i de 1 à 16), on calcule GiDi en posant :

- Gi=Di-1
- Di=Gi-1 XOR f(Di-1,Ki)

XOR est le ou exclusif bit à bit, et f est une fonction de confusion, suite de substitution et de permutations.

Phase4 : permutation finale :

On applique à G16D16 l'inverse de la permutation initiale. $Z=P^{-1}(G16D16)$ est le bloc de 64 bits chiffré à partir de x.

Description du DES *:*

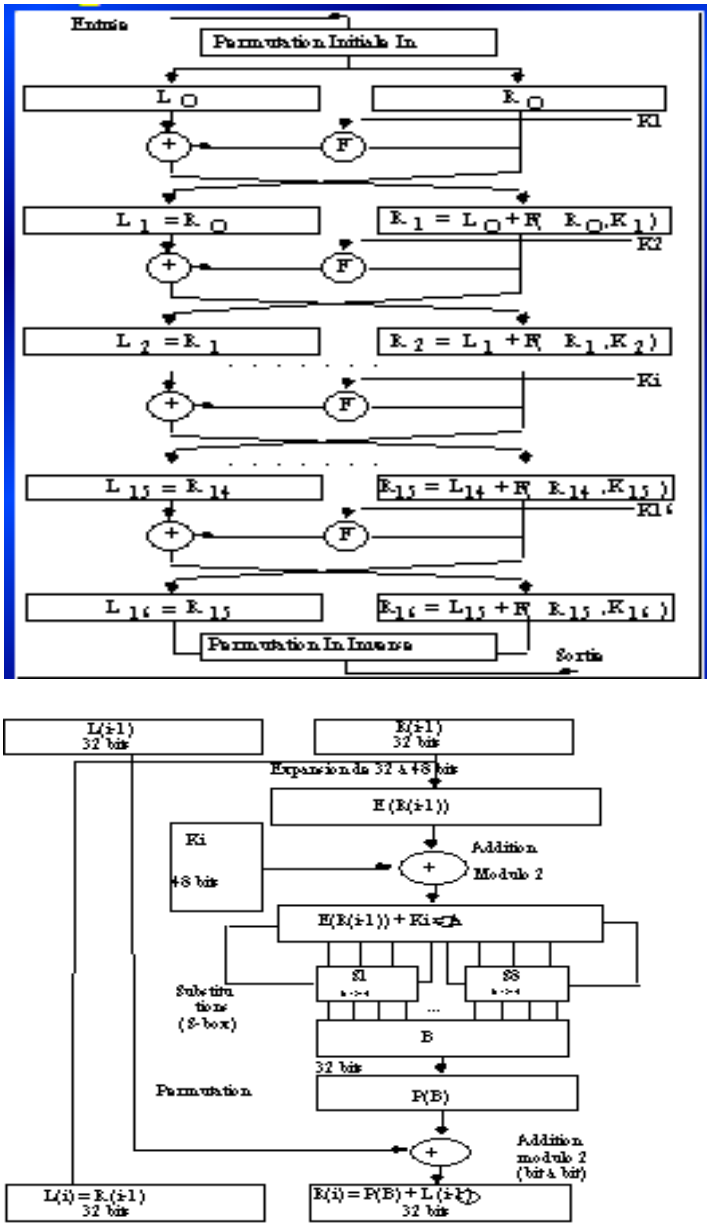

Figure 3.3 : Schémas générale du DES

Le DES utilise une clé K de 56 bits, pour chiffrer des blocs de 64 bits, les blocs chiffrés obtenus ayant aussi 64 bits. Le bloc de texte clair subit d'abord une permutation initiale. Puis on itère 16 fois une procédure identique, ou la moitié droite est recopié telle quelle à gauche, et la moitié gauche est transmise à droite en subissant au passage une modification dépendante de la clé. A la fin, on inverse les moitiés gauches et droites (ou bien, comme sur les schémas, on supprime le croisement de la dernière étape), et on applique l'inverse de la permutation initiale pour obtenir le bloc chiffré. Le schéma général du DES est donc le suivant (on a seulement représenté quelques-unes des 16 étapes). **[7][H]**

