République Algérienne Démocratique et Populaire
Ministère de l'enseignement supérieure et de la recherche scientifique

N Attribué par la bibliothèque

Année Univ : 2017/2018

La cryptographie a base d'ADN : Application sur les images

Mémoire présenté en vue de l'obtention du diplôme de

Master Académique

Université Dr Tahar Moulay - Saïda

Discipline : INFORMATIQUE

Spécialité : Sécurité informatique et cryptographie

par

Chibani Miloud

Berriah Mohammed

Dr : Dr.Kadda benyahia Université Dr Tahar Moulay - Saïda Encadreur

REMERCIEMENTS

Avant tout je remercie, le Dieu tout puissant de mon accordée la volonté et la patience pour accomplir ce modeste travail.

Ce mémoire n'aurait pas été possible sans l'intervention, d'un grand nombre de personnes, je souhaite ici les en remercier.

Je tien d'abord à remercier très chaleureusement mon encadreur de mémoire de fin d'études M_r Kadda Benyahia , pour ses précieux conseils et son orientation tout au long de mes recherches.

Tous les membres de jury d'avoir participé à la commission des examinateurs en vue d'une évaluation prompte et à sa juste valeur.

Je remercie mes chers parents qui m'ont indiqué le bon chemin à entreprendre et qui m'ont encouragé et soutenue tout au long de mon parcours quotidien.

Les conseils que je me a prodigué, la patience, la confiance que je a témoignés ont été déterminants dans la réalisation de mon travail de recherche.

Mes remerciements s'étendent également à tous mes enseignants durant les années des études. $\grave{A}$ mes familles et mes amis qui par leurs prières et leurs encouragements, on a pu surmonter tous les obstacles.

Enfin, je tien à remercier tous ceux qui, de près ou de loin, ont contribué à la réalisation de ce travail.

Je dédie ce modeste travail à : mes parents

Tous mes oncles et tantes, tous mes cousins et cousines.

Tous mes enseignants de département d'informatique.

Tous mes camarades de promotion 2017 /2018.

Résumé

La cryptographie ADN est un domaine nouveau et prometteur pour la sécurité de l'information. C'est une combinaison des solutions classiques de cryptographie avec les avantages du matériel génétique. En effet, il est possible de bénéficier des avantages des systèmes cryptographiques classiques et de les rendre plus efficaces sur certaines méthodes grâce à l'utilisation de l'ADN. Il y a différentes façons d'utiliser l'ADN pour sécuriser le contenu de l'information. Cette thèse propose deux solutions différentes pour utiliser l'ADN dans la cryptographie sous forme numérique.

D'une part, l'ADN numérique peut être utilisé pour le stockage et pour cacher des données à l'intérieur de celui-ci. L'information secrète est placée dans une molécule de l'ADN. Cette méthode est possible grâce à l'indexation des bases nucléotides dans une séquence génétique.

D'autre part, les nombres aléatoires peuvent être générés à partir de séquences numériques d'ADN. En effet, les bases informatiques de données génétiques contiennent des séquences d'ADN sous forme numérique. Ils représentent une solution pour la génération et la transmission des clés OTP (One-Time-Pad) symétriques. La transmission d'une très longue clé de cryptage n'est pas nécessaire, car chaque séquence possède un numéro d'identification unique dans la base de données. Ce numéro, ou une combinaison de ces numéros, peut alors être transmis.

Abstract

DNA cryptographyis is a new and promising field in information security. It is a combination of classical cryptography solutions with the advantages of genetic material. Indeed, it is possible to enjoy the benefits of conventional cryptographic systems and make them more effective on some methods through the use of DNA. There are different ways of using DNA to secure the contents of the information. This thesis proposes two differents solutions for use in DNA cryptography.

On the one hand, the digital DNA can be used for storage and for data hiding inside there of. The secret information is placed in a DNA molecule. This method is possible thanks to the indexing of nucleotide bases in a DNA sequence.

On the other hand, the random numbers can be generated from digital DNA sequences. Indeed, genetic data of computer databases contain DNA sequences in digital form. They represent a solution for the generation and transmission of symmetrical key OTP (One-Time-Pad). Transmitting a long key is not necessary, since each sequence has a unique identification number in the database. This number, or a combination of these numbers may be transmitted.

Table des matières

Introduction et terminologie **8**

1 Généralité sur la cryptographie **10**

1.1 Qu'est ce que la cryptographie : 11

1.1.1 Vocabulaire de base : 11

1.2 Qualités D'un Cryptosysteme : 14

1.2.1 Principes de Kerckhoffs : 14

1.2.2 Les éléments de la cryptographie : 15

1.3 les types de la cryptographie : 16

1.3.1 Cryptosystème à clé symétrique : 16

1.3.2 Cryptosysteme à cle asymetrique : 25

1.3.3 RSA : 26

1.4 les principes de base d'ADN 28

1.5 Comprendre L'ADN : 28

1.6 Définition de quelles que notions : 30

1.6.1 Les bases azotées : 31

1.6.2 Le nucléotide : 32

1.6.3 Le nucléoside : 33

1.6.4 Le brin d'ADN : 33

1.7 Conclusion 34

2 Etat de l'art sur la cryptographie ADN **35**

2.1 Introduction : 36

2.2 ADN informatique 36

2.3 ADN Cryptographie : 37

2.3.1 Réaction de polymérisation en chaîne (RPC) 41

2.3.2 Bimoléculaire Design cryptographique basé sur l'ADN 41
2.4 Substitution : 42
2.4.1 Cartographie XOR 42
2.4.2 Système cryptographique clé symétrique en utilisant l'ADN 42
2.4.3 Système cryptographique clé asymétrique en utilisant l'ADN 42
2.4.4 ADN stéganographie 43
2.4.5 Méthode de cryptographie Pseudo ADN 43
2.4.6 G. Puce à ADN 44
2.4.7 Chaotique de codage 44
2.5 Cryptage d'Images 44
2.5.1 revue de la littérature 45
2.6 Conclusion 48

3 Notre Contribution **50**
3.1 Introduction 51
3.2 Contribution 51
3.2.1 Processus de chiffrement 51
3.2.2 Processus de déchiffrement 52
3.3 Conclusion 53

4 Implémentation et discussion des résultats **55**
4.1 Introduction 56
4.2 Environnement de développement : 56
4.3 Tests et résultats expérimentaux de Crypto-ADN 57
4.3.1 Complexité de l'algorithme 57
4.3.2 Variation du temps d'exécution 58
4.3.3 Variation de la taille d'image chiffré selon la taille d'image clair : . . 59
4.3.4 Comparaison en temps d'exécution entre l'algorithme proposé et AES : 60
4.4 Conclusion 62

Conclusion Générale et Perspectives **63**

Table des figures

1.1 Protocole de chiffrement 11
1.2 Shéma d'un cryptosysteme 12
1.3 Principe Chiffrement / Déchiffrement 13
1.4 Modele de cryptage symetrique 17
1.5 Algorithme DES 19
1.6 Modele de cryptage asymetrique 26
1.7 ADN : vue globale. 29
1.8 Les 4 nucléotides composant l'hélice d'ADN. 30
1.9 Structure d'un chromosome. 31
1.10 Structure Chimique des bases azotèes 32
1.11 Structure de Nucléotide. 32
1.12 Nucléoside vs Nucleotide 33
1.13 Structure d'un brin d'ADN 34

2.1 Central dogma of DNA 38
2.2 DNA Indexing 40
2.3 DIAGRAMME DE Flux de l'information génétique 43
2.4 cryptage d'image 45

4.1 Mesure du temps d'exécution selon la taille des images. 58
4.2 Variation du temps d'exécution selon la taille des images 59
4.3 Variation de la taille d'image chiffré selon la taille d'image clair 59
4.4 la relation entre la taille du d'image clair et la taille du d'image chiffré. . . 60
4.5 AES vs Crypto ADN 61

Introduction et terminologie

Le 21 siècle est une période d'explosion de l'information où l'information est devenue ressource stratégique très importante, et donc la tâche de la sécurité de l'information est devenue augmente important.

La cryptographie est la partie la plus importante de la infrastructure de sécurité de communication et de sécurité informatique. Cependant, il y a beaucoup défauts latents dans certains de la technologie de cryptographie classique de la cryptographie moderne - tels que les algorithmes RSA et DES - qui ont été brisés par certains programmes d'attaque. Certains la technologie de cryptage peut définir une trappe, donnant à ces attaquants qui comprennent ce piège porte la capacité de déchiffrer ce type de technologie de cryptage. Cette information démontre que la technologie de chiffrement cryptographique moderne basée sur mathématique les problèmes ne sont pas aussi fiables qu'avant.

La relation entre la cryptographie et la biologie moléculaire était à l'origine non pertinente, mais avec l'étude approfondie de la biotechnologie moderne et de l'informatique de l'ADN, ces deux les disciplines commencent à travailler ensemble de plus près. Cryptographie d'ADN et information la science est née après des recherches dans le domaine du domaine de l'ADN par Adleman ; c'est un nouveau domaine et est devenu le fer de lance de la recherche internationale sur la cryptographie. De nombreux chercheurs de partout dans le monde ont fait un grand nombre d'études sur la cryptographie d'ADN. Dans termes de cacher des informations, il y a des résultats tels que "Cacher les messages dans les micropoints d'ADN,"Cryptographie avec des brins binaires d'ADN" et ainsi de suite. En termes d'algorithmes d'ADN, il y a des résultats tels que "Une conception de cryptographie bimoléculaire basée sur l'ADN", "Système de clé publique utiliser l'ADN comme une fonction à sens unique pour la distribution de clés, " " système de cryptographie DNASC " etc. Cependant, la cryptographie d'ADN est un domaine émergent de la

cryptographie et de nombreux les études sont encore à un stade précoce.

La cryptographie ADN est basée sur des problèmes biologiques : en théorie, un ordinateur à ADN ne sera pas a seulement la même puissance de calcul qu'un ordinateur moderne mais aura aussi une puissance et fonction que les ordinateurs traditionnels ne peuvent pas égaler. Premièrement, les chaînes d'ADN ont un très grande échelle de parallélisme, et sa vitesse de calcul pourrait atteindre 1 milliard de fois par seconde ; Deuxièmement, la molécule d'ADN - en tant que vecteur de données - a une grande capacité. Il semble que l'un des trillions de bits de données binaires peuvent être stockés dans un décimètre cube d'une solution d'ADN ; troisième, un L'ordinateur moléculaire à ADN a une faible consommation d'énergie, seulement égale à un milliardième de ordinateur traditionnel.

1

Généralité sur la cryptographie

Contents

1.1 Qu'est ce que la cryptographie : 11

1.1.1 Vocabulaire de base : 11

1.2 Qualités D'un Cryptosysteme : 14

1.2.1 Principes de Kerckhoffs : 14

1.2.2 Les éléments de la cryptographie : 15

1.3 les types de la cryptographie : 16

1.3.1 Cryptosystème à clé symétrique : 16

1.3.2 Cryptosysteme à cle asymetrique : 25

1.3.3 RSA : 26

1.4 les principes de base d'ADN 28

1.5 Comprendre L'ADN : 28

1.6 Définition de quelles que notions : 30

1.6.1 Les bases azotées : 31

1.6.2 Le nucléotide : 32

1.6.3 Le nucléoside : 33

1.6.4 Le brin d'ADN : 33

1.7 Conclusion 34

1.1 Qu'est ce que la cryptographie :

1.1.1 Vocabulaire de base :

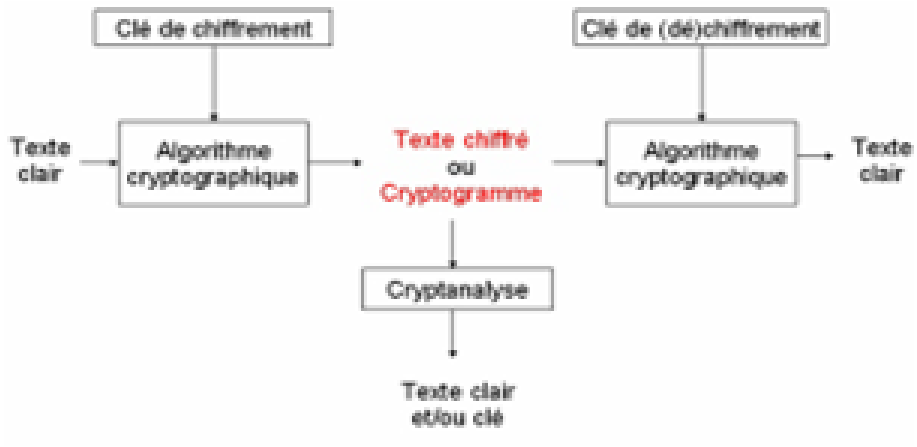

FIGURE 1.1 – Protocole de chiffrement .

Avant d'entamer cette thèse, il est impérativement important de définir certain notions très utilisé en la matière.

- **Cryptologie :** Il s'agit d'une science mathématique comportant deux branches : la cryptographie et la cryptanalyse.[1]

- **Cryptographie :** La cryptographie est l'étude des méthodes donnant la possibilité d'envoyer des données de manière confidentielle sur un support donné. [1]

- **Cryptanalyse :** Opposée à la cryptographie, elle a pour but de retrouver le texte clair à partir de textes chiffrés en déterminant les failles des algorithmes utilisés. [1]

- **Cryptosystème :** Il est déffni comme l'ensemble des clés possibles (espace de clés), des textes clairs et chiffrés possibles associés à un algorithme donné. [1]

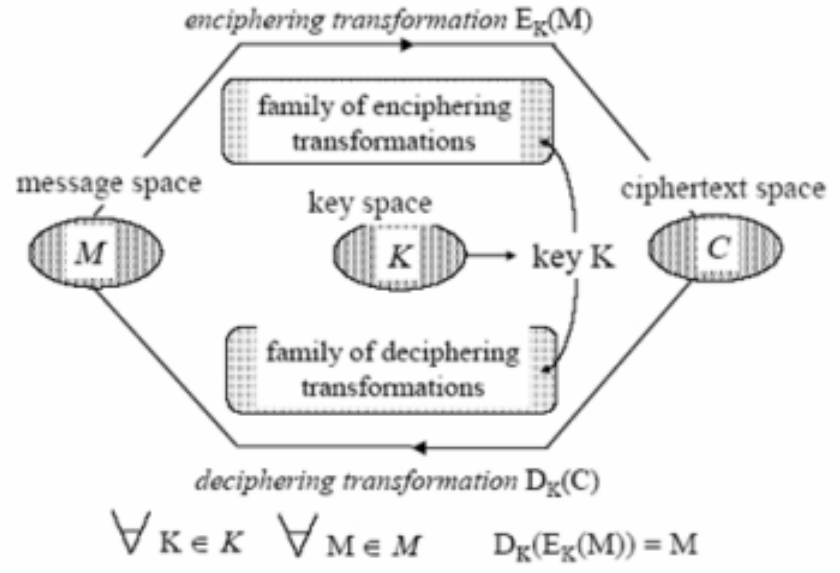

FIGURE 1.2 – Shéma d'un cryptosysteme .

L'algorithme est en réalité un triplet d'algorithmes :
∗ l'un générant les clés K,
∗ un autre pour chiffrer M, et
∗ un troisième pour déchiffrer C.

Remarque : On parle de "décryptage" pour désigner l'action permettant de retrouver le texte clair sans connaître la clef de déchiffrement. On emploie également parfois les termes "cryptage" et "crypter" pour qualifier l'action de chiffrer un message. Les mots "encryptage" et"(en)cryptement" sont des anglicismes dérivés du verbe "to encrypt".

Chiffrement et déchiffrement : Le chiffrement consiste à transformer une donnée afin de la rendre incompréhensible par une personne autre que celle autorisée. La fonction permettant de retrouver le texte clair à partir du texte chiffré porte le nom de déchiffrement . [1]

Texte clair : Texte original intelligible tel qu'il se présentait avant tout chiffrement. [1]

Texte chiffré (cryptogramme) : le texte chiffré est le résultat de l'application d'un chiffrement à un texte clair. [1]

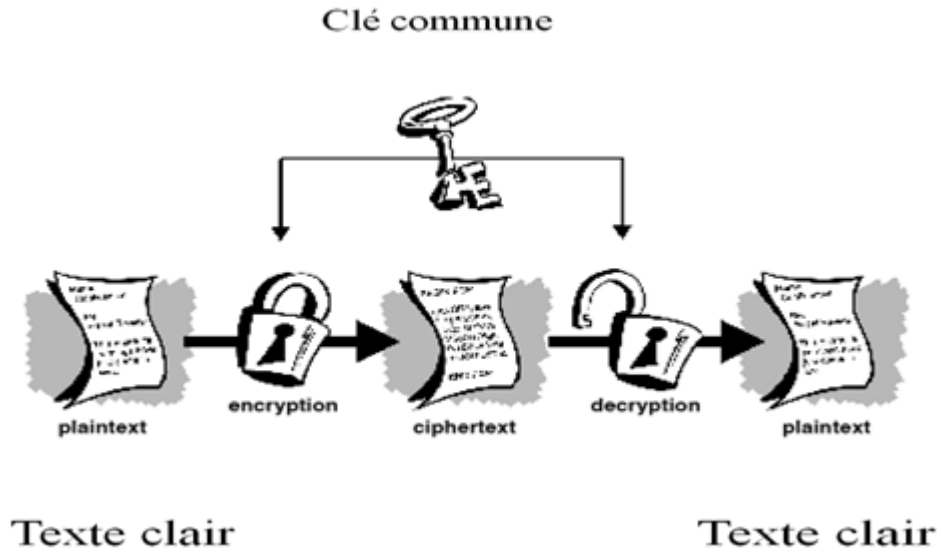

FIGURE 1.3 – Principe Chiffrement / Déchiffrement .

