1.1 Introduction

L'origine de la cryptologie mot réside dans la Grèce antique. La cryptologie est un mot composé de deux éléments : «cryptos », qui signifie caché et « logos » qui signifie mot. La cryptologie est aussi vieille que l'écriture elle-même, et a été utilisé depuis des milliers d'années pour assurer les communications militaires et diplomatiques. par exemple, le célèbre empereur romain Jule César utilisait un algorithme de chiffrement pour protéger les messages à ses troupes. Dans le domaine de l'un de cryptologie peut voir deux visions : la cryptographie et la cryptanalyse. Le cryptographe cherche des méthodes pour assurer la sûreté et la sécurité des conversations alors que le Crypto analyse tente de défaire le travail ancien en brisant ses systèmes.

La cryptographie traditionnelle est l'étude des méthodes permettant de transmettre des données de manière confidentielle et la cryptanalyse, à l'inverse est l'étude des procédés cryptographiques, qui dépendent d'un paramètre appelé clé. [9][1]

1.2. Définition de la cryptologie

La cryptographie est une science mathématique qui comporte deux branches : la **cryptographie** et la **cryptanalyse.**

Le mot **cryptographie** est un terme générique désignant l'ensemble des techniques permettant de **chiffrer** des messages, c'est-à-d permettant de les rendre inintelligibles sans une action spécifique. Le verbe **crypter** est parfois utilisé mais on lui préférera le verbe chiffré.

La **cryptanalyse**, à l'inverse, est l'étude des procédés cryptographiques dans le but de trouver des faiblesses, en particulier, de pouvoir décrypter des messages chiffrés. Le décryptement est l'action consistant à trouver le message en clair sans connaitre la clef de **déchiffrement.**

La cryptologie, étymologiquement « la science du secret », ne peut être vraiment considérée comme une science que depuis peu de temps. Cette science englobe la cryptographie (l'écriture secrète) et la cryptanalyse (l'analyse de cette dernière).

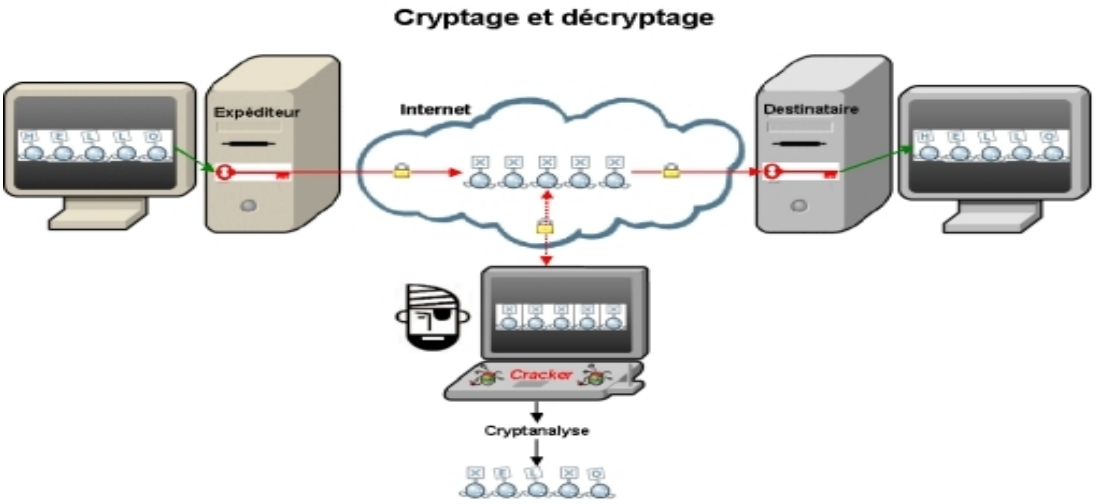


Figure 1.1 : Schéma de cryptage

1.3. Définition de la cryptographie

La cryptographie est l'**art de chiffrer**, coder les messages est devenue aujourd'hui une science à part entière. Au croisement des **mathématiques**, de l'**informatique**, et parfois même de la **physique**, elle permet ce dont les civilisations ont besoin depuis qu'elles existent : le maintien du secret. Pour éviter une guerre, protéger un peuple, il est parfois nécessaire de cacher des choses.

1.4. L'usage de la cryptographie

La cryptographie est traditionnellement utilisée pour dissimuler des messages aux yeux de certains utilisateurs. Cette utilisation a aujourd'hui un intérêt d'autant plus grand que les communications via internet circulent dans des infrastructures dont on ne peut garantir la fiabilité et la confidentialité. Désormais, la cryptographie sert non seulement à préserver la confidentialité des données mais aussi à garantir leur **intégrité** et leur **authenticité.**

- **La confidentialité** : consiste à rendre l'information intelligible 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.
- **L'authentification :** consiste à assurer l'identité d'un utilisateur, c.-à-d 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 crypté) l'accès à des ressources uniquement aux personnes autorisées.
- **La non répudiation :** de l'information est la garantie qu'aucun des correspondants ne pourra nier la transaction. **[2]**

1.5. Mécanisme de la cryptographie

Un algorithme de cryptographie ou un chiffrement est une fonction mathématique utilisée lors du processus de cryptage et de décryptage. Cet algorithme est associé à une clé(un mot, un nombre ou une phrase), afin de crypter une donnée. Avec des clés différentes, le résultat du cryptage variera également. La sécurité des données cryptées repose entièrement sur deux éléments : l'invulnérabilité de l'algorithme de cryptographie et la confidentialité de la clé**.[3]**

Qu'entend-on par clé ?

On appelle clé une valeur utilisée dans un algorithme de cryptographie, afin de chiffrer une donnée. Il s'agit en fait d'un nombre complexe dont la taille se mesure en bits. On peut imaginer que la valeur correspondant à 1024 bits est absolument gigantesque. Voir aussi bits bytes. Plus la clé est grande, plus elle contribue à élever la sécurité à la solution. Toutefois, c'est la combinaison d'algorithme complexe et de clés importantes qui seront la garantie d'une solution bien sécurisée.

Les clés doivent être stockées de manière sécurisée et de manière à ce que seul leur propriétaire soit en mesure de les atteindre et de les utiliser. **[1]**

1.6. Confidentialité et algorithmes de chiffrement

La confidentialité est le premier problème posé à la cryptographie. Il se résout par la notion de chiffrement. Il existe deux grandes familles d'algorithmes cryptographiques à base de clef :

Les algorithmes à clef secrète ou algorithmes symétriques, et les algorithmes à clef publique ou algorithmes asymétriques

- Chiffrement symétrique ou clef secrète : dans la cryptographie conventionnelle, les clefs de chiffrement et de déchiffrement sont identiques : c'est la clef secrète, qui doit être connue des tiers communiquant et d'eux seuls. Le procédé de chiffrement est dit symétrique.

  Les algorithmes symétriques sont de deux types :

- Les algorithmes de chiffrement en continu, qui agissent sur le message en clair un bit à la fois ;
- Les algorithmes de chiffrement par bloc, qui opèrent sur le message en clair par groupes de bits appelés blocs.

Les principaux algorithmes à clé privée sont :

Blowfish

DES/3DES

IDEA

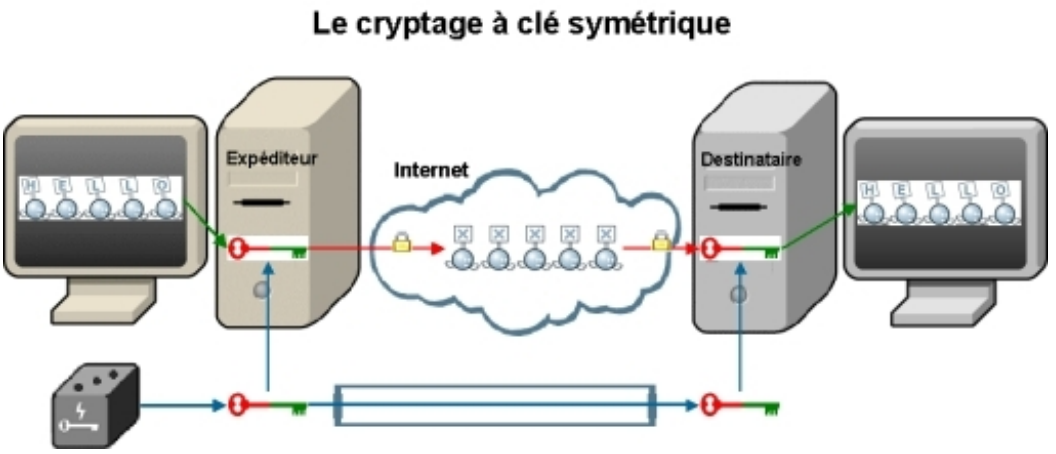


Figure 1.2 : cryptage à clé secrète

- Chiffrement asymétrique ou à clef public : avec les algorithmes asymétriques, les clefs de chiffrement et de déchiffrement sont distinctes et ne peuvent se déduire l'une de l'autre. On peut donc rendre l'une des deux publique tandis que l'autre reste privée. C'est pourquoi on parle de chiffrement à clef publique. Si la clef publique sert au chiffrement, tout le monde peut chiffrer un message, que seul le propriétaire de clef privé pourra déchiffrer. On assure ainsi la confidentialité. Certains algorithmes permettent d'utiliser la clef privée pour chiffrer. Dans ce cas, n'importe qui pourra déchiffrer, mais seul le possesseur de clef privée peut chiffrer. **[4]**

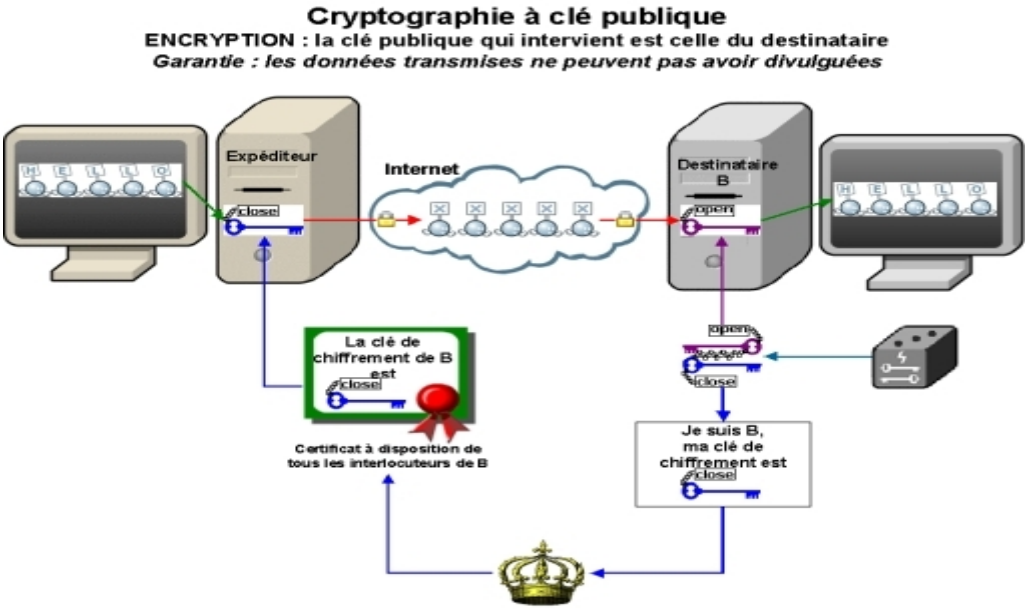


Figure I.3 : cryptage à clé publique

1.6.1. Les avantages et inconvénients de la cryptographie à clé publique comparé à la cryptographie à clé privée

Le premier avantage de la cryptographie à clé publique est d'améliorer la sécurité elle permet d'échanger des messages de manière sécurisée sans aucun dispositif de sécurité. L'expéditeur et le destinataire n'ont plus besoin de partager des clés secrètes via une voie de transmission sécurisée. Les communications impliquent uniquement l'utilisation de clés publiques et plus aucune clé privée n'est transmise ou partagée.

Avec un système à clé secrète, au contraire, il existe toujours le risque de voir la clé récupérée par une personne tierce quand elle est transmise d'un correspondant à l'autre. 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 correspondants sont très onéreux, ce qui constitue un inconvénient supplémentaire.

Le cryptage à clé publique représente une révolution technologique qui offert à tout citoyen la possibilité d'utiliser une cryptographie robuste. En effet, la cryptographie conventionnelle était auparavant la seule méthode pour transmettre des informations secrètes. Les couts d'institutions disposants de moyens suffisants, telles que gouvernements et banque.

Un autre avantage majeur des systèmes à clé publique est qu'ils permettent l'authentification des messages par signature électronique, ce qui peut aussi servir devant un juge, par exemple.

L'inconvénient des systèmes à clé publique est leur vitesse contrairement aux méthodes à clé secrète qui sont plus rapide. Ils sont particulièrement adaptés à la transmission de grandes quantités de données. Mais les deux méthodes peuvent être combinées de manière à obtenir le meilleur de leurs systèmes. Pour le cryptage, la meilleure solution est d'utiliser un système à clé publique pour crypter une clé secrète qui sera alors utilisée pour crypter fichiers et message**.[5]**

1.7. Différence entre chiffrement et codage

Les opérations de chiffrement et du codage font partie de la théorie de l'information. La différence essentielle réside dans la volonté de protéger les informations et d'empêcher des tierces personnes d'accéder aux données dans le cas du chiffrement. Le codage consiste à transformer de l'information (des données) vers un ensemble de mots. Chacun de ces mots est constitué de symboles. La compression est un codage : on transforme les données vers un ensemble de mots adéquats destinés à réduire la taille mais il n'y a pas de volonté de dissimuler (bien que cela se fasse implicitement en rendant plus difficile d'accès le contenu).

Le « code » dans le sens cryptographique du terme travaille au niveau de la sémantique (les mots ou les phrases). Par exemple, un code pourra remplacer le mot « avion » par un numéro. Le chiffrement travaille sur des composants plus élémentaires du message, les lettres ou les bits, sans s'intéresser à la signification du contenu. Un code nécessite une table de conversion, aussi appelée « dictionnaire » (code book en anglais). Ceci étant, « code » et « chiffrement » sont souvent employés de manière synonyme malgré cette différence.

On peut aussi considérer que le chiffrement doit résister à un adversaire « intelligent » qui peut attaquer de plusieurs manières alors que le codage est destiné à une transmission sur un canal qui peut être potentiellement bruité. Ce bruit est un phénomène aléatoire qui n'a pas « d'intelligence » intrinsèque mais peut toutefois être décrit mathématiquement. **[6]**

1.8. Définition de la cryptanalyse

La cryptanalyse s'oppose en quelque sorte à la cryptographie, c'est l'étude des faiblesses des systèmes cryptographiques, elle est effectuée généralement par un intrus qui met en œuvre des méthodes afin de retrouver des informations secrètes tel que la clé, message en clair à partir d'informations considérées comme publique (cryptogramme, algorithmes), la cryptanalyse est une des disciplines de la cryptologie.

Dans la cryptanalyse on part du principe que l'homme est faible et facilement soudoya le, ainsi la force d'un système doit reposer sur la force du principe utilisé.

Si le but de la cryptographie est d'élaborer des méthodes de protection, le but de la cryptanalyse est au contraire de casser ces protections.une tentative de cryptanalyse d'un système est appelé une attaque, et elle peut conduire à différents résultats :

- ***Cassage complet*** : le cryptanalyse retrouve la clef de déchiffrement.
- ***Obtention globale*** : le cryptanalyse trouve un algorithme équivalent à l'algorithme de déchiffrement, mais qui ne nécessite pas la connaissance de la clef de déchiffrement.
- ***Obtention locale*** : le cryptanalyse retrouve le message en clair correspondant à un message chiffrer.
- ***Obtention d'information*** : le cryptanalyse obtient quelque indication sur le message en clair ou la clef (certains bits de la clef, un renseignement sur la forme du message en clair).

D'une manière générale, on suppose toujours que le cryptanalyste connait le détail des algorithmes, fonctions mathématiques ou protocoles employés. Même si ce n'est pas toujours le cas en pratique, il serait risqué de se baser sur le secret des mécanismes utilisés pour assurer la sécurité d'un système, d'autant plus que l'usage grandissant de l'informatique rend de plus en plus facile la reconstitution de l'algorithme à partir du programme. **[7]** [A]

1.8.1 Les niveaux d'attaques

L'intrus peut effectuer quatre niveaux d'attaques, l'attaque est une tentative de cryptanalyse.

- ***L'attaque par cryptogramme*** (par message chiffré seulement) : ou le cryptanalyste ne connait qu'un ensemble de message chiffrés, il peut soit retrouver seulement les messages en clair, soit retrouver la clef. En pratique, il est très souvent possible de deviner certaines propriétés du message en clair (format ASCII, présence d'un mot particulier, …), ce qui permet de valider ou non le décryptement.
- ***L'attaque à message en clair connu*** : ou le cryptanalyste connait non seulement les messages chiffrés mais aussi les messages en clair correspondants, son but est alors de retrouver la clef. Du fait de la présence, dans la plupart des messages chiffrés, de parties connue (en-têtes de paquets, champs communs à tous les fichiers d'un type donné,…).

