الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة سعيدةد. مولاي الطاهر

كلية التكنولوجيا

قسم: الإعلام الآلي

Mémoire de Master

Spécialité : Sécurité informatique et cryptographie

Thème

Stéganographie à base d'ADN

Présenté par :

ZEDROUNI kaouther

BENDOUINA nour elhouda

Dirigé par :

Mr .Henoune mohamed mokhtar

Année universitaire 2022-2023

Remerciement

La réalisation de ce mémoire a été possible grâce au concours de plusieurs personnes à qui je voudrais témoigner toute ma reconnaissance.

Nous exprimons tout d'abord notre gratitude la plus profonde à Dieu, le Tout-Puissant et le Miséricordieux, pour avoir guidé nos pas et nous avoir comblés de force et de patience pour mener à bien ce modeste travail.

Nous remercions sincèrement notre directeur de recherche, ***« Mr. Henoune mohamed mokhtar »****, pour le suivi, l'encouragement et les précieux conseils, pour sa gentillesse et surtout pour sa confiance en nous.*

Nous tenons également à remercier les membres du jury qui accepté d'évaluer ce mémoire et de nous faire part de leurs critiques constructives, qui contribueront sûrement à améliorer ce travail. Nous ne pouvons manquer d'exprimer nos sincères remerciements à tous les enseignants qui nous ont encouragés tout au long du processus d'apprentissage.

Nous tenons également à remercier nos parents pour le soutien inconditionnel dont ils ont fait preuve depuis que notre projet est défini. Merci pour le soutien financier, moral, psychologique et matériel.

Dédicace

Je tiens tout particulièrement à dédier ces mots à ***ma mère****, à qui je suis infiniment redevable. Elle a toujours cru en moi, illuminant ma vie et représentant l'espoir même de mon existence. Grâce à elle, j'ai été en mesure de franchir toutes les étapes jusqu'ici.*

À ***mon cher père****, qui a illuminé mon chemin et m'a constamment encouragé et soutenu tout au long de mes études, je souhaite exprimer ma gratitude infinie.*

Si je suis ici aujourd'hui, c'est grâce à vous!

À mon bonheur, à celui qui est la source de tous mes efforts, à toi, mon cher frère ***Ilyes,*** *je souhaite adresser ces mots remplis d'affection.*

À mon frère bien-aimé, qui est le joyau de ma vie, je t'adresse ces mots empreints de profonde affection. Cher ***yacine****, tu occupes une place si spéciale dans mon cœur.*

À mon amie exceptionnelle, présente à chaque étape de ma vie, et le charme de ma vie ***boutheina****, tu es la définition même d'une amitié parfaite, Je suis incroyablement reconnaissante de t'avoir dans ma vie.*

A toute ma famille

Pour finir j'adresse mes dédicaces à mes très chers amis

Kaouther

Dédicace

Je dédie ce modeste travail

A mes très chers parents, pour leurs patiences, leurs sacrifices, leurs tendresses et soutiens durant mes études, aucun hommage ne pourra être à la hauteur de l'amour dont ils ne cessent de me combler.

Que dieu leurs procure bonne santé et longue vie.

A mes très chers frères et à mes chères sœurs, pour leurs amours et compréhension.

A mon ange, mon petit frère adoré ***MOHAMED ANES***

A mes chers grands parents que dieu les accueillent dans son vaste paradis, ainsi que toute ma famille paternelle et maternelle

A tous mes très chers amis

Que dieu les protège

Nour Elhouda

Résumé

La sécurité informatique est devenue essentielle avec la progression rapide des technologies de l'information et de la communication, car nos informations confidentielles et notre vie privée sont de plus en plus vulnérables aux risques liés à cette interconnexion croissante. Pour faire face à ces menaces, il est essentiel d'investir dans des mesures de sécurité robustes, telles que la cryptographie, qui protège les données en les chiffrant de manière sécurisée. Dans ce mémoire, une méthode cryptographique à clé symétrique basée sur l'ADN a été proposée qui combine la cryptographie ADN et la stéganographie ADN pour renforcer la sécurité des données.

ملخص

أصبح أمن تكنولوجيا المعلومات ضروريًا مع التقدم السريع لتكنولوجيات المعلومات والاتصالات، حيث أصبحت معلوماتنا السرية وخصوصيتنا عرضة بشكل متزايد للمخاطر المرتبطة بهذا الترابط المتزايد لمعالجة هذه التهديدات، من الضروري الاستثمار في تدابير أمنية قوية، مثل التشفير، الذي يحمي البيانات عن طريق تشفيرها بشكل آمن. في هذا الموجز، تم اقتراح طريقة تشفير رئيسية متماثلة تعتمد على الحمض النووي والتي تجمع بين تشفير الحمض النووي و ستيغانوغرافيا الحمض النووي لتعزيز أمن البيانات.

Abstract

Computer security has become essential with the rapid advancement of information and communication technologies, as our confidential information and privacy are increasingly vulnerable to the risks associated with this growing interconnection. To address these threats, it is essential to invest in robust security measures, such as cryptography, which protects data by encrypting it securely. In this brief, a symmetric key cryptographic method based on DNA was proposed that combines DNA cryptography and DNA steganography to enhance data security.

Table de matières

Chapitre II : Etat de l'art autour de la cryptographie

Chapitre III : implémentation et résultat

Liste des figures

Liste des tableaux

Introduction Générale

De nos jours, la sécurité informatique est devenue un enjeu majeur dans notre société moderne. Avec l'accélération des technologies de l'information et de la communication, nos vies sont de plus en plus dépendantes des systèmes informatiques et de l'échange de données en ligne. Malheureusement, cette interconnexion croissante expose nos informations confidentielles et notre vie privée à de nombreux risques.

Le paysage informatique actuel est complexe et en constante évolution, offrant aux cybercriminels de nombreuses opportunités d'exploiter les vulnérabilités pour accéder à des informations confidentielles, causer des perturbations et compromettre la vie privée des individus. Ces attaques peuvent provenir de diverses sources, allant des pirates informatiques individuels aux organisations criminelles et même aux acteurs étatiques.

Face à cette réalité, il est impératif d'investir dans des mesures de sécurité robustes pour protéger nos systèmes et nos données. Cela comprend l'utilisation de techniques avancées telles que la cryptographie, qui joue un rôle essentiel dans la protection des données confidentielles en les transformant de manière sécurisée.

La cryptographie est un pilier essentiel de la sécurité informatique, visant à protéger les données confidentielles en les chiffrant de manière sécurisée. Elle assure la confidentialité des informations en les rendant illisibles sans la clé appropriée et garantit l'intégrité des données en détectant toute altération.

Une des approches innovantes récentes dans le domaine de la cryptographie est l'utilisation de l'ADN. L'ADN, non seulement utilisé comme support de stockage, mais également comme outil de cryptographie et de stéganographie, offre de nouvelles perspectives. Les propriétés uniques de l'ADN, telles que sa capacité de stockage massive et sa robustesse, en font un candidat prometteur pour sécuriser les informations sensibles.

Dans ce travail, nous présenterons un algorithme de chiffrement innovant qui utilise l'ADN comme base. Cet algorithme présente plusieurs caractéristiques :

1. Extraction des clés de chiffrement à partir des séquences d'ADN : L'algorithme utilise les séquences d'ADN pour générer des clés de chiffrement uniques et sécurisées. Ces clés sont essentielles pour le processus de chiffrement et de déchiffrement des données.
2. Utilisation des séquences d'ADN pour l'extraction des codes des bases azotiques : Les codes des bases azotiques de l'ADN (A, T, G, C) sont utilisés pour chiffrer les textes en clair. Les caractéristiques spécifiques de chaque base azotique permettent d'obtenir un chiffrement robuste et difficile à décrypter sans la clé appropriée.
3. Utilisation de la stéganographie pour insérer les textes chiffrés dans des images : L'algorithme exploite également le principe de la stéganographie, qui consiste à cacher des informations secrètes au sein d'un support, tel qu'une image. Les textes chiffrés sont intégrés de manière invisible dans des images, ce qui rend leur détection extrêmement difficile pour les attaquants.

Organisation de mémoire :

L'organisation de notre mémoire comprend trois chapitres distincts. Voici un aperçu de chacun d'entre eux :

Le premier chapitre servira d'introduction générale à la sécurité informatique, en mettant l'accent sur les enjeux actuels et les menaces associées. Nous présenterons les bases de la cryptographie, en abordant à la fois les techniques de chiffrement symétrique et asymétrique.

Dans Le deuxième chapitre, nous ferons un état de l'art sur la cryptographie à base d'ADN, en commençant par une explication détaillée de l'ADN lui-même, de sa structure et de ses composants. Nous explorerons ensuite les différentes approches et les techniques utilisées dans la cryptographie à base d'ADN, en fournissant une brève description des travaux existants dans ce domaine. Ensuite, nous aborderons la stéganographie, en expliquant les concepts de base, les différentes techniques utilisées et comment la stéganographie peut être appliquée à l'ADN.

Le chapitre III se concentrera sur la description approfondie de notre algorithme de chiffrement à base d'ADN. Nous expliquerons en détail les différentes étapes de l'algorithme, y compris l'extraction des clés de chiffrement à partir des séquences d'ADN, l'utilisation des codes des bases azotiques pour chiffrer les textes en clair, et l'application de la stéganographie pour dissimuler les textes chiffrés dans des images. De plus, nous présenterons les résultats des expérimentations réalisées pour évaluer l'efficacité et la sécurité de notre algorithme, en fournissant des analyses et des discussions appropriées.

Chapitre I

La sécurité informatique

I.1/ introduction :

Le marché de la sécurité informatique a connu une croissance significative. L'entreprise Gartner s'attend à ce que le marché du cyber sécurité dépasse les 100 milliards de dollars en 2019 contre 76 milliards de dollars en 2015. **[1]**

Donc, la Cyber sécurité ou encore appelé la sécurité informatique se définit comme l'ensemble des moyens tant techniques qu'organisationnels, juridiques ou humains mis en place pour prévenir et/ou empêcher la diffusion et la modification non autorisée de données ainsi que l'usage non autorisé de ressources informatiques. **[2]**

La sécurité informatique a pour but de protéger contre les attaques malveillantes et Avoir un système de sécurité informatique sécurisé.

I.2/ Les principaux de la sécurité informatique:

I.2.1/ Les niveaux de la sécurité informatique :

- **La sécurité réseau :**

  L'introduction de systèmes distribués et l'utilisation de réseaux et dispositifs de communication pour transporter des données entre un terminal utilisateur et un ordinateur, et entre ordinateurs.

  Les mesures de sécurité des réseaux sont nécessaires pour protéger les données durant leur transmission. On parle alors de sécurité des réseaux. **[3]**

- **La sécurité système :**

  Le système et les services tournés sur un ordinateur (serveur, station de travail, terminal...) sont ciblés par la sécurité. **[3]**

- **La sécurité applicative :**

  La sécurité applicative est le nouveau périmètre de la sécurité informatique. Ce qui nous intéresse ici, c'est un logiciel ou une application en particulier (site, application web...). **[3]**

I.2.2/ Les services de sécurité :

Un service de sécurité est un service de traitement ou de communication qui améliore la sécurité des systèmes de traitement de données et les transferts d'informations d'une organisation. Les services sont destinés à contrer les attaques de sécurité, et ils utilisent un ou plusieurs mécanismes de sécurité pour fournir le service.

La classification utile des services de sécurité est la suivant :

I.2.2.1/ Authentification :

L'authentification consiste à savoir lier, grâce à une caractéristique discriminante (un mot de passe par exemple) une identité à une entité donnée d'un système (la partie administration d'un site, un processus en particulier ou un ordinateur par exemple).

Elle s'applique à l'utilisateur, à l'émetteur d'un message ou à l'auteur d'un document. Pour implémenter ces fonctions, plusieurs approches sont possibles : authentification par **identifiant** et **mot de passe**, authentification par **certificat**, authentification par **carte**, authentification **multimodale** qui associent plusieurs des méthodes précédentes. **[4]**

Les problèmes potentiels à gérer sont nombreux :

- **Dépersonnification :** Comment s'assure-t-on que notre utilisateur est bien la personne qu'il prétend être ?
- **Rejeu** : Comment lutter contre l'espionnage, la capture et la réutilisation des mots de passe par exemple ?
- **Rebond :** Comment lutter contre l'espionnage, la capture et la réutilisation des mots de passe dans une autre partie du système ou sur autre application par exemple ?
- **Altération des messages entre les différents acteurs du système :** Comment s'assure-t-on que personne ne s'approprie une signature illégalement ?
- **Transférabilité du mot de passe :** comment lutter contre les comportements du type : « Tiens, voilà mon mot de passe » ? **[5]**

I.2.2.2/ Contrôle d'accès :

Une fois l'utilisateur authentifié, il est nécessaire de vérifier s'il a les autorisations nécessaires pour accéder aux fonctionnalités de l'application. Pour ce faire, il est essentiel de lier une ressource, telle qu'une base de données, à des droits d'accès spécifiques et à une entité.

Pour gérer cette problématique, il est courant d'attribuer un rôle à chaque utilisateur (par exemple, utilisateur, éditeur, administrateur), qui détermine les privilèges accordés sur les ressources manipulées par l'application. **[4]**

I.2.2.3/ La confidentialité des données :

La confidentialité des données doit être assurée lors d'échange de données sensibles (mot de passe, données bancaires ou médicales.) Il s'agit de garantir que des données acquises illégalement soient inutilisables.

Au-delà des mesures organisationnelles que l'on peut mettre en œuvre (marquage, gestion particulière), les moyens technologiques principaux pour mettre la confidentialité en œuvre reposent sur des mécanismes de chiffrement qui permettent de protéger l'échange et le stockage des données. **[4]**

I.2.2.4/ L'intégrité des données:

L'intégrité, tout comme la confidentialité, peut être appliquée à un flux de messages, à un seul message ou à des champs spécifiques d'un message. La méthode la plus utile et la plus simple consiste à assurer une protection totale du flux.