La clef : Il s'agit du paramètre impliqué et autorisant des opérations de chiffrement et/ou déchiffrement.Dans le cas d'un algorithme symétrique, la clef est identique lors des deux opérations. Dans le cas d'algorithmes asymétriques, elle difère pour les deux opérations. [1]

- **Les clés symétriques :** il s'agit de clés utilisées pour le chiffrement ainsi que pour le déchiffrement. On parle alors de chiffrement symétrique.

- **Les clés asymétriques :** il s'agit de clés utilisées dans le cas du chiffrement asymétrique (aussi appelé chiffrement à clé publique). Dans ce cas, une clé différente est utilisée pour le chiffrement et pour le déchiffrement.

Stéganographie : La stéganographie (du grec steganos, couvert et graphein, écriture) est l'art de cacher un message secret au sein d'un autre message porteur (texte, image, son, vidéo...) de caractère anodin, de sorte que l'existence même du secret en soit dissimulée. Alors qu'avec la cryptographie, la sécurité repose sur le fait que le message chiffré soit incompréhensible pour les personnes non autorisées, avec la stéganographie, la sécurité repose sur le fait que la présence même d'un message secret ne sera sans doute pas soupçonnée et détectée.[2]

Fonctions de hachage : Lors d'échanges de messages cryptés, il est important de pouvoir s'assurer que le message n'a pas été altéré ou modifié par un tiers pendant l'envoi.

Les fonctions de hachage permettent alors de s'assurer de l'intégrité du message.
- Une fonction de hachage h est une fonction qui, à partir d'un document x (fichier) de taille quelconque, calcule une chaine de bits h(x) d'une taille fixèe (m) nommèe empreinte (ou hachè, ou condensè, ou encore rèsumè). [2]

La signature numérique : Les fonctions de hachage permettent de s'assurer de l'intégrité d'un message mais un autre problème se pose : comment être certain que personne n'a usurpé l'identité de l'expéditeur pour vous envoyer un message ? Ou que l'expéditeur ne va pas nier vous l'avoir envoyé ?

C'est le rôle de la signature numérique, celle-ci fournissant donc les services d'intégrité des données, d'authentification de l'origine des données et de non-répudiation.

La façon la plus simple de signer un message est d'utiliser la cryptographie asymétrique pour le chiffrer en utilisant sa clef privée : seul le possesseur de cette clef peut générer la signature et toute personne ayant accès à la clef publique correspondante peut la vérifier. Mais cette méthode est très lente et en pratique elle n'est que peu utilisée.

La méthode réellement utilisée repose non pas sur le chiffrement du message lui-même mais sur l'empreinte de celui-ci. En effet, cette méthode est beaucoup plus rapide du fait de la quantité réduite des données à chiffrer.
Une signature numérique est plus sûre qu'une signature papier car la signature change à chaque message. Elle est de ce fait inimitable (sans la connaissance de la clef secrète bien entendue). [2]

1.2 Qualités D'un Cryptosysteme :

Les qualitès demandèes à un système cryptographique sont rèsumèes par les mots clefs suivants :

1.2.1 Principes de Kerckhoffs :

La sécurité du chiffre ne doit pas dépendre de ce qui ne peut pas être facilement changé.

En d'autres termes, aucun secret ne doit résider dans l'algorithme mais plutôt dans la clé. Sans celle-ci, il doit être impossible de retrouver le texte clair à partir du texte chiffré. Par contre, si on connaît K, le déchiffrement est immédiat.

On parle aussi de la Maxime de Shannon, dérivée du principe énoncé ci-dessus : L'adversaire connait le système.
Remarque : Il faut distinguer les termes "Secret" et "Robustesse" d'un algorithme. Le secret de l'algorithme revient à cacher les concepts de celui-ci, ainsi que les méthodes utilisées (fonctions mathématiques).
La robustesse quant à elle désigne la résistance de l'algorithme à diverses attaques qui seront explicitées dans la suite de ces notes. [2]

1.2.2 Les éléments de la cryptographie :

- **Confidentialitè :** seules les personnes habilitèes ont accès au contenu du message.

- **Intègritè des donnèes :** le message ne peut pas étre falsifiè sans qu'on s'en aperçoive.
- **Authentification :**
  - l'èmetteur est sur de l'identitè du destinataire c'est à dire que seul le destinataire pourra prendre connaissance du message car il est le seul à disposer de la clef de dèchiffrement.
  - le receveur est sur de l'identitè de l'èmetteur.
- **Non-rèpudiation** qui se dècompose en trois :
  1. **non-rèpudiation d'origine** l'èmetteur ne peut nier avoir ècrit le message et il peut prouver qu'il ne l'a pas fait si c'est effectivement le cas.

  2. **non-rèpudiation de rèception** le receveur ne peut nier avoir reçu le message et il peut prouver qu'il ne l'a pas reçu si c'est effectivement le cas.
  3. **non-rèpudiation de transmission** l'èmetteur du message ne peut nier avoir envoyè le message et il peut prouver qu'il ne l'a pas fait si c'est effectivement le cas.

On peut regarder ces quatre qualitès du point de vue de l'èmetteur. Alice veut etre certaine

- qu'une personne non-autorisèe (Eve) ne peut pas prendre connaissance des messages qu'elle envoie, confidentialitè.
- que ses messages ne seront pas falsifiès par un attaquant malveillant (Martin), intègritè.
- que le destinataire (Bob) a bien pris connaissance de ses messages et ne pourra pas nier l'avoir reçu, non-rèpudiation.

de plus elle veut etre certaine que son message ne sera pas brouillè par les imperfections

du canal de transmission (cette exigence ne relève pas du cryptage mais de la correction d'erreur).
Bob veut etre certain
- que personne d'autre que lui (et Alice bien sur) n'a accès au contenu du message, confidentialitè.
- que le message reçu vient bien d'Alice authentification, par exemple qu'un attaquant malveillant (Oscar) ne puisse pas se faire passer pour Alice, mascarade ou usurpation d'identitè
- que le message n'a pas ètè falsifiè par un attaquant malveillant (Martin), intègritè des donnèes
- que l'expèditeur (Alice) ne pourra pas nier avoir envoyè le message,non-rèpudiation [2]

1.3 les types de la cryptographie :

1.3.1 Cryptosystème à clé symétrique :

Caractéristiques :
- Les clés sont identiques : KE = KD = K.
- La clé doit rester secrète.
- Les algorithmes les plus répandus sont le DES, AES, 3DES, ...
- Au niveau de la génération des clés, elle est choisie aléatoirement dans l'espace des clés.
- Ces algorithmes sont basés sur des opérations de transposition et de substitution des bits du texte clair en fonction de la clé.
- La taille des clés est souvent de l'ordre de 128 bits. Le DES en utilise 56, mais l'AES peut aller jusque 256.
- L'avantage principal de ce mode de chiffrement est sa rapidité.
- Le principal désavantage réside dans la distribution des clés : pour une meilleure sécurité, on préfèrera l'échange manuel. Malheureusement, pour de grands systèmes, le nombre de clés peut devenir conséquent. C'est pourquoi on utilisera souvent des échanges sécurisés pour transmettre les clés. En effet, pour un système à N utilisateurs, il y aura N.(N - 1)/2 paires de clés. [3]

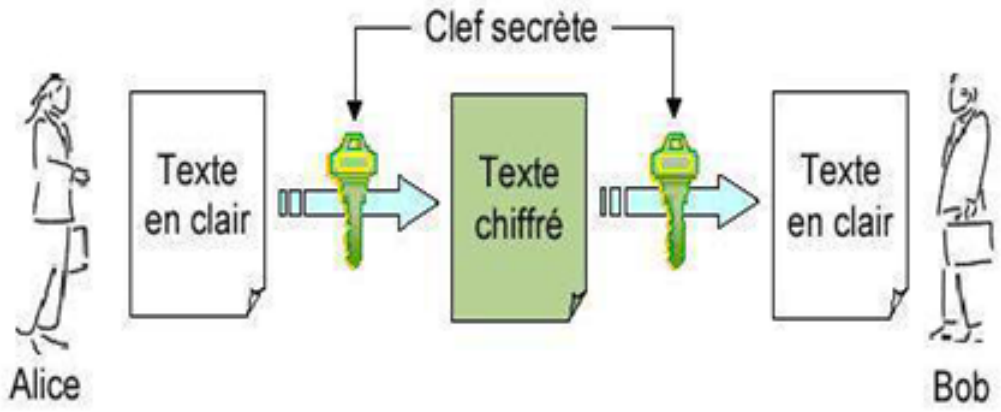

FIGURE 1.4 – Modele de cryptage symetrique .

Cryptosystèmes par flots

Dans un cryptosystème par flots, le cryptage des messages se fait caractère par caractère ou bit à bit, au moyen de substitutions de type César générées aléatoirement : la taille de la clef est donc égale à la taille du message. L'exemple le plus illustratif de ce principe est le chiffre de Vernam. Cet algorithme est aussi appelé « One Time Pad » (masque jetable), c'est à dire que la clef n'est utilisée qu'une seule fois.
Voici un exemple simple de l'application du chiffre de Vernam :

Exemple :
Message en clair : "SALUT"
⇒ (conversion en binaire)
01010011 01000001 01001100 01010101 01010100
XOR
Clef (générée aléatoirement)
01110111 01110111 00100100 00011111 00011010
=
00100100 00110110 01101000 01001010 01001110
⇒ (conversion en caractère)
"Message chiffré : $6jJM"

- Il a été démontré par le mathématicien Claude Elwood Shannon qu'il était impossible de retrouver un message crypté par le principe de Vernam sans connaître la clef. Ce qui ferait en théorie du chiffre de Vernam un cryptosystème incassable. Mais dans la pratique, le cryptosystème par flots pose des problèmes délicats : canaux sûrs de distribution des clefs, taille des clefs encombrantes car de même taille que le message et surtout caractère

aléatoire des générateurs de bits de clefs utilisés. En revanche, un des avantages du système est qu'il est insensible aux phénomènes de propagation d'erreurs : un bit erroné donne une erreur à la réception ou à l'émission, mais est sans incidence sur les bits suivants. [4]

Cryptosystèmes par blocs :

La deuxième classe de cryptosystèmes utilisée aujourd'hui est celle des cryptosystèmes par blocs. Dans ce mode de cryptage, le texte clair est fractionné en blocs de même longueur à l'aide d'une clef unique. Les algorithmes de chiffrement par blocs sont en général construits sur un modèle itératif.
Ce modèle emploie une fonction F qui prend en paramètres une clef k et un message de n bits. F est répétée un certain nombre de fois, on parle de ronde. A chaque ronde, la clef k utilisée est changée et le message que l'on chiffre est le résultat de l'itération précédente.

C1 = F (k1, M)
C2 = F (k2, C1)
...
Cr = F (kr, Cr-1)

- Emetteur et destinataire se partagent une clé K secrète. L'algorithme qui engendre les clefs ki à partir de K se nomme l'algorithme de cadencement des clefs.
- La fonction F doit être inversible, ce qui veut dire qu'il faut pour toute clef k et message M pouvoir recalculer M a partir de F (k', M), sinon le déchiffrement est impossible et on ne dispose pas d'un algorithme utilisable. C'est-à-dire qu'il existe une fonction G vérifiant G (k, F (k, M)) = M et que F est une permutation.
- La sécurité d'un algorithme de chiffrement par blocs réside principalement dans la conception de l'algorithme de cadencement des clefs et la robustesse de la fonction F. Si l'algorithme de cadencement est mal élaboré, les ki peuvent être déductibles les unes des autres. La fonction F doit donc être difficile à inverser sans connaître la clef k ayant servie dans le calcul de C = F (k, M). En d'autres termes, connaissant seulement C, F et G, on ne doit pouvoir retrouver le message M seulement en effectuant une recherche exhaustive de la clef.
- Les caractéristiques de ces systèmes sont en général liées à leur très forte sensibilité à la dépendance inter-symboles, ainsi qu'à leur mécanisme de propagation d'erreurs. Toute erreur commise sur un bloc de texte clair ou chiffré peut perturber gravement le chiffrement/déchiffrement de ses voisins. [4]

Algorithme Data Encryption Standard (DES) :

Publié en 1977 par le NBS (National Bureau of Standards), le DES est un algorithme de chiffrement de données recommandé pour les organisations à caractère fédéral, commercial ou privé. Le DES tire son origine des travaux menés par le groupe cryptographique d'IBM dans le cadre du projet LUCIFER. Le DES a été l'objet de nombreuses implémentations, à la fois en matériel et en logiciel, depuis sa publication. Après une décennie de succès, pendant laquelle les moyens et techniques de cryptanalyse mis en œuvre pour en étudier les caractéristiques n'ont pas permis d'en découvrir des faiblesses rédhibitoires, le DES a, depuis peu, révélé des sensibilités à des attaques nouvelles et puissantes, parfois réalisées sur un simple micro-ordinateur. Aussi l'ISO (International Organization for Standardization) a-t-il récemment refusé la normalisation du DES, ce qui n'empêche pas cet algorithme d'être, de loin, aujourd'hui encore comme le moyen de chiffrement le plus sûr (et le plus largement utilisé) pour des données non militaires.
Le DES est un algorithme de chiffrement symétrique par blocs qui permet de chiffrer des mots de 64 bits à partir d'une clef de 56 bits(56 bits servant à chiffrer + 8 bits de parité servant à vérifier l'intégrité de la clef en réalité). [4]

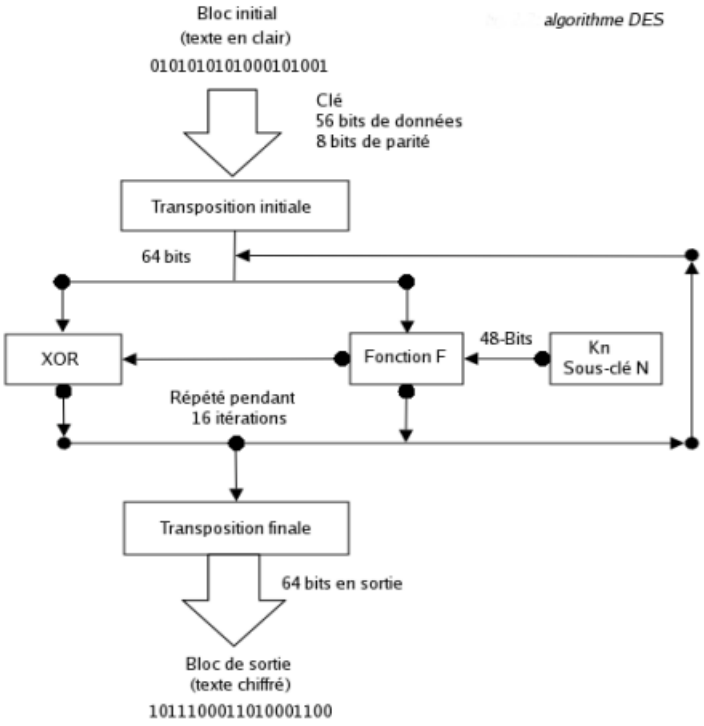

FIGURE 1.5 – Algorithme DES

Voici les différentes étapes de l'algorithme du DES :

- **Fractionnement du message**

Dans un premier temps le message en clair est découpé en blocs de 64 bits.

- **Transposition initiale**

Chaque bit d'un bloc subit une permutation selon l'arrangement du tableau ci-contre c'est-à-dire que le $58^{ème}$ bit du bloc se retrouve en $1^{ère}$ position, le $50^{ème}$ en seconde position,etc...