- ***L'attaque à message en clair choisi*** : ou le cryptanalyste peut, de plus choisir des messages en clair à chiffrer et donc utiliser des messages apportant plus d'informations sur la clef. Si le cryptanalyste peut de plus adapter ses choix en fonction des messages chiffrés précédents, on parle d'**attaque adaptative**.
- ***L'attaque à message chiffré choisi*** : qui l'inverse de la précédente, le cryptanalyste peut choisir des messages chiffrés pour lesquels il connaitra le message en clair correspondant ; sa tache est alors de retrouver la clef. Ce type d'attaques est principalement utilisé contre les systèmes à clef publique, pour retrouver la clef privée. **[8]**

1.9. Conclusion

Un concepteur de système cryptographique est toujours entrain d'essayer d'élaborer un système de chiffrement plus sure mais en même temps des intrus essayent de casser ce dernier, ils se livrent constamment une bataille mais les enjeux sont énorme : c'est la sécurité de nos transmissions qui est menacée.

Dans ce chapitre nous avons présenté une introduction générale sur la cryptographie, en a retrouver deux grandes classes des méthodes de chiffrement, les cryptographies symétriques à clé secrète et le cryptage asymétrique à clé publique, je suis intéressé dans mon mémoire par les deux méthodes de chiffrement appliqué aux textes arabes.

2.1. Introduction

Depuis des temps très reculés, l'homme avait utilisé diverses méthodes et techniques pour envoyer un message secrètement. Ce sont des méthodes qui transforment le message en clair en message incompréhensible ou qui cachent le message par une image, un texte ou autres choses sans qu'une personne étrangère puisse s'en apercevoir. Ce sont des méthodes de cryptographie ou des méthodes de stéganographie.

Les méthodes de cryptographie se basaient et se basent en général sur certaines notions ou certains phénomènes difficiles.

Actuellement, la cryptographie moderne se base en partie sur certaines notions difficiles en théorie des nombres comme la factorisation des grands nombres (RSA) ou le problème du logarithme discret (cryptographie elliptique).

L'utilisation des notions difficiles ou contraire à l'ordinaire pour établir des algorithmes de cryptographie était une tradition chez les cryptographes arabes. Ils avaient utilisé, entre autre, la poésie comme moyen de transmission et ont utilisé, par exemple, la difficulté d'écrire des vers de poésie (ou des morceaux de vers) suivant un modèle donné ou des vers qu'on peut lire de droite à gauche et en même temps de gauche à droite comme base d'algorithmes de cryptographie.

Ainsi, la poésie Arabe était un moyen de transmission, d'information, de publicité et de cryptographie.

Les Arabes ont utilisé la cryptographie même avant l'Islam ; mais les piliers de la cryptographie Arabe étaient bâtis par EL Khalil (718-786) et EL Kindi (801-873). Al Khalil avait :

- Modélise la poésie Arabe en 16 modèles.
- Elaboré un dictionnaire qui ne donne pas seulement la définition d'un mot donné mais donne aussi les définitions de tous les mots obtenus par permutation des lettres du mot

initial. Ceci permettra de décrypter tout mot crypté par permutation de lettres. Ainsi, c'est de plus un dictionnaire de cryptanalyse.

- Ecrit un livre de cryptographie qui n'a jamais été retrouvé.
- Introduit les statistiques linguistiques et l'analyse combinatoire.

El Kindi, le plus connu des savants Arabe en cryptographie, avait laissé un grand nombre de livres dans plusieurs domaines (philosophie, logique, mathématique, chimie, astronomie, poésie, médecine, musique, politique,…), en particulier en cryptographie. Il avait montré que tout message crypté à l'aide des méthodes de substitution peut être décrypté. Il avait utilisé, en particulier, l'analyse des fréquences de lettres, pour la cryptanalyse de plusieurs méthodes de cryptographie. El Kindi est donc le premier cryptanalyste Arabe.

2.2. La cryptographie Andalous-Marocaine

2.2.1. Historique[14][11]

Depuis 711 jusqu'à 1568, l'Andalousie avait connu une domination totale ou partielle des musulmans. De 714 à 756 c'était une province de l'Empire des Omeyades au moyen orient, et après la chute de ces derniers contre les Abbassides, la province de l'Andalousie devenait indépendante sous l'égide de certains Omeyades qui avaient fuit le pouvoir des Abbassides en orient. Cette indépendance a durée de 757 jusqu'à 1010, ou l'Andalousie était devenue un ensemble de plusieurs petits royaumes. Chacun des rois de ces petits royaumes voulait unifier l'Andalousie sous son autorité, ce qui avait mis l'Andalousie dans un état de Guerre, entre tous ces royaumes, entre 1010 et 1085. Après cette époque, elle avait été dominée par les Dynasties Marocaines « les Almoravides (1090-1143) »,et « les Mérinides (1273-1302) ».
Après la chute des Mérinides, il y avait une domination Musulmane partielle par le royaume de grande (1354-1568).

L'Epoque des petits royaumes, ou il avait un état de Guerre civile entre ces derniers, est l'époque qui a connu un développement de méthodes d'écriture des messages secrets.

Ces dernières méthodes sont devenues bien connues au Maroc et en Andalousie, pays qui étaient unis sous l'égide de plusieurs dynasties et pendant plus de trois siècles.

On trouve d'autres méthodes au Maroc et en Andalousie comme l'écrit Marocain en cryptographie qui avait été rédigé par Malloul ibn Ibrahim as-Sanhagi, secrétaire d'Ibn

Toumart (~1130) au début du mouvement des Almohades. C'était au sujet de la proclamation d'Ibn Toumart comme «Mahdi». Cet écrit avait été rédigé en langue secrète qui était un composé de la langue syriaque et de certains cryptogrammes.

Après cela, au Maroc on n'a rien trouvé jusqu'à l'arrivé de la dynastie sadienne ou on a trouvé des éléments qui méritent d'être exposés plus en détail dans les paragraphes suivants.

2.2.2. L'exemple du Roi Cryptographe Al Moetamid[13][15]

Al Moetamid Ibn Abade était le Roi de Ichbilia, la ville qu'on appelle aujourd'hui Séville, de 1069 à 1092. C'était un grand poète qui n'avait choisi son entourage et ses ministres que parmi les grands poètes, comme le célèbre poète Andalous Ibn Zaydoune et le poète Ibn Ammare.

Il est bien connu que parmi les oiseaux, on trouve des porteurs de lettres. Ce sont des oiseaux entrainés sur la transmission des lettres d'une personne à une autre. Ainsi, les oiseaux étaient un symbole de transmission de messages. C'est ainsi que Al Moetamid et Ibn Zaydoune avaient l'idée d'utiliser les oiseaux pour envoyer et recevoir des messages secret :

- Tout d'abord Al Moetamid et Ibn Zaydoune faisaient une correspondance entre l'ensemble des lettres de l'alphabet Arabe et un ensemble de noms d'oiseaux.
- Pour que l'un d'eux envoie un message donné à l'autre, il transforme l'ensemble des lettres du message en un ensemble ordonné de noms d'oiseaux. Ensuite, il compose une poésie ou il va citer les noms d'oiseaux obtenus par la transformation du message, dans l'ordre obtenu lors de la correspondance entre les lettres et les noms d'oiseaux.

Par la suite, il envoie cette poésie au destinataire. Le destinataire El Moetamid était surtout son ministre Ibn Zaydoune, qui a très bien su exécuter les différentes étapes de cette méthode de cryptographie et ainsi assurer une ligne secrète de messagerie avec le roi Al Moetamid. C'est ce dernier, qui avait envoyé un jour à Al Moetamid un message secret lui signalant qu'il était en force d'attaquer son ennemi et un autre jour, il lui avait envoyé un message secret disant « détruis ton ennemi et sauve toi ».

Cette méthode là, avait été probablement utilisée aussi pour échanger des clefs pour une méthode de cryptographie utilisant tout simplement une substitution entre les lettres de

l'alphabet. Car dans ce cas, la clef c'est uniquement l'écriture des lettres transformées chacune suivie par son image par la transformation utilisée lors du chiffrement.

2.3. La cryptographie Numérique Arabe

Avant de passer à la cryptographie numérique, on va définir le codage numérique Arabe et le calcul Arabe « Hissab Al Joummal », qui est un calcul utilisé par les Arabes pour cacher certains chiffres ou certaines dates importantes.

2.3.1. Codage numérique Arabe

Les valeurs numériques des lettres Arabes (codage numérique) sont données dans le tableau suivant :

10 ي	**9** ط	**8** ح	**7** ز	**6** و	**5** ه	**4** د	**3** ج	**2** ب	**1** ا
200 ر	**100** ف	**90** ض	**80** ف	**70** ع	**60** ص	**50** ن	**40** م	**30** ل	**20** ك
		1000 ش	**900** غ	**800** ظ	**700**	**600** خ	**500** ث	**400** ت	**300** س

Tableau 2.1 : codage numérique des lettres arabes

2.3.2. Calcul Arabe « Hissab Al-Joummal »[13][14][11][15]

Le calcul Arabe « Hissab Al-Joummal », est une fonction arithmétique h qui fait correspondre à chaque mot ou à chaque phrase un entier naturel qui n'est rien d'autre que la somme des valeur des valeurs numériques des lettres constituant le mot ou la phrase. Cette fonction était utilisée pour écrire certaines dates (comme les années de naissances ou de décès ou bien certain événements important) au milieu d'une phrase (généralement dans des vers de poésie).

La fonction h ainsi définit n'est pas une injection, ce qui veut dire que deux mots différents, peuvent avoir la même image par cette fonction. Par suite, si on a un nombre n et on veut déterminer un mot qui a cinq lettres et dont l'image par cette fonction est égale à n ; alors on peut avoir plusieurs solutions et suivants d'autres contraintes on pourra déterminer ce mot.

Mais il y a des exceptions ou on ne peut pas trancher, et dans ce cas on ne peut dire que la solution fait partie d'un ensemble qu'on peut déterminer. Le cardinal de ce dernier ensemble devient très grand si le nombre n devient assez grand et le nombre de lettres du mot cherché est aussi assez grand. Ainsi, cette fonction correspond aux fonctions de Hachage utilisées dans la cryptographie moderne ; mais pas avec les mêmes exigences.

Cette méthode avait été utilisée par les Arabes pour intégrer certaines dates sous forme de lettres dans un texte. Par exemple, on trouve, au Maroc, une poésie de Mohammed Bno Ahmed Eddadssi El Kabîr à l'époque de la dynastie saàdienne, ou il avait décrit les grands événements de son époque en les datant à l'aide de Hissab Al Joummal. De même Azzayani au 19éme siècle avait utilisé les mêmes principes pour décrire les événements de son époque.

2.3.3. Substitution Affine et le Codage numérique Arabe

Le codage numérique des lettres, avait été utilisé dans le monde Arabe pour crypter des messages dés le 13éme siècle :

- une première façon, était de remplacer les lettres par leurs codes numériques et en suite écrire les chiffres obtenus en lettres (10=dix).

- une deuxième façon, était de remplacer les lettres par leurs codes numériques, faire une multiplication par deux des chiffres obtenus (par exemple) et ensuite revenir aux lettres à l'aide de la correspondance entre lettres et chiffres dans le codage numérique. Ainsi, on obtient un texte crypté. Ceci correspond à la méthode de substitution affine d'aujourd'hui.

2.4. La cryptographie d'Or : période de la dynastie Saàdienne[10][12][15]

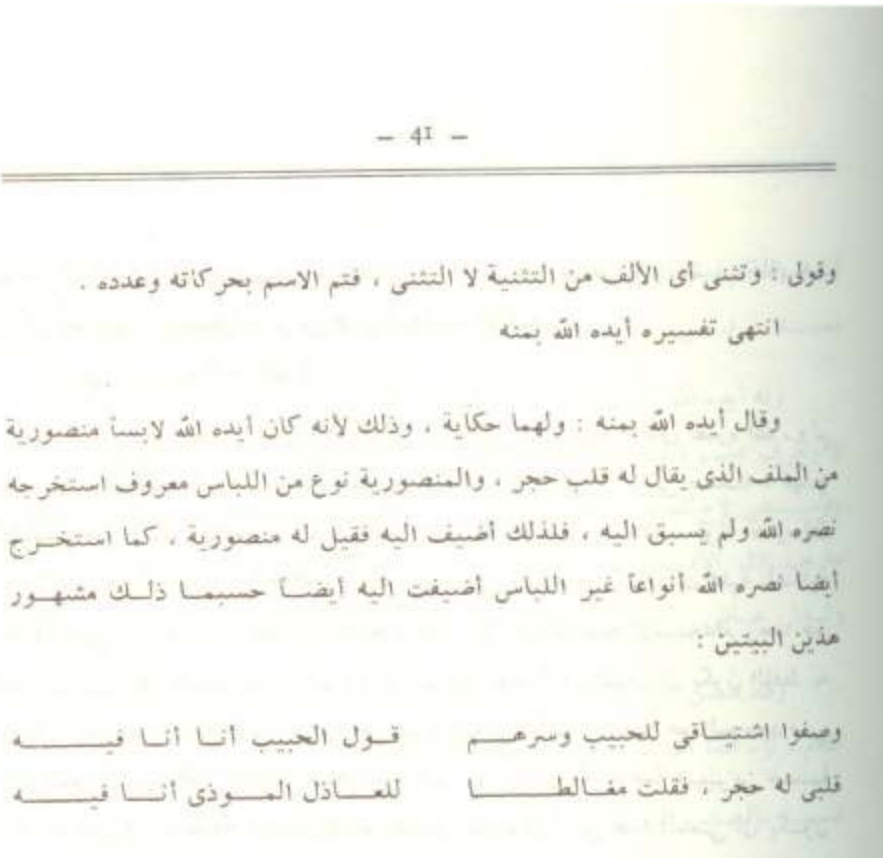
Les Saadiens avaient pris le pouvoir total du Maroc vers 1554. Ils avaient régné dans un climat très agité : luttes contre les occupations espagnoles et portugaises au nord et les Ottomans à l'Est. En particulier, ils avaient pu gagner la bataille d'Oued Almakhazine, ou bataille des trois Rois. A la suite de cette bataille, avec une bonne réputation international et un grand Roi El Mansour (le victorieux) le doré. Le sultan Ahmed El Mansour avait suivi une politique de développement et d'innovation dans tous les domaines scientifiques, industriels, militaires et sociaux. Il avait fait plusieurs expéditions au Sud saharien d'où il ramena du Sel et de l'Or. Ainsi, son époque avait connu un développement exceptionnel dans tous les domaines.

Entouré des Ottomans, des Espagnols et des portugais et devant leurs convoitises, El Mansour avait besoin d'une diplomatie qualifiée et sure. Comme il envoyait des émissaires et des Ambassadeurs pour tous les pays de son voisinage au Nord, à l'Est, au Sud et même à l'intérieur de son pays, alors il avait besoin de méthodes de messagerie très sures. Pour cela, il s'est intéressé lui-même à la cryptographie et avait inventé un cryptogramme secret qu'il avait utilisé à l'intérieur du Maroc avec ses gouverneurs et à l'étranger avec ses ambassadeurs ou ses émissaires.

2.4. Exemple de cryptogrammes publiés d'El Mansour[15]

Le Sultan El Mansour était un savant ; il avait de grandes connaissances en mathématiques, en sciences coraniques, en grammaire, en poésie et en cryptographie. En particulier, il avait développé la cryptographie Arabe par plusieurs réalisations et qui sont ses propres inventions. Les deux vers, qui se trouvent dans un livre d'El-Makkari et dans un livre d'Ibn Al Kadi, en sont un exemple.

Cette page (qui est identique à celle d'Ibn Al Kadi), qui contient les deux vers en plus de l'explication de la méthode numérique utilisé pour crypter et décrypter, dans ce paragraphe car El-Makkari ne faisait dans cette page, que décrire une conférence du Sultan El Mansour, sur le chiffrement et le déchiffrement du cryptogramme se trouvant dans les deux vers.



— 41 —

وقولى : وتثنى أى الألف من التثنية لا التثنى ، فتم الاسم بحركاته وعدده .