3.3.3. Les avantages

Le cryptage conventionnel comporte un avantage majeur : sa rapidité, il est particulièrement adapté à la transmission de grandes quantités de données, la cryptographie symétrique est très utilisée et se caractérise par une grande rapidité (cryptage à la volée), des implémentations aussi bien software (Krypto Zone, firewalls logiciels type firewall-1, et VPN-1 de check point) que hardware (carte dédiées, processeurs cryptos 8 à 32 bits, algorithmes câblés…) ce qui accélère nettement les débits et autorise son utilisation massive. **[1][7]**

3.3.4. Les faiblesses

Ces systèmes nécessitent la connaissance de la clé par l'émetteur et par le destinataire. C'est la transmission de cette clé entre les intervenants qui représente la faiblesse inhérente du système, s'ils se trouvent à des emplacements géographique différentes, ils devront faire confiance à une tierce personne ou un moyen de communication sécurisé, toute personne interceptant la clé lors d'un transfert peut ensuite lire, modifier et falsifier toutes les informations cryptées ou authentifiées avec cette clé.

De la norme de cryptage de données DES au code secret de Jules César, la distribution des clés reste le problème majeur du cryptage conventionnel. (Autrement dit, comment faire parvenir la clé à son destinataire sans qu'aucune personne ne l'intercepte ?). les moyens à déployer pour garantir la distribution sécurisée des clés entre les correspondants sont très onéreux, ce qui constitue un inconvénient supplémentaire. **[1][7]**

Malgré toutes ses évolutions et ses mises en œuvre, la cryptographie à clé secrète est toujours entravée par un défaut : la condition sine qua non de son succès est et restera le secret de sa clé Bien qu'ayant pu au fil du temps réduire sa taille, les cryptographes ont toujours été confrontés au problème de la transmission de cette clé... Mais le progrès ne s'arrête jamais ! Si le problème est de conserver le secret de la clé, pourquoi ne pas le contourner... en inventant un système qui la rend ***publique.***

3.4. Systèmes asymétriques à clé publique

3.4.1. Définition et fonctionnement

La cryptographie asymétrique à clé publique est apparue pour la première fois en 1976 avec la publication d'un ouvrage sur la cryptographie par Whitfield Diffie et Martin Hellman, c'est méthode de chiffrement qui s'oppose à la cryptographie symétrique.

Dans un tel crypto système, les clés existent en paires d'où l'appellation bi-clés :

- Une clé publique pour le chiffrement.
- Une clé secrète pour le déchiffrement.

L'utilisateur d'un crypto système asymétrique, choisit une clé aléatoire (la clé privé), à partir de cette clé et en appliquant la fonction à sens unique il calcule la clé publique qu'il diffuse au travers d'un canal non sécurisé.
Lorsqu'une personne désire lui envoyer un message il lui suffit de chiffrer ce dernier à l'aide de la clé publique.

Le destinataire sera en mesure de déchiffrer le message à l'aide de sa clé privé.

Ce système est basé sur une fonction facile à calculer dans un sens (appelé fonction à trappe à sens unique) et mathématiquement très difficile à inverser sans la clé privée appelé trappe. **[7] [1][4]**