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

- **Scindement en bloc de 32 bits**

Le bloc de 64 bits est scindé en deux blocs de 32 bits notés G et D. On notera G0 et D0 l'état initial de ces deux blocs. [4]

G_0

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8

D_0

57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

On remarque que G0 contient tous les bits pairs du message initial et D0 tous les bits impairs.

- **Rondes**

Les blocs Gi et Di sont soumis à un ensemble de transformation appelées rondes.
Une ronde est elle-même composée de plusieurs étapes :

Fonction d'expansion :

Les 32 bits du bloc D0 sont étendus à 48 bits grâce à une table d'expansion dans laquelle 32 bits sont mélangés et 16 d'entre eux sont dupliqués. Ainsi, le $32^{ème}$ bit devient le premier, le premier devient le second... Les bits 1,4,5,8,9,12,13,16,17,22,21,24,25,28,29 et 32 sont dupliqués et disséminés pour former un bloc de 48 bits que l'on nommera D'0 .

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

OU exclusif (XOR) avec la clef :

DES procède ensuite à un OU exclusif entre D'0 et la première clef k1 générée à partir de la clef K (que doivent se partager émetteur et destinataire) par l'algorithme de cadencement des clefs que nous décrirons plus bas. Nous appellerons D"0 le résultat de cette opération. [4]

Boîtes de substitution :

D"0 est découpée ensuite en 8 blocs de 6 bits, noté D"0i . Chacun de ces blocs passe par des boîtes de substitution(S-boxes), notées généralement Si .

Les premier et dernier bits de chaque D0i déterminent la ligne de la fonction de substitution, les autres bits déterminent la colonne. Grâce à cela la fonction de substitution « choisit » une valeur codée sur 4 bits (de 0 à 15).

Voici la première boîte de substitution :

S_1

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Soit D0i égal à 010101, les premiers et derniers bits donnent 01, c'est-à-dire 1 en binaire. Les bits autres bits donnent 1010, soit 10 en binaire. Le résultat de la fonction de substitution est donc la valeur située à la ligne num 1, dans la colonne num 10. Il s'agit de la valeur 6, soit 0110 en binaire. Chacun des 8 blocs de 6 bits est passé dans la boîte de substitution correspondante. Voici les autres S-Boxes :

S_2

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_3

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	5	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S_4

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S_5

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S_6

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S_7

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S_8

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

On obtient donc en sortie 8 blocs de 4 bits. Ces bits sont regroupés pour former un bloc de 32 bits. [4]

Permutation :

Le bloc de 32 bits subit une permutation dont voici la table :

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

OU exclusif :

Le bloc de 32 bits ainsi obtenu est soumis à un OU exclusif avec le G0 de départ pour donner D1 et le D0 initial donne G1.

L'ensemble de ces étapes est itérée seize fois.

Transposition initiale inverse

Au bout des seize itérations, les deux blocs G16 et D16 sont « recollés » pour reformer un seul bloc de 64 bits puis subit la transposition initiale inverse selon l'arrangement du tableau ci-contre.

On obtient alors le bloc initial chiffré.

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Reconstruction du message chiffré

Tous les blocs sont collés bout à bout pour obtenir le message chiffré.

Algorithme de cadencement des clefs

Nous allons décrire l'algorithme qui permet de générer à partir d'une clef de 64 bits, 8 clefs diversifiées de 48 bits chacune servant dans l'algorithme du DES.

De prime abord les clefs de parité sont éliminées pour obtenir une clef de 56 bits.

Ce bloc subit une permutation puis est découpée en deux pour obtenir 2 blocs de 28 bits décrits par les matrices ci-dessous :

40	8	48	16	56	24	64
39	7	47	15	55	23	63
38	6	46	14	54	22	62
37	5	45	13	53	21	61

40	8	48	16	56	24	64
39	7	47	15	55	23	63
38	6	46	14	54	22	62
37	5	45	13	53	21	61

Ces deux blocs subissent une rotation à gauche, c'est-à-dire que les bits en seconde position prennent la première position, ceux en troisième position la seconde, celle en première position la dernière...

14	17	11	24	1	5	3	28	15	6	21	10
13	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	57	45
44	49	39	56	34	53	46	42	50	36	29	32

Les deux blocs sont regroupés pour faire un bloc de 56 bits qui passe par une permutation fournissant un bloc de 48 bits représentant la clef ki. : Des itérations de l'algorithme permettent de donner les 16 clefs utilisées dans l'algorithme du DES. [4]

1.3.2 Cryptosysteme à cle asymetrique :

Le principe de base de la cryptographie asymétrique (à clé publique) est d'utiliser une paire de clés secrètes. Dans de tels crypto-systèmes, le chiffrement est effectué avec une clé publique et le déchiffrement avec sa paire clé privée. La clé de chiffrement (publique) est différente de la clé de déchiffrement (privé), mais ils sont fortement liés.

Caractéristiques :

- Une clé publique PK (symbolisée par la clé verticale),
- Une clé privée secrète SK (symbolisée par la clé horizontale),
- Propriété : La connaissance de PK ne permet pas de déduire SK ,
- DSK(EPK(M)) = M,
- L'algorithme de cryptographie asymétrique le plus connu est le RSA,
- Le principe de ce genre d'algorithme est qu'il s'agit d'une fonction unidirectionnelle à trappe. Une telle fonction à la particularité d'être facile à calculer dans un sens, mais dificile voire impossible dans le sens inverse. La seule manière de pouvoir réaliser le calcul inverse est de connaître une trappe. Une trappe pourrait par exemple être une faille dans le générateur de clés. Cette faille peut être soit intentionnelle de la part du concepteur (défenition stricte d'une trappe) ou accidentelle.
- Les algorithmes se basent sur des concepts mathématiques tels que l'exponentiation de grands nombres premiers (RSA), le problème des logarithmes discrets (ElGamal), ou encore le problème du sac à dos (Merkle-Hellman).
- La taille des clés s'étend de 512 bits à 2048 bits en standard. Dans le cas du RSA, une clé de 512 bits n'est plus sûre au sens "militaire" du terme, mais est toujours utilisable de particulier àparticulier.
- Au niveau des performances, le chiffrement par voie asymétrique est environ 1000 fois plus lent que le chi ?rement symétrique.

- Cependant, à l'inverse du chiffrement symétrique où le nombre de clés est le problème majeur, ici, seules n paires sont nécessaires. En effet, chaque utilisateur possède une paire (SK , PK) et tous les transferts de message ont lieu avec ces clés.
- La distribution des clés est grandement facilitée car l'échange de clés secrètes n'est plus nécessaire. Chaque utilisateur2 conserve sa clé secrète sans jamais la divulguer. Seule la clé publique devra être distribuée. [4]

FIGURE 1.6 – Modele de cryptage asymetrique .

1.3.3 RSA :

L'algorithme le plus célèbre d'algorithme à clef publique a été inventé en 1977 par Ron Rivest, Adi Shamir et Len Adleman, à la suite de la publication de l'idée d'une cryptographie à clef publique par Diffie et Hellman. Il fut appelé RSA, des initiales de ces inventeurs.
RSA est basé sur la difficulté de factoriser un grand nombre en produit de deux grands facteurs premiers. L'algorithme fonctionne de la manière suivante :
Imaginons que Bob souhaite recevoir d'Alice des messages en utilisant RSA.
1. génération des clefs :
a. p et q, deux grands nombres premiers sont générés au hasard grâce à un algorithme de test de primalité probabiliste, avec n = pq.
b. Un nombre entier e premier avec (p-1)(q-1) est choisi. Deux nombres sont premiers entre eux s'ils n'ont pas d'autre facteur commun que 1.
c. L'entier d est l'entier de l'intervalle [2, (p-1)(q-1)[tel que ed soit congrue à 1 modulo (p-1)(q-1), c'est-à-dire tel que ed-1 soit un multiple de (p-1)(q-1).
2. distribution des clefs : le couple (n, e) constitue la clef publique de Bob. Il la rend disponible à Alice en lui envoyant ou en la mettant dans un annuaire. Le couple(n, d)

constitue quand à lui sa clef privée.

3. chiffrement du message : Pour crypter le message Alice représente le message sous la forme d'un ou plusieurs entiers M compris entre 0 et n-1. Elle calcule C= Me mod n grâce à la clef publique (n, e) de Bob et envoie C à Bob.

4. déchiffrement du message : Bob reçoit C et calcule grâce à sa clef privée Cd mod n. Il obtient ainsi le message initial M.

Exemple :

Bob choisit p = 17 et q = 19, n = p x q = 323 et e = 5.

Sa clef privée est alors d=173 car 173 x 5 = 1 (mod (16 x 18))

Supposons qu'Alice veuille lui envoyer le message « BONJOUR » en se servant du tableau suivant pour transformer les lettres en nombre :

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
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Cela donne :

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

Après avoir chiffré en remplaçant chaque nombre b par (be mod n) on obtient :

32	2	29	193	2	89	18

Qu'Alice envoie à Bob.

Bob réalise pour chaque nombre b du message bd mod n pour trouver :

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

qui est bien le message initial.
RSA est basé sur la difficulté de factoriser n. En effet celui qui arrive à factoriser n peut retrouver facilement la clef secrète de Bob connaissant seulement sa clef publique. C'est pourquoi dans la pratique la taille des clefs est au minimum de 512 bits. [4]

1.4 les principes de base d'ADN

L'information est la plus puissante et la plus recherchée temps et c'est pourquoi il a besoin de protection. Afin de protéger information, l'écriture secrète a été utilisée depuis l'Antiquité et est utilisé aussi bien de nos jours. Bien connu et largement utilisé les techniques qui mettent en œuvre l'écriture secrète sont la cryptographie et la stéganographie. Ces deux sciences manipulent informations afin de chiffrer ou de cacher son existence.

Pourquoi un tel intérêt pour la cryptographie ADN ? C'est un nouveau champ cryptographique né basé sur la recherche de l'ADN l'informatique. Merci à Adleman la fondation pour la un nouveau champ de recherche en bio-informatique a été mis en place. Son expérience était de résoudre Hamiltonian Path problème en utilisant unique molécules d'ADN échouées et une série de procédures adaptées de la biologie moléculaire. La cryptographie à base d'ADN était introduit par qui a donné des procédures pour deux ADN onetime-pad schémas de chiffrement : substitution et XOR.

Notre papier étudie une variété de bioinformatique méthodes et propose deux algorithmes différents pour cryptage et décryptage des données stockées en réel ou artificiel Forme numérique de l'ADN. Dans les sections 2 et 3 nous présentons description des algorithmes cryptographiques d'ADN.

Mais avant d'entamer le sujet il est primordial de définir la molécule d'ADN d'un côté purement biologique en parcourant ses structures physique et chimique ainsi que ses caractéristiques. Ensuite les différentes techniques de la biologie moléculaire qui permettent la manipulation de l'ADN et le calcul à l'ADN.

1.5 Comprendre L'ADN :

Que signifie ADN ?
Définition simple : L'acide désoxyribonucléique ou ADN est un composé organique dont les molécules contiennent les instructions génétiques qui coordonnent le développement et le fonctionnement de tous les êtres vivants et quelques virus, et qui transmettent les

caractéristiques héréditaires de chaque être vivant.
ADN est le sigle de acide désoxyribonucléique, un acide nucléique composé de désoxyribose, de phosphate, d'adénine, de cytosine, de guanine et de thymine. L'ADN contient les instructions génétiques utilisées dans le développement et le fonctionnement de tous les organismes vivants et de certains virus, et qui est responsable de sa transmission héréditaire.

Cette macromolécule constitue le support des informations génétiques de tous les êtres vivants exceptés les virus à ARN. Elle est formée d'une double chaîne hélicoïdale de désoxyribonucléotides, chaque chaîne ou brin étant complémentaire de l'autre.

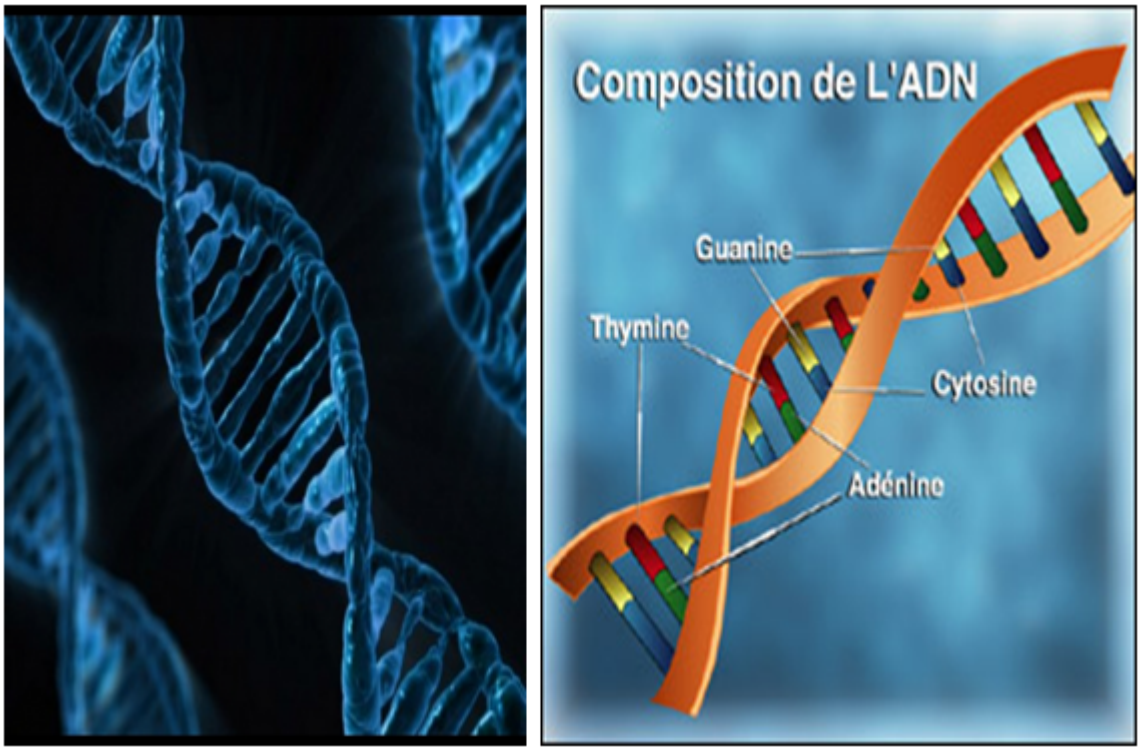

FIGURE 1.7 – ADN : vue globale.

Structure et principe :
La molécule ADN est constituée d'un grand nombre de nucléotides (environ 3,3 milliards de paires de nucléotides) qui vont permettre la création d'acides aminés, composants des protéines. On compte 4 sortes de nucléotides (appelés aussi bases) symbolisés par les lettres A, C, G et T respectivement nommés Adénine, Cytosine, Guanine et Thymine. Un nucléotide est une structure chimique composée d'une base azotée, d'un phosphate et d'un sucre.

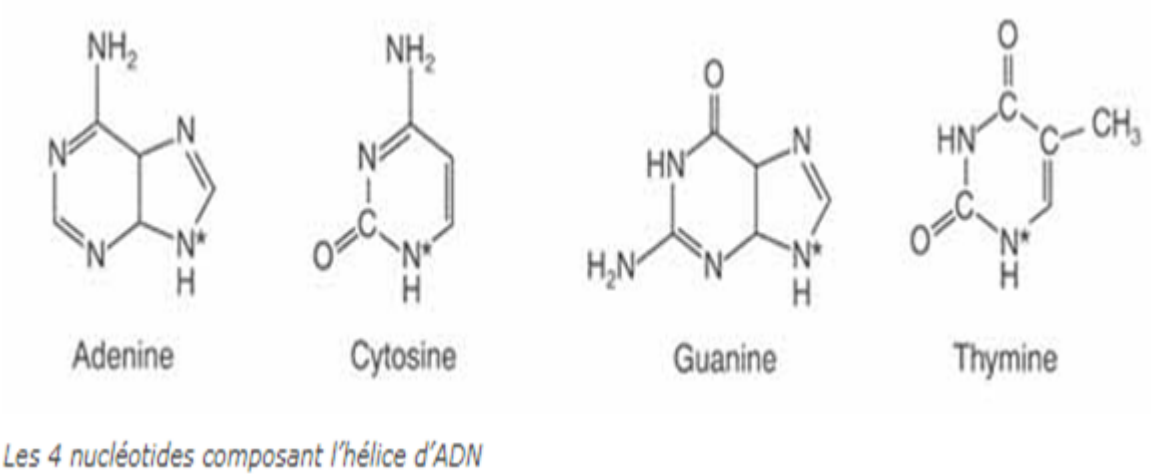

FIGURE 1.8 – Les 4 nucléotides composant l'hélice d'ADN.