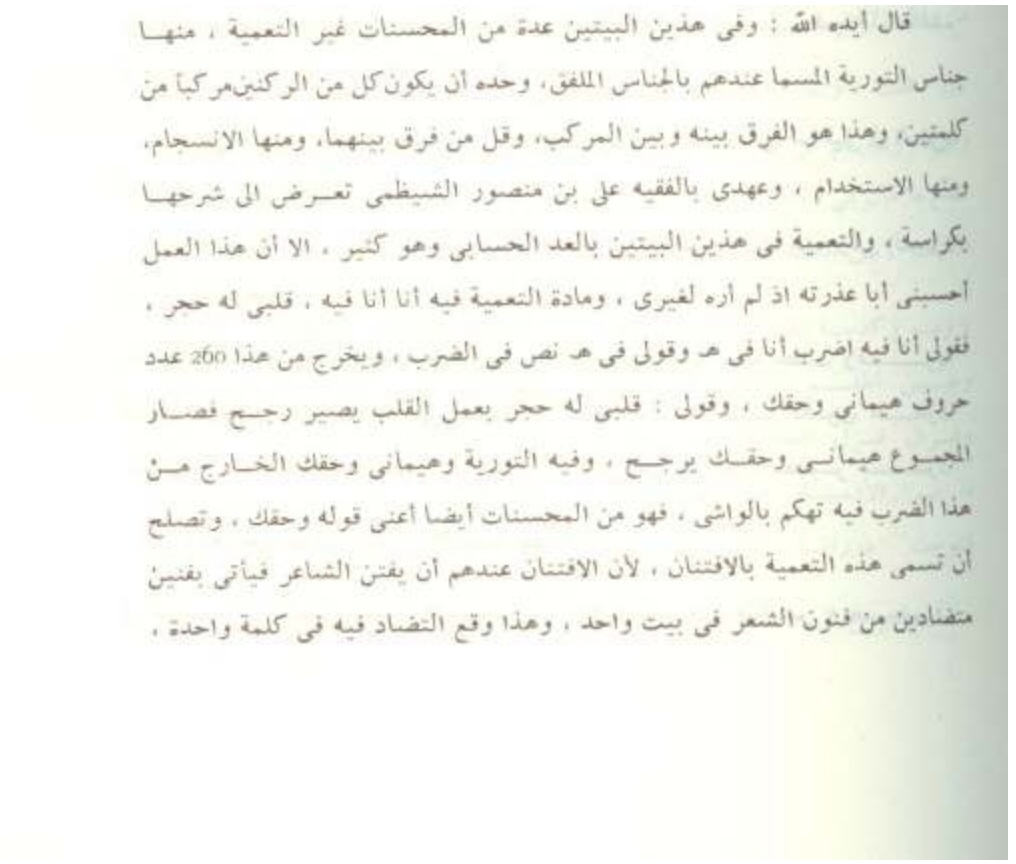
انتهى تفسيره أيده الله بمنه

وقال أيده الله بمنه : ولهما حكاية ، وذلك لأنه كان أيده الله لابساً منصورية من الملف الذى يقال له قلب حجر ، والمنصورية نوع من اللباس معروف استخرجه نصره الله ولم يسبق اليه ، فلذلك أضيف اليه فقيل له منصورية ، كما استخرج أيضا نصره الله أنواعاً غير اللباس أضيفت اليه أيضاً حسبما ذلك مشهور هذين البيتين :

وصفوا اشتياقى للحبيب وسرهم ... قول الحبيب أنا أنا فيه

قلبى له حجر ، فقلت مغالطا ... للعاذل المؤذى أنا فيه

En fait, ces deux vers contiennent deux parties qui sont cryptées par deux méthodes différentes. C'est en fait une composition ou une superposition de deux méthodes de cryptographie :



قال أيده الله : وفي هذين البيتين عدة من المحسنات غير التعمية ، منها جناس التورية المسما عندهم بالجناس الملفق، وحده أن يكون كل من الركنين مركباً من كلمتين، وهذا هو الفرق بينه وبين المركب، وقل من فرق بينهما، ومنها الانسجام، ومنها الاستخدام ، وعهدي بالفقيه علي بن منصور الشيظمي تعرض الى شرحها بكراسة ، والتعمية في هذين البيتين بالعد الحسابي وهو كثير ، الا أن هذا العمل أحسبني أبا عذرته اذ لم أره لغيري ، ومادة التعمية فيه أنا أنا فيه ، قلبي له حجر ، فقولي أنا فيه اضرب أنا في هـ وقولي في هـ نص في الضرب ، ويخرج من هذا 260 عدد حروف هيماني وحقك ، وقولي : قلبي له حجر بعمل القلب يصير رجح فصار المجموع هيماني وحقك يرجح ، وفيه التورية وهيماني وحقك الخارج من هذا الضرب فيه تهكم بالواشي ، فهو من المحسنات أيضا أعني قوله وحقك ، وتصلح أن تسمى هذه التعمية بالافتنان ، لأن الافتنان عندهم أن يفتن الشاعر فيأتي بفنين متضادين من فنون الشعر في بيت واحد ، وهذا وقع التضاد فيه في كلمة واحدة ،

Figure 2.1 : cryptogrammes publiés d'El Mansour

- ***Cryptogramme numérique* :** le premier cryptogramme se trouve dans la deuxième partie du premier vers. Les lettres de ce cryptogramme contiennent les lettres du signe de la multiplication numérique ; qui sépare le cryptogramme en deux parties de lettres. En transformant les deux parties de lettres par leurs valeurs numériques et en effectuant la multiplication on obtient le nombre 260 qui par le calcul numérique Arabe Hissab El Joummal correspond à un ensemble de mots qui vont constituer le déchiffrement du cryptogramme.

ه	في	أنا
5	x	52

Tableau 2.2 : exemple de Hissab Al-Joummal

Ici, on remarque bien que El Mansour avait fait une transformation numérique avec une utilisation de l'astuce du symbole de multiplication qui se trouve à l'intérieur du cryptogramme pour trouver une valeur numérique et ensuite il fait une transformation inverse en utilisant le calcul Arabe « Hissab Al-Joummal » pour avoir des lettres qui vont constituer le texte chiffré.

Ainsi, pour crypter un message clair, on le transforme en chiffre à l'aide de Hissab Al-Joummal, en suite on met le chiffre obtenu sous forme d'un produit de deux chiffre dont le dernier a pour valeur numérique 5= ه 6=ها 45=هم 55=هن ... et ensuite on transforme le produit en lettres (les chiffres par leurs images moyennant Hissab Al-Joummal et le symbole de la multiplication écrit en lettres « **في**»).

Le même procédé peut se faire aussi en utilisant les lettres de l'une des opérations sur les entiers naturels, soit attachées avec d'autres lettres soit entre les lettres de deux morceaux d'une phrase. Ces lettres peuvent être celles des mots suivants ou bien d'autres mots qui ont l'un des sens des opérations entre les entiers naturels.

Multiplié	**Plus**	**Moins**	**Divisé**
ضرب في	**زائدا زد**	**إلا ـقص**	**على قسم**

Tableau 2.3 : les lettres arabe des opérations

Dans cette méthode, on opère numériquement sur une partie du message et non pas sur les lettres une après l'autre ; ce qui ressemble à ce qu'on fait au message dans la cryptographie moderne après le codage numérique (par exemple, avec la méthode RSA, on élève une part du message à une puissance donnée ou encore la méthode d'Elgamal ou on multiplie le message par la clé).

- ***Cryptogramme d'Inversion :*** le deuxième cryptogramme se trouve dans la première partie du second vers. Cette dernière méthode n'est rien que l'opération de lecture d'un mot dans le sens inverse de la lecture en langue Arabe.

2.4.1. Le Cryptogramme d'Or[15]

Le Sultan El-Mansour ne s'est pas contenté des méthodes de cryptographie qu'il avait publiée et enseigné à tous ceux qui avaient assistés à ses conférences (Majalisses), mais il avait

inventé un système cryptographique qui associe à chaque lettre de la langue Arabe un autre caractère secret. Il employait ces caractères secrets en les mélangeant avec la langue courante. Il avait utilisé ce cryptogramme dans ses différentes correspondances avec ses fils ou certains de ses émissaires ou ambassadeurs.

C'était un cryptogramme secret, appelé le ***cryptogramme de la diplomatie d'Or***, qu'El-Mansour avait utilisé, en particulier ,avec Abdelouahed ben Massoude Anoun ,son Ambassadeur auprès de la Reine Elizabeth en 1600.

Celui-ci était resté six mois à Londres et avait pour but de convaincre les Anglais de s'allier avec les Marocains contre l'Espagne et aussi de contacter le savant Edward Ourught pour l'achat d'instruments scientifiques. Il n'y avait pas assez d'informations sur le système cryptographique d'Or .seul, Mohammed Assghir Al-Yafrani dans son livre « Nozhat Al Hadi » (1728), en parlant du génie d'El –Mansour avait écrit :

« Voici l'un des traits de son caractère ferme et génial : il avait inventé des signes d'écriture en nombre égal à celui de l'alphabet arabe et qu'il utilisait pour écrire tout ce qu'il voulait garder confidentiel et indéchiffrable par l'ennemi. A chaque fois qu'il chargera l'un de ses fils ou de ses émissaires d'une mission, il lui donnait un spécimen de cette écriture pour l'utiliser dans ses écrits confidentiels concernant sa mission ».

D'autre part, un auteur inconnu, avait écrit sur la page de garde d'un manuscrit Arabe (traitant les carrés magiques et donnant des explications sur l'utilisation des notations arithmétique d'El-Hissab EL-Fassi), une note précisant qu'il avait trouvé une lettre secrète du secrétaire Anoun au Sultan El-Mansour qu'il avait envoyée lors de sa mission à Londres. L'auteur inconnu avait signalé de plus qu'il avait essayé de la déchiffrer avec l'aide de plusieurs connaisseurs de la cryptographie, sans pouvoir trouver la moindre information. Il ajoutait, qu'après plus de quinze ans, il avait trouvé la correspondance entre les caractères secrets et les lettres originales de la langue Arabe et avait ainsi déchiffré le message secret d'Anoun. Une copie de cette note avait été publiée dans un article de 1929. Un extrait de cette note est le suivant

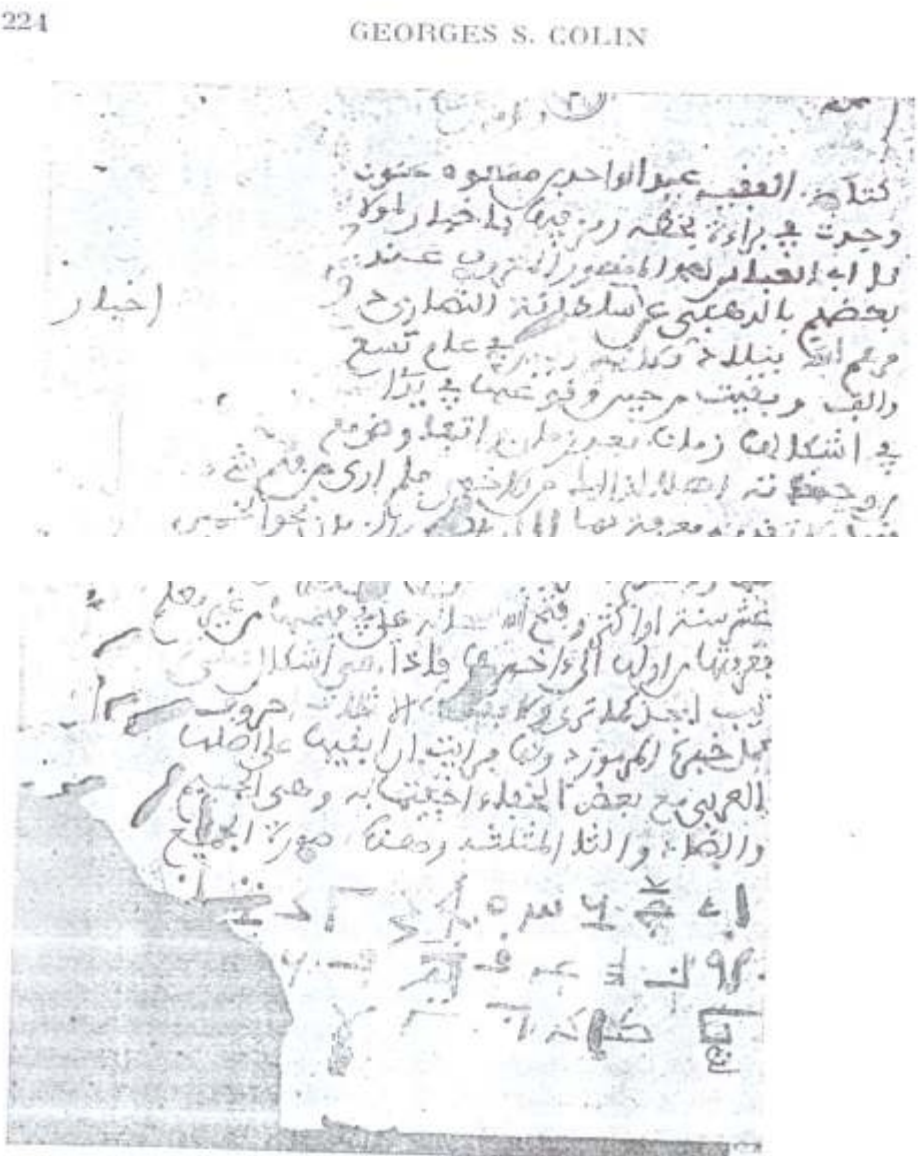


Figure 2.2 : une note de message secret d'Anoun

Ce cryptogramme avait été utilisé dans les missions qui nécessitaient un secret total et une sécurité parfaite. Le Roi El-Mansour avait formé certains de ses propres secrétaires ou les secrétaires de ses fils et de ses émissaires pour pouvoir utiliser cette écriture.

2.4.2. Le Cryptogramme d'Or et la plume de Fès[15]

Les savants, Juges et notaires Marocains avaient utilisé des symboles particuliers pour désigner les nombres. Cette écriture là avait été utilisée dans un premier temps à Fès par les juges et les notaires pour crypter certains chiffres, qui se trouvaient surtout dans les actes de partage d'héritages ou les actes financiers, afin qu'ils ne soient pas changé ou falsifiés. La

forme de ces derniers chiffres, qui sont connus par AL-Kalam EL-Fassi (plume de Fès), avait été décrite par le poète Abou Assaoude Abdelkader EL-Fassi (mort en 1680) dans une poésie.

D'après Mohammed EL-Fassi, cette écriture arithmétique avait été utilisée même avant le 16éme siècle. Les documents trouvés jusqu'à présent prouvent que cette notation des nombres avait été utilisée au début de la dynastie Alaouite. D'autre part, une lettre d'El-Maemoun au Sultan EL-Mansour le doré avait été daté par des symboles inconnus et qui pourrait être cette notation là. Ainsi, la cryptographie au Maroc n'avait pas été utilisée aussi pour la sécurité des biens et des actes financiers.une copie des formes de ces chiffres, tracés par Mohammed EL-Fassi.

Il est fort possible que la plume de Fès était utilisée même avant la dynastie saàdienne ; et puisque elle porte le nom de Fès, on peut dire qu'elle avait été utilisé pour la première fois par une dynastie qui avait Fès comme capitale et ça ne pouvait être que la dynastie Mérinide ou la dynastie des Fatimides. Tandis que le cryptogramme d'Or a été utilisé par le Sultan El Mansour à Marrakech. Les deux écritures se compètent et constituent un vrai cryptogramme d'écriture. Le cryptogramme d'Or avait cessé d'être utilisé juste après la mort de ses créateurs ; mais la plume de Fès avait continué à être utilisée jusqu'à 17éme siècle par les juges et notaires, mais à partir du 19éme siècle elle avait commencé à perdre son importance puisqu'elle n'avait été utilisée que par certains écrivains pour numéroter les pages de leurs livres comme Azzayani. Aujourd'hui, la plume de Fès n'est plus utilisée.

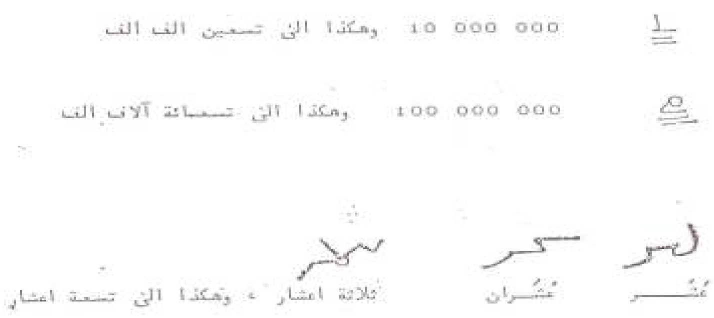


Figure 2.3 : la plume de Fès

2.5. Signature

Les Arabes ont donné une grande importance aux signatures de messages. Le Sultan Ahmed El-Mansour le doré, avait écrit au Roi d'Espagne Philipe II qu'il avait constaté que son dernier message ne portait pas la même signature que ses messages précédents et l'a conseillé de prendre ses précautions à ce sujet.

On voit bien qu'El-Mansour avait pris ses précautions lors qu'il avait utilisé son écriture secrète d'Or pour crypter tout un message et aussi pour signer un message clair. Ceci avait été constaté sur certaines lettres écrites surtout par son fils Elmaemoun.

Une autre forme de signature avait été utilisée par les poètes arabes d'AlMalhoun. La signature n'est rien autre qu'une transformation numérique du nom par le calcul « Hissab El Joummal ». Seulement cette méthode de signature ne permettait pas d'authentifier le signataire. C'est le cas par exemple de la Kassida Al Kadi (le juge***) L£ ÜŽiƟŊJ*** qui est signé à l'aide de Hissab El-Joummal par 254 et dont les solutions possibles sont nombreuses comme « Ennajjare ». Il existe plusieurs exemples de poètes qui avaient signé numériquement leurs poésies en utilisant Hissab El-Joummal.