Un service d'intégrité axé sur la connexion garantit que les messages sont reçus exactement tels qu'ils ont été envoyés, sans aucune duplication, insertion, modification, réorganisation ou répétition. **[5]**

I.2.2.5/ Non répudiation :

Le non répudiation empêche l'émetteur ou le récepteur de refuser un message transmis. Ainsi, lorsqu'un message est envoyé, le destinataire peut prouver que l'expéditeur présumé a en effet envoyé le message. De même, lorsqu'un message est reçu, l'expéditeur peut prouver que le prétendu séquestre a effectivement reçu le message. **[4]**

I.2.2.6/ Disponibilité :

La disponibilité est la propriété d'un système ou une ressource système accessible et utilisable à la demande par une entité système autorisé, selon les spécifications de performance du système.

Une variété d'attaques peut entraîner la perte ou la réduction de la disponibilité. Certaines de ces attaques sont soumises à des contre- mesures automatises, telles que l'authentification et le cryptage, tandis que d'autres nécessitent une sorte d'action physique pour éviter ou se remettre de la perte de disponibilité des éléments d'un système distribué.

En outre, la disponibilité en tant que propriété d'être associée à divers services de sécurité. Un service de disponibilité est celui qui protège un système pour assurer sa disponibilité. Ce service répond aux problèmes de sécurité soulevés par les attaques de déni de service. **[4]**

I.3/ Les failles de la sécurité informatique:

Le terme **cyberattaque** fait référence à une action conçue pour cibler un ordinateur ou tout élément d'un système d'informations informatisé visant à modifier, détruire ou voler des données, ainsi qu'à exploiter ou nuire à un réseau. Les **cyberattaques** ont augmenté parallèlement à la numérisation des entreprises qui est devenue de plus en plus populaire ces dernières années.Bien qu'il existe des dizaines de différents types de **cyberattaques. [2]**

I.3.1/ Principaux défauts de la sécurité :

Les défauts de sécurité d'un système d'information les plus souvent constatés sont :

- Installation des logiciels et matériels par défaut.
- Mises à jour non effectuées.
- Mots de passe inexistants ou par défaut.
- Pas de séparation des flux opérationnels des flux d'administration des systèmes.
- Procédures de sécurité obsolètes.
- Eléments et outils de test laissés en place dans les configurations en production.
- Authentification faible.
- Télémaintenance sans contrôle fort. **[6]**

I.3.2/ Quelques termes et leurs définitions:

I.3.2.1/ La vulnérabilité logicielle:

Une vulnérabilité logicielle est une faiblesse dans la conception, l'implémentation ou la configuration d'un logiciel, permettant de détourner son fonctionnement prévu. Les attaquants peuvent exploiter ces vulnérabilités pour exécuter un code malveillant, accéder à des informations sensibles ou perturber le système. Il est crucial de les détecter et de les corriger afin de préserver la sécurité et l'intégrité des systèmes informatiques. **[7]**

Elle est typiquement le fait :

- d'un développeur mal formé aux bonnes pratiques en matière de sécurité logicielle
- La conséquence d'un des trois phénomènes suivants :
  - ✓ la connectivité
  - ✓ l'extensibilité
  - ✓ la complexité des applications logicielles actuelles. **[3]**

I.3.2.2/ attaque de sécurité :

Une action qui compromet la sécurité de l'information possédée par une organisation. **[7]**

- **Internet Engineering Task Force** définit l'attaque dans RFC 2828 [23] comme :

« *Un assaut sur la sécurité du système qui découle d'une menace intelligente, c'est-à-dire d'un acte intelligent qui est une tentative délibérée (en particulier dans le sens d'une méthode ou d'une technique) pour échapper aux services de sécurité et violer la politique de sécurité d'un système.* » **[1]**

- **Le gouvernement des États-Unis**, selon l'instruction CNSS n°4009 du 26 avril 2010 par le Comité des systèmes de sécurité nationale des États-Unis d'Amérique [24] définit une attaque comme suit :

« Toute *activité malveillante qui tente de collecter, perturber, nier, dégrader ou détruire les ressources du système d'information ou l'information elle-même*. » **[1]**

I.3.2.2.1/ Les Types d'attaques :

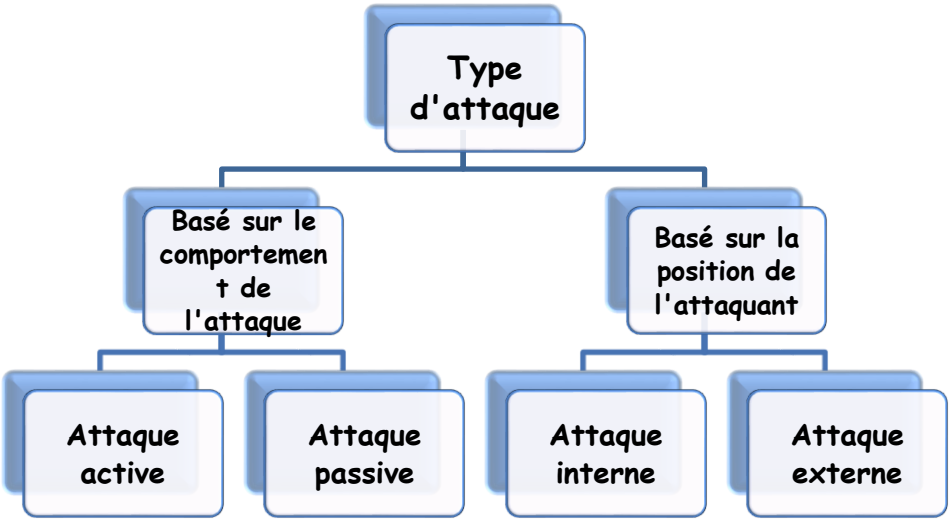


Figure I.1 : Les types d'attaques

➢ Comme présenté dans la **Figure I.1**, une attaque peut être classée par son comportement ou par la position de l'attaquant.

- Une attaque peut être classée comme active ou passive :
  - Une « **attaque active** » vise à modifier les ressources du système ou à perturber leur fonctionnement. Son objectif est de causer des dommages, de compromettre l'intégrité des données ou de prendre le contrôle du système.
  - Une « **attaque passive** » vise à obtenir des informations du système sans altérer ou perturber ses ressources. Elle se concentre sur l'interception de données confidentielles ou sensibles, telles que l'écoute téléphonique ou l'interception de communications. **[8]**

- Une attaque peut être classée comme interne ou externe, selon l'origine de l'attaquant :
  - Une « **attaque interne** » est initiée par une entité se trouvant à l'intérieur du périmètre de sécurité de l'organisation. Il s'agit souvent d'un individu ou d'un employé ayant déjà accès aux ressources du système, mais qui les utilise de manière non autorisée ou abusive.
  - Une « **attaque externe** » est initiée depuis l'extérieur du périmètre de sécurité de l'organisation. Cela peut être effectué par des individus malveillants, des pirates informatiques ou des organisations criminelles qui tentent d'exploiter des vulnérabilités pour accéder aux ressources du système ou causer des dommages. **[8]**

I.3.2.3/ Virus:

Les virus est un exécutable qui va exécuter des opérations plus ou moins destructrices sur votre machine. Les virus existent depuis que l'informatique est née et se propageaient initialement par disquettes de jeux ou logiciels divers... Sur Internet, les virus peuvent contaminer une machine de plusieurs manières :

- Téléchargement de logiciel puis exécution de celui-ci sans précautions.
- Ouverture sans précautions de documents contenant des macros.
- Pièce jointe de courrier électronique.
- Ouverture d'un courrier au format HTML contenant du javascript exploitant une faille de sécurité du logiciel de courrier.
- Exploitation d'un bug du logiciel de courrier (effectuer régulièrement les mises à jour).

Les virus peuvent être très virulents mais ils coûtent aussi beaucoup de temps en mise en place d'antivirus et dans la réparation des dégâts causés. On peut malheureusement trouver facilement des logiciels capables de générer des virus et donc permettant à des « amateurs » (aussi appelés crackers) d'étaler leur incompétence.

La meilleure parade est l'utilisation d'un antivirus à jour et d'effectuer les mises à jour des logiciels (pour éviter l'exploitation des bugs). **[9]**

I.3.2.4/ Ver:

Un ver est un programme autonome qui se reproduit et se propage à l'insu des utilisateurs. Contrairement aux virus, un ver n'a pas besoin d'un logiciel hôte pour se dupliquer. Le ver a habituellement un objectif malicieux, par exemple :

- ✓ espionner l'ordinateur dans lequel il réside ;
- ✓ offrir une porte dérobée à des pirates informatiques;
- ✓ détruire des données sur l'ordinateur infecté;
- ✓ envoyer de multiples requêtes vers un serveur internet dans le but de le saturer.

Le ver Blaster avait pour but de lancer une attaque par déni de service sur le serveur de mises à jour de Microsoft. **[9]**

I.3.2.5/ Cheval de Troie :

Un exemple de cheval de Troie est le Trojan.ByteVerify, qui se présente sous la forme d'une applet Java. Ce cheval de Troie exploite une vulnérabilité présente dans la machine virtuelle Java de Microsoft, ce qui permet à un attaquant d'exécuter du code arbitraire sur la machine infectée. Par exemple, Trojan.ByteVerify peut modifier la page d'accueil du navigateur Internet Explorer pour rediriger l'utilisateur vers des sites Web malveillants ou compromettre la sécurité du système.

Il est essentiel de maintenir ses logiciels à jour, d'utiliser des solutions de sécurité fiables et de faire preuve de vigilance lors du téléchargement de fichiers ou de l'ouverture de

pièces jointes pour se protéger contre les chevaux de Troie et autres formes de logiciels malveillants. **[10]**

I.3.2.6/ Le piratage :

Le piratage est l'acte d'identifier puis d'exploiter les faiblesses d'un système ou d'un réseau informatique, généralement dans le but d'obtenir un accès non autorisé à des données personnelles ou d'entreprise. **[9]**

I.3.2.6.1/ Les types de piratage :

- **Piratage chapeau blanc (white hat) :**

Les hackers chapeaux blancs, également appelés **« hackers éthiques »**, sont des spécialistes de la **cybersécurité** qui testent la sécurité des systèmes. **[9]**

Bien qu'un chapeau blanc utilise des méthodes similaires à celles d'un pirate informatique **(cybercriminel**) pour pénétrer un système, il existe une distinction cruciale. **[9]**

- **Piratage chapeau noir (black hat) :**

Les chapeaux noirs sont des criminels qui s'introduisent dans des réseaux informatiques avec des intentions malveillantes. Ils peuvent également publier des logiciels malveillants qui détruisent des fichiers, prennent des ordinateurs en otage ou volent des mots de passe, des numéros de carte de crédit et d'autres informations personnelles. **[9]**

Les chapeaux noirs sont motivés par des raisons intéressées, comme le gain financier, la vengeance ou simplement le désir de semer le chaos. Il peut arriver que leur motivation soit idéologique, en ciblant des personnes avec lesquelles ils sont en profond désaccord. **[9]**

- **Piratage chapeau gris (gray hat) :**

Les chapeaux gris se trouvent à mi-chemin entre les chapeaux noirs et les chapeaux blancs. Les pratiques des chapeaux gris sont un mélange de celles des chapeaux noirs et des chapeaux blancs.

Les chapeaux gris recherchent souvent les failles d'un système sans l'autorisation ni la connaissance du propriétaire. S'ils constatent des problèmes, ils les signalent au propriétaire, en demandant parfois une petite rémunération pour résoudre le problème. **[9]**

I.4/ Les attaques réseaux :

Les attaques réseaux peuvent être classées selon le type de menace, et mises en correspondance avec des méthodes et des outils de piratage associés, à savoir, les attaques

contre le contrôle d'accès, les attaques contre la confidentialité, les attaques contre l'intégrité, les attaques contre l'authentification, et les attaques contre la disponibilité.

I.4.1/ Attaques contre le contrôle d'accès:

Ces attaques tentent de pénétrer dans un réseau en utilisant des mesures de contrôle d'accès WLAN sans fil.

I.4.1.1/ L'attaque « Ad Hoc Associations »:

Les réseaux ad hoc présentent un risque majeur lié à l'écoute électronique. En raison de l'absence de mécanismes de cryptage traditionnels tels que WEP et WPA, les données transmises dans ces réseaux peuvent être interceptées par des attaquants. Pour atténuer ce risque, il est recommandé d'utiliser des protocoles de sécurité tels que WPA2 et de configurer des mots de passe solides. Il est essentiel de prendre des mesures de sécurité appropriées pour protéger les données et prévenir les écoutes électroniques dans les réseaux ad hoc. **[1]**

I.4.1.2/ L'attaque « MAC Spoofing »:

La falsification MAC, également connu sous le nom de spoofing MAC, est une technique permettant de modifier l'adresse de contrôle d'accès aux médias (MAC) attribuée à une interface réseau sur un périphérique. Normalement, l'adresse MAC d'une carte réseau est codée en usine et ne peut pas être modifiée. Cependant, de nombreux pilotes de périphériques réseau permettent de modifier cette adresse MAC.

Le spoofing MAC consiste à faire en sorte que le système d'exploitation croie que la carte réseau a une adresse MAC différente de celle réellement attribuée. Cela peut être fait à l'aide d'outils logiciels spécifiques. En modifiant l'adresse MAC, un ordinateur peut se faire passer pour un autre sur le réseau, masquant ainsi son identité réelle.