Ces quatre nucléotides suffisent pour coder la fabrication de 20 acides aminés présents dans notre corps. Des chaines de 100 à 1000 acides aminés vont constituer les protéines qui sont les "hommes à tout faire" de notre corps. Les protéines vont en effet permettre le bon fonctionnement de nos organes, de nos yeux, nos muscles et de toutes les fonctions vitales de notre organisme. Les milliers de protéines présentes dans notre corps gèrent toute notre activité biologique en passant par la création de molécules ou par la transmission d'informations. Les protéines qui ont une activité de catalyseur sont appelées des enzymes. Ainsi la protéine qui permet de copier une molécule ADN en deux molécules ADN identiques est une enzyme appelée ADN polymérase.

1.6 Définition de quelles que notions :

Qu'est ce qu'un Chromosome ? Un chromosome est une structure cellulaire microscopique représentant le support physique des gènes et de l'information génétique, toujours constituée d'ADN, et souvent de protéines. Les chromosomes existent dans les cellules de tous les êtres vivants, en nombre variable, spécifique à chaque espèce.

Fonction :

Les chromosomes constituent le matériel héréditaire des cellules. Supports de l'information génétique, ils portent les gènes qui sont transmis de génération en génération.

Chaque gène occupe un emplacement précis sur un chromosome donné : c'est son locus. Un même gène sera toujours situé sur un même locus pour tous les individus d'une espèce donnée.

Un seul chromosome porterait en moyenne 3000 gènes.Ces séquences codantes ne semblent pourtant occuper que 30% des chromosomes. Les séquences restantes correspondent à des portions responsables de la régulation de l'expression des gènes, ainsi qu'à des zones de

fonction inconnue.

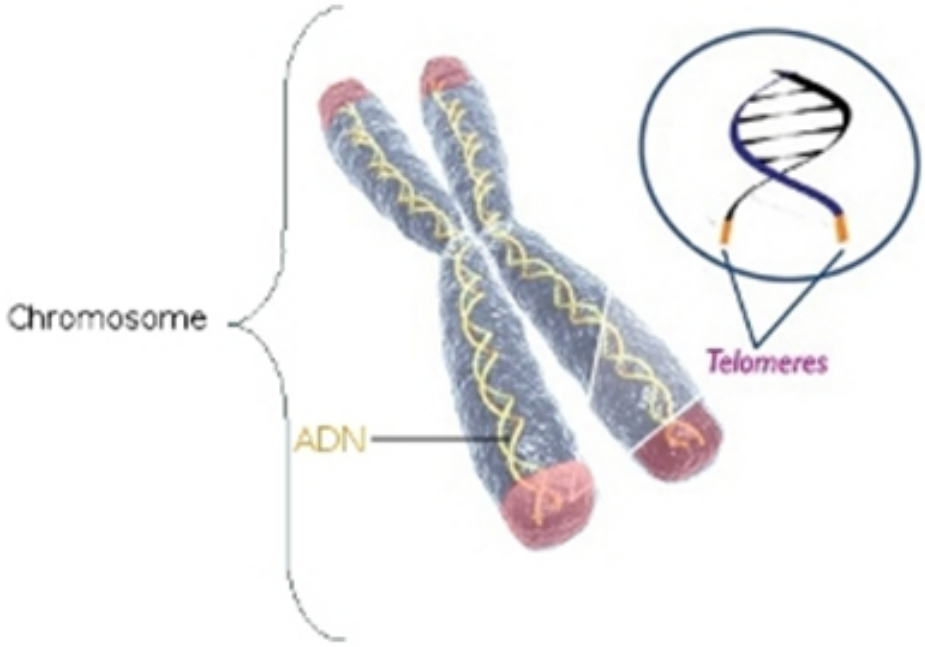

FIGURE 1.9 – Structure d'un chromosome.

1.6.1 Les bases azotées :

Une base azotée est aussi appelée base nucléique ou nucléobase. Une base azotée qualifie un corps hétérocyclique azoté, un composé organique possédant des propriétés basiques. Dans les cellules, les bases azotées sont constitutives des acides nucléiques.
c'est l'élément porteur de l'information des nucléotides. L'ADN est constitué des 4 bases suivantes : A = adénine ; G = guanine ; C = cytosine ; T = thymine.
Une reformulation donne : l'ADN contient deux bases puriques, l'adénine et la guanine, et deux bases pyrimidiques, la cytosine et la thymine ; Si l'on assimile la molécule d'ADN à une échelle, les bases azotées en constituent les barreaux. Les liaisons complémentaires sont réalisées par un nombre différent de liaisons hydrogène : 2 entre adénine et thymine, 3 entre cytosine et guanine, ce qui détermine une différence dans la force de ces liaisons.

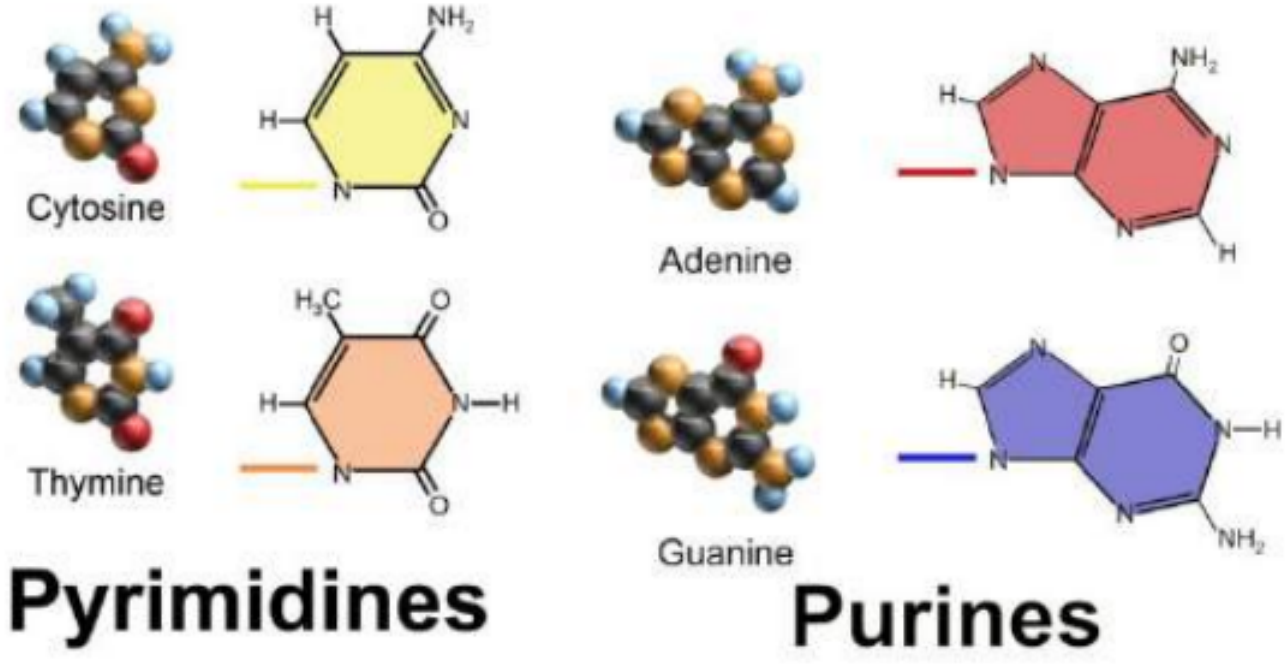

FIGURE 1.10 – Structure Chimique des bases azotées .

1.6.2 Le nucléotide :

Un nucléotide est une molécule formée d'un nucléoside lié à un phosphate, c'est-à-dire un nucléoside monophosphate. Les acides nucléiques sont des polynucléotides (polymères de nucléotides)

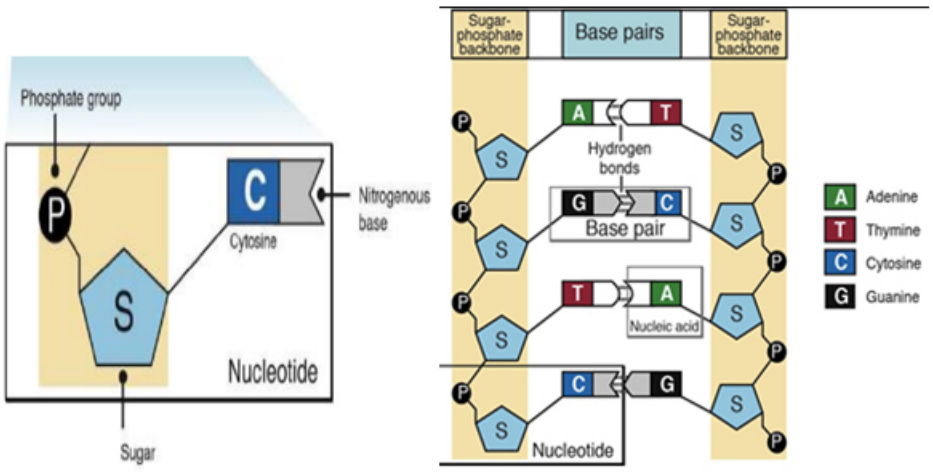

FIGURE 1.11 – Structure de Nucléotide.

1.6.3 Le nucléoside :

Un nucléoside est l'ensemble d'une base azotée, d'un sucre. En d'autre termes, c'est un nucléotide sans groupe de phosphate.

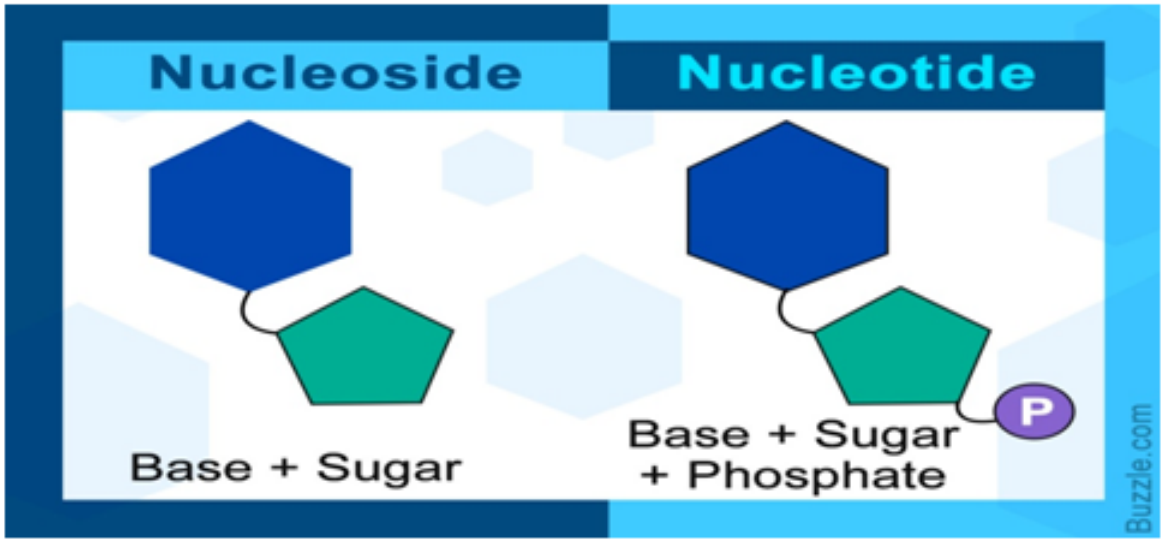

FIGURE 1.12 – Nucléoside vs Nucleotide .

1.6.4 Le brin d'ADN :

L'ADN est composé de deux brins se faisant face, et formant une double hélice. Ceci est possible car les nucléotides trouvés dans un brin possèdent des nucléotides complémentaires avec lesquels ils peuvent interagir.En face d'une adénine, on trouve toujours une thymine ; en face d'une cytosine, on trouve toujours une guanine. Deux brins d'une double hélice sont donc complémentaires. Les extrémités des brins portent un numéro : une extrémité est 3' et l'autre 5'. On dit que la double hélice d'ADN est assemblée de façon antiparallèle, c'est-à-dire assemblée « tête bêche » : l'extrémité 3' d'un brin faisant face à l'extrémité 5' du brin complémentaire.

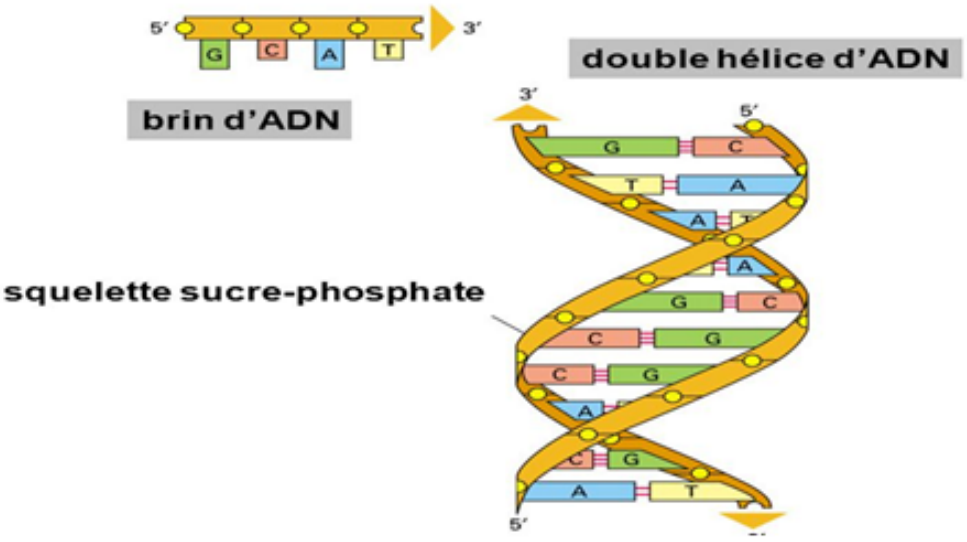

FIGURE 1.13 – Structure d'un brin d'ADN .

1.7 Conclusion

Nous avons vu un panel de méthodes de chiffrement de l'antiquité à nos jours, les attaques existantes sur les cryptosystèmes actuels les plus utilisées et les moyens inventés pour s'assurer de l'intégrité, de l'authentification de l'expéditeur et du destinataire d'un message.

Ainsi, la cryptographie est une science en perpétuelle évolution, la cryptanalyse aidant à trouver les failles d'un système pour toujours avancer. Cette évolution est importante car la cryptographie joue un grand rôle dans la sécurité internationale, tout étant aujourd'hui informatisé.

Pourtant, même si la cryptanalyse permet de faire avancer la cryptographie avec des méthodes de chiffrement et une technologie toujours plus poussées, elle représente aussi un danger à l'échelle internationale. En effet, qu'adviendrait-il demain si un mathématicien découvrait une vérité mathématique permettant de casser les algorithmes RSA et ElGamal par exemple ?

Toute la sécurité informatique serait remise en question et ce que nous connaissons aujourd'hui tels que les sites de vente en ligne basées sur ces algorithmes ne fonctionneraient plus. Par conséquent, c'est non seulement la sécurité internationale qui serait touchée, mais aussi toute une économie.

C'est pourquoi tout est mis en œuvre pour assurer la sécurité de demain avec des perspectives telle que la cryptographie quantique, théoriquement incassable puisqu'elle serait une technique similaire au chiffre de Vernam (cryptosystème par flots) où la clé est aussi longue que le message. [5]

2

Etat de l'art sur la cryptographie ADN

Contents

2.1 Introduction : 36

2.2 ADN informatique 36

2.3 ADN Cryptographie : 37

2.3.1 Réaction de polymérisation en chaîne (RPC) 41

2.3.2 Bimoléculaire Design cryptographique basé sur l'ADN 41

2.4 Substitution : 42

2.4.1 Cartographie XOR 42

2.4.2 Système cryptographique clé symétrique en utilisant l'ADN . . 42

2.4.3 Système cryptographique clé asymétrique en utilisant l'ADN . 42

2.4.4 ADN stéganographie 43

2.4.5 Méthode de cryptographie Pseudo ADN 43

2.4.6 G. Puce à ADN 44

2.4.7 Chaotique de codage 44

2.5 Cryptage d'Images 44

2.5.1 revue de la littérature 45

2.6 Conclusion 48

2.1 Introduction :

La cryptographie ADN est une nouvelle branche scientifique large, qui comprend une variété de domaines scientifiques. La sécurité de l'information (cryptographie, stéganographie, gestion de clés), la biologie moléculaire, la bio-informatique, le calcul biomoléculaire. C'est un nouveau et prometteur domaine de la sécurité de l'information. Elle combine les solutions classiques en cryptographie avec la résistance du matériau génétique. L'ADN biologique peut être utilisé dans la stéganographie et cryptographie comme matériau de stockage. Le calcul moléculaire peut être effectué avec les structures d'ADN biologiques et ensuite appliqué sur les chiffres classiques. Plusieurs projets de séquençage de génome offrent la possibilité d'exploiter les bases de données d'ADN numériques pour des fins cryptographique.