2.6. Conclusion

Dans ce chapitre nous avons donné une brève historique sur la cryptographie arabe précisément au Maroc. Les arabes ont utilisé des méthodes de cryptographie basée sur la substitution comme la méthode El Hissab El Joummal et la méthode des oiseaux dans ces changes et dans leurs poèmes.

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**	
Cl	**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	**Le**
	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	

é	**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	**t**
	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	**r**
U	**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	**e**
t	**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	
i	**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	**c**
l	**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	**h**
i	**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	**i**
s	**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	**f**
é	**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	**f**
e	**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	**r**
	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	**é**
	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	**e**
	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.

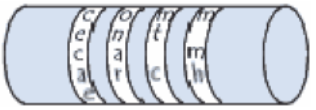


Figure 3.1 : la technique assyrienne **[D]**

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.

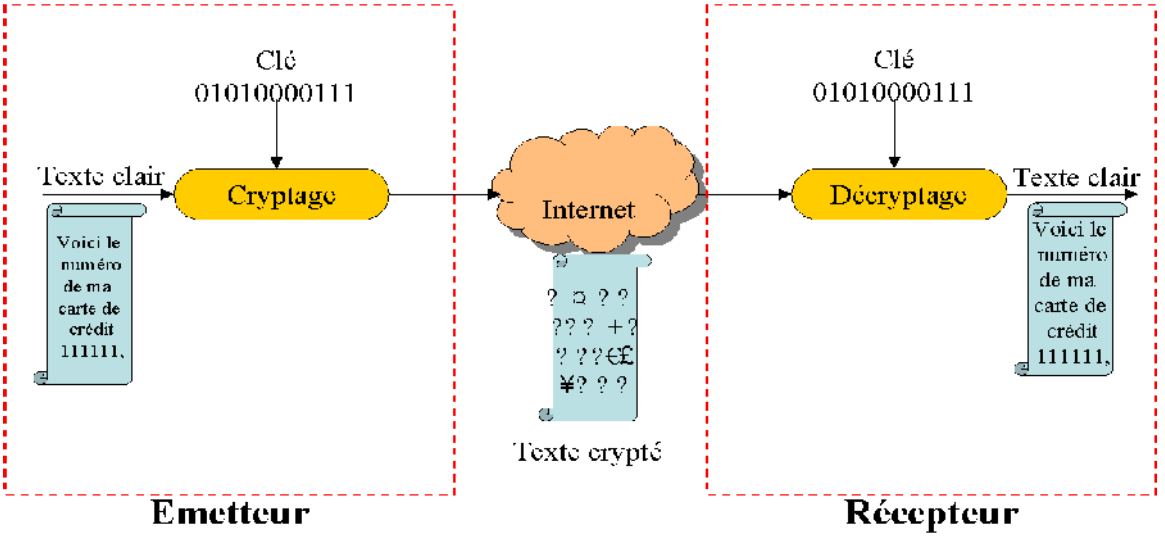


Figure 3.2 : cryptographie symétrique

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 :

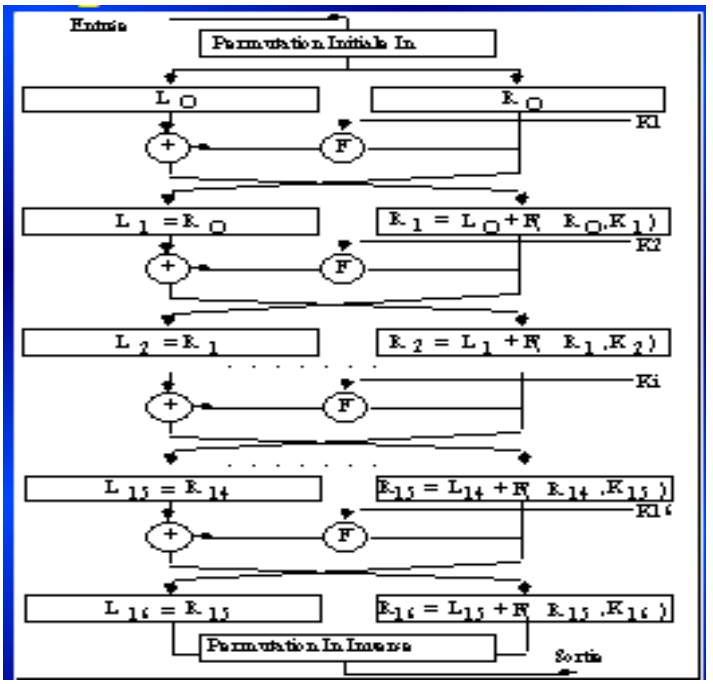
- Gi=Di-1
- Di=Gi-1 XOR f(Di-1,Ki)

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 *:*



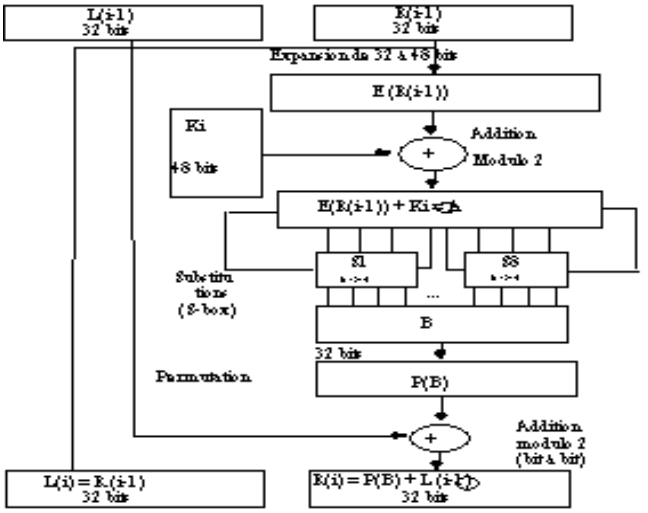


Figure 3.3 : Schémas générale du DES

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]**

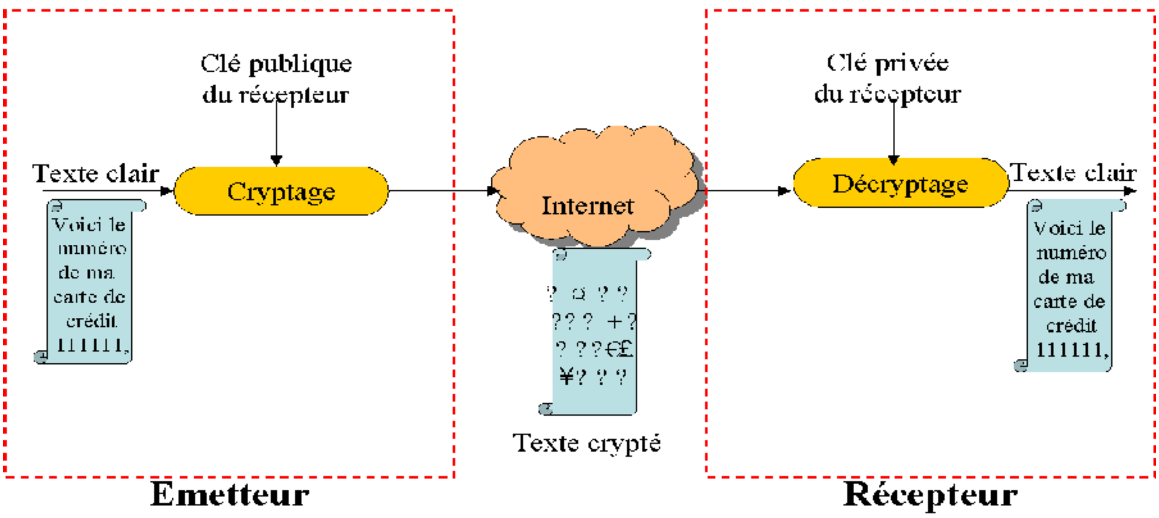


Figure 3.4 : cryptographie asymétrique

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 $\mathbf{C = B^e \bmod n}$ (où C est le bloc chiffré) :

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

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 :

$k_a = n^a \bmod p$
$k_b = n^b \bmod p$

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 :

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

- ✓ **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).

4.1. Introduction

Dans ce chapitre on essaye d'implémenter l'ensemble des techniques permettant de **chiffrer** des textes arabes, c'est-à-d permettant de les rendre inintelligibles sans une action spécifique.

4.2. Objectif

Dans notre application nous avons tenté à voir les différents algorithmes de cryptographie appliquée aux textes arabes savoir une meilleure qualité de protection de messages.
Parmi ces algorithmes on a choisi d'implémenter l'algorithme à clé secrète DES, et l'algorithme à clé publique le RSA.

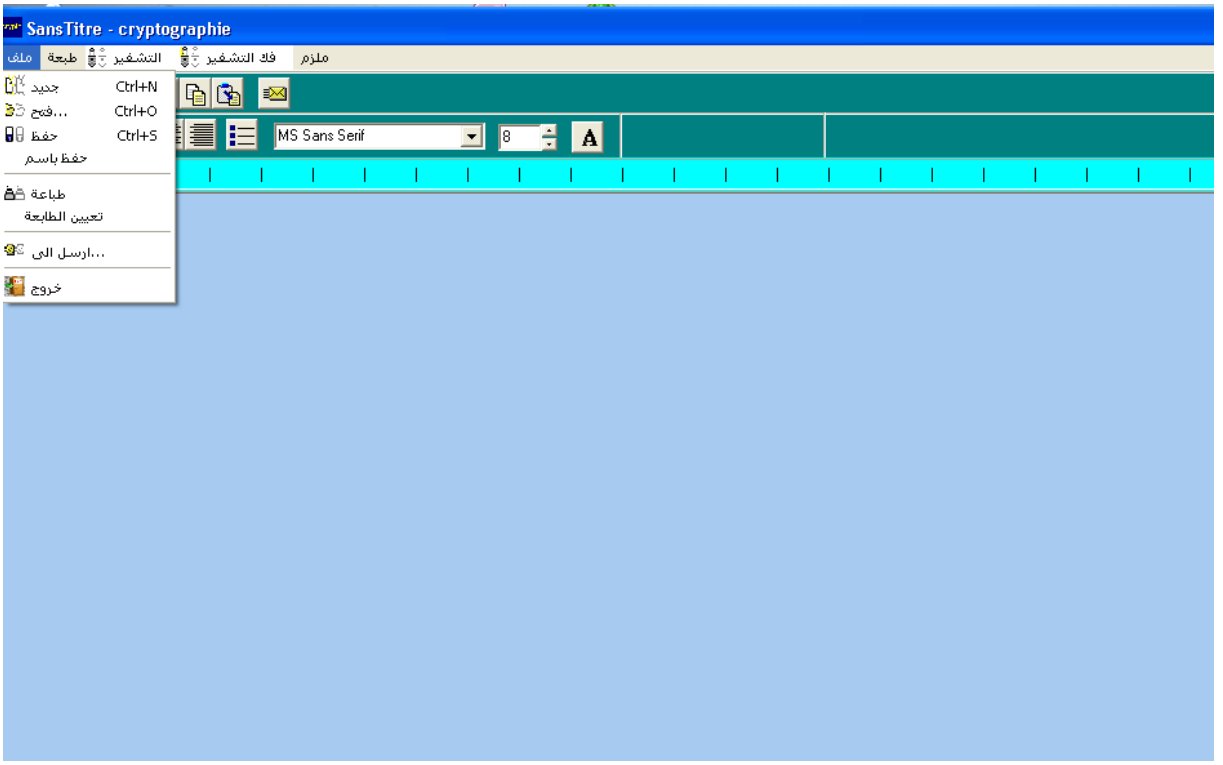
4.3. Logiciel utilisé

C++ builder 6

Le langage choisi pour réalisation de notre application est le **BORLAND C++ BUILDER6.** Ce choix repose sur le fait que Borland possède tout la puissance du langage C++ oriente objet comme il offre la possibilité de développer rapidement des applications sous Windows grâce a ses différentes bibliothèques. Il permet la création instantanée des interfaces utilisateurs car il offre une gestion de l'interface.

4.3.1. Description de l'interface et composantes

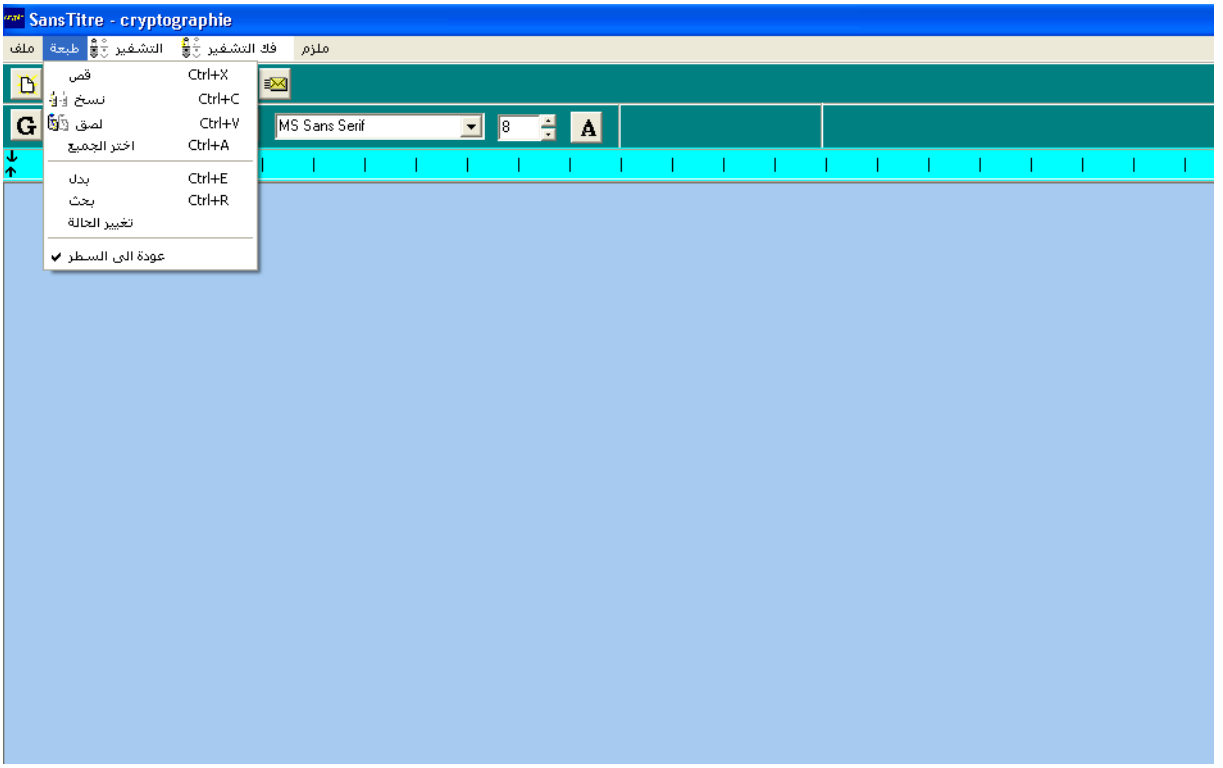
4.4. Le contenu du menu « ملف»



- **جديد**: une nouvelle page.
- **فتح** ouvrir un texte arabe .
- **حفظ**: enregistrer le texte.
- **حفظ بلسم**: enregistrer sous.
- **طباعة**imprimer la page.

- تعيين الطابعة: choisir une imprimante.
- أرسل إلى: envoyer vers.
- خروج: sort du programme.