Le spoofing MAC peut être utilisé pour diverses raisons, notamment pour contourner les restrictions d'accès basées sur les adresses MAC, pour éviter la détection ou pour mener des attaques réseau. Il est important de noter que le spoofing MAC est relativement facile à réaliser. **[1]**

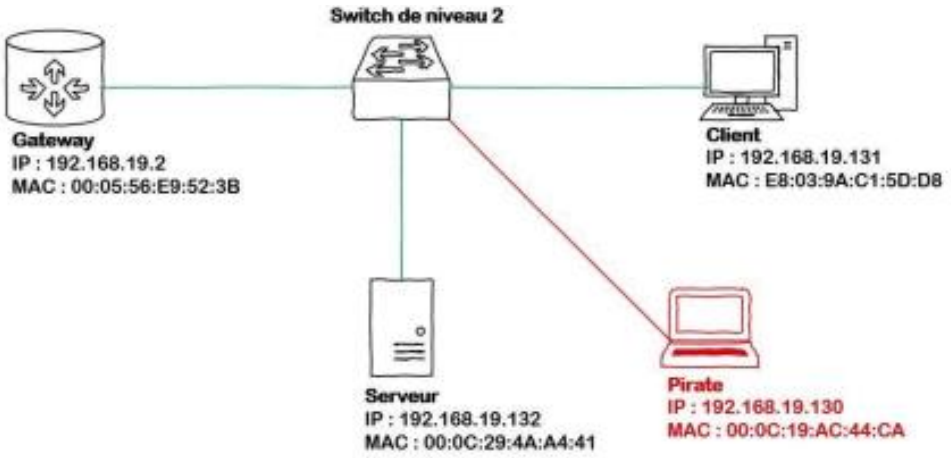


Figure I.2 : L'attaque « MAC Spoofing »

- Comme présenté dans **la Figure I.2**, le changement de l'adresse MAC assignée peut permettre de contourner les listes de contrôle d'accès sur les serveurs ou les routeurs, soit en cachant un ordinateur sur un réseau, soit en la permettant d'imiter un autre périphérique réseau. La falsification MAC est effectuée à des fins légitimes et illicites.

I.4.2/ Attaques contre la confidentialité :

Le rôle des attaques visant la confidentialité des informations, est simplement de casser le modèle de chiffrement utilisée dans le déploiement sans fil.

I.4.2.1/ L'interception :

Une tierce partie non autorisée obtient un accès à un atout. C'est une attaque portée à la confidentialité. Il peut s'agir d'une personne, d'un programme ou d'un ordinateur. Une écoute téléphonique dans le but de capturer des données sur un réseau, ou la copie non autorisée de fichiers ou de programmes en sont des exemples. **[11]**

I.4.2.2/ L'attaque « Man in the Middle»:

L'attaque "Man in the Middle" est une technique où un attaquant s'insère de manière invisible entre deux parties qui communiquent afin d'intercepter, modifier ou falsifier les messages échangés. **[6]**, comme présenté dans la **Figure I.3** :

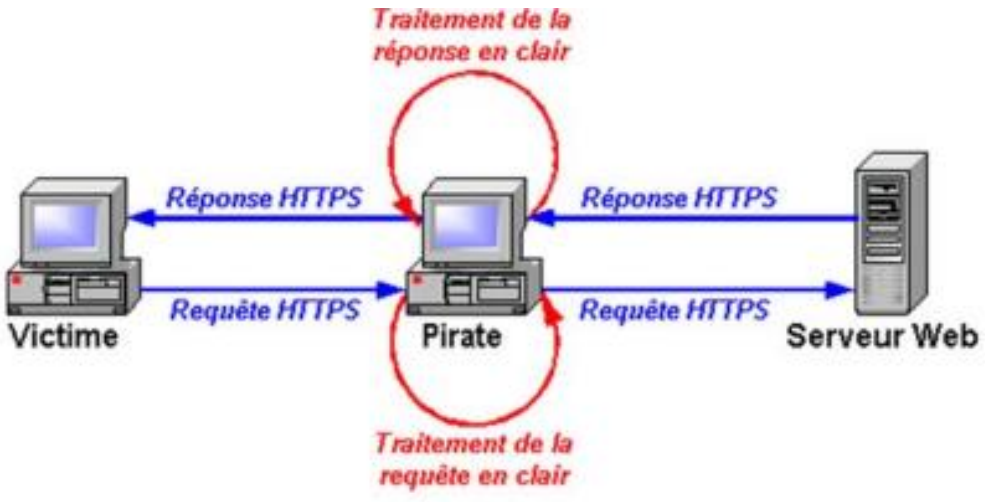


Figure I.3 : L'attaque « Man in the Middle »

Les points sensibles permettant cette technique sont :

- **DHCP** : ce protocole n'est pas sécurisé et un pirate peut fournir à une victime des paramètres réseau qu'il contrôle.
- **ARP** : si le pirate est dans le même sous réseau que la victime et le serveur (même si commutateur), il peut envoyer régulièrement des paquets ARP signalant un changement d'adresse MAC aux deux extrémités.
- **ICMP** : Un routeur peut émettre un ICMP redirect pour signaler un raccourci, le pirate peut alors demander de passer par lui.
- **RIP** : Le pirate envoie une table de routage à un routeur indiquant un chemin à moindre coût et passant par un routeur dont il a le contrôle.
- **DNS** : par « ID spoofing » un pirate peut répondre le premier à la requête de la victime et par « cache poisoning » il corrompt le cache d'un serveur DNS.
- **Proxy http** : Par définition un proxy est en situation d'homme du milieu. Une confiance dans son administrateur est nécessaire de même qu'un contrôle du proxy lors de son départ ! **[6]**

I.4.3/ Attaques contre l'intégrité :

Les attaques contre l'intégrité se basent sur l'envoi des contrôles forgés, de la gestion ou des trames de données sur un réseau sans fil pour induire le destinataire ou faciliter un autre type d'attaque.

I.4.3.1/ modification:

Une tierce partie non autorisée obtient accès à un atout et le modifie de façon (presque) indétectable. Il s'agit d'une attaque portée à l'intégrité.

Changer des valeurs dans un fichier de données, altérer un programme de façon à bouleverser son comportement ou modifier le contenu de messages transmis sur un réseau sont des exemples de telles attaques. **[11]**

I.4.3.2/ l'attaque DoS:

Une attaque **Denial of Service (DoS)** est une tentative d'empêcher les utilisateurs légitimes d'un service d'accéder à ce service. Les attaques **DoS** utilisent souvent les bugs logiciels pour "crasher" ou "geler" un service, ou les limites de bande passante en utilisant une attaque flood pour saturer toute la bande passante.

Un **DDoS (Distributed Denial of Service)** consiste à lancer une attaque **DoS** de nombreux sites contre un seul hôte. Une telle attaque est généralement plus utilisée que les attaques **DoS** pour faire tomber de gros sites corporatif.

Une attaque **DDoS** typique se résume à maître, esclave et victime. Le maître étant l'attaquant, l'esclave étant les systèmes compromis et la victime est bien sûre la cible de l'attaquant. Une fois que l'attaquant envoi une commande spécifique aux systèmes esclaves ou zombis, l'attaque est lancée. **[6]**

I.4.4/ Attaques contre l'authentification :

Les attaquants contre l'authentification utilisent ces attaques pour voler les identités et les informations d'identification des utilisateurs légitimes pour accéder aux réseaux et services privés.

I.4.4.1/ La fabrication:

Une tierce partie non autorisée insère des contrefaçons dans le système. C'est une attaque portée à l'authenticité. Il peut s'agir de l'insertion de faux messages dans un réseau ou l'ajout d'enregistrements à un fichier. **[11]**

I.4.4.2/ Usurpation d'adresses IP :

L'usurpation d'adresse IP consiste à remplacer l'adresse IP de l'expéditeur d'un paquet par une autre. Cette pratique, à la portée des hackers les moins expérimentés, permet essentiellement de protéger leur anonymat et d'abuser de la confiance de leurs cibles.

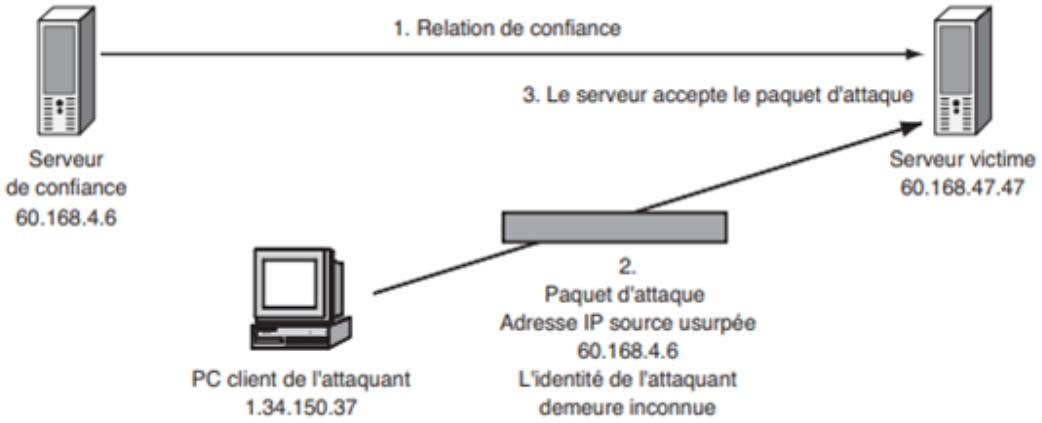


Figure I.4 : Usurpation d'adresses IP

I.4.5/ Attaques contre la disponibilité :

I.4.5.1/ Interruption :

Un atout du système est détruit ou devient indisponible ou inutilisable. C'est une attaque portée à la disponibilité. La destruction d'une pièce matérielle (tel un disque dur), la coupure d'une ligne de communication, ou la mise hors service d'un système de gestion de fichiers en sont des exemples. **[11]**

I.5/ La protection de sécurité informatique:

Un système de protection informatique est un ensemble de techniques et de mesures visant à se protéger contre les attaques et les piratages informatiques. L'objectif principal est d'empêcher la copie non autorisée de contenus sur un support (tel qu'un logiciel) ou de rendre toute intrusion dans le système inutilisable. **[1]**

Les systèmes de protection informatique les plus connus sont :

- Les anti-virus ;
- Les systèmes de détection d'intrusion (IDS) ;
- Les systèmes de détection de prévention (IPS) ;
- Les firewalls ;
- La cryptographie ;

I.5.1/ Les Anti-virus:

Les antivirus sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants (*dont les virus informatique ne sont qu'une catégorie).*

Ces derniers peuvent se baser sur l'exploitation de failles de sécurité, mais il peut également s'agir de logiciels modifiant ou supprimant des fichiers, que ce soit des documents de l'utilisateur stockés sur l'ordinateur infecté, ou des fichiers nécessaires au bon fonctionnement de l'ordinateur (*le plus souvent ceux du système d'exploitation).*

Il est intéressant de noter qu'une fois un fichier infecté, il ne l'est jamais deux fois. En effet, un virus est programmé de telle sorte qu'il signe le fichier dès qu'il est contaminé. On parle ainsi de signature de virus. Cette signature consiste en une suite de bits apposée au fichier. Cette suite, une fois décelée, permettra de reconnaitre le virus.

Lorsque le virus est détecté par l'antivirus, plusieurs possibilités sont offertes pour l'éradiquer :

- ✓ Supprimer le fichier infecté ;
- ✓ Supprimer le code malicieux du fichier infecté ;
- ✓ Placer le ou les fichiers infectés en "quarantaine" pour un traitement futur. **[9]**

I.5.1.1/ Le fonctionnement de l'Anti-virus:

Un logiciel antivirus vérifie les fichiers et courriers électroniques, les secteurs de démarrage (*afin de détecter les virus de boot*), mais aussi la mémoire vive de l'ordinateur, les médias amovibles (*clefs USB, CD, DVD, etc*.), les données qui transitent sur les éventuels réseaux (*dont internet*) **[9]**

Différentes méthodes sont utilisées pour la détection des codes malveillants :

- **Analyse basée sur les signatures** : Les principaux antivirus sur le marché utilisent cette méthode. Ils comparent les signatures virales connues avec les codes à vérifier. Si une correspondance est trouvée, le fichier est considéré comme malveillant. Cependant, cette méthode repose sur des signatures préexistantes et peut manquer de nouveaux codes malveillants pour lesquels aucune signature n'a encore été identifiée. [9]
- **Méthode heuristique :** Cette méthode vise à découvrir des codes malveillants en analysant leur comportement plutôt que de se baser sur des signatures connues. Elle examine le code d'un programme inconnu pour détecter des comportements suspects ou des modèles caractéristiques de malveillance. Cette méthode est plus puissante, mais peut également entraîner de fausses alertes lorsqu'elle identifie à tort un programme légitime comme malveillant. **[9]**

- **Analyse basée sur les règles (Rege-xp) :** Cette méthode repose sur l'utilisation de règles prédéfinies pour filtrer et détecter les codes malveillants. Les règles sont généralement mises en place dans un fichier "Junk" et peuvent être très efficaces pour les serveurs de messagerie électronique qui utilisent des moteurs de filtrage basés sur les expressions régulières (Rege-xp), tels que Postfix. Cette méthode ne repose pas sur des fichiers de signatures, ce qui permet de détecter des variantes de codes malveillants. **[9]**

I.5.2.2/ Techniques de détection des Anti-virus:

En général, la guerre entre virus et antivirus est bien réelle. Dès qu'un groupe agit, le camp opposé tente de trouver la parade. Pour détecter les virus, les antivirus doivent user de plusieurs techniques spécialement :

- **Le scanning des signatures (Dictionnaire) :**

La détection des virus repose sur la recherche de leurs signatures dans une base de données spécifique. Cette méthode permet de détecter les virus avant qu'ils ne causent des dommages. Cependant, il est essentiel que la signature du virus soit présente dans la base de données pour qu'il soit détecté. Il est donc nécessaire de maintenir régulièrement à jour la base de signatures pour pouvoir détecter les nouveaux virus. En résumé, la détection basée sur les signatures offre une protection efficace contre les virus connus, mais nécessite une mise à jour régulière pour détecter les nouvelles menaces. **[9]**

- **Le moniteur de comportement :**

Le moniteur de comportement est une technique de sécurité informatique qui consiste à surveiller en continu les activités suspectes d'un système. Il permet de détecter les lectures et écritures anormales dans des fichiers exécutables, ainsi que les tentatives d'écriture dans les secteurs de partitions et de démarrage du disque. En identifiant ces comportements suspects, le moniteur de comportement peut signaler ou bloquer les actions malveillantes en temps réel, renforçant ainsi la sécurité du système. Cette approche proactive aide à prévenir les attaques informatiques en surveillant activement les activités suspectes et en prenant des mesures appropriées pour les contrer. **[9]**

- **Liste blanche :**

La liste blanche est une technique de plus en plus utilisée pour lutter contre les logiciels malveillants. Plutôt que de rechercher des logiciels connus comme malveillants, cette méthode empêche l'exécution de tout logiciel, à l'exception de ceux qui sont considérés comme fiables par l'administrateur système.