Ce chapitre se concentre sur la revue de la littérature de la cryptographie de l'ADN dans l'ordre chronologique. En étudiant les données par le biais de nombreuses sources, nous travaillons versez l'avenir pour améliorer les performances de la cryptographie de l'ADN dans le domaine de la sécurité.

2.2 ADN informatique

En 1994, Adleman [**1**] a posé la fondation d'informatique d'ADN en donnant des solutions des problèmes combinatoires en utilisant le calcul moléculaire, dont l'un est le problème du 'chemin Hamiltonien. Il a résolu l'instance de graphique contenant sept sommets en l'encodant dans la forme moléculaire en utilisant un algorithme, puis les opérations de calcul ont été effectuées à l'aide de certaines enzymes standard [13]. Cela a été résolu par la méthode de la force brute .

En 1995, Lipton [15] a étendu le travail d'Adleman en résolvant un autre problème NP-complet appelé "satisfaction" en utilisant des molécules d'ADN dans un tube à essai pour coder le graphique pour des nombres à 2 bits.

En 1996, Dan Boneh et autres. [6] ont appliqué les approches de l'informatique de l'ADN utilisées par Adleman et Lipton, afin de casser l'un des algorithmes de clés symétriques utilisés à des fins cryptographiques connu sous le nom de DES (Data Encryption Standard). Ils ont effectué des opérations biologiques sur les brins d'ADN dans un tube à essai, tels que l'extractionla polymérisation par ADN polymérase, l'amplification par PCR et effectuer des opérations sur les brins d'ADN qui ont le codage des chaînes bi-

naires. Ensuite, l'attaque DES est planifiée en générantPuis DES attaque est prévueen générant le DES-1 de solution, en raison de laquelle la clé peut être facilement deviné à partir du texte chiffré, et de mieux évaluer le DES circuit, table de recherche et de portes XOR. À l'aide de leur approche moléculaire, ils ont cassé DES en seulement 4 mois.

En 1997, Qi Ouyang et autre. [21] appliqué les approches de la théorie moléculaire de l'ADN afin de générer la solution pour le problème de la clique maximale, qui est un autre problème NP-complet. Montre ainsi l'efficacité de l'ADN : Versez résoudre dur-problèmes et vaste parallélisme inhérent à ce qui rend les opérations rapides.

2.3 ADN Cryptographie :

En 2003, Jie Chen [8] a présenté l'approche cryptographique ADN basé sur la théorie moléculaire, one-time-pad et effectué de cryptage/décryptage de l'image 2D.

En 2004, Ashish Gibert et autres. [4] a posé la fondationdes bases de la cryptographie de l'ADN en utilisant de l'approche moléculaire et le concept de one-time-pad qui a un secret parfait (confidentialité), selon de Vernam et Shannon : inventeur du one-time pad. Ils ont proposé une méthode chiffrement et de déchiffrement qui repose sur une puce à ADN et one-time pad. Il est donc très difficile pour l'adversaire d'obtenirle message chiffré.

En 2005, Kazuo Tanaka et autre. [16] a proposé l'approche cryptographique ADN basé sur la clé publique (one way). Dans cette approche, qu'ils ont clairement expliquées sur la formation des clés publiques à l'aide de solides soutient mélange pour PKA et ODN mélange pour PKB. Après avoir généré les clés, message est encodé dans une séquence d'ADN à l'aide de l'un de la clé publique, qui est également synthétisée avec le synthétiseur d'ADN et ensuite la séquence de message codé est ligaturée avec une autre clé publique. Maintenant le résultat de la procédure précédente est transmis au processus d'immobilisation et ensuite pour l'amplification PCR, où l'amplification est faite avec l'aide de la séquence secrète, afin de décoder la séquence d'ADN codée.

En 2006, Sherif T. Amin et al. [[23] a proposé l'approche cryptographique d'ADN basée sur la clé symétrique, où les séquences clés sont obtenues à partir de la base de données génétiques et restantes aux deux extrémités (expéditeur et récepteur). Message / texte en clair est d'abord convertir en format binaire. Une fois que la substitution a été effectuée et que le message est sous la forme d'une séquence d'ADN, Ensuite, nous choisissons le quadruple de la séquence que nous avons obtenue et nous l'associons à la séquence des-

clés. Lorsque la correspondance se produit, nous notons la position. Comme ceci, toutes les positions aléatoires pour chaque caractère dans le texte en clair sont obtenues et le fichier qui contient ces positions est notre texte chiffré qui est envoyé au récepteur, puis le déchiffrement est exécuté dans l'ordre inverse.

En 2008, Anil Verma et al., [2, 3] a proposé un nouveau paradigme pour l'acheminement sécurisé dans les réseaux mobiles ad hoc (Manet) qui utilise l'approche de la cryptographie de Pseudo ADN afin d'assurer les réseaux ad hoc. Adhoc network est un réseau sans fil qui n'a pas d'infrastructure fixe et où chaque nœud agissent comme un hôte et routeur et il n'y a aucune autorité centralisée, ce qui les rend vulnérables aux attaques de sécurité présents dans les réseaux. Approche de cryptographie de Pseudo ADN qu'ils ont utilisé est basé sur le dogme central de biologie moléculaire. Notion de comment les messages sont stockés dans l'ADN et puis transfèrent à l'ARNm (transcription), puis aux protéines (traduction) qui est notre texte chiffré. Texte chiffré est envoyé à travers le canal sécurisé vers le destinataire et une clé symétrique avec one-time pad est utilisée aux extrémités (chiffrement et le déchiffrement)

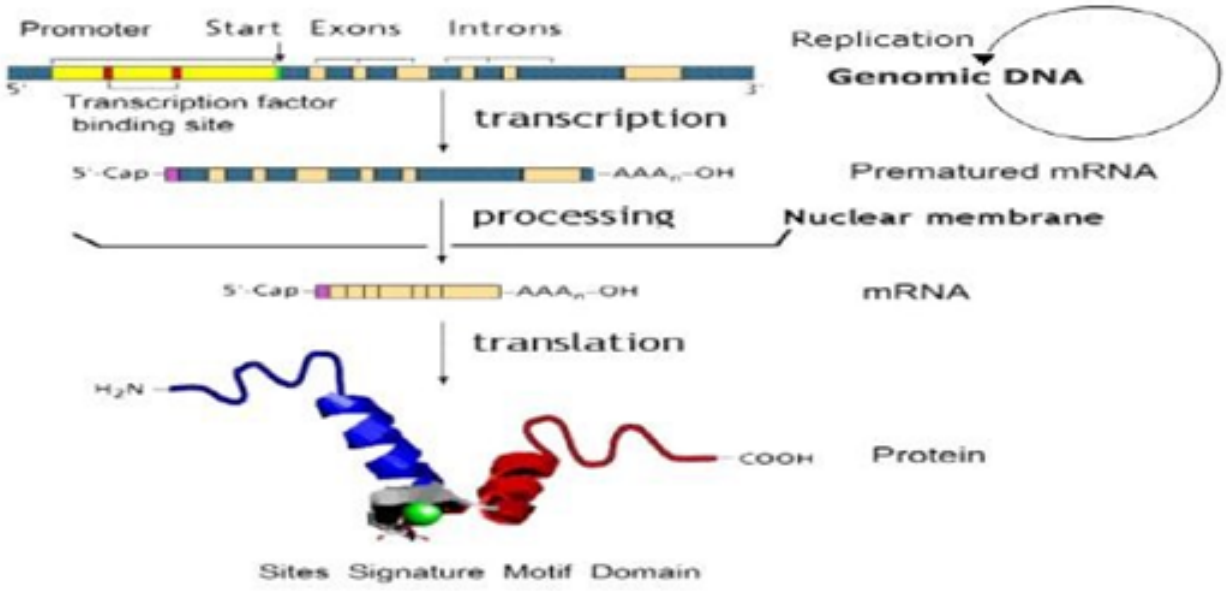

FIGURE 2.1 – Central dogma of DNA .

En 2008, Guangzhao Cui et autres . [10] ont proposé la technique de cryptage à clé publique qui utilise la synthèse d'ADN, le codage numérique de l'ADN et l'amplification par PCR pour assurer la sécurité pendant la communication. Ce schéma de chiffrement a une

grande force confidentielle.

En 2010, Xuejia Lai et autres. [17] a proposé un ADN crypto système à clé publique qui est basé sur des puces à ADN/la technologie de la puce dans lequel la puce à ADN est fabriqué avec des sondes. Un ensemble de sondes sont utilisées pour les processus de chiffrement et un autre pour le processus de déchiffrement. Dans le processus de génération de clé existant sondes sont sélectionnés en tant que clés de la National Centre d'Ingénierie pour la Biopuce à sanghai. Certains signaux sont également sélectionnés qui sont utilisés pour la mesure de l'intensité de sondes après hybridation résultat. Si les sondes ont une intensité supérieure à la valeur fixe, il est noté que la sonde 1 et si les sondes ont une intensité moindre que certaines valeur fixe, il est noté que la sonde 0.Chaque clé de chiffrement se compose d'un nombre égal de la sonde de 0 et de la sonde 1. Pour les processus de chiffrement deux clés sont utilisées PKs (expéditeur) et PKr (récepteur) pour chiffrer le texte en clair. Tout d'abord le texte en clair est converti en son code ASCII puis son équivalent en code binaire. Ces codes binaires sont disposés en forme de matrice. Pour 0 dans la matrice de la sonde 0 est sélectionné à partir de la clé de chiffrement et repéré sur la puce à ADN, de 1 dans la matrice de la sonde 1 est sélectionné à partir de la clé de chiffrement et repéré sur la puce à ADN. La puce fabriquée selon le concept ci-dessus est désigné comme un cryptogramme. Récepteur s'hybride texte chiffré avec la clé de déchiffrement Sk. Tache lumineuse dans la puce indiquer l'intensité élevée de l'hybridation et notée chiffre binaire 1 et tache sombre indique le chiffre 0.

En 2011, Deepak Kumar et Shailendra Singh [11] ont proposé un nouveau secret de données techniques basées sur les séquences d'ADN d'écriture. Ils ont expliqué cet algorithme en utilisant un exemple simple de « HELLO » comme un texte clair et génèrent une clé d'one-time pad ADNsb de 350 bits qui est 70 fois plus longue que le texte brut et effectuent le chiffrement et le déchiffrement sur le texte en clair à l'aide de chiffrement à clé symétrique. Donc, pour trouver la clé exacte, l'adversairedoit rechercher parmi 4310 ADNsb différentes cordes, qui est presque impossible.

En 2012, Sabari Pramanik et Sanjit Kumar Setua [22] ont proposé une technique nouvelle de la cryptographie des ADN parallèle à l'aide de la structure moléculaire de l'ADN et de la technique d'hybridation qui certainement réduire au minimum l'exigence du délai. Ils ont expliqué comment message est d'échanger en toute sécurité entre l'expéditeur et le récepteur avec un exemple.

En 2012, HH Zhang et al., [25] a proposé une cryptographie ADN basée sur l'as-

semblage des fragments de DNA. Dans leur algorithme, elles ont mentionné clairement comment l'expéditeur convertit le texte en clair en séquence binaire et puis dans la longue chaîne de l'ADN, qui est plus fragmenté en petites chaînes d'ADN. Clé de l'implantation à chaîne courte se déroule dans les fragments d'et vers l'avant au récepteur comme un texte crypté puis récepteur déchiffre et commence le fragment remonté pour obtenir le texte en clair.

En 2013, Olga Tornea et Monica E. Borda [20, 7] ont proposé un chiffrement basé sur l'ADN basé sur l'indexation de l'ADN. Ils prennent la séquence d'ADN aléatoire de la base de données génétique et l'utilisent comme une touche de touche unique, qui est envoyée au récepteur par un canal de communication sécurisé. Les mécanismes de chiffrement ont lieu en convertissant le texte en clair en son code ASCII, puis le convertit en format binaire qui est converti en la séquence d'ADN (A, C, G et T). Maintenant, la séquence d'ADN formée est la recherche dans la séquence de touches et écrit les numéros d'index. Le tableau des nombres entiers obtenus est notre texte chiffré qui est déchiffré par le récepteur en utilisant uniquement la clé et le pointeur d'index.

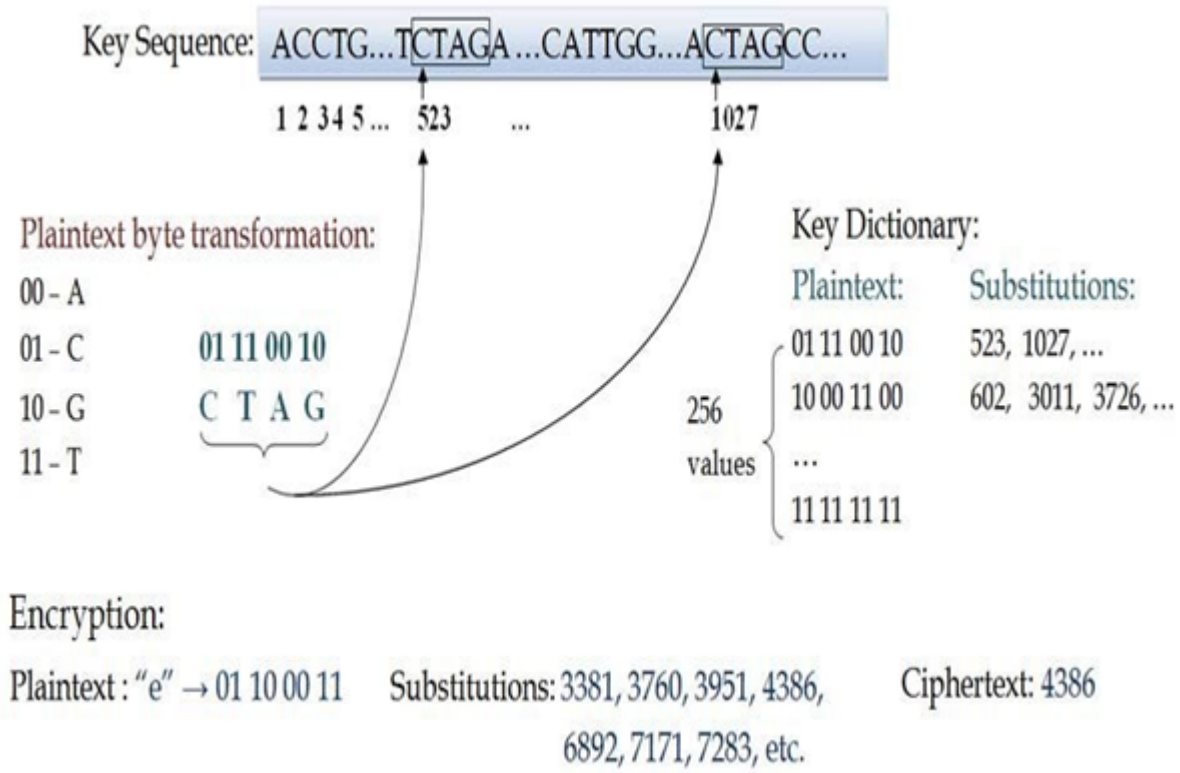

FIGURE 2.2 – DNA Indexing .

Il existe différentes Techniques de cryptographie l'ADN qui a été développé Certaines des techniques d'ADN qui sont largement utilisés et mise au point récemment sont indiquées :

2.3.1 Réaction de polymérisation en chaîne (RPC)

La RPC (Polymerase Chain Reaction en anglais) est une technique moléculaire d'amplification génique in vitro qui permet de produire d'importantes quantités de séquences d'ADN ou ARN à partir d'une faible quantité d'acides nucléiques.

C'est une méthode récente, remontant au milieu des années 1980, et découverte par Kary Mullis. Cette découverte lui aura valu le prix Nobel de chimie en 1993. Pour un segment d'ADN spécifique et peu abondant (soit car l'échantillon est trop petit, trop abîmé, soit parce que l'ADN d'un composant est mélangé à d'autres ADN), la PCR va permettre d'aller chercher la séquence d'un gène voulu, fraction infime de l'ADN total, et de la dupliquer des millions de fois, de manière exponentielle, suivant un principe de dénaturation des brins d'ADN, hybridation d'amorces spécifiques et de synthèse (de reconstitution des brins complémentaires par la polymérase). Une fois en quantité suffisante, la séquence d'ADN visée pourra être étudiée.