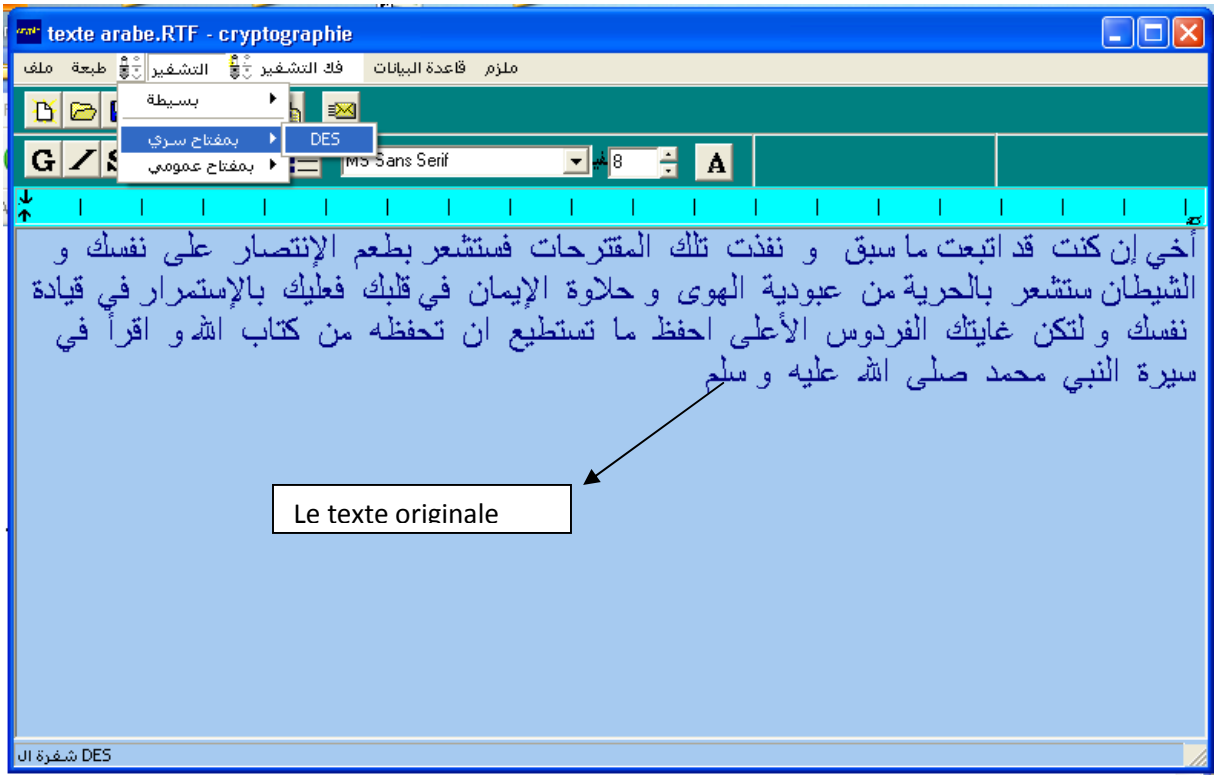
4.5. Le contenu du menu « طبعة»



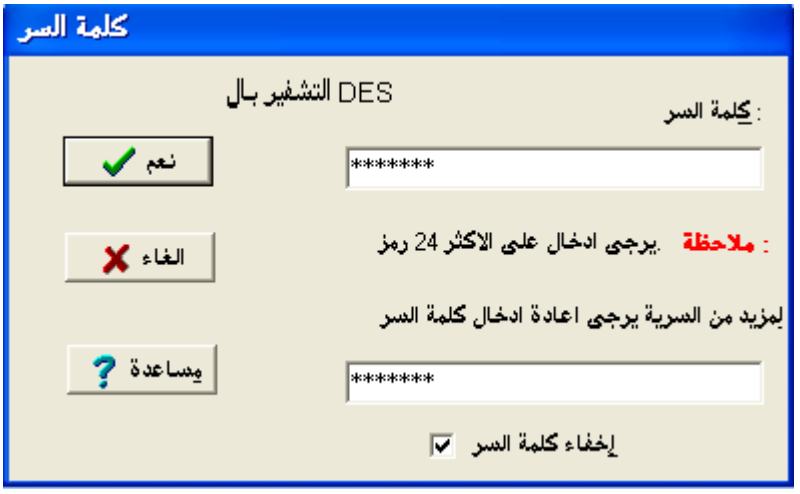
- قص:couper.
- نسخ:copier.
- لصق:coller.
- اختر الجميع:sélectionner tout.
- بحث: chercher.
- بدل:changer.
- تغيير الحالة:modifier.
- عودة إلى السطر:retour a la ligne

4.6. Exemple de quelque opérateur

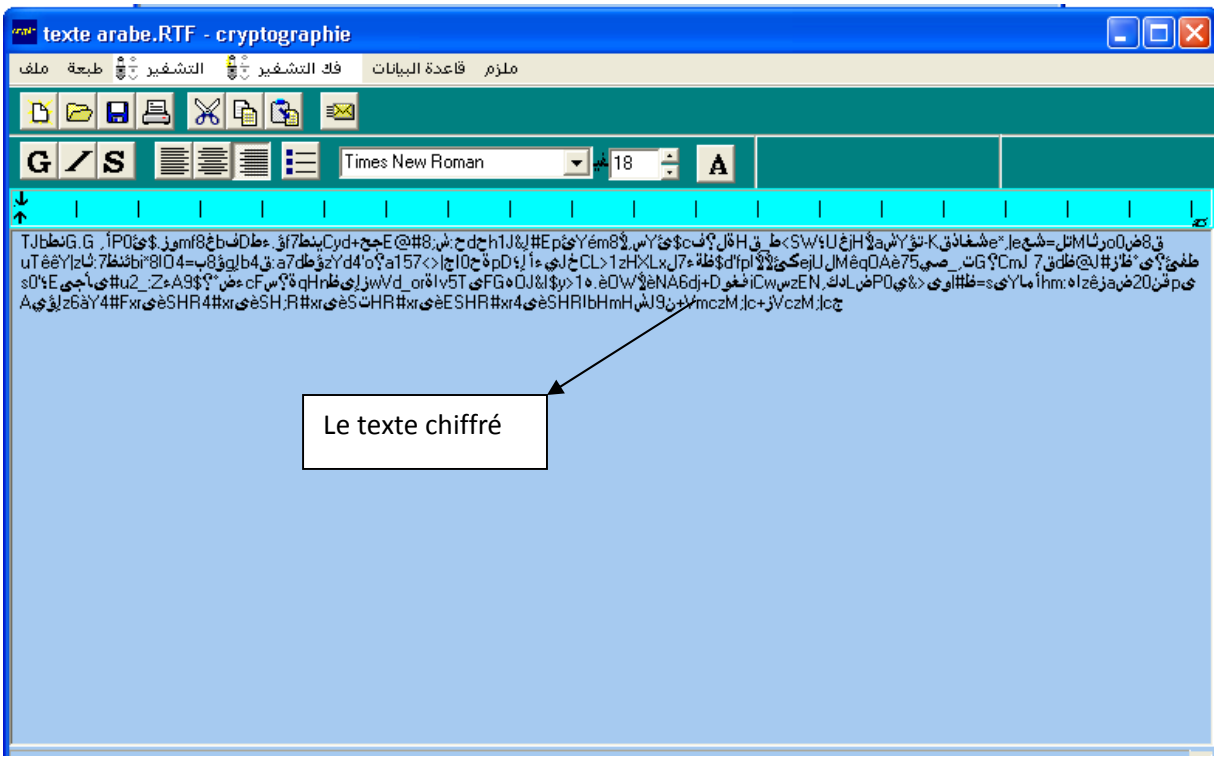
4.6.1. Exemples de chiffrement à clé secrète (DES)



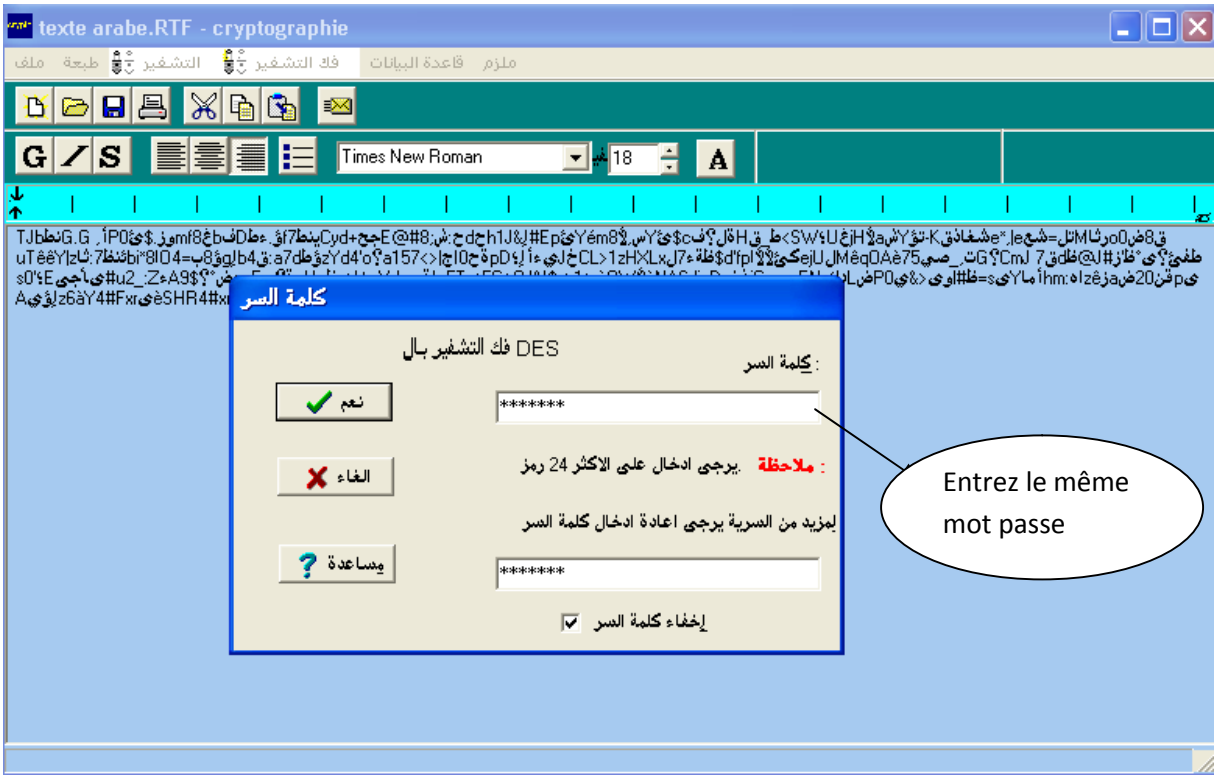
Introduction de la clé:

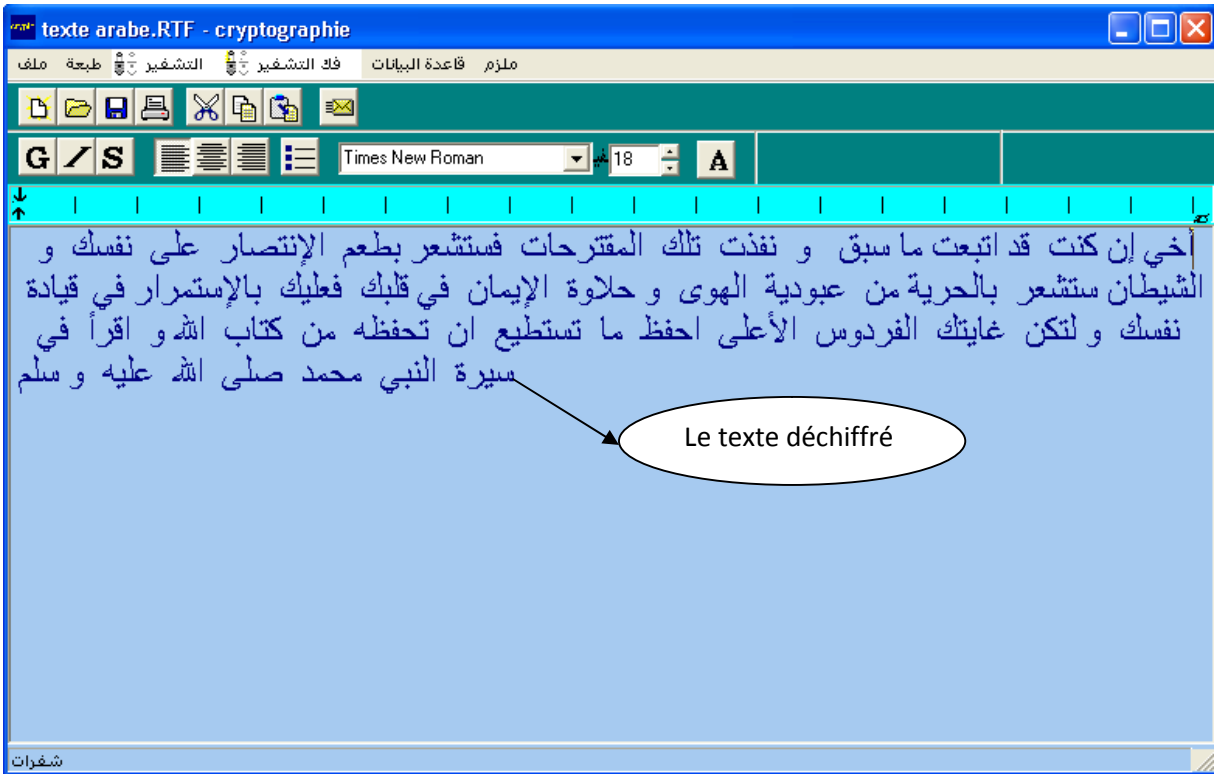


Le texte chiffré :