En adoptant cette approche de blocage par défaut, on évite les problèmes liés à la mise à jour des fichiers de signatures de virus et on empêche l'exécution de logiciels indésirables. L'efficacité de cette technique dépend de la capacité de l'administrateur à établir et à maintenir à jour une liste blanche fiable. L'utilisation d'outils d'automatisation des processus d'inventaire et de maintenance peut faciliter cette tâche. **[9]**

- **Le contrôleur d'intégrité :**

Le contrôleur d'intégrité est une méthode utilisée par les antivirus pour maintenir une liste des fichiers exécutables associés à des informations telles que leur taille, leur date de création, leur date de modification ou leur CRC (Contrôle de Redondance Cyclique). L'utilisation du CRC permet de vérifier qu'un fichier exécutable n'a pas été modifié en comparant sa somme de contrôle avant et après son exécution. Cette méthode permet de détecter les modifications non autorisées d'un fichier exécutable.

Cependant, les virus peuvent mémoriser ces valeurs et les restaurer par la suite, ce qui limite l'efficacité du contrôleur d'intégrité. D'autres mesures de sécurité complémentaires sont donc nécessaires pour renforcer la protection contre les logiciels malveillants. **[9]**

I.5.2/ Les systèmes de détection d'intrusion :

Un système de détection d'intrusion (ou **IDS : Intrusion Detection System**) est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte).

Il permet ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions. **[12]**

I.5.2.1/ Typologie de détection d'intrusion :

Il existe trois grandes familles distinctes d'IDS:

I.5.2.1.1/ Les NIDS (IDS réseau) :

Le NIDS **(*Network Based Intrusion Detection System*)** fait partie de l'infrastructure réseau et surveille les paquets qui la traversent. Il coexiste avec les appareils avec une capacité de prise, de répartition ou de mise en miroir comme les commutateurs. NIDS est positionné à un ou plusieurs points stratégiques d'un réseau pour surveiller le trafic entrant et sortant de tous les appareils connectés.

Il analyse le trafic traversant l'ensemble du sous-réseau, en faisant correspondre le trafic passant les sous-réseaux à la bibliothèque d'attaque connue. Une fois que NIDS a identifié les attaques et détecté un comportement anormal, il alerte l'administrateur du réseau.

Vous pouvez installer un NIDS derrière les pare-feu sur le sous-réseau et surveiller si quelqu'un essaie ou non d'infiltrer votre pare-feu. NIDS peut également comparer les signatures de paquets similaires avec des enregistrements correspondants pour lier les paquets malveillants détectés et les arrêter.

Il existe deux types de NIDS :

- Le NIDS en ligne ou le NIDS en ligne traite un réseau en temps réel. Il analyse les paquets Ethernet et applique des règles spécifiques pour déterminer s'il s'agit d'une attaque ou non.
- Le NIDS hors ligne ou le mode tap traite les données collectées. Il passe les données à travers certains processus et décide du résultat. **[13]**

I.5.2.1.2/ Les HIDS (IDS machine) :

Les systèmes de détection d'intrusion basés sur l'hôte **(*HostBased Intrusion Detection System*)** sont la solution qui s'exécute sur des appareils ou des hôtes distincts sur un réseau. Il ne peut surveiller que les paquets de données entrants et sortants des appareils connectés et alerter l'administrateur ou les utilisateurs en cas de détection d'une activité suspecte. Il surveille les appels système, les modifications de fichiers, les journaux d'application, etc.

HIDS prend des instantanés des fichiers actuels dans le système et les fait correspondre aux précédents. S'il constate qu'un fichier critique est supprimé ou modifié, le HIDS envoie une alerte à l'administrateur pour enquêter sur le problème.

Par exemple, HIDS peut analyser les connexions par mot de passe et les comparer aux modèles connus utilisés pour effectuer **attaques par force brute** et identifier une brèche.

Ces solutions IDS sont largement utilisées sur des machines critiques dont les configurations ne devraient pas changer. Comme elle surveille les événements directement sur les hôtes ou les appareils, une solution HIDS peut détecter les menaces qu'une solution NIDS pourrait manquer. **[13]**

I.5.2.1.3/ Les IDS hybride :

Les IDS hybrides sont basés sur une architecture distribuée, où chaque composant unifie son format d'envoi d'alerte **(*typiquement IDMEF : IntrusionDetection Message Exchange Format*)** permettant à des composants divers de communiquer et d'extraire des alertes plus pertinentes.

Les avantages des IDS hybrides sont multiples :

- Moins de faux positifs ;
- Meilleure corrélation ;
- Possibilité de réaction sur les analyseurs. **[13]**

I.5.2.2/ Techniques d'analyse de trafic des IDS :

Il existe principalement deux techniques d'analyse du trafic, chacune ayant des avantages et des inconvénients :

- **L'analyse comportementale (*AIDS: Anomaly Intrusion Detection System*) :**

À partir d'un comportement normal déterminé, l'IDS analyse le comportement des machines. Si un ordinateur se connecte en pleine nuit alors que personne n'est présent, cela pourrait lever une alerte pour l'IDS. Ainsi, dans ce type d'analyse, un profil est dressé et lorsque la machine liée s'éloigne du profil type, l'IDS réagit. **[14]**

- **Avantage** : ce type d'analyse permet de détecter des attaques inconnues, elle ne nécessite pas de base de données.
- **Inconvénient** : cette détection est assez aléatoire, elle peut produire de fausses alertes relativement facilement. **[14]**

- **L'analyse par scénario (*MIDS: Misuse Intrusion Detection System*) :**

L'IDS utilise ici une base de données de signatures d'attaques. Ces signatures peuvent être assimilées à des déroulements d'attaques. En effet, chaque attaque possède des caractéristiques propres (*numéro de port, taille de paquet, protocole employé...).*

Ces caractéristiques peuvent être collectées et placées dans une base de données Qu'interrogera l'IDS. Ce type d'IDS utilise les fichiers journaux (log). Dès qu'il détectera des séquences suspectes (*relatives à une signature de sa base de données*), il déclenchera une alerte. **[14]**

- **Avantage** : on peut gérer les attaques de façon très précise.
- **Inconvénient** : on doit maintenir une base de données à jour. **[14]**

I.5.3/ Les systèmes de prévention des intrusions (IPS) :

Le système de prévention des intrusions (IPS) est également appelé système de détection et de prévention des intrusions (IDPS).

Il s'agit d'une solution logicielle qui surveille les activités d'un système ou d'un réseau à la recherche d'incidents malveillants, enregistre des informations sur ces activités, les signale à l'administrateur ou au personnel de sécurité et tente de les arrêter ou de les bloquer. **[15]**

I.5.3.1/ Typologie de systèmes des préventions des intrusions:

En général, les systèmes de prévention des intrusions (IPS) sont de quatre types :

I.5.3.1.1/ Les NIPS:

NIPS peut identifier et empêcher les activités suspectes ou malveillantes en analysant les paquets de données ou en vérifiant l'activité du protocole sur l'ensemble d'un réseau. Il peut collecter des données du réseau et de l'hôte pour détecter les hôtes, les systèmes d'exploitation et les applications autorisés sur le réseau. De plus, NIPS enregistre les données sur le trafic normal pour trouver des changements à partir de zéro. Cette solution IPS atténue les attaques en limitant l'utilisation de la bande passante, en envoyant des connexions TCP ou en rejetant des paquets. Cependant, NIPS n'est pas efficace pour analyser le trafic chiffré et gérer les attaques directes ou les charges de trafic élevées. **[16]**

I.5.3.1.2/ Les WIPS:

WIPS peut surveiller un réseau sans fil pour détecter le trafic ou les activités suspectes en analysant les protocoles de réseau sans fil et en prenant des mesures pour les empêcher ou les supprimer. WIPS est généralement implémenté en superposant l'infrastructure de réseau LAN sans fil actuelle.

Cependant, vous pouvez également les déployer de manière autonome et appliquer une politique sans fil dans votre organisation.

Cette solution IPS peut empêcher les menaces comme un point d'accès mal configuré, attaques par déni de service (DOS), pot de miel, usurpation MAC, attaques de l'homme du milieu, et plus encore. **[16]**

I.5.3.1.3/ Les NBA:

NBA fonctionne sur la détection d'anomalies, en recherchant des anomalies ou des écarts entre un comportement normal et un comportement suspect dans le réseau ou le système. Par conséquent, pour que cela fonctionne, la NBA doit passer par une période de formation pour apprendre le comportement normal d'un réseau ou d'un système.

Une fois qu'un système NBA apprend le comportement normal, il peut détecter les écarts et les signaler comme suspects. C'est efficace, mais cela ne fonctionnera pas pendant la phase d'entraînement. Cependant, une fois diplômé, vous pouvez compter sur lui. **[16]**

I.5.3.1.4/ Les HIPS :

Les solutions HIPS peuvent surveiller les systèmes critiques à la recherche d'activités malveillantes et les empêcher en analysant le comportement de leur code. Ce qu'il y a de mieux avec eux, c'est qu'ils peuvent également détecter les attaques cryptées en plus de protéger les données sensibles liées à l'identité personnelle et à la santé des systèmes hôtes. Il fonctionne sur un seul appareil et est souvent utilisé avec un IDS ou IPS basé sur le réseau. **[16]**

- ***Comment fonctionne un IDS ?***

IDS utilise trois méthodes de détection pour surveiller le trafic à la recherche d'activités malveillantes :

- **Détection basée sur les signatures ou basée sur les connaissances :**

La détection basée sur les signatures consiste à surveiller des modèles spécifiques tels que les signatures de logiciels malveillants ou les séquences d'octets dans le trafic réseau. Elle fonctionne de manière similaire à un logiciel antivirus en identifiant les menaces par leur signature. L'avantage de cette méthode est qu'elle permet d'identifier facilement les menaces connues. Cependant, elle peut être moins efficace contre les nouvelles attaques pour lesquelles aucun modèle ou signature n'est disponible. En effet, la détection basée sur les signatures repose uniquement sur des modèles d'attaque ou des signatures antérieures, ce qui limite sa capacité à détecter les attaques inconnues ou émergentes. **[17]**

- **Détection basée sur les anomalies ou basée sur le comportement :**

Dans la détection basée sur les anomalies, l'IDS surveille les violations et les intrusions en examinant les journaux du système et en identifiant les activités qui semblent anormales par rapport au comportement habituel d'un appareil ou d'un réseau. Cette méthode permet de détecter les cyberattaques inconnues. Pour accomplir cette tâche, l'IDS peut utiliser des techniques d'apprentissage automatique pour créer un modèle fiable du comportement normal, qui servira de référence pour comparer de nouvelles activités et détecter les anomalies.

Les modèles d'IDS basés sur les comportements peuvent être entraînés selon les configurations matérielles, les applications et les besoins spécifiques du système. Par conséquent, ils offrent une meilleure sécurité par rapport aux IDS basés sur les signatures. Bien qu'ils puissent parfois générer des faux positifs, ils sont efficaces dans de nombreux autres aspects. **[17]**

- **Détection basée sur la réputation :**

L'IDS basé sur la réputation est une méthode de détection qui utilise les niveaux de réputation pour reconnaître les menaces. Il analyse la communication entre un hôte amical à l'intérieur du réseau et un autre hôte qui tente d'accéder au réseau, en se basant sur la réputation de ce dernier en termes de violations ou d'actions malveillantes.

Pour ce faire, il collecte et suit différents attributs de fichier tels que la source, la signature, l'âge et les statistiques d'utilisation des utilisateurs qui utilisent le fichier. En

utilisant un moteur de réputation avec des analyses statistiques et des algorithmes, il analyse les données pour déterminer si elles représentent une menace ou non.

L'IDS basé sur la réputation est principalement utilisé dans les logiciels anti-malware ou antivirus, et il est mis en œuvre sur des fichiers batch, des fichiers exécutables et d'autres fichiers susceptibles de contenir un code dangereux. **[17]**

- ***Comment fonctionne un IPS ?***

Semblable à l'IDS, IPS fonctionne également avec des méthodes telles que la détection basée sur les signatures et les anomalies, en plus d'autres méthodes.

- **Détection basée sur les signatures:**

Les solutions IPS (Intrusion Prevention System) utilisant la détection basée sur les signatures surveillent les paquets de données entrants et sortants dans un réseau, en le comparant à des modèles d'attaque ou à des signatures précédemment connues. Elles s'appuient sur une bibliothèque de modèles connus contenant des menaces contenant un code malveillant. Lorsqu'un exploit est découvert, l'IPS enregistre et stocke sa signature, puis l'utilise ultérieurement pour la détection.

Il existe deux types d'IPS basés sur les signatures :

- **Signatures d'exploits :** L'IPS identifie les intrusions en comparant les signatures avec celles des menaces présentes dans le réseau. Lorsqu'une correspondance est trouvée, l'IPS tente de la bloquer.
- **Signatures de vulnérabilité :** Les pirates ciblent les vulnérabilités existantes dans votre réseau ou système, et l'IPS cherche à protéger votre réseau contre ces menaces qui pourraient passé inaperçues. **[17]**

- **Détection statistique basée sur les anomalies ou basée sur le comportement :**

L'IDS utilisant la détection statistique basée sur les anomalies surveille le trafic réseau à la recherche d'incohérences ou d'anomalies. Il établit une ligne de base pour définir le comportement normal du réseau ou du système, puis compare le trafic réseau à cette ligne de base pour détecter les activités suspectes qui s'écartent du comportement habituel.