2.3.2 Bimoléculaire Design cryptographique basé sur l'ADN

Le système cryptographique bimoléculaire brouille les données en code ADN en utilisant des séquences oligonucléotidiques [17]. Il utilise la technique de cryptographie One Time Pad (OTP) qui repose sur le principe de l'incassable [13]. L'expérience réelle de schéma cryptographique suit OTP qui ont une limitation dans la transmission sur les médias électroniques de convention en raison de la taille de l'OTP. Les brins d'ADN sont très soignés car les supports de stockage et une petite quantité d'ADN suffisent pour une grande quantité d'OTP [9]. Nous utilisons le cryptage One Pad, qui utilise un livre de code pour brouiller la partie du message en clair. Message texte. Le livre de codes utilisé ici est un livre de codes aléatoires, c'est-à-dire qu'un code secret est utilisé une seule fois pour le chiffrement et le déchiffrement, pas de manière répétée. L'OTP du message en clair est distribué à l'avance à l'expéditeur et au destinataire [19]

Le chiffrement cryptographique bimoléculaire ayant après régimes basé sur l'ADN.

2.4 Substitution :

Dans la méthode de substitution que la cartographie sage paire est réalisée entre les bibliothèques de blocs différents, qui sont générés au hasard. Ici le processus de cryptage est aléatoire et réversible, laquelle est convertie en texte brut pour chiper brins et des volets en clair sont supprimés. Par la suite la substitution de l'ADN utilise longs tampons d'ADN qui contiennent diverses parties et chaque partie d'un mot de chiffrement suivi d'un mot en clair. Ici le mot chiffrement est collé au mot en clair sur Word pairs forme. Il sert également de site d'hybridation pour la liaison d'amorce. Word-paire ici établis aux brins d'ADN est utilisées comme une table de choix dans le brouillage de texte brut à texte chiffré.

2.4.1 Cartographie XOR

Ce mappage XOR utilise le calcul moléculaire et les index, les chaînes clés aléatoires. Il mappe les brins d'ADN dans aléatoire réversible qui, en clair est brouillé à brins de chiffrement et volets en clair sont supprimés.

2.4.2 Système cryptographique clé symétrique en utilisant l'ADN

Le système symétrique utilise la même clé pour le processus de chiffrement et de déchiffrement [23]. Ceux-ci sont extrêmement rapide et largement utilisés pour le processus sur l'énorme quantité de données.
C'est d'avoir une menace d'attaque lors de la transmission sur les médias de communication, par exemple l'homme au milieu. Ils sont accessibles par l'extérieur. Dans cette méthode le texte brut est converti en séquence d'ADN dans lequel les brins d'ADN sont utilisées comme clé unique pour le chiffrement et le déchiffrement [12].

2.4.3 Système cryptographique clé asymétrique en utilisant l'ADN

Le système asymétrique utilise deux clés différentes pour le processus de chiffrement et de déchiffrement [23]
. Nous pouvons aussi être appelés il comme la cryptographie à clé publique-ADN. Ceux-ci sont extrêmement rapidement et largement utilisés pour le processus sur une quantité énorme de données parce qu'il est bien sûr comme comparer le processus de chiffrement à clé symétrique. Il ne peut pas être facilement accessible par les utilisateurs externes. Dans cette méthode le texte brut est converti en séquence d'ADN dans lequel les brins d'ADN sont utilisées comme clé unique pour le chiffrement et le déchiffrement [14].

2.4.4 ADN stéganographie

La stéganographie est la technique de cacher un message secret en dehors de l'expéditeur et le récepteur. Le supplément de la cryptographie classique d'ADN peut affirmer ADN stéganographie. La stéganographie ADN possède une contrainte que cette méthode est ouverte à une attaque [17].
Dans ce processus, le message d'origine est couvert par les échantillons d'ADN d'une taille de micro points.
Dans le processus de chiffrement ADN stéganographie, le message d'origine est converti en brins d'ADN et les brins sont combinés avec les autres brins d'ADN pour générer un brin d'ADN mannequin de taille et de longueur égale. Cependant le cryptage n'est pas d'une importance primordiale dans la stéganographie, c'est pourquoi un chiffrement par substitution simple peut être encoder au caractère en triolets de l'ADN. Décryptage de traiter la clé secrète, les brins d'ADN factices sont amplifiés en appliquant des processus PCR. Le message de chiffrement sera être converti en message d'origine que par le destinataire qui connaît l'amorce PCR ou la clé ou la séquence de brins PCR.

2.4.5 Méthode de cryptographie Pseudo ADN

La cryptographie Pseudo ADN est variant de cryptographie de l'ADN. Cette méthode dépend de la fonction de l'ADN non sur les brins d'ADN. Dans cette méthode, le processus de brouillage et déchiffrer repose sur la circulation de l'information génétique des organismes biologiques [15].
L'expéditeur traduire forme d'ARNm des données dans la protéine selon le tableau du code génétique. La clé sont envoyer au récepteur à un canal sécurisé.

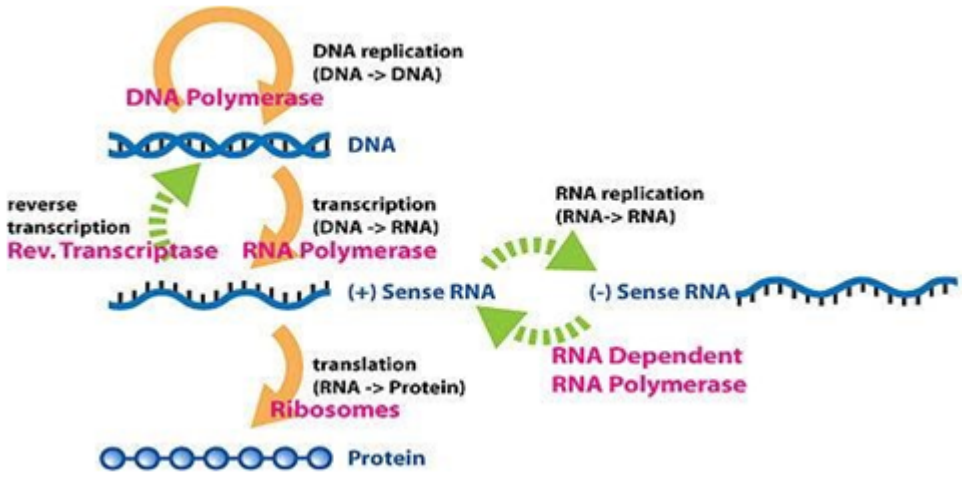

FIGURE 2.3 – DIAGRAMME DE Flux de l'information génétique .

2.4.6 G. Puce à ADN

Les Technologies Basées surTechnologie des puces à ADN utilise des micro tableaux de molécules, qui sont restreindre sur la surface solide pour l'analyse biochimique.
Les Puces à ADN sont utiles dans la manipulation de la grande quantité de données de séquençage du génome et de trouver des parallèles expression Des différents gènes [5].
Puce à ADN contenant la matrice de moles de Séquence d'ADN appelée comme sonde.
Le chiffrement et leprocessus de déchiffrement dans les Puces à ADN ne sont pas stables comme la propriété de nucléotides avec les changements climatiques ou aux alentours conditions [18]

2.4.7 Chaotique de codage

Chaos encodage est l'étude comportementale des systèmes dynamiques qui sont très dépendants de la condition initiale.
Le Chaos s'entend de l'état de trouble. Nous devons suivre les propriétés suivantes.
1. Il doit être dépend de la condition initiale.
2. Il doit être topologiquement mixte.
3. Il doit avoir dense orbites périodiques.
Cyclisme chaos est utilisé pour le codage des pixels de l'image positions et en réarrangeant les pixels de niveau de gris en utilisant l'ADN le séquençage de masquage. Lorsqu'un processus aléatoire dans un système dynamique non linéaire, il est dit d'être le chaos. Chaotiqueles systèmes sont principalement utilisés pour les systèmes dynamiques. Cette méthode est largement utilisée dans le cryptage des images. Des amorces d'ADN magasin de la codé les pixels de l'image dans la forme de la matrice [36].
Le cryptage des images se fait par Ak+1 = μ.ak. (1-ak)
Où a0 est la condition initiale, il varie entre 0 et 1. μ est le paramètre de contrôle ayant une valeur comprise entre 0,3 <μ <4[27].

2.5 Cryptage d'Images

Les techniques de cryptage d'image sont différentes des techniques de cryptage de données. Et il existe plusieurs problèmes de sécurité associés au traitement d'image numérique ettransmissions, il est donc nécessaire de maintenir l'intégrité et la confidentialité d'image. De plus, les images numériques sont comparativement moins sensibles que les données car toutseul changement dans les pixels du change pas l'image entière. En d'autres termes,

une petite modification de l'image numérique est acceptable par rapport aux données mais elle est plus sujette auxattaquants. La figure 1 montre un processus de cryptage d'image général enutilisant n'importe quelle imagealgorithme de cryptage et image cryptée résultante.

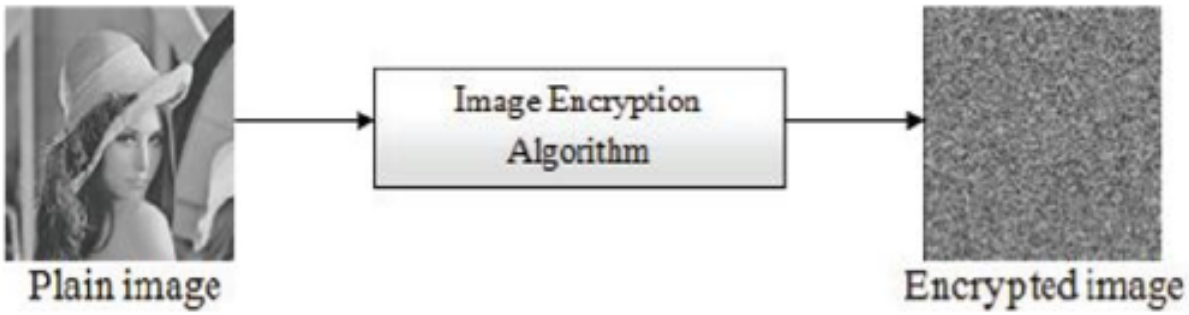

FIGURE 2.4 – cryptage d'image .

2.5.1 revue de la littérature

nouvel algorithme de cryptage Image comme un miroir et son architecture de VLSI.

Jiun-In Guo et Jui-Cheng Yen [2] ont présenté un algorithme qui a été le miroir comme. Dans cet algorithme, il y a 7 étapes. Dans le premier, 1D système chaotique est déterminé un point initial x (0) et ses séries k = 0. Ensuite, le chaoticSequence est généré par le système chaotique. Après cette séquence binaire est généré à partir de système chaotique. Et dans les 4 dernières étapes les pixels de l'image sont réorganisés à l'aide de la fonction swap selon la séquence binaire.

un nouvel algorithme de cryptage image basé sur le chaos

La méthode proposée par Tiegang Gao et Zengqiang Chen[25], utilise l'hyper-chaos pour crypter l'image. La méthode est divisée en deux parties. Dans la première partie, le brassage total des pixels de l'image a lieu. Dans la deuxième partie, l'image de brassage est cryptée à l'aide de l'hyper chaos. L'hyper chaos est utilisé pour changer les valeurs de gris des pixels de l'image. La première partie contient ensuite la transformation des lignes basée sur la carte logistique, à l'aide de laquelle les lignes de l'image simple sont mélangées. Ensuite, la transformation des colonnes a lieu, qui dépend également de la carte logistique. Les colonnes de l'image line-transformée sont alors encore plus mélangé.

Après le lieu debrassageles pixels de l'image sont dispersés de façon aléatoire et les pixels de l'image sont dispersésl'image devient cryptée mais l'histogramme de l'imagemélangée reste inchangé même que celle de l'histogramme de l'image en clair. L'image mélangée a lieu sur la base du système hyper-chaotique.

Un nouvel algorithme de cryptage d'images en couleur basé sur l'opération de séquence d'ADN et système hyper-chaotique, 2011

Présenté par Xiaopeng Wei, Ling Guo, QiangZhanga, Jianxin Zhang et ShiguoLian[4].Dans cet article, un nouvel algorithme de cryptage d'image couleur basé sur l'opération de séquence d'ADN et le système hyper- chaotique est proposé. Dans le schéma proposé, le système hyper-chaotique de Chen est utilisé pour brouiller la position des pixels. L'image couleur est convertie en trois matrices pour R, G et B qui sont ensuite transformées en matrices binaires. Ensuite, ces matrices sont codées selon la règle d'encodage de l'ADN. La séquence hyper-chaotique du chen est utilisée pour brouiller les R, G et B. Les R, G et B brouillés sont convertis en blocs et ensuite l'opération d'addition d'ADN est effectuée sur les blocs. Maintenant, les blocs sont recombinés et l'opération de décodage de l'ADN est effectuée pour obtenir les matrices binaires. Ces matrices binaires sont ensuite combinées pour obtenir l'image chiffrée. La méthode améliore la capacité à résister aux attaques différentielles en utilisant la distance de hamming pour générer les clés secrètes De plus les résultats expérimentaux et l'analyse de sécurité montrent que l'algorithme a un bon effet de cryptage. Plus grand espace clé secrète et très sensible à la clé secrète.

Schéma de cryptage et d'authentification des images, 2011

Le schéma a été proposé par Jing Qiu et ping Wang [5] La méthode présente un schéma rapide de cryptage et d'authentification d'images. Dans le schéma, un code d'authentification de message de 512 bits (MAC) de l'image simple est converti en 64 octets et ces 64 octets sont remplacés par les pixels de l'image d'une manière ou d'une autre. Les pixels remplacés sont ensuite intégrés dans l'image par une technique d'intégration de données réversible. Ensuite, l'image incorporée est masquée en utilisant la séquence pseudo-aléatoire en mode Larsen. Le MAC fournit l'authentification et fournit également un certain cryptage de l'image. Le schéma fournit le cryptage ainsi que l'authentification de l'image le MAC intégré joue un rôle important dans la détermination de l'intégrité de l'image.

Cryptographie d'images : L'approche de l'algorithme génétique, 2011

L'approche par algorithme génétique a été proposée par SandeepBhowmik et SriyankerAcharya[6]. Dans cette approche, l'algorithme génétique est une importante méthode d'intelligence artificielle qui a été appliquée pour générer une clé pour l'algorithme de cryptage. Dans ce travail on utilise une technique hybride appelée BlowGA qui est une combinaison de Blowfish et GA. Cette nouvelle approche a surpassé le résultat Blowfish et GA séparément.

Cryptage d'image par l'approche d'évolution différentielle en Fréquence

Domain Ibrahim S I Abuhaiba et Maaly A S Hassan [7] présentent une nouvelle méthode efficace pour le chiffrement d'image qui utilise la manipulation de magnitude et de phase en utilisant l'approche de l'évolution différentielle (DE). Afin de démontrer la sécurité du nouvel algorithme de cryptage d'image, l'analyse de l'espace clé, l'analyse statistique et l'analyse de la sensibilité des clés a été effectuée par ces derniers.

Un cryptage d'image basé sur des automates cellulaires élémentaires

Un nouveau schéma de chiffrement d'image symétrique basé sur des automates cellulaires élémentaires(ECA) est proposé par Jun JIN en2012 [8]. Le concept principal du régime est dérivé du étude analytique du comportement de transition d'état de longueur 8 ECA avec périodicitéConditions aux limites. Un automate cellulaire (CA) est un modèle mathématique d'un système ayant des entrées et des sorties discrètes. Il représente le séquentiel d'un certain nombre decellules interconnectées, disposées de manière régulière. Chaque cellule a un ensemble finie de valeurs possibles. Une AC s'exécute en temps discrets et la valeur d'une cellule particulière (état local) est affectée par les valeurs de cellule dans son voisinage le plus proche à l'étape précédente. Les valeurs d'une cellule dépendent également d'une fonction connue sous le nom de CA. L'élémentaire CA est le cas le plus simple, qui est un tableau linéaire de cellules, avec trois dépendances de voisinage, et l'état de chaque cellule est 0 ou 1. quand on traite des conditions limites finies de l'AC finies (pour les limites cycliques)

Un schéma de chiffrement d'image authentifié basé sur des cartes chaotiques et automates cellulaires mémoire 2013

La méthode proposée par AtiehBakhshandeh et ZibaEslami [9], permet l'authentification et le cryptage de l'image à partir de cartes chaotiques et d'automates cellulaires à mémoire linéaire (LMCA). Les automates cellulaires sont des systèmes dynamiques discrets composés d'un ensemble de N objets identiques appelés cellules. Chaque cellule peut

contenir un état 0,1. Chaque cellule est mise à jour de façon synchrone en fonction d'une fonction de transition locale en pas de temps discrets. L'état mis à jour de chaque cellule dépend de l'entrée de la fonction. L'entrée est l'état précédent d'un ensemble de cellules, y compris les cellules qui s'appellent le voisinage.