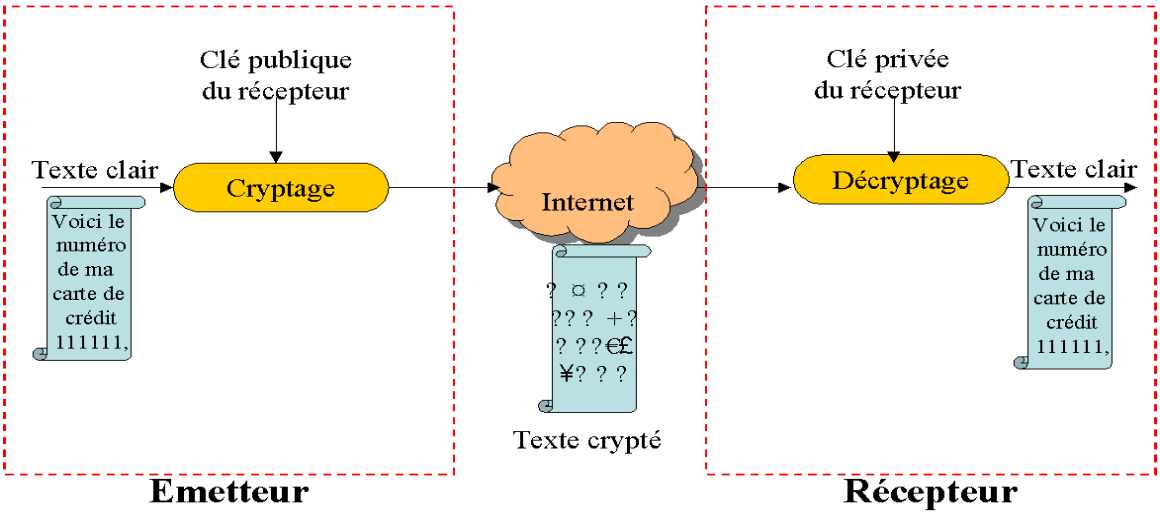

Figure 3.4 : cryptographie asymétrique

Les principaux algorithmes asymétriques à clé publiques sont :

RSA (chiffrement et signature)

DSA (signature)

Diffie-Hellman (échange de clé) **[7]**

3.4.2. L'algorithme RSA

Le principe

Le premier système à clé publique solide à avoir été inventé, et le plus utilisé actuellement, est le système RSA. Publié en 1977 par Ron **R**ivest, Adi **S**hamir et Leonard **A**dleman de l'Institution de technologie du Massachusetts, le RSA est fondé sur la difficulté de factoriser des grands nombres, et la fonction à sens unique utilisée est une fonction "puissance".

L'algorithme de chiffrement

Départ :

- Il est facile de fabriquer de grands nombres premiers p et q (+- 100 chiffres)
- Etant donné un nombre entier n = p*q, il est très difficile de retrouver les facteurs p et q

1) Création des clés

- La clé secrète : 2 grands nombres premiers p et q
- La clé publique : n = p*q ; un entier e premier avec (p-1) (q-1)

2) Chiffrement : le chiffrement d'un message M en un message codé C se fait suivant la transformation suivante :

$C = M^e \bmod n$

3) Déchiffrement : il s'agit de calculer la fonction réciproque

$M=C^d \bmod n$
tel que $e.d = 1 \bmod [(p-1)(q-1)]$

Exemple : chiffrer BONJOUR

1) Alice crée ses clés :

- La clé secrète : **p = 53, q = 97** (Note : en réalité, p et q devraient comporter plus de 100 chiffres !)
- La clé publique : **e = 7 (premier avec 52*96), n = 53*97 = 5141**

2) Alice diffuse sa clé publique (par exemple, dans un annuaire).

3) Bob ayant trouvé le couple **(n, e)**, il sait qu'il doit l'utiliser pour chiffrer son message. Il va tout d'abord remplacer chaque lettre du mot BONJOUR par le nombre correspondant à sa position dans l'alphabet :

B = 2, O = 15, N = 14, J = 10, U = 21, R = 18

BONJOUR = 2 15 14 10 15 21 18

4) Ensuite, Bob découpe son message chiffré en blocs de même longueur représentant chacun un nombre plus petit que **n**. Cette opération est essentielle, car si on ne faisait pas des blocs assez longs (par exemple, si on laissait des blocs de 2 chiffres), on retomberait sur un simple chiffre de substitution que l'on pourrait attaquer par **l'analyse des fréquences**.