Par exemple, la ligne de base peut être une bande passante spécifiée ou un protocole utilisé dans le réseau. Si l'IDS détecte une augmentation soudaine de la bande passante ou l'utilisation d'un protocole différent, il déclenchera une alarme et bloquera éventuellement le trafic. **[17]**

- **Analyse de protocole avec état:**

Un IPS (Intrusion Prevention System) utilisant une analyse de protocole avec état détecte les divergences par rapport à l'état attendu d'un protocole, similaire à la détection basée sur les anomalies. Il utilise des profils universels prédéfinis en conformité avec les meilleures pratiques établies par les leaders de l'industrie et les fournisseurs.

L'IPS examine les flux de données en analysant les protocoles réseau et en vérifiant que les communications respectent les règles et les états définis pour chaque protocole spécifique. Si des écarts sont détectés, cela peut indiquer une activité suspecte ou potentiellement malveillante. L'IPS peut alors prendre des mesures pour bloquer ou prévenir cette activité. **[17]**

I.5.4/ Les Firewalls (PARE-FEU) :

Un pare-feu, également connu sous le nom de coupe-feu, garde-barrière, barrière de sécurité ou firewall, est un logiciel et/ou un matériel utilisé pour appliquer la politique de sécurité d'un réseau. Dans un environnement Unix BSD (Berkeley Software Distribution), il sert à définir quels types de communications sont autorisés sur le réseau informatique.

Le principal objectif d'un pare-feu est de surveiller et contrôler les applications et les flux de données (paquets), en empêchant les connexions non autorisées sur le réseau informatique. Il agit comme une barrière de protection en filtrant le trafic entrant et sortant, en vérifiant les règles de sécurité prédéfinies et en autorisant uniquement les communications conformes à la politique de sécurité. **[9]**

Un pare-feu peut être configuré à différents niveaux pour contrôler l'accès au réseau et filtrer les flux de données. Voici quelques exemples de niveaux de configuration :

- **Niveau des adresses IP :** Le pare-feu peut être configuré pour accepter ou bloquer les flux de données provenant d'une plage d'adresses IP spécifique ou même d'une adresse unique.
- **Niveau des noms de domaine :** Il est possible de restreindre l'accès à certaines adresses Internet en utilisant des noms de domaine.
- **Niveau des protocoles :** Le pare-feu peut être configuré pour bloquer ou autoriser certains protocoles tels que FTP, Telnet ou HTTP, limitant ainsi les types de communications réseau autorisées.
- **Niveau des ports :** En spécifiant des règles au niveau des ports, il est possible de refuser les connexions sur des ports spécifiques, comme le port 21 pour le FTP.
- **Niveau des mots ou phrases :** Le pare-feu peut être configuré pour détecter et bloquer les paquets contenant des mots ou des phrases spécifiques, similaires à l'utilisation des expressions régulières. **[9]**

Figure I.5 : Structure simple d'un pare-feu

D'une manière concrète, un pare-feu un système matérielle et immatérielle dédiée au routage entre LAN et Internet. Le trafic est analysé au niveau des datagrammes IP (adresse, utilisateur, contenu...).

Un datagramme non autorisé sera simplement détruit, IP sachant gérer la perte d'information. Une translation d'adresse pourra éventuellement être effectuée pour plus de sécurité (protocole NAT Network Address Translation). Deux types d'architectures peuvent être exploités -l'architecture classique et l'architecture concentrée :

- **L'architecture classique :**

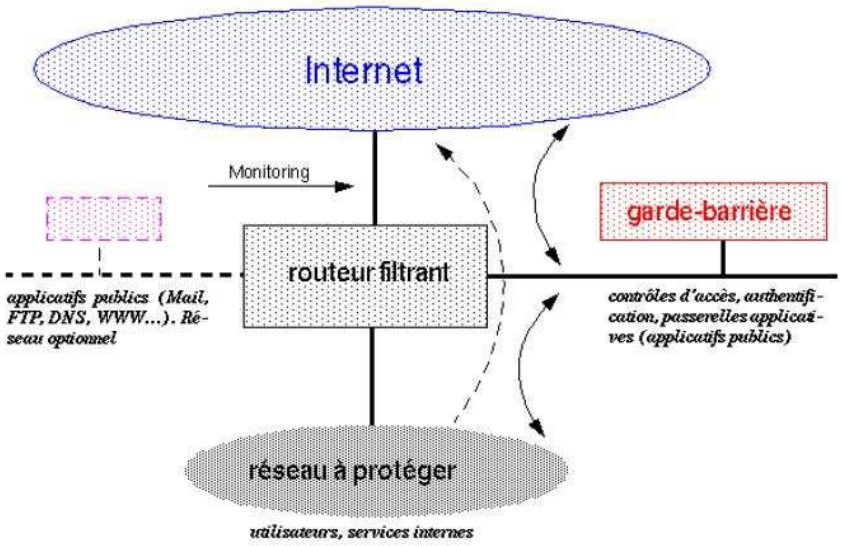


Figure I.6 : L'architecture classique

- **L'architecture concentrée :**

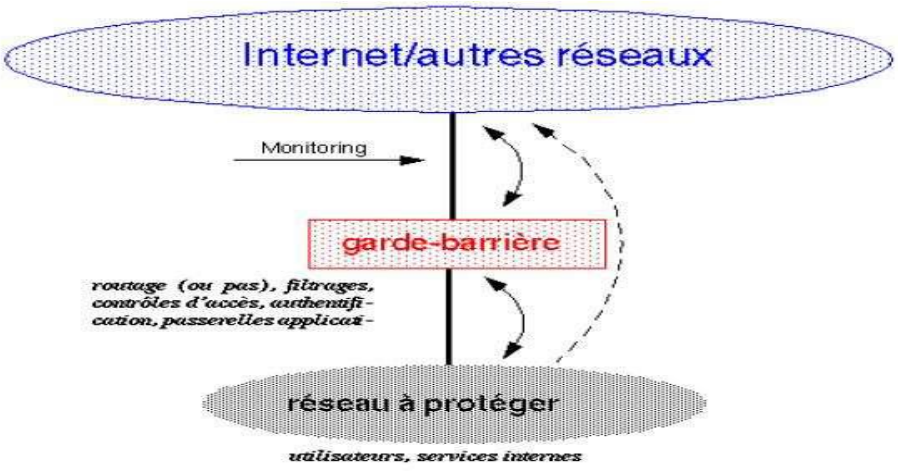


Figure I.7 : L'architecture concentrée

I.5.4.1/ Principes de fonctionnement des Pare-feux :

Le pare-feu a longtemps été considéré comme une composante essentielle de la sécurité d'un réseau informatique, bien que son importance ait diminué ces dernières années avec la généralisation de l'utilisation du protocole HTTP sur TLS, qui court-circuite en grande partie les mécanismes de filtrage traditionnels.

Son rôle principal est d'appliquer une politique d'accès aux ressources réseau, en contrôlant le trafic entre différentes zones de confiance et en filtrant les flux de données qui y circulent. Les principales zones de confiance incluent généralement Internet (une zone de confiance minimale) et au moins un réseau interne (une zone de confiance plus élevée).

L'objectif est de fournir une connectivité contrôlée et sécurisée entre les différentes zones de confiance, en appliquant une politique de sécurité et en utilisant un modèle de connexion basé sur le principe du moindre privilège. Cela permet de limiter les accès non autorisés, de protéger les ressources internes et de prévenir les attaques provenant de l'extérieur du réseau. **[9]**

On peut alors distinguer 3 types de principes de fonctionnement des pare-feux :

- **Le filtrage de paquets (Packet Filtering) :**

Lors de l'analyse des paquets, le pare-feu les compare à un ensemble de filtres ou règles spécifiées dans sa table des autorisations. Les champs IP, TCP/UDP des paquets sont examinés et confrontés à ces règles. En fonction des règles configurées par l'administrateur réseau, les paquets sont soit rejetés, soit acceptés et transmis au réseau interne.

Les critères couramment utilisés pour le filtrage comprennent l'origine et la destination des paquets (èadresse IP, ports TCP ou UDP, interface réseau), les options contenues dans les données (fragmentation, validité), les caractéristiques des données elles-mêmes (taille, correspondance à un motif) et, plus récemment, les utilisateurs.

Le filtrage par paquet présente l'avantage de la rapidité et de la simplicité d'implémentation dans un réseau. Cependant, il ne peut pas constituer à lui seul une mesure de sécurité complète. D'une part, maintenir un niveau élevé de sécurité devient difficile à mesure que le nombre de règles augmente. D'autre part, ce type de filtrage est limité dans son accès aux informations, car il identifie seulement la machine et non l'utilisateur. **[9]**

- **Le filtrage du flux (Circuit Filtering) :**

Le filtrage de flux, contrairement au filtrage de paquets, ne prend pas en compte le contenu des paquets lorsqu'ils transitent sur la connexion. Par conséquent, il ne peut pas être utilisé pour assurer l'authentification des parties ou la sécurité du protocole utilisé pour la connexion.

Le filtrage de flux est restrictif et ne permettra le flux entre deux entités que si une connexion existe entre elles. On peut le voir comme la création d'un tunnel sécurisé entre deux machines. En conséquence, le filtrage de flux est souvent utilisé en complément d'une passerelle applicative (application gateway).

L'application gateway, également appelée proxy, est responsable de l'analyse en profondeur du contenu des paquets et de l'application de politiques de sécurité plus avancées, telles que l'authentification, la validation des protocoles et la gestion des flux de données. **[9]**

- **La passerelle applicative (Application Gateway) :**

À la différence du filtrage de paquets, qui analyse les paquets individuellement, l'application Gateway permet de limiter les commandes à un service plutôt que de les interdire complètement.

Le fonctionnement de l'application Gateway empêche le trafic direct entre le réseau protégé et Internet dans les deux sens. Ainsi, aucun trafic interne n'atteindra Internet et aucun trafic Internet ne pourra circuler sur le réseau interne.

Dans ce principe, chaque client interne se connecte à un serveur proxy qui joue un rôle central. Toutes les communications passent par ce serveur proxy, qui détermine si le service demandé par l'utilisateur est autorisé. En cas d'autorisation, le serveur proxy se connecte au destinataire pour établir la communication. **[9]**

I.5.4.2/ Catégorie de Pare-feu :

Il existe 3 modèles de firewalls. Chacun possède des avantages et désagréments. Il faudra donc préalablement analyser les besoins réels en termes de sécurité, ainsi que les coûts engendrés avant toute utilisation :

- **Les firewalls Bridge** :

Les firewalls de type Bridge se présentent sous la forme d'un simple câble réseau, sans dispositif distinct. Ils sont invisibles et indétectables pour les pirates, car leur adresse MAC ne circule jamais sur le réseau. Ces firewalls sont généralement intégrés aux switches et agissent en tant que passerelle obligatoire pour toutes les requêtes réseau.

Les firewalls Bridge offrent plusieurs avantages. Ils sont relativement peu coûteux et faciles à déployer, car ils ne nécessitent pas de configuration spécifique. De plus, ils fonctionnent de manière transparente, sans perturber les connexions réseau existantes.

Cependant, ces firewalls ont quelques inconvénients. Il est possible de contourner leurs protections en adaptant les attaques pour éviter leur détection. De plus, les fonctionnalités offertes par les firewalls Bridge sont souvent limitées par rapport à d'autres types de pare-feu plus avancés. **[9]**

- **Les firewalls hardware :**

Les firewalls hardware sont des boîtes noires avec un accès limité à leur code. Ils offrent une intégration facile au réseau, une administration simplifiée et un niveau de sécurité élevé. Cependant, leur caractère propriétaire restreint les mises à jour et les modifications. Les mises à jour dépendent entièrement du constructeur et les possibilités de modification sont limitées en raison de l'architecture matérielle. Malgré ces inconvénients, les firewalls hardware sont appréciés pour leur efficacité et leur simplicité d'utilisation. **[9]**

- **Les firewalls logiciels:**

Les pare-feu logiciels sont disponibles à la fois sous forme commerciale et gratuite. La sécurité peut varier considérablement, indépendamment de leur origine. Les logiciels commerciaux peuvent mettre l'accent sur la facilité d'installation et de configuration, mais

cela peut se faire au détriment de la sécurité. En revanche, les logiciels gratuits et/ou open source offrent souvent plus de flexibilité et d'options, mais nécessitent généralement de bonnes connaissances en réseautage pour être configurés de manière optimale sans compromettre la sécurité. Il est donc important de choisir un pare-feu qui correspond à vos besoins de sécurité spécifiques tout en tenant compte de vos compétences et ressources disponibles pour sa configuration et sa gestion. **[9]**

I.5.5/ la cryptographie :

La définition formelle de la cryptographie pourrait être notée de diverses manières. La cryptographie est essentiellement la science qui utilise une logique mathématique pour maintenir l'information sécurisée. Elle permet à quelqu'un de stocker de manière sécurisée de informations sensibles ou de transmettre des informations de manière sécurisée à travers des réseaux peu sûrs pour éviter qu'ils ne soit piraté, masqué ou modifié. **[9]**

I.5.5.1/ Terminologie:

- **Plaintext (Texte en Clair):**
  C'est l'information qu'un expéditeur veut transmettre à un récepteur.
- **Encryptions (Cryptage):**
  Le cryptage est la procédure d'encodage de messages (ou d'informations) de telle sorte que les écoutes ou les pirates ne peuvent pas le lire, mais les parties autorisées peuvent.
- **Ciphertext (Texte chiffré) :**
  Le texte chiffré est le résultat du cryptage effectué en texte clair à l'aide d'un algorithme appelé un chiffrement.
- **Cipher (chiffrement):**
  Un chiffrement est un algorithme pour l'exécution du cryptage ou du décryptage - une série d'étapes bien définies qui peuvent être suivies comme une procédure.
- **Decryption (Décryptage) :**
  Il s'agit du processus de décodage du texte chiffré et de le récupérer dans le format en texte clair.
- **Cryptographic key (Clé cryptographique):**
  Généralement, une clé ou un ensemble de clés est impliqué dans le cryptage d'un message.
  Une clé identique ou un ensemble de clés identiques est utilisé par la partie légitime pour décrypter le message. Une clé est une information (ou un paramètre) qui détermine la sortie fonctionnelle d'un algorithme ou d'un chiffrement cryptographique. **[1]**

I.5.5.2/ La cryptographie symétrique :

La cryptographie symétrique (ou le cryptage des clés symétriques) est une classe d'algorithmes de cryptographie qui utilisent les mêmes clés cryptographiques pour le cryptage du texte clair et le décryptage du texte chiffré. **[9]**

FigureI.7 montre l'aperçu des étapes de la cryptographie symétrique.