Algorithme de chiffrement et de décryptage pour l'image basée sur l'ADN

En 2013, un nouvel algorithme de cryptage d'image couleur basé sur le fonctionnement de la séquence d'ADN et le système hyper-chaotique a été proposé Dans cet article [10], le système hyper-chaotique de chen est utilisé pour brouiller la position des pixels, puis l'image couleur est convertie en trois matrices pour R, G et B qui sont transformées en matrices binaires et une opération d'addition d'ADN est effectuée.
L'analyse de sécurité montrera que l'algorithme a un bon effet de cryptage, un plus grand espace de clé secrète et une haute sensibilité à la clé secrète peut faire les deux positions change le brouillage et changer de niveau de gris brouillage en même temps.

Cryptage d'images basé sur la décomposition de plans de bits et la décomposition aléatoire

ScramblingQiudong Sun, Wenying Yan, Jiangwei Huang, WenxinMa[11] en général été conçue avec un degré de brouillage plus stable que la méthode de brouillage. méthode classique transformée d'Arnold. Dans un premier temps ils ont décomposé une image grise en plusieurs des images de bit-plane. Puis nous les avons mélangés par un algorithme de brouillage aléatoire séparément. Enfin nous avons fusionné les images de bit-plane brouillées en fonction de leurs niveaux d'origine sur bit-planes et obtenu une image cryptée. En raison de chaque bit-plane l'image est brouillée en utilisant différentes séquences aléatoires de brouillage, les bits localisés les mêmes coordonnées dans différents plans de bit sont presque pas rester sur l'original positions lorsque chaque bit-plane est brouillé séparément. Pour chaque pixel, tous ses bits de niveau de gris peuvent donc provenir de pixels situés à des positions différentes Par conséquent les niveaux de gris reconstruits de l'image sont inéluctables. C'est évident que notre méthode peut faire les deux positions d'échange de brouillage et de niveau de gris. changement de brouillage en même temps.

2.6 Conclusion

Dans ce chapitre, nous avons présenté la structure basique de la molécule d'ADN.
Beaucoup de chercheurs se sont intéressés à la capacité du calcul à l'ADN pour résoudre d'autres problèmes complexes. Le développement remarquable du calcul à l'ADN donne la naissance de la cryptographie à l'ADN et ceci en exploitant le parallélisme ainsi que la

capacité importante du stockage qu'offre cette molécule. La recherche en cryptographie à l'ADN est dans sa phase initiale et il reste beaucoup de problèmes à résoudre.

Cependant les avantages de l'ADN en stockage, parallélisme ainsi que le développement remarquable des équipements de la biologie moléculaire donnent l'espoir de voir des méthodes cryptographiques à l'ADN s'imposer comme étant des méthodes très puissantes dans les systèmes cryptographiques modernes. Et comme il se fut un temps où un ordinateur occupait une salle entière et aujourd'hui il occupe une surface de quelque centimètres carrés, il arrivera certainement un jour où la cryptographie à l'ADN pourra être pratiquée d'une manière très simple et avec des équipements plus petits et moins onéreux.

Et en attendant ce jour, plusieurs chercheurs ont préféré s'inspirer de l'ADN ou d'autres systèmes biologiques pour concevoir des méthodes cryptographiques offrant un bon niveau de sécurité.

3

Notre Contribution

Contents

3.1 Introduction 51

3.2 Contribution 51

3.2.1 Processus de chiffrement 51

3.2.2 Processus de déchiffrement 52

3.3 Conclusion 53

3.1 Introduction

Les algorithmes de chiffrement symétriques ont une grande importance dans la sécurité des systèmes informatiques, essentiellement dans la sécurisation des transferts de données via des réseaux non sécurisés. La plupart des systèmes de chiffrement actuels sont des systèmes bloc cipher(chiffrement par bloc), car ils offrent un niveau de sécurité très élevé et un temps d'exécution relativement court. Dans ce chapitre, nous proposons de concevoir un algorithme cryptographique symétrique par bloc inspiré de l'ADN. Nous avons étudiés l'approche de " Olga TORNEA " et on s'est inspiré de cette approche afin de lui apporter des modifications et des améliorations. Comme nous allons essayer de se rapprocher du chiffrement parfait de Vernam on se basant sur la diversité et la quantité de l'information contenue dans l'ADN. Tout au long de ce chapitre, nous présenterons en détails les techniques et principes utilisés dans la conception de cet algorithmes.

3.2 Contribution

Les deux parties (Alice and Bob) doivent préalablement partagé un brin ADN de leurs choix avec une longueur L.

3.2.1 Processus de chiffrement

Phase 1 : La clé

Dans cette phase, une clé -qui représente un index dans le brun ADN- est calculée. Et pour cela Alice choisis un chiffre très grand soit A et l'envoie en claire par une voie publique a Bob.

Pour calculer la clé K=A mod L. Le reste de division (soit K) de cette clé A par L (la longueur du brun ADN) représente l'index d'une séquence ADN (S) avec une longueur similaire à celle du texte clair M.

Phase 2 : Codage binaire et découpage en blocs

Chaque pixel de l'image est codé sur 256 bits binaire est découpé en blocs de 32 bits.

Phase 3 : Codage en base nucléotide

Dans cette étape, nous allons procéder à une substitution de chaque paire de bits en une base nucléotide selon le codage : A :00 (010) C :01(110) G :10(210) T :11(310) Au résultat comme étant chaque paire de bit est convertit en un seul caractère qui représente une base nucléotide. A partir de chaque bloc de 16 bits, nous obtiendrons un bloc de 16 caractères (bases).

Phase 4 : Chiffrement

Une addition modulo 4 est effectuée entre le texte clair M et la séquence S. Nous obtien-

drons une séquence ADN chiffré C.

Exemple :

C	1	T	3	G	2	A	0	T	3	G	2	T	3	C	1
+															
T	3	A	0	C	1	G	2	A	0	T	3	G	2	C	1
=															
A	0	T	3	T	3	G	2	T	3	C	1	C	1	G	2

Phase 5 : Confusion

Cette étape consiste à effectuer un brouillage du texte clair afin d'éliminer l'ordre logique des lettres dans le but de défendre le chiffrement de la cryptanalyse " attaque statistique ".Nous avons utilisé une boite de permutation de la façon suivante :

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits pairs descendant								Bits impairs ascendant							
16	14	12	10	8	6	4	2	1	3	5	7	9	11	13	15

Le nombre de tours est spécifié de la façon suivante :

NbrTour=1+(Nbr(A)*Nbr(C)*Nbr(G)Nbr(T) Mod 15)s

Après chaque tour, nous ferons un décalage d'un bit à gauche.

3.2.2 Processus de déchiffrement

Phase 1 : La clé

La clé est calculée de la même manière qua la phase 3 du processus de chiffrement. Bob récupère le chiffre (A) envoyé par Alive et pour calculer la clé K=A mod L.

Le reste de division (soit K) de cette clé A par L (la longueur du brun ADN) représente l'index d'une séquence ADN (S) avec une longueur similaire à celle du texte chiffré C.

Phase 2 : Enlevé la confusion

Le texte chiffré C est découpé en blocs de 32 bits.

Cette étape consiste à effectuer une opération inverse de la phase 5 du processus de chiffrement.

16	14	12	10	8	6	4	2	1	3	5	7	9	11	13	15
Bits pairs descendant								Bits impairs ascendant							
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Le nombre de tours est calculé de la façon suivante :
NbrTour=1+(Nbr(A)*Nbr(C)*Nbr(G)Nbr(T) Mod 15)s
Après chaque tour, nous ferons un décalage d'un bit à droite.

Phase 3 : Déchiffrement

Une soustraction modulo 4 est effectuée entre le texte obtenu résultat de la phase 2 et la séquence S de la phase 1. Nous obtiendrons une séquence ADN chiffré C.

Exemple :

A	0	T	3	T	3	G	2	T	3	C	1	C	1	G	2
-															
T	3	A	0	C	1	G	2	A	0	T	3	G	2	C	1
=															
C	1	T	3	G	2	A	0	T	3	G	2	T	3	C	1

Phase 4 : Décodage des bases nucléotide

Dans cette étape, nous allons procéder à une substitution de chaque base nucléotide en paire de bits binaire : 00 (A) 01(C) 10(G) 11(T)
Au résultat, comme chaque base est codée sur deux bits, nous obtiendrons des blocs de 32 bits.

Phase 5 : concaténation des blocs est reconstitution de l'image

Dans cette étape, nous allons concaténer tout les blocs obtenus, et comme c'est un codage à longueur fixe, chaque 256 bits représente un pixel.

3.3 Conclusion

Dans ce chapitre, nous avons présenté nos contributions cryptographiques, ainsi que les détails de chaque étape les constituants. Nos algorithmes sont inspirés de techniques déjà connues qui ont prouvé leur efficacité. **CryptoADN :** Cet algorithme est un chiffrement

qui consiste en bref d'effectuer un brouillage du message secret à l'aide de boite de substitution en combinant DES et ENIGMA, ensuite d'extraire aléatoirement des séquences ADN pour appliquer le chiffre de VERNAM.

4

Implémentation et discussion des résultats

Contents

4.1 Introduction 56

4.2 Environnement de développement : 56

4.3 Tests et résultats expérimentaux de Crypto-ADN 57

4.3.1 Complexité de l'algorithme 57

4.3.2 Variation du temps d'exécution 58

4.3.3 Variation de la taille d'image chiffré selon la taille d'image clair : 59

4.3.4 Comparaison en temps d'exécution entre l'algorithme proposé et AES : 60

4.4 Conclusion 62

4.1 Introduction

Dans ce chapitre nous allons présenter la mise en œuvre des algorithmes proposés, ainsi que les résultats des différents tests effectués dans le but d'évaluer leurs performances. Les tests des méthodes cryptographiques s'effectuent sur deux axes importants :
Axe temps d'exécution : Ces tests ont pour objectifs d'évaluer les performances de l'algorithme de point de vue temps de chiffrement/déchiffrement et ceci en variant certains de ses paramètres (nombre de tours, longueur de la séquence ADN ... etc)
Axe sécurité : Ces tests ont pour objectifs d'évaluer la sécurité de l'algorithme, Autrement dit, évaluer la résistance de l'algorithme devant les attaques des cryptanalyste.

4.2 Environnement de développement :

Les approches proposées dans ce travail ont été implémentées et testées dans un environnement possédant les caractéristiques suivantes : Un processeur Intel(R)Core (TM) i7-4200 U CPU @ 2.60Ghz2.30Ghz, doté d'une capacité de mémoire de8GB, sous Windows 7 64 bits. Nous avons utilisé l'environnement de développement NetBeans. **Langage de programmation Java :** Java est à la fois un langage de programmation informatique orienté objet et un environnement d'exécution portable. Il est créé par James Gosling et Patrick Naughton employés de Sun Microsystems avec le soutien de Bill Joy (cofondateur de Sun Microsystems en 1982), présenté officiellement le 23 mai1995 au SunWorld.
Le langage Java a la particularité principale que les logiciels écrits avec ce dernier sont très facilement portables sur plusieurs systèmes d'exploitation tels que : Unix, Microsoft Windows, Mac OS ou Linux avec ou sans modifications. C'est la plate-forme qui garantit la portabilité des applications développées en Java.
Java est devenu aujourd'hui une direction incontournable dans le monde de la programmation, parmi les différentes caractéristiques qui sont attribuées à son succès, nous avons :

- L'indépendance de toute plate-forme : le code reste indépendant de la machine sur laquelle il s'exécute. Il est possible d'exécuter des programmes Java sur tous les environnements qui possèdent une Java Virtual Machine.
- Java est également portable, permettant à la simulation d'être distribuée facilement sans avoir à recompiler le code pour les différents systèmes.
- Le code est structuré dans plusieurs classes dont chacune traite une partie différente de la simulation.
- Java est multitâches : il permet l'utilisation de Threads qui sont des unités d'exécution isolées.

Environnements de développement

NetBeans est un environnement de développement intégré - un outil pour les programmeurs pour écrire, compiler, déboguer et déployer des programmes. Il est écrit en Java - mais peut supporter n'importe quel langage de programmation. NetBeans est disponible sous Windows, Linux, Solaris ou sous une version indépendante des systèmes d'exploitation (requérant une machine virtuelle Java). Un environnement Java Développement Kit JDK est requis pour les développements en Java.

Les classes principales :

L'ensemble des classes et leurs méthodes respectives pour les deux algos sont :

- **ChiffrementBloc :**Cette classe regroupe les différentes procédures et fonctions nécessaires pour le chiffrement d'un bloc (64 bits).
- **DéchiffrementBloc :**Cette classe regroupe les différentes procédures et fonctions nécessaires pour le déchiffrement d'un bloc (64 bits).
- **génerer le clé :**Cette classe contient plusieurs procédures et fonctions qu'on aura besoin dans notre application.

4.3 Tests et résultats expérimentaux de Crypto-ADN

Dans ce qui suit, nous allons présenter les différents tests et évaluations effectués ainsi que les résultats obtenus sur l'algorithme crypto-ADN.

On tien à préciser que les tests ont été effectués sur une machine HP Pro 3500 dotée d'un processeur i7-3770 3ème génération de 3.40 Ghz avec 8 Go de RAM, et d'un système d'exploitation Windows 7 Professionnel 64 bits.

4.3.1 Complexité de l'algorithme

L'analyse de la complexité d'un algorithme est importante car elle révèle son efficacité pour les applications en temps réel. Dans ce travail, le temps de calcul de l'algorithme a été analysé à l'aide des méthodes de la théorie de la complexité. Les conclusions obtenues ont été testées pour être vrai à travers les résultats de mise en œuvre.

Le temps d'exécution d'un algorithme est considéré comme la somme de toutes les opérations. Le nombre d'opérations peut être constant ou variable et dépend des paramètres d'entrée. Selon les approximations de la théorie de la complexité, la limite inferieur de la fonction est utilisée pour exprimer le taux de croissance de l'exécution de l'algorithme [36]. Par conséquent, si le nombre d'opérations est par exemple 1 + 2n, la complexité serait O(n) ; si le nombre d'opérations est 4 + n + n3, alors la complexité serait O(n3).

Dans ce travail, la complexité analysé pour 3 opérations importantes de l'indexation de l'ADN : Calcul du dictionnaire de clé, le cryptage et le décryptage. La phase computation

du dictionnaire des index est calculée en m opérations, m est la longueur de la séquence ADN utilisée. La phase cryptage et le décryptage sont exécutés en n opérations.
Pour le chiffrement : Le calcul du dictionnaire des index est O(m) et pour le processus de chiffrement est O(n). Ça implique que la complexité de l'indexation et chiffrement est O(m+n). Cela signifie que le taux croissant du temps de calcul est linéaire en fonction de la longueur du la séquence ADN et la taille d'image clair.
Pour le déchiffrement : Le processus de déchiffrement est O(n). Cela signifie que le taux croissant du temps de calcul est linéaire en fonction de la taille d'image clair uniquement et que la longueur du la séquence ADN n'a pas d'influence sur le temps d'exécution. Où n est le nombre des pixels d'image clair et d'image chiffré. La complexité résultante.

4.3.2 Variation du temps d'exécution

Selon la longueur de la séquence ADN clé :

Dans ce test, nous avons sélectionné des images avec des tailles différentes ; Ensuite, nous avons effectué le test Puis nous avons évalué le temps moyen de chiffrement/déchiffrement.

Image Dimension	Image size	Encryption time	Decryption time
150x150	66 k	5 sec.	3 sec.
200x200	117 k	7 sec.	5 sec.
240x240	168 k	13 sec.	7 sec.
260x260	198 k	18 sec.	8 sec.
520x520	792 k	25 sec.	17sec.

FIGURE 4.1 – Mesure du temps d'exécution selon la taille des images.