BONJOUR = 002 151 410 152 118

5) Bob chiffre chacun des blocs que l'on note **B** par la transformation $\mathbf{C = B^e mod\ n}$ (où C est le bloc chiffré) :

$C_1 = 2^7 \text{mod } 5141 = 128$
$C_2 = 151^7 \text{mod } 5141 = 800$
$C_3 = 410^7 \text{mod } 5141 = 3761$
$C_4 = 152^7 \text{mod } 5141 = 660$
$C_5 = 118^7 \text{mod } 5141 = 204$

On obtient donc le message chiffré C : 128 800 3761 660 204

3.4.3 Le protocole de Diffie et Hellman

Parallèlement à leur principe de cryptographie à clé publique, Diffie et Hellman ont proposé un protocole d'échanges de clés totalement sécurisé, basé sur des fonctions difficiles à inverser.

1) Alice et Bob se mettent d'accord publiquement sur un très grand nombre premier "p" et sur un nombre "n" inférieur à "p".

2) Alice engendre une clé secrète "a" et Bob une clé secrète "b".

3) Alice calcul l'élément public k_a et Bob l'élément public k_b :

$k_a = n^a \text{ mod } p$
$k_b = n^b \text{ mod } p$

4) Alice transmet sa clé publique k_a à Bob, et Bob transmet sa clé publique k_b à Alice.

5) Alice et Bob profitent ensuite de la commutativité de la fonction exponentielle pour établir leur secret commun :

$K_{Alice} = (k_b)^a = (n^b)^a \text{ mod } p$
$K_{Bob} = (k_a)^b = (n^a)^b \text{ mod } p$
$\Rightarrow K_{Alice} = K_{Bob} = n^{ab} \text{ mod } p$

- ✓ **Les avantages**

  - Le problème consistant à se communiquer la clé de déchiffrement n'existe plus, dans la mesure où les clés publiques peuvent être envoyées librement. Le chiffrement par clés publiques permet donc à des personnes d'échanger des messages chiffrés sans pour autant posséder de secret en commun, seule la clé secrète à besoin d'être conservée de manière secrète.
  - Selon l'usage, une paire de clé (publique/secrète) peut être utilisée plus longtemps qu'une clé symétrique.
  - La cryptographie à clé publique permet de réaliser des schémas de signature électronique assurant un service de non répudiation.
  - Dans un grand réseau, le nombre de clés est beaucoup plus petit que dans un système symétrique car seulement 2n clés sont nécessaires s'il y a n utilisateurs dans le réseau. **[7][1][4].**

- ✓ **Inconvénients**

Tout le challenge consiste à s'assurer que la clé publique que l'on récupère est bien celle de la personne à qui l'on souhaite faire parvenir l'information chiffrée.

Les performances des systèmes asymétriques sont beaucoup moins bonnes que celles des systèmes symétriques car ces systèmes nécessitent de pouvoir calculer sur des grands nombres.

La taille des clés est généralement plus grande pour ces systèmes que pour les systèmes à clé secrète.

Aucun crypto système à clé publique n'a été prouvé inconditionnellement sur, car la base de ces crypto systèmes sont la fonction à sens unique dont la réciproque est en pratique impossible à calculer et donc le crypto système impossible à casser, mais on n'a pas la certitude qu'une fonction considérée aujourd'hui à sens unique ne sera pas demain résolu et considérée comme banale.

La cryptographie à clé publique nécessite la mise en place d'une infrastructure de gestion de clé afin d'éviter les attaques par le milieu. **[7][1][4]**

3.5. Conclusion

Dans ce chapitre on a décrit quelques algorithmes de chiffrements les plus utilisés, mais bien sur il en existe beaucoup d'autres.

Le choix de l'algorithme doit dépondre de l'application envisagée et donc des caractéristiques désirées et de l'espace mémoire disponible.

Dans notre projet nous somme intéressé aux méthodes de chiffrement moderne comme algorithme DES (clé secrète) et l'algorithme RSA (clé publique).