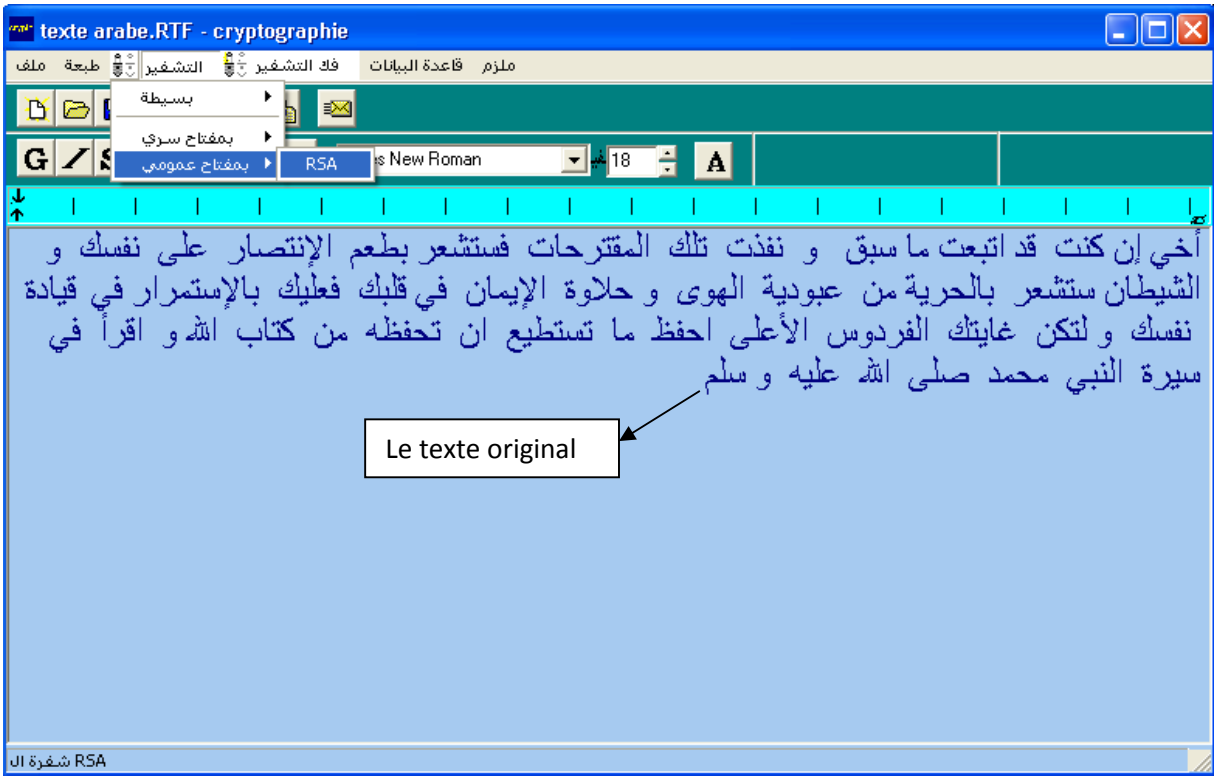


Pour déchiffrer

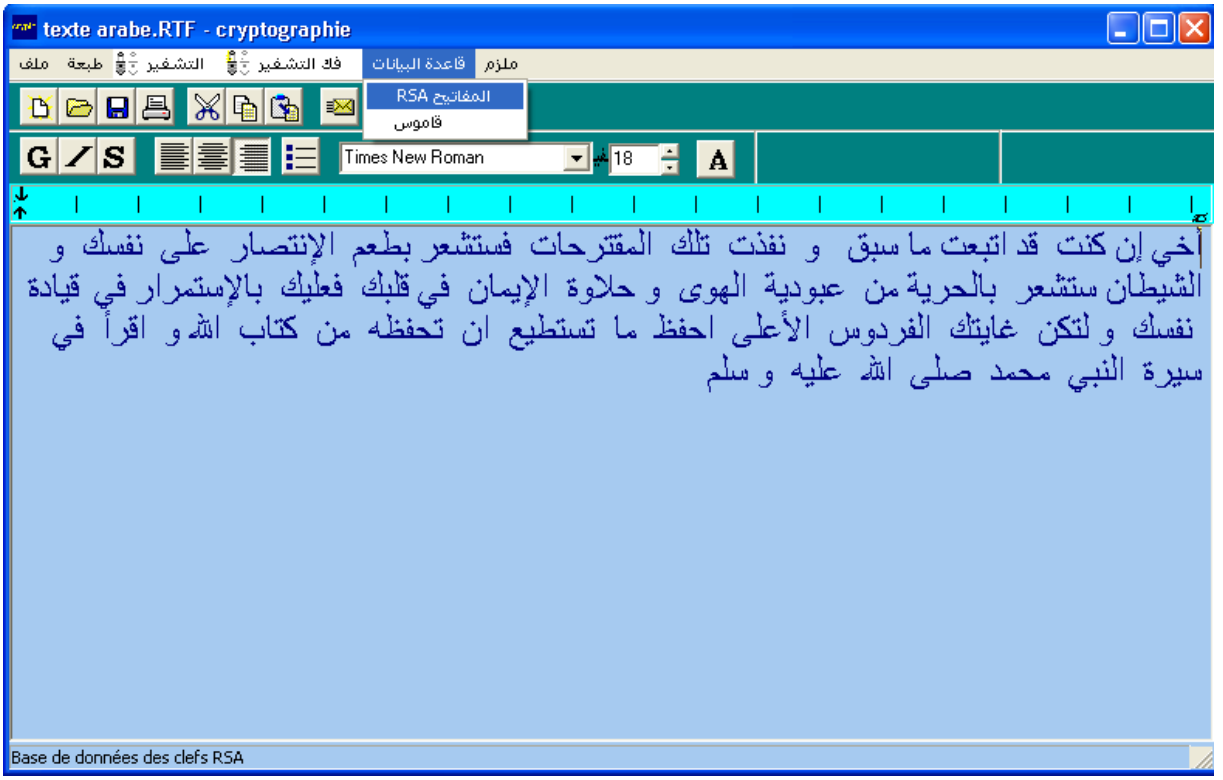


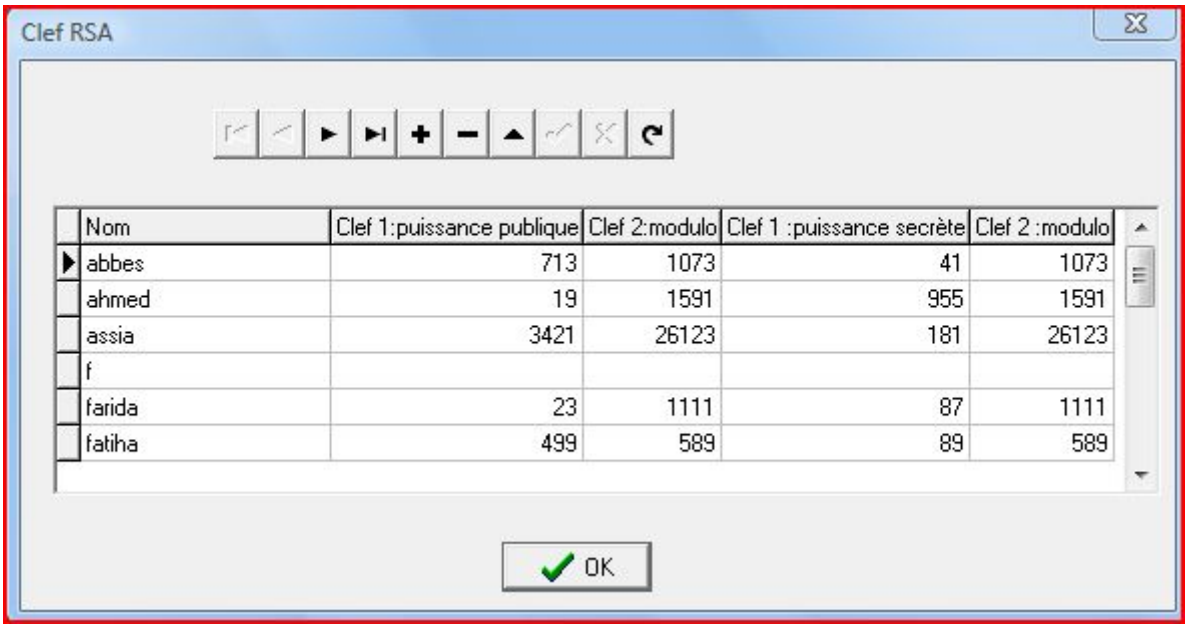


4.6.2. Exemple de chiffrement à clé publique (RSA)



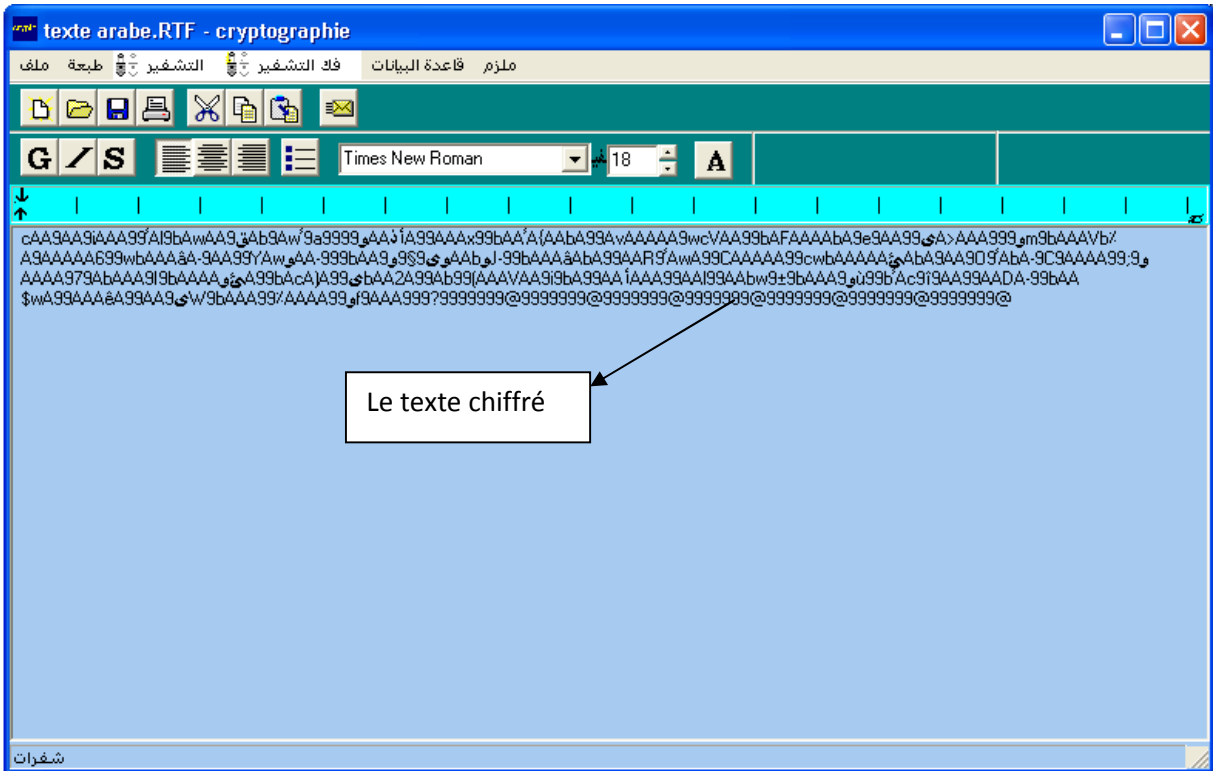
Les clefs RSA :



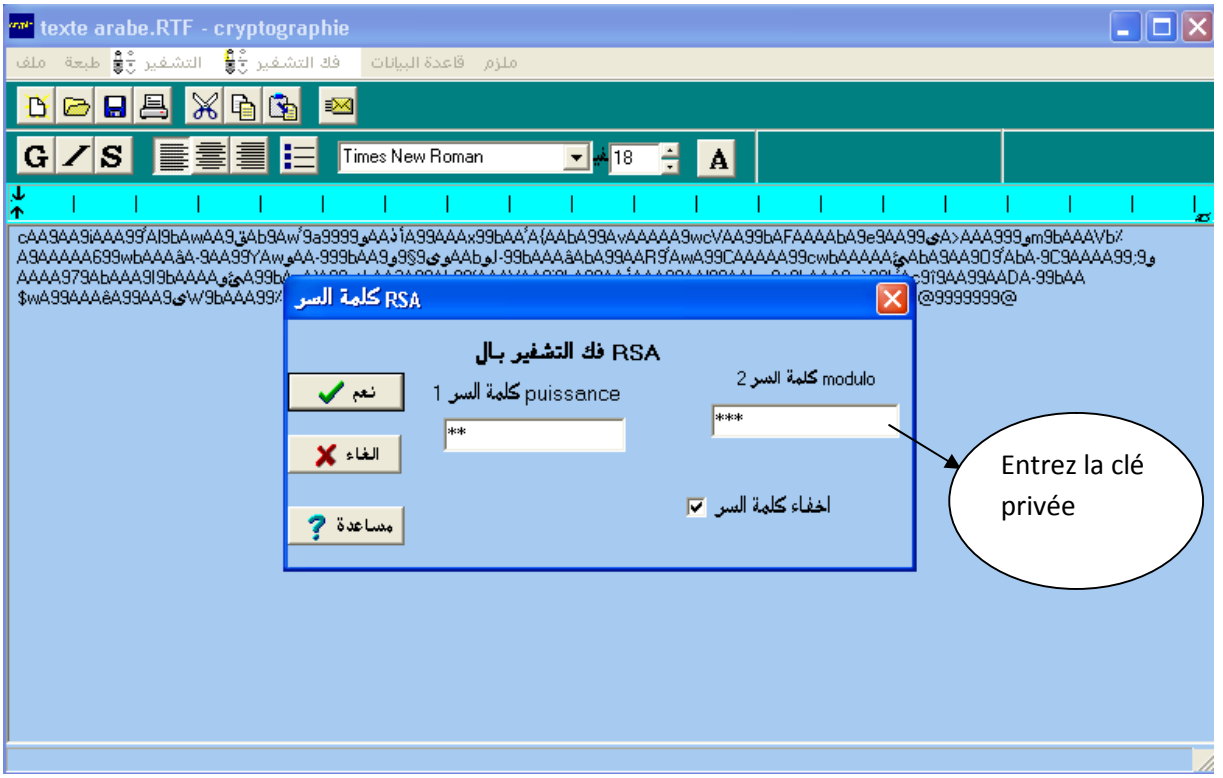


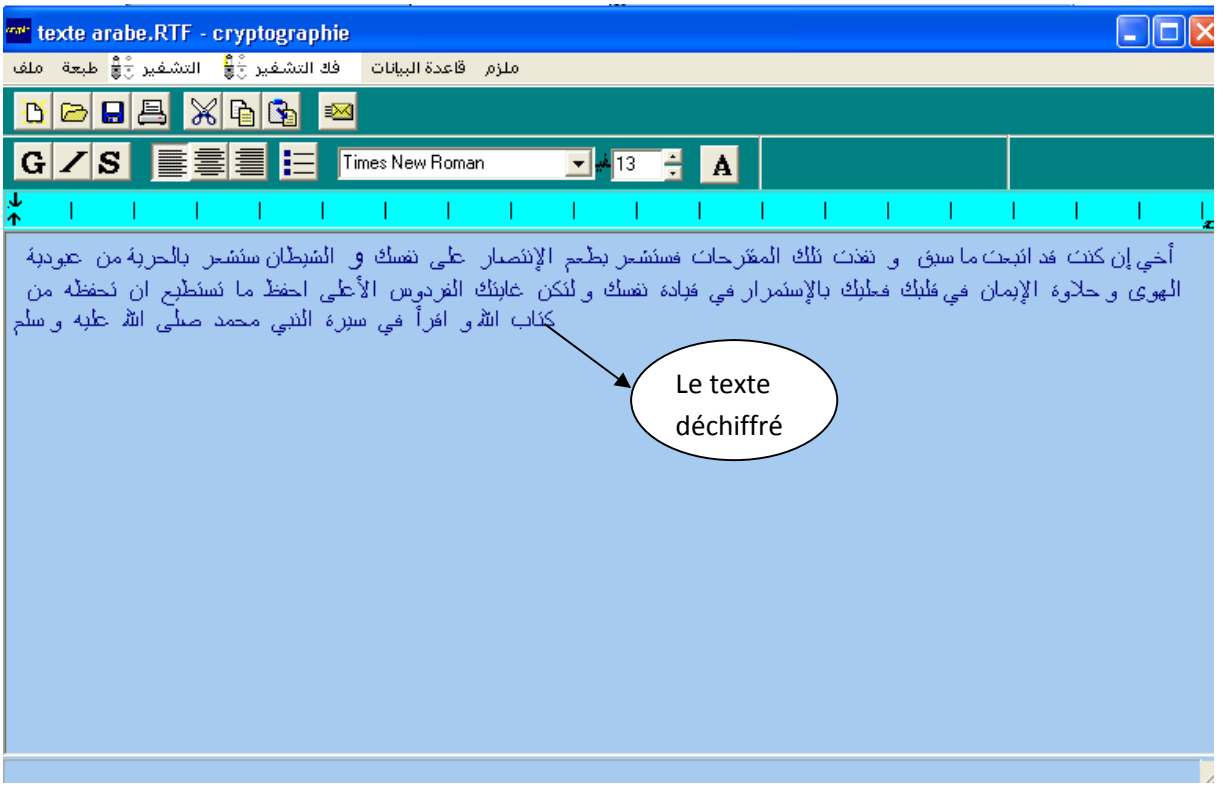
La fenêtre de clé publique entrer :

Le texte chiffré :



Pour déchiffrer


texte arabe.RTF - cryptographie
ملف طبعة التشفير فك التشفير قاعدة البيانات ملزم
Times New Roman
18
كلمة السر RSA
فك التشفير بال RSA
نعم
الغاء
مساعدة
كلمة السر 1 puissance
**
كلمة السر 2 modulo
***
اخفاء كلمة السر
Entrez la clé privée


texte arabe.RTF - cryptographie
ملف طبعة التشفير فك التشفير قاعدة البيانات ملزم
Times New Roman
13
أخي إن كنت قد ابتعت ما سبق و نفذت تلك المقترحات فستشعر بطعم الإنتصار على نفسك و الشيطان ستشعر بالحرية من عبودية الهوى و حلاوة الإيمان في قلبك فعليك بالإستمرار في قيادة نفسك و لتكن غايتك الفردوس الأعلى احفظ ما تستطيع ان تحفظه من كتاب الله و اقرأ في سيرة النبي محمد صلى الله عليه و سلم
Le texte déchiffré

4.7. Lettre Arabe

Utilisés pour l'écriture arabe.

Les caractères U+0600 à U+0603 et U+06DD sont des signes de contrôle de format.

Les caractères U+0610 à U+0615, U+064B à U+065E, U+0670, U+0, U+06D6 à U+06DC, U+06DF à U+06E4, U+06E7, U+06E8 et U+06EA à U+06ED sont des signes diacritiques se combinant avec le caractère qu'ils suivent ; ils sont combinés ici avec la lettre arabe *sīn* « س» (U+0633) à des fins de lisibilité.

Note : certaines polices de caractères arabes indiquent supporter tout ce sous-ensemble de caractères, mais n'affichent aucun glyphe pour certains d'entre eux.

Table des caractères

voir PDF : fr en	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
060	ـــ	ـــ	ـــ	صـ								فـ	،	؍	ـــه	ﻉ
061	س ً	س ٌ	س ٍ	س ّ	س ّ	س ٔ	س ٕ					؛			؞	؟
062		ء	آ	أ	ؤ	إ	ئ	ا	ب	ة	ت	ث	ج	ح	خ	د
063	ذ	ر	ز	س	ش	ص	ض	ط	ظ	ع	غ					
064	ـ	ف	ق	ك	ل	م	ن	ه	و	ى	ي	سً	سٌ	سٍ	سَ	سُ
065	سِ	سّ	سْ	سٓ	سٔ	سٕ	س ِ	س ً	س ٌ	س ٍ	س ّ	س ْ	س .	س ٖ	س ٗ	
066	٠	١	٢	٣	٤	٥	٦	٧	٨	٩	٪	ر	،	⋆	ـب	و
067	س ٰ	اً	أ	إ	ئ	ا	ؤ	ؤ	ئ	ٹ	ٹ	ٻ	ٽ	ٽ	پ	ٹ
068	ڀ	ځ	خ	ج	ج	څ	چ	چ	ڈ	ډ	ډ	ڈ	ڈ	ډ	ڈ	ڈ
069	ڈ	ڑ	ڑ	ڑ	ڑ	ڑ	ڑ	ز	ژ	ڑ	ښ	ږ	ږ	ږ	ږ	ظ
06A	غ	ف	ب	ف	ق	پ	ڤ	ف	ق	ک	ے	گ	ګ	ګ	ګ	گ
06B	گ	گ	گ	گ	گ	ڵ	ڵ	ڵ	ڵ	ڼ	ں	ڻ	ڼ	ڼ	ھ	چ
06C	ۀ	ه	ۀ	ة	ۆ	ۆ	ۆ	ۇ	ۇ	ۋ	ۋ	ۋ	ی	ۍ	ێ	ۆ
06D	ې			ئے	۔	ه	س ۖ	س ۗ	س ۘ	س ۙ	س ۚ	س ۛ	س ۜ	◯	۞	۔
06E	س ۠	س ۡ	س ۢ	س ۣ	س ۤ	س ۥ	ۦ	س ۧ	س ۨ	𐋡	س ۫	س ۬	س ۭ	س ۮ	ڈ	ڑ
06F	۰	۱	۲	۳	۴	۵	۶	۷	۸	۹	ۺ	ۻ	ۼ	۽	۾	ھ

4.7.1. Table des caractères ASCII

La première colonne de cette table renferme le code MARC à 8 bits (en hex) pour le caractère tel que provenant du jeu graphique G0; la seconde colonne de cette table renferme le code MARC à 8 bits (en hex) pour le caractère tel que provenant du jeu graphique G1; la troisième colonne contient le code UCS/Unicode à 16-bits (en hex), et la quatrième colonne contient le code UTF-8 (en hex) pour les caractères UCS; la cinquième colonne contient une image d'une représentation du caractère; la sixième colonne indique les noms des caractères : nom MARC / nom UCS. Si le nom MARC est le même que le nom UCS, ou s'il est semblable à ce dernier, seul le nom UCS apparaît.