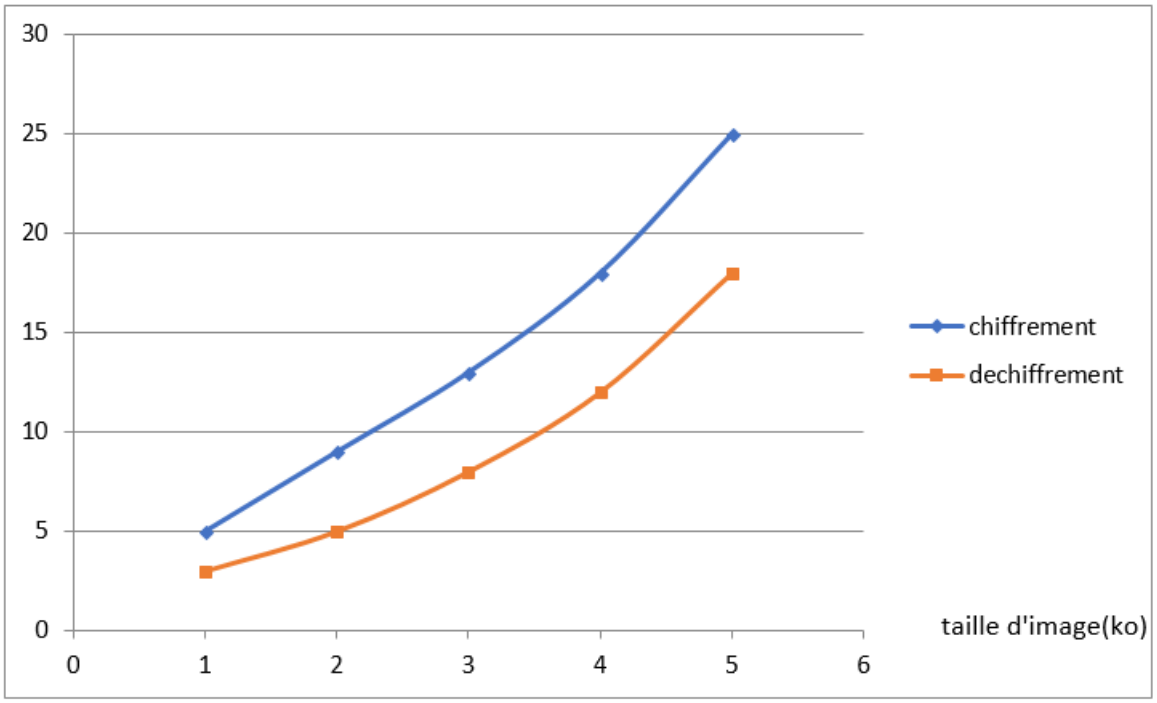

FIGURE 4.2 – Variation du temps d'exécution selon la taille des images

Analyse : On remarque que le temps de déchiffrement est beaucoup plus inferieur au temps de chiffrement. Cela est du au faite que le chiffrement contient la phase computation du dictionnaire des index qui prend beaucoup de temps. Par contre, dans le processus du déchiffrement il s'agit d'un accès indexé direct. C'est pour ça qu'il est beaucoup plus rapide. On remarque aussi que le temps de chiffrement (respectivement déchiffrement) augmente d'une façon linéaire avec l'augmentation de la taille du d'image clair.

4.3.3 Variation de la taille d'image chiffré selon la taille d'image clair :

Dans ce test, nous avons suivi la variation de la taille du d'image chiffré en augmentant la taille de d'image clair, et nous avons reporté les résultats dans le tableau suivant :

Taille d'Image clair	Taille d'Image chiffré
10 ko	40 ko
25 ko	100 ko
60 ko	240 ko
250 ko	1000 ko
500 ko	2000 ko

FIGURE 4.3 – Variation de la taille d'image chiffré selon la taille d'image clair

Le graphe suivant représente la relation entre la taille du d'image clair et la taille du d'image chiffré.

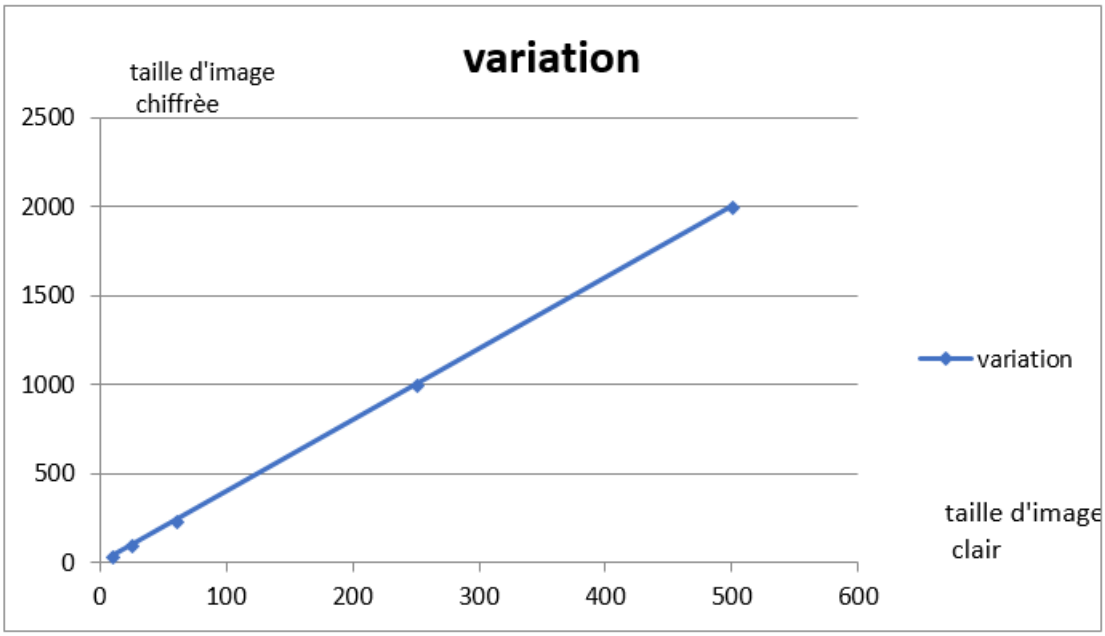

FIGURE 4.4 – la relation entre la taille du d'image clair et la taille du d'image chiffré.

Analyse :
On remarque que la taille du d'image chiffré et toujours quatre fois supérieure à la taille d'image clair. Tout simplement parce que chaque caractère et chiffré en quatre bases nucléotides.

4.3.4 Comparaison en temps d'exécution entre l'algorithme proposé et AES :

Dans ce test, nous avons effectué une étude comparative entre notre algorithme et le standard connu AES en temps de chiffrement / déchiffrement, ce dernier a été implémenté dans le même environnement de développement (java) et la même machine. Cette implémentation est téléchargeable gratuitement sur « www.code-source.com ».

Taille d'image (ko)	Aes		Crypto ADN	
	Chiffrement	Déchiffrement	Chiffrement	Déchiffrement
Img1 =324	60 ms	50ms	96 s 5 ms	74 s 1 ms
Img2=416	80ms	72ms	2min 26 s 8 ms	1min 14 s 7 ms
Img 3= 520	95ms	81ms	2min 45 s 4 ms	2min 2 s 6 ms
Img4 = 630	150ms	119ms	3min 24 s 9 ms	2min 56 s 4 ms
Img5 =720	260ms	223ms	4min 29 s 7 ms	3min 47 s 28 ms

FIGURE 4.5 – AES vs Crypto ADN

Analyse :

Ces tests montrent que AES est beaucoup plus rapide que notre algorithme exécuté dans les mêmes conditions. Cette différence est dû à : Dans AES, on trouve quatre procédures : SubByte (Substitution), ShiftRow (Décalage ligne), MixColomn (Permutation) et un XOR. Il est évident que ces quatre procédures consomment moins de temps parce qu'il s'agit de manipulation de chaine de caractère. Alors que notre algorithme contient dans le processus de chiffrement cinq procédures :

1. **image2Bin :**Conversion d'image en binaire.
2. **Bin2Base :**Conversion du code binaire en bases nucléotides.
3. **KeyGen :**Génération de la clé de chiffrement.
4. **addADN :**addition avec des séquences ADN.
5. **SubBase :**Substitution des blocs de bases.

Les trois premières procédures et la cinquième sont très rapides. C'est la quatrième procédure qui est très couteuse en temps d'exécution parce qu'il s'agit d'un accès disque à la base de données génétique afin d'extraire les séquences ADN désignées par la clé générée. De même pour le déchiffrement notre algorithme contient quatre procédures :

1. **BaseSub :**Enlever le brouillage à l'aide des boites de substitution.
2. **ADNsubstr :**substraction avec des séquences ADN avec l'image chiffré.
3. **Base2Bin :**Conversion des base nucléotide en binaire.
4. **Bin2Texte :**Conversion du code binaire en texte.

Uniquement la deuxième procédure est très couteuse en temps d'exécution parce qu'il s'agit d'un accès disque afin d'extraire les séquences ADN désignées par la clé.

4.4 Conclusion

L'algorithme proposé améliore deux critères d'un chiffrement de bloc standard, qui sont confus et diffusion en mode feistel avec l'informatique de l'ADN. L'opération d'ADN telle que (addition, soustraction, complément) n'a plus de complexité car les opérations sont simples. Permutation de l'ADN l'opération dépend de la longueur de la chaîne dans l'ADN présent. En outre, l'ADN peut stocker plus de données dans la chaîne que chaque présentation de deux bits dans un caractère. Image de cryptage du réseau feistel et L'informatique d'ADN produit plus de chiffrage de complexité. La clé secrète utilisée pour trouver plusieurs clés crypter les blocs pour augmenter le cryptage de qualité. L'ADN de codage et de décodage consomme plus de temps.
La permutation de l'ADN a été utilisée pour faire plus de différence dans le pixel du voisinage.

Conclusion Générale et Perspectives

Ce travail est une recherche scientifique sur la cryptographie ADN. C'est une direction émergente et prometteuse en cryptographie. Ces méthodes peuvent utiliser l'ADN dans sa structure biologique dans un laboratoire avec des outils biologique adéquats. Comme ils peuvent utiliser l'ADN dans sa structure numérique avec des ordinateurs comme outils de travail. Dans le chapitre 3, une méthode de chiffrement symétrique grâce à l'indexation de l'ADN, est présentée. Elle a été conçue pour utiliser des bases de données génétiques afin de récupérer des séquences d'ADN et les utiliser pour les opérations de substitution comme une clé secrète. Et pour cela, la succession des bases nucléotide et la capacité de stockage de la molécule ADN, ont été explorées.

C'est le principe de notre contribution Inspiré du chiffre de Vernam, qui stipule que la clé doit être aléatoire, aussi longue que le texte et à usage unique. Dans cette méthode, il n'est pas nécessaire de générer une clé aléatoire aussi longue que le texte, il suffit de générer des chiffres correspondant à des blocs de séquences ADN de 32 bases. De ce fait, la clé (OTP) est 32 fois inferieur à la longueur du texte claire et c'est un grand avantage pour la transmission de la clé de chiffrement.

Le temps de calcul a été estimé par une analyse pratique. Basé sur les mesures obtenues et une vue graphique de différente variation a été établi pour chaque opération.

La sécurité des deux algorithmes, a été mesurée. Une analyse théorique des attaques de cryptanalyse par force brute (espace de clé) a été réalisée. Une comparaison à un autre algorithme d'un principe similaire a été réalisée en utilisant la théorie de la complexité.

Bibliographie

[1] Leonard M Adleman. Molecular computation of solutions to combinatorial problems. *Science*, 266(5187) :1021–1024, 1994.

[2] AK Verma, Mayank Dave, and RC Joshi. Dna cryptography : a novel paradigm for secure routing in mobile ad hoc networks (manets). *Journal of Discrete Mathematical Sciences and Cryptography*, 11(4) :393–404, 2008.

[3] AK Verma, Mayank Dave, and RC Joshi. Securing ad hoc networks using dna cryptography. In *IEEE International Conference on Computers and Devices for Communication (CODEC06)*, pages 781–786, 2006.

[4] A Gehani, TH LaBean, and JH Reif. Dna-based cryptography, 5th dimacs workshop on dna based computers, 1999.

[5] Behrouz A. Forouzan. Cryptography and network security. *TMH Inc,New York*, 2010.

[6] Richard J Lipton. Breaking dbs using a molecular computer dan boneh christopher dimworth. *DNA based computers*, 27 :37, 1996.

[7] Monica Borda and Olga Tornea. Dna secret writing techniques. In *Communications (COMM), 2010 8th International Conference on*, pages 451–456. IEEE, 2010.

[8] Jie Chen. A dna-based, biomolecular cryptography design. In *Circuits and Systems, 2003. ISCAS'03. Proceedings of the 2003 International Symposium on*, volume 3, pages III–III. IEEE, 2003.

[9] Jonathan PL Cox. Long-term data storage in dna. *TRENDS in Biotechnology*, 19(7) :247–250, 2001.

[10] Guangzhao Cui, Limin Qin, Yanfeng Wang, and Xuncai Zhang. An encryption scheme using dna technology. In *Bio-Inspired Computing : Theories and Applications, 2008. BICTA 2008. 3rd International Conference on*, pages 37–42. IEEE, 2008.

[11] Deepak Kumar and Shailendra Singh. Secret data writing using dna sequences. In *Emerging Trends in Networks and Computer Communications (ETNCC), 2011 International Conference on*, pages 402–405. IEEE, 2011.

[12] Eric Conrad. Explanation of three types of cryptosystem. *CISSP Papers*, page 1, 2006.

[13] G. Rozenberg and A. Salomaa. Dna computing : New ideas andparadigms,. *Lecture Notes in Computer Science (LNCS),*, 2006.

[14] Jonathan Katz and Yehuda Lindell. Introduction to modern cryptography : principles and protocols. cryptography and network security, 2008.

[15] Richard J Lipton. Dna solution of hard computational problems. *science*, 268(5210) :542–545, 1995.

[16] Kazuo Tanaka, Akimitsu Okamoto, and Isao Saito. Public-key system using dna as a one-way function for key distribution. *Biosystems*, 81(1) :25–29, 2005.

[17] XueJia Lai, MingXin Lu, Lei Qin, JunSong Han, and XiWen Fang. Asymmetric encryption and signature method with dna technology. *Science China Information Sciences*, 53(3) :506–514, 2010.

[18] MingXin Lu, XueJia Lai, GuoZhen Xiao, and Lei Qin. Symmetric-key cryptosystem with dna technology. *Science in China Series F : Information Sciences*, 50(3) :324–333, 2007.

[19] Ashish Kumar Kaundal and AK Verma. *Fiestel Inspired Structure For DNA Cryptography*. PhD thesis, 2014.

[20] Olga Tornea and Monica E Borda. Security and complexity of a dna-based cipher. In *Roedunet International Conference (RoEduNet), 2013 11th*, pages 1–5. IEEE, 2013.

[21] Qi Ouyang, Peter D Kaplan, Shumao Liu, and Albert Libchaber. Dna solution of the maximal clique problem. *Science*, 278(5337) :446–449, 1997.

[22] Sabari Pramanik and Sanjit Kumar Setua. Dna cryptography. In *Electrical & Computer Engineering (ICECE), 2012 7th International Conference on*, pages 551–554. IEEE, 2012.

[23] Sherif T Amin, Magdy Saeb, and Salah El-Gindi. A dna-based implementation of yaea encryption algorithm. In *Computational Intelligence*, pages 120–125, 2006.

[24] William Stallings. *Cryptography and network security : principles and practice*. Pearson Education India, 2003.

[25] GZ Cui, Y Liu, and X Zhang. New direction of data storage : Dna molecular storage technology. *Computer Engineering and Applications*, 42(26) :29–32, 2006.

[26] Kazuo Tanaka, Akimitsu Okamoto, and Isao Saito. Public-key system using dna as a one-way function for key distribution. *Biosystems*, 81(1) :25–29, 2005.

[27] Thomas H. LaBean Ashish Gehani and John H. Reif. Dna-based cryptography ?5th annual dimacs meeting on dna based computers(dna 5),mit, cambridge. 1999.

[28] Jie Chen. A dna-based, biomolecular cryptography design. In *Circuits and Systems, 2003. ISCAS'03. Proceedings of the 2003 International Symposium on*, volume 3, pages III–III. IEEE, 2003.

[29] A Gehani, T LaBean, and J Reif. Dna based cryptography. germany : Aspects of moleculer computing, 2004.

[30] Atul Kahate. *Cryptography and network security.* Tata McGraw-Hill Education, 2013.

[31] MingXin Lu, XueJia Lai, GuoZhen Xiao, and Lei Qin. Symmetric-key cryptosystem with dna technology. *Science in China Series F : Information Sciences*, 50(3) :324–333, 2007.

[32] XueJia Lai, MingXin Lu, Lei Qin, JunSong Han, and XiWen Fang. Asymmetric encryption and signature method with dna technology. *Science China Information Sciences*, 53(3) :506–514, 2010.

[33] Kang Ning. A pseudo dna cryptography method. *arXiv preprint arXiv :0903.2693*, 2009.

[34] MingXin Lu, XueJia Lai, GuoZhen Xiao, and Lei Qin. Symmetric-key cryptosystem with dna technology. *Science in China Series F : Information Sciences*, 50(3) :324–333, 2007.

[35] N. Kiran V. M. M. Shyam. A novel encryption scheme based on dna computing. In *in 14th IEEE International Conference*, Tia, India, 2007.