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

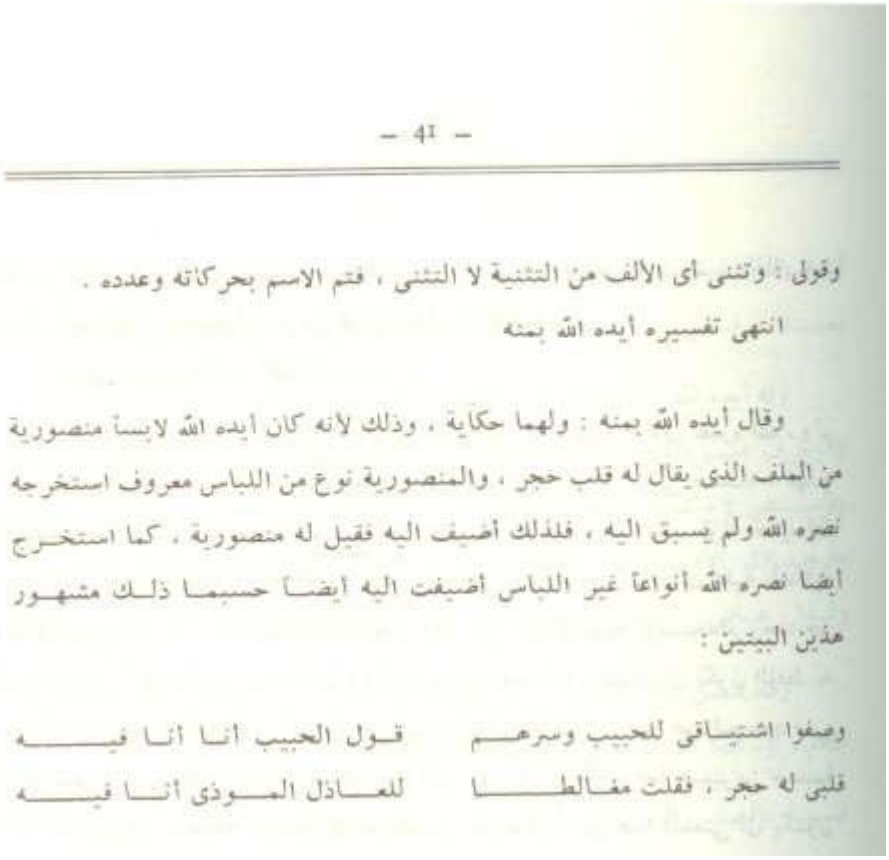
et de l'Or. Ainsi, son époque avait connu un développement exceptionnel dans tous les domaines.

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 وسرعتى ... قول الحبيب أنا أنا فيه

قلبى له حجر ، فقلت مغالطا ... للعاذل الموذى 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 احسبني 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**
في ضرب	**زد زائدا**	**نقص إلا**	**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

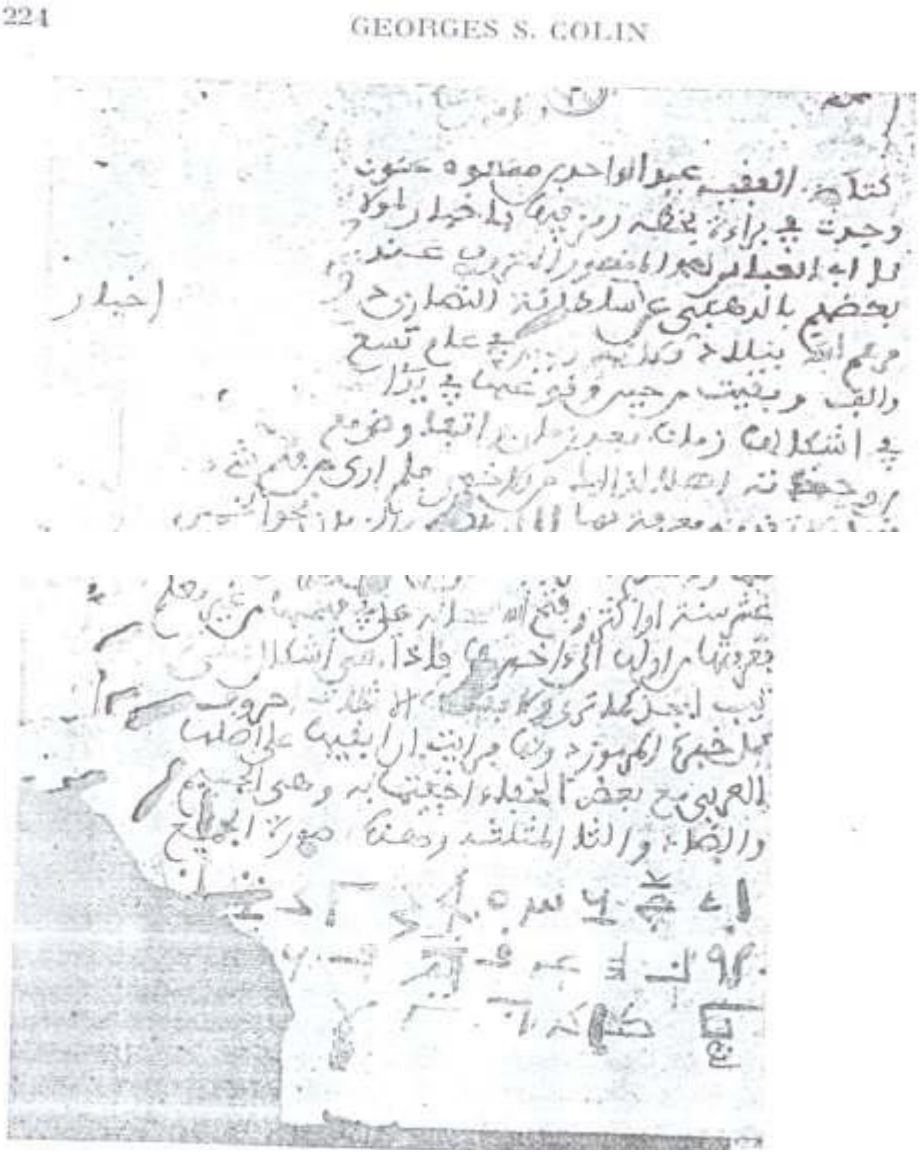


Figure 2.2 : une note de message secret d'Anoun

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.

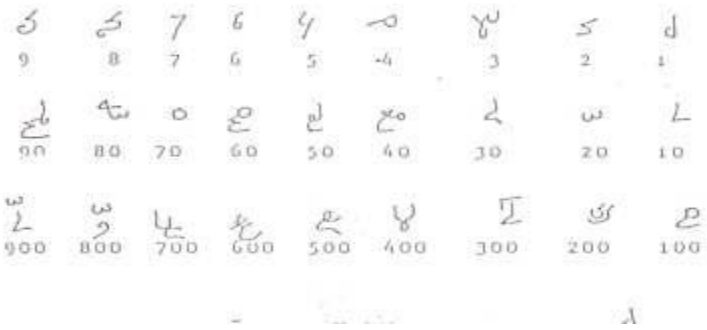


Figure 2.3 : la plume de Fès

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***) قصيدة القاضي*** 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.