MARC-8 jeu G0	MARC-8 jeu G1	UCS	UTF-8	Caractères	Nom MARC / Nom UCS
21	A1	0021	21	!	Point d'exclamation
22	A2	0022	22	"	Guillemet anglais
23	A3	0023	23	#	Symbole de numéro
24	A4	0024	24	$	Symbole de dollar
25	A5	066A	D9AA	٪	Signe pour cent / Signe pour cent arabe
26	A6	0026	26	&	Perluète
27	A7	0027	27	'	Apostrophe
28	A8	0028	28	(	Parenthèse ouvrante / Parenthèse gauche
29	A9	0029	29	)	Parenthèse fermante / Parenthèse droite
2A	AA	066D	D9AD	٭	Astérisque / Étoile à cinq pointes arabe
2B	AB	002B	2B	+	Signe plus
2C	AC	060C	D88C	،	Virgule arabe
2D	AD	002D	2D	-	Trait-d'union - signe moins
2E	AE	002E	2E	.	Point, point décimal / Point
2F	AF	002F	2F	/	Barre oblique / Cotice
30	B0	0660	D9A0	٠	Chiffre zéro arabe-indo-aryen / Chiffre arabe-hindi zéro
31	B1	0661	D9A1	١	Chiffre un arabe-indo-aryen / Chiffre arabe-hindi un
32	B2	0662	D9A2	٢	Chiffre deux arabe-indo-aryen / Chiffre arabe-hindi deux
33	B3	0663	D9A3	٣	Chiffre trois arabe-indo-aryen / Chiffre arabe-hindi trois
34	B4	0664	D9A4	٤	Chiffre quatre arabe-indo-aryen / Chiffre arabe-hindi quatre
35	B5	0665	D9A5	٥	Chiffre cinq arabe-indo-aryen / Chiffre arabe-hindi cinq

36	B6	0666	D9A6	٦	Chiffre six arabe-indo-aryen / Chiffre arabe-hindi six
37	B7	0667	D9A7	٧	Chiffre sept arabe-indo-aryen / Chiffre arabe-hindi sept
38	B8	0668	D9A8	٨	Chiffre huit arabe-indo-aryen / Chiffre arabe-hindi huit
39	B9	0669	D9A9	٩	Chiffre neuf arabe-indo-aryen / Chiffre arabe-hindi neuf
3A	BA	003A	3A	:	Deux points
3B	BB	061B	D89B	؛	Point virgule arabe
3C	BC	003C	3C	<	Signe inférieur à
3D	BD	003D	3D	=	Signe égal à
3E	BE	003E	3E	>	Signe supérieur à
3F	BF	061F	D89F	؟	Point d'interrogation arabe
41	C1	0621	D8A1	ء	Hamzah / Lettre arabe hamza
42	C2	0622	D8A2	آ	Lettre arabe alef avec madda au-dessus / Lettre arabe alif madda en chef
43	C3	0623	D8A3	أ	Lettre arabe alef avec hamza au-dessus / Lettre arabe alif hamza en chef
44	C4	0624	D8A4	ؤ	Lettre arabe waw avec hamza au-dessus / Lettre arabe waw hamza en chef
45	C5	0625	D8A5	إ	Lettre arabe alef avec hamza en dessous / Lettre arabe alif hamza souscrit
46	C6	0626	D8A6	ئ	Lettre arabe yeh avec hamza au-dessus Lettre arabe ya' hamza en chef
47	C7	0627	D8A7l	ا	Lettre arabe alef / Lettre arabe alif
48	C8	0628	D8A8	ب	Lettre arabe beh / Lettre arabe ba'
49	C9	0629	D8A9	ة	Lettre arabe the marbuta / Lettre arabe té' marbouta
4A	CA	062A	D8AA	ت	Lettre arabe the / Lettre arabe té'
4B	CB	062B	D8AB	ث	Lettre arabe theh / Lettre arabe thé'

4C	CC	062C	D8AC	ج	Lettre arabe jeem / Lettre arabe djîm
4D	CD	062D	D8AD	ح	Lettre arabe hah / Lettre arabe ha'
4E	CE	062E	D8AE	خ	Lettre arabe khah / Lettre arabe kha'
4F	CF	062F	D8AF	د	Lettre arabe dal / Lettre arabe dal
50	D0	0630	D8B0	ذ	Lettre arabe thal / Lettre arabe dhal
51	D1	0631	D8B1	ر	Lettre arabe reh / Lettre arabe ra'
52	D2	0632	D8B2	ز	Lettre arabe zain / Lettre arabe zaïn
53	D3	0633	D8B3	س	Lettre arabe seen / Lettre arabe sîn
54	D4	0634	D8B4	ش	Lettre arabe sheen / Lettre arabe chîn
55	D5	0635	D8B5	ص	Lettre arabe sad / Lettre arabe çad
56	D6	0636	D8B6	ض	Lettre arabe dad
57	D7	0637	D8B7	ط	Lettre arabe tah / Lettre arabe ta'
58	D8	0638	D8B8	ظ	Lettre arabe zah / Lettre arabe zza'
59	D9	0639	D8B9	ع	Lettre arabe ain / Lettre arabe 'aïn
5A	DA	063A	D8BA	غ	Lettre arabe ghain / Lettre arabe ghaïn
5B	DB	005B	5B	[	Crochet ouvrant / Crochet de gauche
5D	DD	005D	5D	]	Crochet fermant / Crochet de droite

60	E0	0640	D980	ـ	Tatweel arabe / Tatouil arabe
61	E1	0641	D981	ف	Lettre arabe feh / Lettre arabe fa'
62	E2	0642	D982	ق	Lettre arabe qaf / Lettre arabe qaf
63	E3	0643	D983	ك	Lettre arabe kaf / Lettre arabe kaf
64	E4	0644	D984	ل	Lettre arabe lam / Lettre arabe lam
65	E5	0645	D985	م	Lettre arabe meem / Lettre arabe mîm
66	E6	0646	D986	ن	Lettre arabe noon / Lettre arabe noûn
67	E7	0647	D987	ه	Lettre arabe heh / Lettre arabe hé'
68	E8	0648	D988	و	Lettre arabe waw
69	E9	0649	D989	ى	Lettre arabe alef maksura / Lettre arabe alif maksoura
6A	EA	064A	D98A	ي	Lettre arabe yeh / Lettre arabe ya'
6B	EB	064B	D98B	ً	Fathatan arabe
6C	EC	064C	D98C	ٌ	Dammatan arabe
6D	ED	064D	D98D	ٍ	Kasratan arabe

6E	EE	064E	D98E	َ	Fatha arabe
6F	EF	064F	D98F	ُ	Damma arabe
70	F0	0650	D990	ِ	Kasra arabe
71	F1	0651	D991	ّ	Shadda arabe / Chadda arabe
72	F2	0652	D992	ْ	Sukun arabe / Soukoun arabe
73	F3	0671	D9B1	ٱ	Lettre arabe alef wasla / Lettre arabe alif wasla
74	F4	0670	D9B0	ٰ	Lettre arabe majuscule alef / Lettre arabe alif en chef
78	F8	066C	D9AC	٬	Séparateur milliers arabe
79	F9	201D	E2809D	”	Guillemet double droit
7A	FA	201C	E2809C	“	Guillement double gauche

Table 4.1 : table de codage ASCII

Voila la table de codage des lettres qu'on a utilisée dans notre implémentation

```
struct cde { char lettre; unchar entier;};
struct cde table1[]={
{'٧،'ئ'}   ،{٦،'ط'}   ،{٥،'ص'}   ،{٤،'ض'}   ،{٣،'ذ'}   ،{٢،'ى'}   ،{١،'ق'},
{'١٤،'ع'}  ،{١٣،'غ'}  ،{١٢،'ف'}  ،{١١،'ق'}  ،{١٠،'ث'}   ،{٩،'أ'}  ،{٨،'ط'},
{'٢١،'س'}  ،{٢٠،'ش'}  ،{١٩،'د'}  ،{١٨،'ج'}  ،{١٧،'ح'}  ،{١٦،'ل'}  ،{١٥،'ه'},
{'٢٨،'ك'}  ،{٢٧،'م'}  ،{٢٦،'ن'}  ،{٢٥،'ت'}  ،{٢٤،'ا'}  ،{٢٣،'غ'}  ،{٢٢،'ي'},
{'٣٥،'ة'} ،{٣٤،'لـى'} ،{٣٣،'لا'}  ،{٣٢،'ر'}  ،{٣١،'ؤ'}  ،{٣٠،'ء'}  ،{٢٩،'ئ'},
{'٣٩،'إ'}  ،{٣٨،'ظ'}  ،{٣٧،'ز'}  ،{٣٦،'و'},  {'a',40},  {'b',41},  {'c',42},
{'d',43},  {'e',44},  {'f',45},  {'g',46},  {'h',47},  {'i',48},  {'j',49},
{'k',50},  {';',51},  {'à',52},  {'l',53},  {'m',54},  {'n',55},  {'o',56},
{'p',57},  {'q',58},  {'é',59},  {'è',60},  {'r',61},  {'s',62},  {'t',63},
{'u',64},  {'v',65},  {'w',66},  {'\'',67}, {' ',68},  {'x',69},  {'y',70},
{'z',71},  {'A',72},  {'B',73},  {'C',74},  {'D',75},  {',',0},   {'E',76},
{'K',77},  {'L',78},  {'M',79},  {'N',80},  {'٨٧،'.'}  ،{٨١،'ب'},  {'O',111},
{'ê',116}, {'P',83},  {'Q',84},  {'R',85},  {'S',86},  {'T',87},  {'U',88},
{'V',89},  {'W',90},  {'X',91},  {'Y',92},  {'Z',93},  {'F',94},  {'G',95},
{'H',96},  {'I',97},  {'J',98},  {'1',99},  {'2',100}, {'3',101}, {'4',102},
{'5',103}, {'6',104}, {'7',105}, {'8',106}, {'9',107}, {'0',108}, {'_',109},
{'@',110}, {'^',161}, {'$',112}, {'*',113}, {'+',114}, {'-',115}, {'|',117},
{':',118}, {'١٢٤،'#'} ،{١٢٣،'؟'} ،{١٢٢،'<'} ،{١٢١،'='} ،{١٢٠،'>'} ،{١١٩،'!'},
{'°',125}, {'&',126}, {'²',127}, {'"',128}, {'%',129}, {'!',130}, {'«',131},
{'»',132}, {'±',133}, {'/',134}, {'{',135}, {'!',136}, {')',137} ,{'،',138},
{'[',139}, {']',140}, {'(',141}, {'¶',142}, {'ç',143}, {'¨',144}, {'£',145},
{'¤',146}, {'µ',147}, {'§',148}, {'ù',149}, {',',150}, {'û',151}, {'î',152},
{'ô',153}, {'½',154}, {'©',155}, {'١٥٦،'}, {'â',157}, {'ï',158}, {'ⁱ',159},
{'١٦٠،'Ï'}};
```

Table 4.2 table de codage des lettres

4.8. Code source de différentes implémentations

4.8. 1. Code source de l'algorithme DES

Chiffrement par l'algorithme DES

```
void __fastcall TMainForm::DES1Click( TObject *Sender)
{
//chiffrement DES
Form1->Label5->Caption="";
Form1->Label5->Caption="التشفير بال DES";
Form1->ShowModal();
// texte vide
int S = RichEdit1->GetTextLen();
if((S==0)&&(Accepter)){
          Accepter=false;
          ShowMessage("لا يمكن تشفير نص فارغ");
          }
//***
if(Accepter){
int star=clock();
int i,j,k;
int Size = RichEdit1->GetTextLen();
char *Buffer = new char[Size+1];
RichEdit1->GetTextBuf(Buffer,Size+1);
RichEdit1->Text="";
unchar t1[8], t2[8];

int n56=Size/56;
if (Size % 56 != 0) n56 = (n56+1)*56;
        else n56 = Size;
unchar *tab1 = new unchar[n56+1];
unchar *tab2 = new unchar[n56+1];

ProgressBar1->Visible=true;
ProgressBar1->Position=0;
ProgressBar1->Min=0;
ProgressBar1->Max=4;

for (i=0;i<n56;i++)  tab1[i]= 0;
```

```
for (i=0;i<Size;i++){
            j=0;
            while (Buffer[i]!=table1[j].lettre && j++<160);
            tab1[i]=table1[j].entier;
};
delete Buffer;

// Chiffrement
byte Clef[8];
for (i=0;i<8;i++) Clef[i]=0;

if (taille_pass > 8) taille_pass=8;
for (i=0;i<taille_pass;i++){
            j=0;
            while (pass[i]!=table1[j].lettre && j++<160);
            Clef[i]=table1[j].entier;
};
ProgressBar1->Position=1;
/* générateur aléatoire */

/* L'extension de la clef */
deskey(Clef,0);
chiffrer_des(n56,tab1,tab2);
ProgressBar1->Position=2;
// fin du chiffrement

// pour eviter un eventuel pb d'affichage.
int som;
som = n56/7;
som++;
unchar *TabEtend = new unchar[n56+som+1];
```

```
int enc=0;
i=0;k=0;
while(i<n56){
    for(j=0;j<7;j++,i++)  t1[j]= tab2[i];//le tableau contenat les ent chiffres
    de7vers8(t1,t2);enc++;
    for(j=0;j<8;j++,k++) TabEtend[k] = t2[j];
};
delete tab1;
delete tab2;
ProgressBar1->Position=3;
char *les_cars = new char[n56+enc+1];
for (i=0;i<n56+enc;i++){
       j=0;
       while ( ( TabEtend[i]!=table1[j].entier) && j++<160);
       les_cars[i]= table1[j].lettre;
};
les_cars[n56+enc]='\0';
ProgressBar1->Position=4;
RichEdit1->Text = les_cars;
delete les_cars;
delete TabEtend;
ProgressBar1->Visible=false;
int end=clock();
Label2->Caption="";
Label2->Caption=((end-star)*0.001);
};
}
```

déchiffrement DES

```
void __fastcall TMainForm::DES2Click(TObject *Sender)
{
/* Déchiffrement DES */
Form1->Label5->Caption="";
Form1->Label5->Caption="فك التشفير بال DES";
Form1->ShowModal();
/* texte vide*/
int S = RichEdit1->GetTextLen();
if((S==0)&&(Accepter)){
          Accepter=false;
          ShowMessage("لا يمكن فك تشفير نص فارغ");
          }

if(Accepter){
int star=clock();
int i,j,k;
int Size2 = RichEdit1->GetTextLen();

char *Buffer2 = new char[Size2+1];
RichEdit1->GetTextBuf(Buffer2,Size2+1);
RichEdit1->Text="";
unchar t3[8],t4[8];

/*
int n64=Size2/64;
if (Size2 % 64 != 0) n64 = (n64+1)*64;
        else n64 = Size2;
*/

int som2;
som2 = Size2/8;
```

```
unchar *tab2 = new unchar[Size2+1];
// barra de progression
ProgressBar1->Visible=true;
ProgressBar1->Position=0;
ProgressBar1->Min=0;
ProgressBar1->Max=4;

for (i=0;i<Size2;i++)  tab2[i]= 0;

for (i=0;i<Size2;i++){
           j=0;
           while (Buffer2[i]!=table1[j].lettre && j++<160);
           tab2[i]=table1[j].entier;
};
delete Buffer2;
//maintenant intervient ma fonction avancee
unchar *TabRes = new unchar[Size2+1];
i=0;k=0;
while(i<Size2)
{
    for(j=0;j<8;j++,i++)  t3[j]= tab2[i];
    de8vers7(t3,t4);
    for(j=0;j<7;j++,k++) TabRes[k] = t4[j];
};
ProgressBar1->Position=1;
// Déchiffrement

unchar *tab3 = new unchar[k+1];

byte Clef2[8];
for (i=0;i<8;i++) Clef2[i]=0;
if (taille pass > 8) taille pass=8;
```

```
for (i=0;i<taille_pass;i++)
{
            j=0;
            while (pass[i]!=table1[j].lettre && j++<160);
            Clef2[i]=table1[j].entier;
};
ProgressBar1->Position=2;


deskey(Clef2,1);
chiffrer_des(k,TabRes,tab3);
ProgressBar1->Position=3;
for( i=0; i<k; i++)
        tab3[i] =(unchar)(tab3[i]&0x7f);


char *les_cars2 = new char[Size2-som2+1];
for (i=0;i<Size2-som2;i++){
       j=0;
       while((tab3[i]!=table1[j].entier) && j++<160);
       les_cars2[i]= table1[j].lettre;
};
les_cars2[Size2-som2]='\0';
ProgressBar1->Position=4;
RichEdit1->Text = les_cars2;
delete les_cars2;
delete tab2;
delete tab3;
ProgressBar1->Visible=false;
int end=clock();
Label2->Caption="";
Label2->Caption=((end-star)*0.001);
};}
```