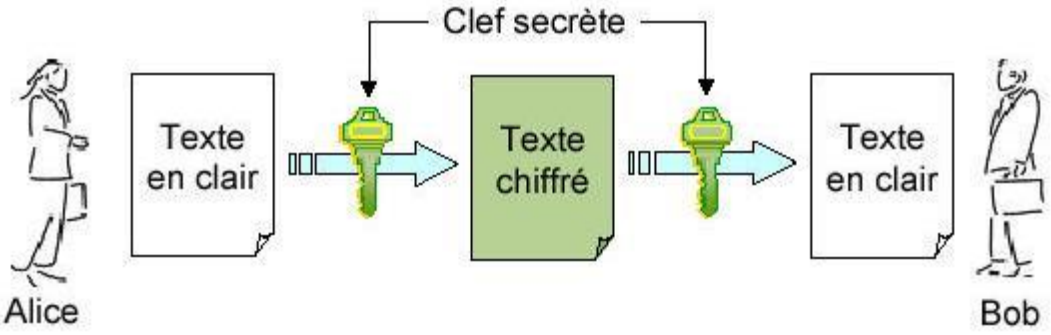


Figure I.8 : Modèle opérationnel de la cryptographie symétrique

I.5.5.2.1/ Le chiffrement AES:(Advanced Encryption Standard) :

Est une norme ou spécification de chiffrement comme RSA, DES. On peut aussi le nomme **Rijndael** qui est le nom de créateur.

C'est un chiffrement par bloc, le nombre de blocs est indiqué par le numéro : **AES-128, AES-192 ou encore AES-256**.

AES est implémentation dans des logiciels et du matériel à travers le monde pour chiffrer les données sensibles. Il est essentiel pour la sécurité informatique, la cybersécurité et la protection des données électroniques.

Mais on le trouve de plus en plus tous les jours pour le chiffrement de base de données ou de stockage de données. **[1]**

- **Comment ça marche :**

Le chiffrement AES est un chiffrement symétrique. C'est-à-dire qu'une meme clé permet de chiffrer et de déchiffrer le contenu. Le schéma suivant explique comment AES permet de chiffrer et déchiffrer symétriquement des données. **[1]**

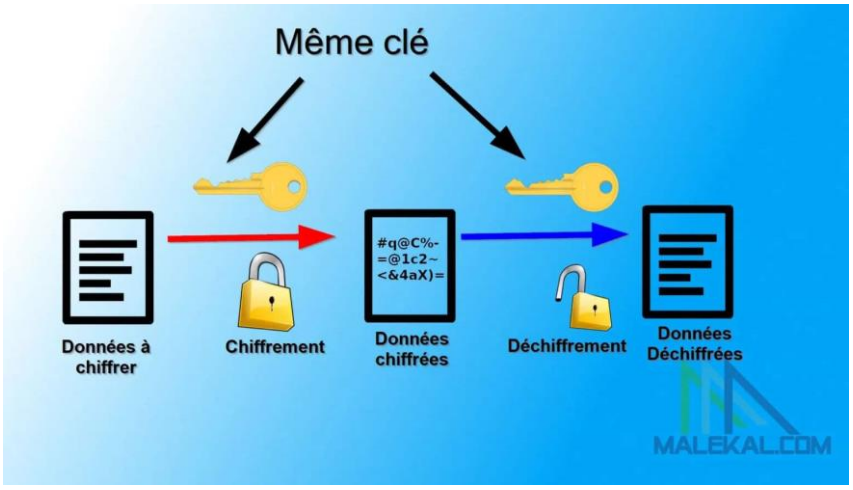


Figure I.9 : Le chiffrement AES

I.5.5.3/ La cryptographie asymétrique :

La cryptographie à clé publique (PKC), également appelée cryptographie asymétrique, se réfère à un algorithme cryptographique qui nécessite deux clés distinctes, dont l'une est secrète (ou privée) et l'autre public.

Bien que différentes, les deux parties de cette paire de clés sont liées mathématiquement. **[9]**

La **Figure I.10** montre une vue d'ensemble des opérations PKC.

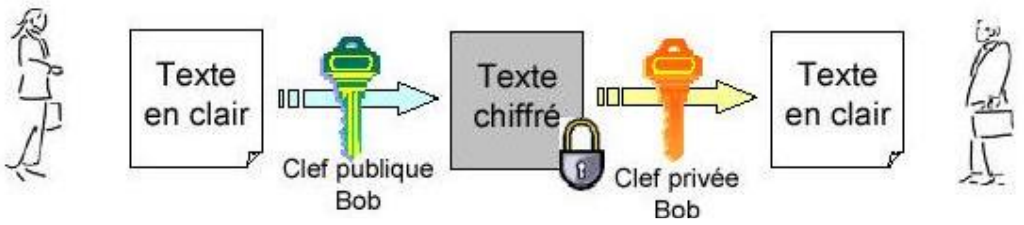


Figure I.10 : Modèle opérationnel de la cryptographie asymétrique (PKC)

La cryptographie à clé publique permet le **cryptage et décryptage**. Ces deux opérations permettent à deux parties communicantes de déguiser les données qu'elles se transmettent. L'expéditeur crypte les données avant de les envoyer via un support de communication. Le récepteur décrypte ou déchiffre les données après leur réception. Tandis que pendant la transmission, les données cryptées ne sont pas comprises par un tiers illégitime. **[9]**

I.5.5.3.1)-Le chiffrement RSA :

Le chiffrement RSA est un algorithme de cryptographie asymétrique, qui est très utilisé dans le commerce électronique, et plus généralement pour échanger des données confidentielles sur Internet. Cet algorithme a été décrit en 1977 par Ronald Rivest, Adi Shamir et Leonard Adleman.

- Le chiffrement RSA utilise une paire de clés (des nombres entiers) composée d'une clé publique pour chiffrer et d'une clé privée pour déchiffrer des données confidentielles.
- Les deux clés sont créées par une personne, souvent nommée par convention.
- Alice, qui souhaite que lui soient envoyées des données confidentielles. **[18]**

➢ **Fonctionnement RSA :**

L'algorithme RSA se base sur trois étapes, à savoir :

a. Création des clés:

L'étape de création des clés est à la charge d'Alice. Elle n'intervient pas à chaque chiffrement car les clés peuvent être réutilisées, la difficulté première, que ne règle pas le chiffrement, est que Bob soit bien certain que la clé publique qu'il détient est celle d'Alice. Le renouvellement des clés n'intervient que si la clé privée est compromise, ou par précaution au bout d'un certain temps.

1/ Choisir *p* et *q*, deux nombres premiers distincts ;
2/ calculer leur produit $n = pq$, appelé *module de chiffrement* ;
3/ calculer $\varphi(n) = (p - 1)(q - 1)$ (c'est la valeur de l'indicatrice d'Euler en *n*) ;
4/ choisir un entier naturel *e* premier avec $\varphi(n)$ et strictement inférieur à $\varphi(n)$, appelé *exposant de chiffrement* ;
5/calculer l'entier naturel *d*, inverse de *e* modulo $\varphi(n)$, et strictement inférieur à $\varphi(n)$, appelé *exposant de déchiffrement* ; *d* peut se calculer efficacement par l'algorithme d'Euclide étendu.
Le couple (*n*, *e*) est la *clé publique* du chiffrement, alors que le nombre *d'*est sa *clé privée*, sachant que l'opération de déchiffrement ne demande que la clef privée *d* et l'entier *n*, connu par la clé publique (la clé privée est parfois aussi définie comme le triplet (*p, q, d*)). **[18]**

b. Chiffrement du message :

Si *M* est un entier naturel strictement inférieur à *n* représentant un message, alors le message chiffré sera représenté par $C \equiv M^e \pmod n$. L'entier naturel *C* étant choisi strictement inférieur à *n*. **[18]**

c. Déchiffrement du message :

Pour déchiffrer *C*, on utilise *d*, l'inverse de *e* modulo $(p - 1)(q - 1)$, et l'on retrouve le message clair *M* par $M \equiv C^d \pmod n$. **[18]**

I.6/ Conclusion :

Le message que nous avons essayé le passer dans ce chapitre est que nous vivons dans un monde où le système d'information prenant une place très importante, Alors il doit de connaisse les différentes risques et les menaces.

Dans notre chapitre, Nous ne nous sommes pas seulement concentrés sur les problèmes de sécurité informatique mais aussi sur leurs solutions et comment les gérer.

Chapitre II

Etat de l'art autour de la cryptographie

II.1/ Introduction :

La cryptographie à base d'ADN est un domaine de recherche émergent qui explore les possibilités d'utiliser l'ADN comme support pour le chiffrement et la sécurité des données. Cette approche multidisciplinaire combine plusieurs domaines scientifiques tels que la sécurité de l'information, la biologie moléculaire, la bio-informatique et le calcul biomoléculaire. **[19]**

L'ADN, connu pour sa capacité à stocker des données biologiques alors nous pouvons exploiter cet avantage en stéganographie et en cryptographie comme matériau de stockage. Les brins d'ADN synthétiques contenant les données chiffrées peuvent être conservés de manière sécurisée, permettant ainsi de protéger les informations confidentielles.

La stéganographie à base d'ADN présente également un large éventail d'applications potentielles, elle consiste à cacher des informations à l'intérieur de la séquence nucléotidique de l'ADN. Elle peut être utilisée dans le domaine de la sécurité pour le transfert clandestin d'informations sensibles, offrant ainsi une méthode discrète de communication. De plus, la stéganographie à base d'ADN peut être utilisée pour le stockage à long terme des données, exploitant la stabilité de l'ADN pour préserver les informations sur de longues périodes.

Dans ce chapitre, nous présenterons quelques notions de base de l'ADN, sa fonction, sa structure avec tous ses caractéristiques biologiques, ensuite nous allons aborder la cryptographie ADN, dans laquelle nous explorerons ce domaine en détail et expliquerons comment les avantages de l'ADN sont exploités dans le domaine de la cryptographie à l'ADN, puis nous discuterons la stéganographie ADN, les avantages et les défis de cette approche.

II.2/ Notion de base de l'ADN :

Le nom biochimique : l'acide désoxyribonucléique

II.2.1/ Définition :

L'ADN est le support de notre information génétique, également celui de l'hérédité. On peut définir l'ADN comme suit, est une molécule biologique qui présente l'information génétique d'un individu et qui définit leur caractéristique et leur fonctionnalité.

Une molécule d'ADN contient plusieurs nucléotides associées au désoxyribose, chaque nucléotide se compose de trois composantes essentielles à savoir : une sucre pentose, un ensemble de phosphate et des bases azotées. **[20]**

La figure suivante donne un aperçu de l'ADN :

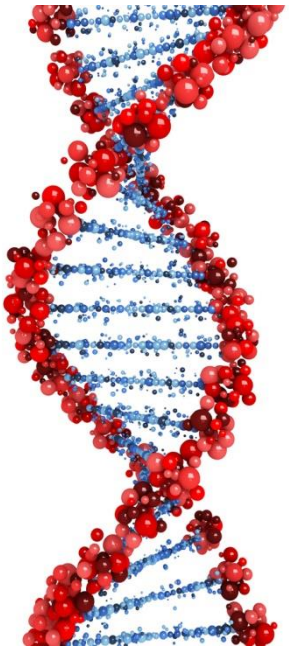


Figure II.1 : ADN- vue globale-

II.2.2/ un peu d'histoire sur l'ADN :

Les acides nucléaires ont été observés pour la première fois en 1869 par le chimiste suisse ***Friedrich Miescher***. Il a détecté dans le noyau des cellules vivantes une substance riche en phosphate, qui a été nommée au 20e siècle **« ADN ».**

En 1882 ***Walther Flemming***, met en évidence Les chromosomes qui compose de molécules d'ADN et qui regroupe plusieurs gènes. Pour la première fois, il décrit **la mitose**. Lequel les cellules se divisent et permettent la croissance et le renouvellement cellulaires.

Puis, en 1952, les scientifiques chercheurs ***James Watson*** le biologiste américain et ***Francis Crick*** le physicien anglais déterminent la structure en double hélices de l'ADN**. [21]**

II.2.3/ La fonction de l'ADN :

L'ADN est présent dans chaque cellule de notre corps. Il est organisé sous forme de chromosomes dans le noyau des cellules. C'est une molécule allongé doté de super pouvoir, son code chimique contient la totalité des informations qui détermine nos caractéristiques.