4.8.2. Code source de l'algorithme RSA

Chiffrement par l'algorithme RSA

```
void __fastcall TMainForm::RSA1Click(TObject *Sender)
{
// chiffrement RSA
Form4->Label4->Caption="";
Form4->Label4->Caption="التشفير بال RSA";
Form4->ShowModal();
/*Texte vide*/
int S = RichEdit1->GetTextLen();
if((S==0)&&(Accepter_rsa)){
          Accepter_rsa=false;
          ShowMessage("لا يمكن تشفير نص فارغ");
          }
/*phase de chiffrement*/
if (Accepter_rsa){
int star=clock();
int i,j,k;
int Size = RichEdit1->GetTextLen();

char *Buffer = new char[Size+1];
RichEdit1->GetTextBuf(Buffer,Size+1);
RichEdit1->Text="";
unchar t1[8], t2[8];

ProgressBar1->Visible = true;
ProgressBar1->Min = 0;

unsigned long e,n;
e =(clef1);
n =(clef2);
```

```
int n56=Size/7;
if (Size % 7 != 0) n56 = (n56+1)*7;
        else n56 = Size;

ProgressBar1->Max = n56;

unchar *tab1 = new unchar[n56+1];
unchar *tab2 = new unchar[n56+1];

for (i=0;i<n56;i++)  tab1[i]= table_rsa[114].entier;

for (i=0;i<Size;i++){
           j=0;
           while (Buffer[i]!=table_rsa[j].lettre && j++<159);
           tab1[i]=table_rsa[j].entier;
};
delete Buffer;
ProgressBar1->Position=1;
// Chiffrement
for(i=0;i<n56;i++)
    tab2[i] = modexp(tab1[i], e, n);
delete tab1;
ProgressBar1->Position=2;
// fin du chiffrement

// pour eviter un eventuel pb d'affichage.
int som;
som = n56/7;
som++;
unchar *TabEtend = new unchar[n56+som+1];
int enc=0;
i=0;k=0;
```

```
while(i<n56){
    for(j=0;j<7;j++,i++)  t1[j]= tab2[i];//le tableau contenat les ent chiffres
    de7vers8(t1,t2);enc++;
    for(j=0;j<8;j++,k++) TabEtend[k] = t2[j];
};
delete tab2;
ProgressBar1->Position=3;
//////
char **les_cars;

les_cars = new char*[1];
    les_cars[0] = new char[n56+enc+1];

for (i=0;i<n56+enc;i++){
       j=0;
       while((TabEtend[i]!=table_rsa[j].entier) && j++<159);
       les_cars[0][i]= table_rsa[j].lettre;
};
les_cars[0][n56+enc]='\0';

for (i=0;i<n56+enc;i++){
if(i%5==0) ProgressBar1->Position=i;
RichEdit1->Text = RichEdit1->Text + les_cars[0][i];}
////////
desallouer_rsa(les_cars);
delete TabEtend;
////////
ProgressBar1->Visible=false;
int end=clock();
Label2->Caption="";
Label2->Caption=((end-star)*0.001);
}
}
```

Déchiffrement par l'algorithme RSA

```
void __fastcall TMainForm::RSA2Click(TObject *Sender)
{

//déchiffrement RSA
Form4->Label4->Caption="";
Form4->Label4->Caption="فك التشفير بال RSA";
Form4->ShowModal();

int S = RichEdit1->GetTextLen();
if((S==0)&&(Accepter_rsa)){
         Accepter_rsa=false;
         ShowMessage("لا يمكن فك تشفير نص فارغ");};

if (Accepter_rsa){
int star=clock();
int i,j,k;
int Size2 = RichEdit1->GetTextLen();
unsigned long e,n;
e = (clef1);
n = (clef2);

char *Buffer2 = new char[Size2+1];
RichEdit1->GetTextBuf(Buffer2,Size2+1);
RichEdit1->Text="";
unchar t3[8],t4[8];

ProgressBar1->Visible = true;
ProgressBar1->Min = 0;
```

```
int n64=Size2/8;
if (Size2 % 8 != 0) n64 = (n64)*8;
        else n64 = Size2;

ProgressBar1->Max = n64;
int som2;
som2 = Size2/8;

unchar *tab2 = new unchar[Size2+1];
for (i=0;i<Size2;i++)  tab2[i]= table_rsa[114].entier;

for (i=0;i<Size2;i++){
           j=0;
           while (Buffer2[i]!=table_rsa[j].lettre && j++<159);
           tab2[i]=table_rsa[j].entier;
};
delete Buffer2;
ProgressBar1->Position=1;
//maintenant intervient ma fonction avancee
unchar *TabRes = new unchar[Size2+1];
i=0;k=0;
while(i<Size2)
{
    for(j=0;j<8;j++,i++)  t3[j]= tab2[i];
    de8vers7(t3,t4);
    for(j=0;j<7;j++,k++) TabRes[k] = t4[j];
};
// Déchiffrement
ProgressBar1->Position=2;
unchar *tab3 = new unchar[k+1];
```

```
for(i=0;i<k;i++)
    tab3[i] = modexp(TabRes[i], e, n);
delete tab2;
ProgressBar1->Position=3;
// fin du chiffrement

for( i=0; i<k; i++)
        tab3[i] =(unchar)(tab3[i]&0x7f);
char **les_cars2;

les_cars2 = new char*[1];
    les_cars2[0] = new char[Size2-som2+1];
//char *les_cars2 = new char[Size2-som2+1];
for (i=0;i<Size2-som2;i++){
       j=0;
       while((tab3[i]!=table_rsa[j].entier) && j++<159);
       les_cars2[0][i]= table_rsa[j].lettre;
};
les_cars2[0][Size2-som2]='\0';
//RichEdit1->Text = les_cars2;
for (i=0;i<Size2-som2;i++){
if (i%5==0) ProgressBar1->Position=i;
RichEdit1->Text = RichEdit1->Text + les_cars2[0][i];}
desallouer_rsa(les_cars2);
delete tab3;
ProgressBar1->Visible=false;
int end=clock();
Label2->Caption="";
Label2->Caption=((end-star)*0.001);}}
```

4.9. Conclusion

Nous sommes intéressé dans notre projet de fin d'étude par le cryptage des lettres arabes. Il existe deux classes d'algorithmes de cryptages dans le domaine de la cryptographie.

Notre objectif est basé sur le cryptage des textes arabe par l'algorithme de chiffrement à clé secrète DES et l'algorithme de chiffrement à clé publique RSA.

Nous souhaitons dans les prochains projets de continué dans ce domaine mai en utilisons d'autre algorithmes de chiffrements standard plus puissante et reconnu dans le monde comme AES et Diffi HELMAN.

Taille de texte en KO	**DES (ms)**	**RSA (ms)**
10	60	22400
20	71	88500
40	81	250891
80	120	501782
100	131	627227

Comparaison sur le temps de chiffrement

Taille de texte en KO	**DES (ms)**	**RSA (ms)**
10	50	22400
20	60	88500
40	80	250891
80	90	501782
100	110	627227

Comparaison sur le temps d'attaque

Taille de texte en KO	**DES (s)**	**RSA (s)**
10	17	250
20	25	311
40	48	450
80	150	128
100	500	2150

Conclusion générale

Les cryptographes n'ont cessés de redoubler d'ingéniosité, faisant se succéder des dizaines des systèmes de chiffrement plus recherchés les uns que les autres, se livrant bataille pour la gloire ou l'argent.

La cryptographie profite de l'évolution de la technologie, mais elle est en même temps victime de cette évolution car les intrus peuvent utiliser ces nouvelles technologies dans la cryptanalyse de ces algorithmes.

Aujourd'hui la cryptographie est une science très prisée, les exemples, d'utilisation de système cryptographique sont très nombreux par exemple :
Les banque font partie des premiers utilisateurs de systèmes cryptographiques, les cartes bancaires possèdent trois niveaux de sécurité : le code confidentiel qu'est la suite de chiffres à mémoriser et à saisir à l'abri des regards indiscrets, la signature RSA qui permet de vérifier l'identité de la carte sans avoir besoin de secret et l'authentification DES qui apporte une preuve de légitimité de la carte.

La cryptographie est assimilé à ce jour a une arme de guerre de seconde catégorie, car son utilisation n'a pas toujours été dans un but noble.

Au cours de notre mémoire, nous avons étudié et implémenté les différents algorithmes de cryptographie à clef secrète et publique lié à la protection des textes arabes comme le RSA et le DES, on a donné aussi dans notre mémoire une historique importante pour la cryptographie arabe précisément la cryptographie de nord de l'Afrique utilisé par les marocaine, lorsque on dit des marocaine c'est le Maghreb et l'Andalousie avec sa puissance évolution dans les siècles passé pour l'échanger des secrets par plusieurs méthodes comme la méthode Hissab el Joummal et la méthode des oiseux.

Introduction générale

Depuis que l'homme a été crée, il vit parmi ses semblable et communique avec eux et donc ressent parfois le besoin de dissimiler des informations secrètes en les rendant illisibles car le maintien du secret est une nécessité qui offre parfois la sécurité et donc la cryptographie a toujours été parmi nous.

La cryptographie est la « «science du secret », regroupe deux branches : d'une part, la cryptographie, qui permet de coder des messages, et d'autre part, la cryptanalyse, qui permet de les décoder.

La cryptographie informatique professionnelle est un phénomène récent, rendu indispensable du fait que les informations sont accessibles pratiquement à tous par des réseaux publics.

La cryptographie moderne est orientée vers la manipulation des chiffres et utilise avec abondance des résultats de l'arithmétique, établit souvent il y a longtemps et dont l'utilité pratique n'avait pas été prouvé.

L'informatique par la puissance de calcul qu'elle offre est un outil essentiel de la cryptographie moderne.

Nous sommes intéressé dans notre projet de fin d'étude par la cryptographie des textes arabes on utilisons l'algorithme à clé secrète DES et l'algorithme à clé publique RSA.

Notre mémoire est structuré comme suite :

Chapitre 1 : regroupe les généralités de la cryptographie.

Chapitre 2 : présente un historique de la cryptographie arabe.

Chapitre 3 : est consacré à la présentation des principales méthodes de cryptage comme RSA et DES.

Chapitre 4 : le dernier chapitre concerne la partie développement de l'application du notre projet, qui détaille l'implémentation de l'algorithme DES et RSA pour le cryptage des textes arabe.

Liste des figures

LISTE DES TABLEAUX

Référence Bibliographique

[1] : L. Ghislaine, Introduction à la cryptologie, 1998

[2] : G. Zennor, Cours de cryptographie, 2000.

[3] : B. Martin, Codage, Cryptologie et application, 2001.

[4] : M. Riguidel, Quelque rappels sur les techniques cryptographiques, 2002.

[5] : W. Diffie, dix premières années de la cryptographie à clef publique. Edition 1988.

[6] : B. Schneier, Cryptographie appliquée. 2ième édition, 1996.

[7] : « Cryptographies Mathématiques », Guy Chassé, Maitre assistant de mathématiques, Ecole des Mines de Nantes.

[8] : « Théorie des nombres et Cryptographie », François Arnauld, Univercité de Limoges, cours de D.E.A.

[9] : « Introduction à la cryptographie », Hervé Schauer, 2001.

[10] : Diwane Al Moetamid Ibn Abad. Hamid Abdelmajid, Ahmed Ahmed Badaoui, 4ème

édition, Imprimerie "Dar Al Kotob Wa Al Wathaik Alkaemia Alkahira" Egypt 2002 .

[11] : Arabic Originis of Cryptology, Volumes 1, 2, 3 and 4. M. Mrayati, Y Meer Alam and M.H.At-Tayyan. Published by KFCRIS & KACST Riyadh 2000.

[12] : Arrihla Al Ayachiia RPS_PTNl R_UNl, Abou Salim Abdellah Ben Mohamed El Ayachi. Vol. 2. Edition révisé par Saïd El Fadhili et Solaiman El Korachi. Dar Essouaidi Linachr Wa Attawzie, Abou Dabie, EAU. 2006.

[13] : G. S. Colin, Note sur le Système Cryptographique du Sultan Ahmad Al-Mansur, Hespéris Tome VII, 2ème trimestre 1927

[14] : Origins of cryptology: The Arab contributions. Ibrahim A. Al-Kadi Cryptologia 16 (1992), 97 – 126.

[15] : Abdelmalek Azizi, Extraits de l'Histoire de la Cryptographie au Maroc, Université Mohammed Premier Oujda, Maroc 2009.

Sommaire

Chapitre3 : Les crypto-systèmes :

Webographie

[A] : http:// www.wikipidia.org

[B] : http:// www.apprendre-en-ligne .net

[C] : http:// www.secondeguerre.net

[D] : http:// www.grappa.univ-lille3.fr

[E] : http:// www.site-sciences.fr

[F] : http:// www.webauvages.net

[G] : http:// www.geekants.com

[H] : http:// www.developpez.com

ملخص

إنّ الهدف الأساسي من مشروعنا هذا ، هو دراسة مختلف الخوارزميات المستعملة في عملية التشفير و حماية المعلومات المتنقلة عبر الشبكة المعلوماتية

يتم تقسيم نظم التشفير الحديث إلى قسمين:
أنظمة التشفير المتناظر ، التي تستخدم نفس المفتاح لتشفير وفك تشفير ولها ميزة كونها سريعة.
أنظمة التشفير غير المتناظر للنظام التشفير التي تتطلب مفاهيم الرياضيات الأساسية وباستخدام المفتاح العمومي لتشفير والمفتاح الخاص لفك ولهم الاستفادة من مفاتيح الأمان.

إنّ الأهمية المعطات لعملية تشفير اللغة العربية يرجع إلى مختلف الدراسات و الأعمال المنجز من قبل العلماء العرب في الحقب الزمنية الماضية

لقد تمّ إختيار التشفير المتناظر مثل DES و التشفير غير المتناظر مثل RSA في عملية تشفير اللغة العربية

Résumé

L'objectif principal de notre projet est d'étudier les différents algorithmes de cryptage utilisés pour le chiffrement et la protection des données circulée dans les réseaux informatique.
La cryptographie moderne se décomposés en deux classes :
La cryptographie symétrique qui utilise la même clé pour chiffrer et déchiffrer des messages et qui a l'avantage d'être rapide.
Le cryptage asymétrique nécessitant des notions essentiel en mathématiques et qui utilise une clé publique pour chiffrer et une clé privée pour déchiffrer et qui a l'avantage de la sécurité des clés.
L'importance donner à l'opération de cryptage de la langue arabe revient à l'étude des différents travaux qui était faite par les savants arabes dans l'histoire.
Nous avons choisit comme exemple de cryptage à clé secrète DES et à clé publique RSA afin de chiffrer des textes arabe.

Abstract

L'objectif principal de notre projet est d'étudier les différents algorithmes de cryptage utilisés

The main aim of our project is to study the various algorithms of encryption used for the ciphing and the data protection circulated in the networks data processing.
Modern cryptography devised into two classes:
The symmetrical cryptography which uses the same key to encryption and decipher messages and which with the advantage of being fast.
The asymmetrical cryptography requiring of the notions main part in mathematics and which uses a public key to encryption and a key private to decryption and which with the advantage of safety of the keys.
The importance to give to the operation encryption of the Arab language returns being studied of various works which was made by the Arab scientists in the history.
We have chooses like example of secret key cipher DES and with public key RSA in order to encryption texts Arab.

pour le chiffrement et la protection des données circulée dans les réseaux informatique.
La cryptographie moderne se décomposés en deux classes :
La cryptographie symétrique qui utilise la même clé pour chiffrer et déchiffrer des messages et qui a l'avantage d'être rapide.
Le cryptage asymétrique nécessitant des notions essentiel en mathématiques et qui utilise une clé publique pour chiffrer et une clé privée pour déchiffrer et qui a l'avantage de la sécurité des clés.
L'importance donner à l'opération de cryptage de la langue arabe revient à l'étude des différents travaux qui était faite par les savants arabes dans l'histoire.
Nous avons choisit comme exemple de cryptage à clé secrète DES et à clé publique RSA afin de chiffrer des textes arabe.

The main aim of our project is to study the various algorithms of encryption used for the ciphing and the data protection circulated in the networks data processing.
Modern cryptography devised into two classes:
The symmetrical cryptography which uses the same key to encryption and decipher messages and which with the advantage of being fast.
The asymmetrical cryptography requiring of the notions main part in mathematics and which uses a public key to encryption and a key private to decryption and which with the advantage of safety of the keys.
The importance to give to the operation encryption of the Arab language returns being studied of various works which was made by the Arab scientists in the history.
We have chooses like example of secret key cipher DES and with public key RSA in order to encryption texts Arab.