L'ADN sert principalement à stocker, à transmettre et à transcrire l'information génétique nécessaire à la synthèse des protéines. **[20]**

a) Stocker l'information génétique : il contient l'ensemble des gènes qui déterminent les caractéristiques héréditaire de l'être vivant comme la couleur des yeux, la taille..Etc. **[20]**

b) Transmission de l'information génétique : l'ADN est transmis des parents à leurs descendances. Chaque parent contribue avec une moitié de son ADN, ce qui permet une combinaison unique de l'information génétique dans chaque individu. **[20]**

c) Réplication de l'ADN : La réplication de l'ADN est le processus par lequel une molécule d'ADN existante est copiée pour produire une version identique de lui-même. Ce processus est très important pour la transmission de l'information génétique lors de la division cellulaire et de la reproduction. **[20]**

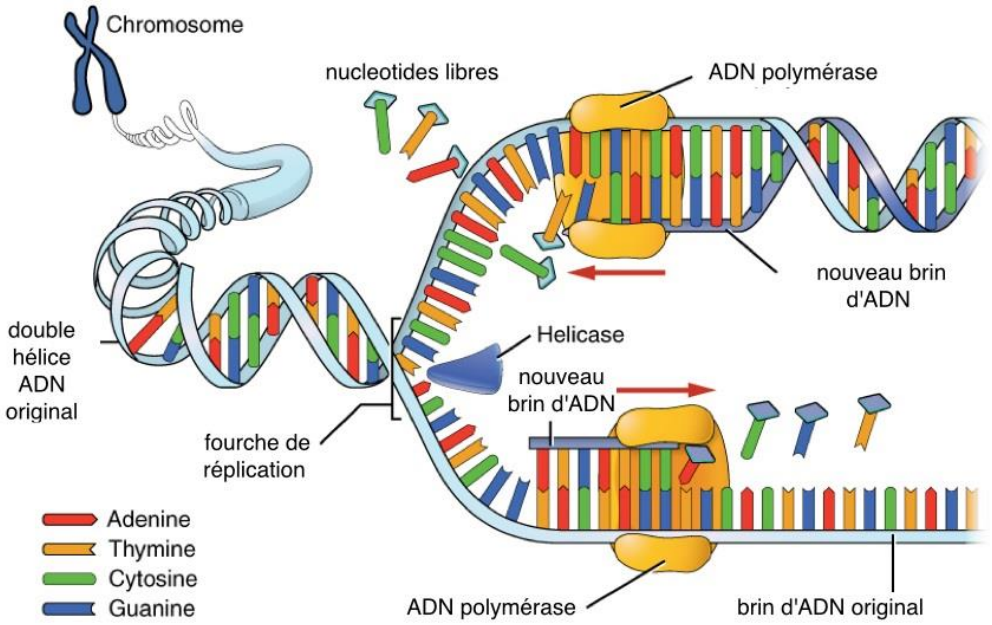


Figure II.2 : La réplication de l'ADN

d) Transcription et traduction génétiques :

- **La transcription génétique :**

La transcription est un processus biologique qui se déroule au niveau des noyaux chez les eucaryotes et donne le cytoplasme chez les procaryotes, et aussi permet la production d'une copie de l'information génétique portée par l'ADN et le convertir en ARN messager grâce à un enzyme de la polymérisation s'appelle l'ARN polymérase.

La transcription est la première étape de l'expression génétique, qui permet de synthétiser des protéines. [**21**]

Avant d'aborder les détails, nous en apprenons un peu plus sur l'ARN et ses composants.

L'**ARN** est une longue chaine, plus court que l'ADN. Il a un simple brin, se présenter au niveau des noyaux et dans le cytoplasme. Les nucléotides de l'ARN sont composés de trois principaux composants à savoir : un ensemble de phosphate, le ribose (sucre à cinq carbones) et une base azotée qui peut être : l'adénine (**A**), la cytosine (**C**), la guanine (**G**) et l'uracile (U) à la place de la thymine (T) dans l'ADN. **[22]**

Maintenant, nous expliquons le processus de la transcription. Lors de l'initiation de la transcription, une partie de la double hélice de l'ADN s'ouvre et se déroule. L'un des brins d'ADN déroulés sert de matrice pour la formation d'un brin complémentaire d'ARN, appelé ARN messager (ARNm). Par la suite, l'ARNm se détache de l'ADN et quitte le noyau de la cellule. Il se déplace ensuite vers le cytoplasme, la partie de la cellule située en dehors du noyau.

- **La traduction génétique :**

Une fois dans le cytoplasme, l'ARNm se fixe à un ribosome, une structure cellulaire minuscule où se déroule la synthèse des protéines. Le ribosome lit la séquence d'ARNm et assemble les acides aminés correspondants pour former une protéine spécifique. Ce processus s'appelle la traduction génétique et c'est là que l'information génétique contenue dans l'ARNm est utilisée pour créer une séquence précise de protéines. **[21]**

Ainsi, la transcription génère l'ARNm à partir de l'ADN, et l'ARNm traduit ensuite en protéines par les ribosomes lors de la traduction, permettant ainsi la synthèse des protéines nécessaires à la cellule.

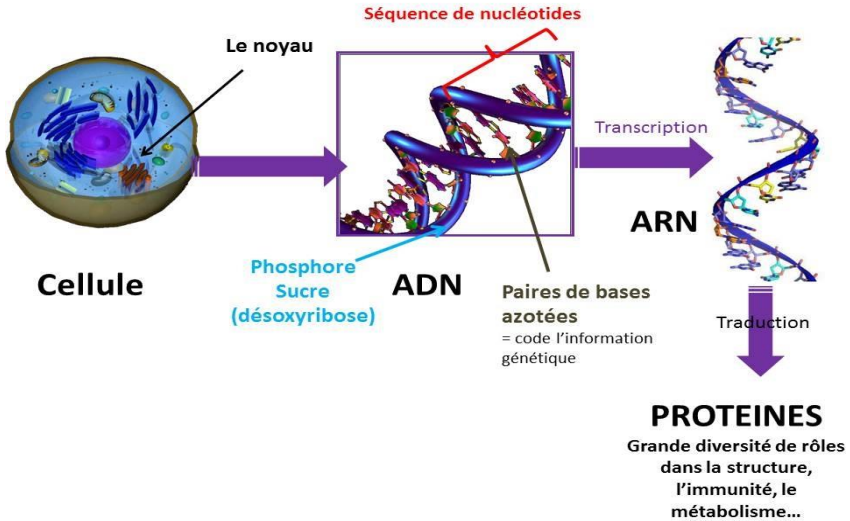


Figure II.3 : La transcription et la traduction génétique

II.2.4/ La structure de l'ADN :

L'ADN a une structure simple et répétitive, il se trouve dans le noyau cellulaire si bien que le noyau occupe 10% de la cellule.

Selon ***Watson*** et ***Crick*** une molécule d'ADN formé de deux brins enroulés l'un autour de l'autre de manière en double hélice, l'ADN est un polymère contenant des chaines de monomère appelé **nucléotide.**

Un nucléotide se compose de trois composants différent : en haut **un phosphate** celui-ci est relié à **un sucre pentose** (sucre à cinq carbones) et enfin **une base azotée**.

Tous les nucléotides possèdent le même sucre (le sucre présent dans l'ADN est le **désoxyribose**) et le même phosphate, par contre il existe quatre bases azotées différentes : adénine (**A**), thymine (**T**), cytosine (**C**) et guanine (**G**). Il existe donc quatre nucléotides différentes dans l'**ADN** chacun correspondant à une base azotée différente. **[23]**

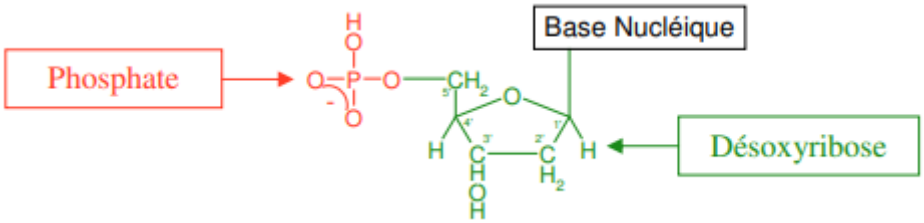


Figure II.4 : Les trois composantes d'un nucléotide

Les bases cytosine (**C**) et thymine (**T**), qui ont un cycle unique, sont appelées **pyrimidine**, tandis que les bases adénine (**A**) et guanine (**G**) ont deux cycle appelées **purines**.

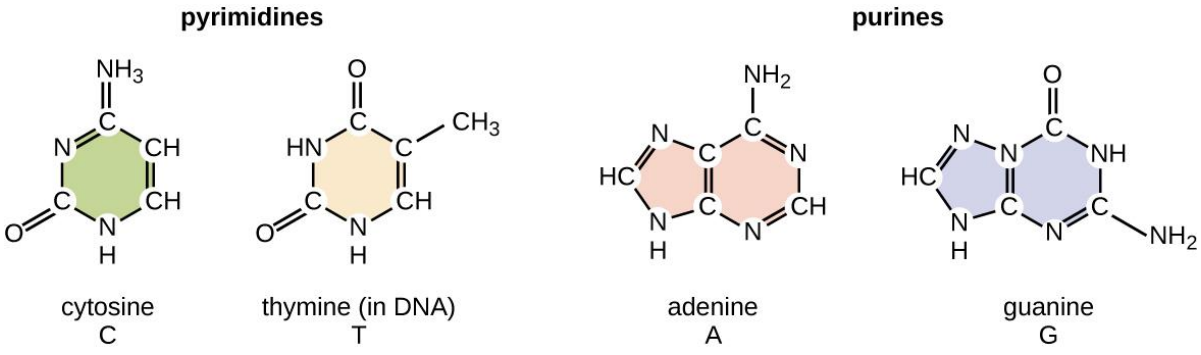


Figure II.5 : Les 4 nucléotides composant l'hélice d'ADN

Un brin d'ADN est donc constitué d'une succession de ces quatre types de ces nucléotides. Les deux brins sont appariés c'est-à-dire en quelque sorte attachés l'un à l'autre par des liaisons entre les nucléotides.

Selon les règles complémentaires de ***Watson-Crick,*** les nucléotides sont reliés entre eux par des liaisons hydrogènes. Un nucléotide (**A**) sur un brin relié toujours à un nucléotide (**T**) sur l'autre brin et inversement par deux liaisons hydrogène. De même, un nucléotide (**C**) sur un brin relié toujours à un nucléotide (**G**) sur l'autre brin et bien sur inversement par trois liaisons hydrogène. **[20]**

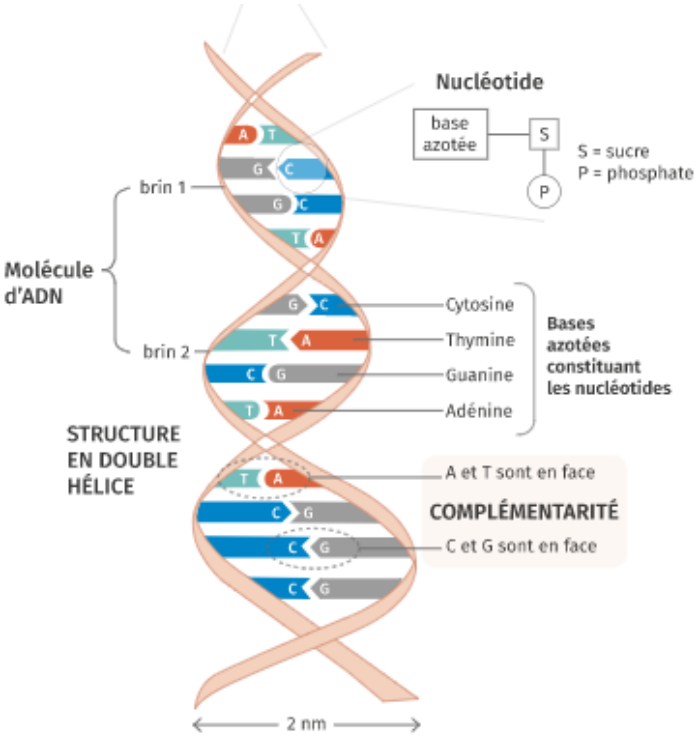


Figure II.6 : la structure d'ADN

- ***La question qui se pose maintenant, Comment l'information génétique est-elle codée dans la molécule d'ADN ?***

La molécule d'ADN contient toute l'information génétique nécessaire au développement, au fonctionnement et à la reproduction d'un être vivant. Et comme l'ADN est composé de nucléotide, l'information génétique est codée par une succession de nucléotide. On appelle ces séquences de nucléotides des **Gènes**. **[20]**

Autrement dit, un **gène** est un fragment d'ADN qui contient toute l'information nécessaire pour que la cellule effectuée une instruction comme la production d'une molécule.

L'ensemble des processus par lesquels l'information peut être lue dans un gène dans lequel la molécule est produite est appelée **expression génétique**. On dit qu'un gène s'exprime lorsqu'il est lu par la cellule pour réaliser une instruction. **[23]**

II.2.5/ Quelques termes-clef et leurs définitions :

- **La cellule :**

La cellule correspond à l'unité de construction et l'unité fonctionnelle de tous les êtres vivants. Chaque cellule de notre organisme provient de la première cellule qui a commencé notre histoire biologique personnelle. La cellule est divisée et redivisée des milliers de fois, en estime que le corps humain est composée d'environ 100 milles milliards cellules. **[24]**

- **Les chromosomes :**

Les chromosomes sont des structures microscopiques localisés dans le noyau des cellules de notre organisme. Ils sont composés de molécule d'ADN et de protéines.

Les chromosomes sont de longs brins d'ADN enroulés autour de protéines appelées histones. Ils contiennent les gènes qui déterminent les caractéristiques héréditaires d'un individu.

Il existe normalement 46 chromosomes dans le corps humain, repartis en 23 paires, dont 22 paires de chromosomes autosomes et une paire de chromosomes sexuels (XX chez les femmes et XY chez les hommes). **[24]**

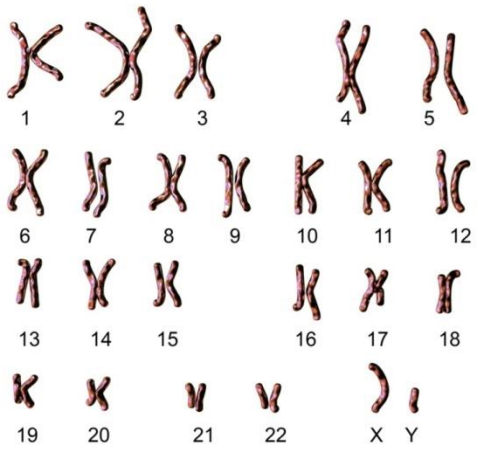


Figure II.7 : Les chromosomes d'un individu

- **Génome :**

Le génome humain présent dans les cellules de notre corps. Il est l'ensemble complet de l'information génétique, son composant principal est l'ADN. Le génome humain contient toutes les instructions nécessaires pour le développement, le fonctionnement de notre organisme. **[25]**

Figure II.8 : Le génome humain

- **Acide Aminé :**

Un acide aminé est une petite molécule organique qui est essentielle à la formation des protéines dans les organismes vivants. Il existe 20 acides aminés différents utilisés pour fabriquer les protéines. **[22]**

- **Les enzymes :**

Les enzymes sont des protéines spécialisées présentes dans les cellules vivantes qui jouent un rôle essentiel dans les réactions chimiques du métabolisme. Les enzymes sont des sortes d'outils chimiques qui permettent chacun à une réaction chimique précise de se dérouler.

Les enzymes jouent un rôle crucial dans de nombreuses fonctions biologiques, telles que la digestion des aliments, la production d'énergie, la synthèse des protéines, la réparation de l'ADN et bien d'autres processus métaboliques. Sans les enzymes, de nombreuses réactions chimiques nécessaires à la vie seraient trop lentes pour se produire de manière efficace. Il existe des milliers d'enzymes différentes, chacune ayant sa propre fonction spécifique dans le corps. Leur activité est étroitement régulée pour maintenir l'équilibre et l'efficacité des processus biologiques. **[24]**

- **ARN messager (ARNm**) :

Photocopie du gène, il sert à transférer l'information génétique de son lieu de stockage (le chromosome) jusqu'au lieu de synthèse des protéines (les ribosomes). **[22]**

- **Le code génétique :**

Le code génétique est un système de correspondance entre les séquences de nucléotides dans l'ARN messager (ARNm) et les acides aminés qui constituent les protéines. La séquence des acides nucléiques est une combinaison de 4 lettres (A, C, G, T dans l'ADN ; A, C, G, U dans l'ARN), la combinaison de ces 4 bases va permettre de "coder" pour les 20 acides aminés.

Le code génétique fonctionne avec des « mots » de trois bases : les triplets. Avec trois bases et quatre possibilités pour chacune des bases, il est possible d'obtenir 64 (4×4×4) combinaisons, donc plus qu'il n'en faut pour 20 acides aminés : le code génétique est redondant, car un même acide aminé peut être codé par plusieurs codons (par exemple GAA et GAG codent tous deux pour l'acide glutamique). À chaque séquence de trois bases consécutives portées par l'ARNm, correspond un acide aminé donné et un seul. **[26]**

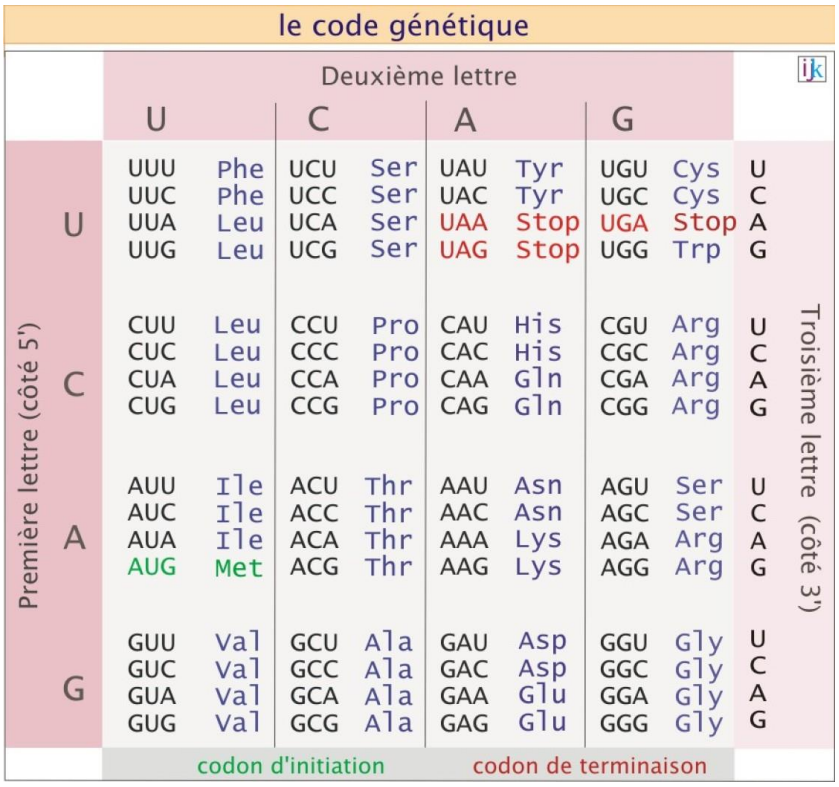


Figure II.9 : Le codage ADN

- **Le séquençage ADN :**

La séquence d'ADN est une représentation linéaire de l'ordre nucléotidique sur la chaîne d'ADN. Chaque nucléotide est composé d'une base azotée (A, T, C ou G), d'un groupement phosphate et d'un sucre désoxyribose.

La séquence d'ADN contient l'information génétique qui détermine les caractéristiques et les fonctions d'un organisme. Elle code les instructions pour la synthèse des protéines. **[27]**

II.3/ La cryptographie à base d'ADN :

La cryptographie à base d'ADN est une méthode de cryptage qui utilise des techniques de manipulation de séquences d'ADN pour sécuriser les informations. L'objectif principal de la cryptographie ADN est de chiffrer le texte en claire et le cacher sous forme numérique. Elle s'agit d'un nouveau domaine qui se développe rapidement, elle mélange les solutions cryptographiques conventionnelles et classiques pour avoir des chiffrements robustes offrant une résistance élevée contre les virus et autres attaques. **[19]**

Comme ce que nous avons mentionné plus tôt, L'ADN est une molécule se trouve dans les chromosomes, il présente sous forme de deux longues chaines se rassemblent autour de l'autre pour former une structure en double hélices. La cryptographie à base d'ADN exploite cette complexe structure pour le stockage des données et pour crypter et décrypter les informations sensibles.

La cryptographie à base d'ADN est une méthode extrêmement bénéfique, précieuse et très utile car ces avantages tels que :

a) **Tout d'abord**, la grande capacité de stockage **:** l'ADN offre une densité informationnelle considérable, il peut potentiellement stocker une quantité massive de données dans un petit volume, il besoin une cinquantaine d'atomes seulement pour stocker 1 bit. **[28]**
b) **En outre**, la longévité est aussi l'un de ses points forts, une molécule d'ADN peut survivre des dizaines de milliards d'années ce qui en fait un support de stockage potentiellement à long terme pour les données sensibles, tandis que les données stockées sur des supports classiques nécessitent d'être recopiée tous les 5 à 10 ans afin de prévenir de leurs dégradations. **[28]**
c) **Ainsi**, l'amélioration de la sécurité : l'ADN a une complexité naturelle qui le rend difficile à analyser et à manipuler. Les techniques de cryptage à base d'ADN peuvent exploiter cette complexité pour renforcer la sécurité des données.
d) **par la même**, La dissimulation des données : L'utilisation de l'ADN comme support de cryptage permet de dissimuler les données sensibles dans des échantillons biologiques ou des séquences génomiques, offrant ainsi une couche supplémentaire de sécurité et de confidentialité. **[28]**
e) **En effet,** la consommation d'énergie : les ordinateurs à base d'ADN n'ont pas besoin d'électricité car les procédés chimiques qui produisent les unités composant l'ADN deviennent déroulent sans nécessiter d'énergie externe.

Pour chiffrer en utilisant l'ADN, l'émetteur et le récepteur utilisent une approche de codage similaire pour créer un tableau de codage de l'ADN. Le texte en claire est divisé en deux parties égales en vue de son codage, si le texte en claire n'est pas de taille égale, un remplissage aléatoire est effectué. Une table de conversion basée sur l'émetteur est utilisée pour convertir la première moitié du texte en claire en une séquence d'ADN, tandis qu'une table de conversion basée sur le récepteur est utilisée pour convertir la seconde moitié du texte en claire en une séquence d'ADN.

Le cryptage par ADN est une nouvelle méthode qui exploite l'ADN comme support d'information pour sécuriser les communications de bout en bout.

II.4/ La stéganographie à base ADN :

II.4.1/ Notion de base de la stéganographie :

II.4.1.1/ Définition de la stéganographie :

La stéganographie (en anglais: **steganography** ou **data hiding**) est le pratique de dissimulation d'informations dans un autre message ou un objet physique pour éviter que celles-ci soient détectées. En fait le mot stéganographie tire son origine d'une étymologie grecque : steganos signifiant caché et graphs signifiant écriture, littéralement on traduit par « écriture dissimulée » **[29]**

L'objectif principal de la stéganographie est de cacher un message secret dans une image, audio ou une vidéo, nommée média cover (originale), d'où le média résultant appelé média stégo, Pas très différent des médias originaux, du moins à l'œil humain Cela signifie que l'existence du message secret dans le média sténographique est pratiquement indétectable.

II.4.1.2/ Les modes de stéganographie:

Il existe deux modes de stéganographie :

- **sténographie linguistique :**

La stéganographie linguistique est un domaine de recherche relativement limité par rapport à d'autres formes de stéganographie utilisant des médias non linguistiques. La raison probable de cette limitation est que la modification des propriétés linguistiques d'un texte pour cacher l'information est plus difficile à réaliser sans être détecté par un observateur. Cependant, il existe plusieurs formes de stéganographie linguistique, dont voici quelques exemples :

  - **Sémagramme :** Il s'agit de la forme la plus connue de stéganographie linguistique. Dans ce procédé, le système sténographique est totalement dissimulé à l'observateur. Un exemple célèbre est celui d'Alfred de Musset, qui a utilisé des

poèmes pour entretenir une relation secrète avec Georges Sand entre 1833 et 1834. **[30]**

- **Acrostiche :** Cette méthode consiste à transmettre des données en utilisant les lettres initiales de chaque vers d'un poème, qui, lorsqu'elles sont lues de haut en bas, forment un mot ou une expression. Il existe de nombreuses variantes de cette technique, comme placer le mot dans des vers ou des chapitres spécifiques. **[30]**

- **Ponctuation :** Les prisonniers de guerre ont également utilisé la ponctuation, telle que les points, la hauteur des lettres et les virgules, pour transmettre des messages à leur famille. En utilisant ces signes de ponctuation de manière spécifique, ils étaient en mesure de coder des informations cachées. **[30]**

- **Nulles :** Les codes camouflés, également appelés "nulles", consistent à marquer certaines lettres d'un texte avec un signe particulier, tel que des piqûres d'aiguilles sur ou sous les lettres. En rassemblant ensuite les lettres marquées, on peut former un mot ou un message caché. **[30]**

- **Insertion d'erreurs** : Cette technique consiste à mettre en valeur l'information en introduisant délibérément des erreurs ou des variations stylistiques dans un texte. Cela permet de dissimuler le message dans le texte lui-même, en utilisant des motifs spécifiques d'erreurs ou de variations pour transmettre l'information secrète. **[30]**

Ces différents procédés restent néanmoins difficiles et longs à réaliser et laissent vite suspecter la possibilité d'un message dissimulé. De nombreuses censures ont été ainsi appliquées afin de limiter l'usage de ces techniques.

- **La stéganographie technique :**

La stéganographie technique regroupe un ensemble de techniques qui permettent de dissimuler des données dans différents types de médias, sans jouer sur les mots. Voici quelques exemples de stéganographie technique :

- **Stéganographie audio :** Cette technique consiste à cacher de l'information de manière imperceptible dans un signal audio. Différentes méthodes peuvent être utilisées, telles que l'utilisation de sons plus forts pour cacher d'autres sons, la dissimulation temporaire d'un son lorsqu'il est moins fort et placé avant ou après un son plus fort, etc. **[30]**

- **Stéganographie d'images et de vidéos :** Les images et les vidéos peuvent également être utilisées pour dissimuler un message. Les images sont composées de pixels, et il est possible d'insérer des bits du message secret à

l'intérieur de ces pixels sans que les modifications soient visuellement détectables. **[30]**

- **Stéganographie dans les réseaux informatiques :** Cette technique consiste à cacher de l'information dans les différents protocoles et couches du modèle OSI, tels qu'IP, TCP, ICMP, HTTP, DNS, etc. Cela peut être réalisé en utilisant des canaux cachés ou du tunneling, permettant de faire passer des données secrètes à travers les communications réseau sans éveiller les soupçons. **[30]**

II.4.1.3/ Les différents types de technique stéganographie :

- **Stéganographie pure :**

La stéganographie pure est une méthode de dissimulation de données qui ne fait pas appel à des clés privées ou à des mécanismes de chiffrement. Elle repose entièrement sur la discrétion pour cacher les informations sans l'utilisation de techniques de cryptographie. **[30]**

- **Stéganographie clé secrète :**

La stéganographie à clé secrète est une méthode de dissimulation de données qui utilise une clé individuelle pour incorporer les informations dans un objet. Cette clé, similaire à une clé symétrique, est utilisée à la fois pour le chiffrement et le déchiffrement des données dissimulées. Cela garantit que seules les personnes ayant la clé appropriée peuvent accéder aux informations secrètes. **[30]**

- **Stéganographie à clé publique :**

La stéganographie à clé publique utilise deux types de clés : une clé privée pour le chiffrement et une clé publique pour le déchiffrement. La clé privée est utilisée pour crypter les données et est gardée secrète par le destinataire. La clé publique, quant à elle, est utilisée par l'émetteur pour décrypter les données et est disponible publiquement dans une base de données. Ce mécanisme permet à l'émetteur de dissimuler les informations de manière sécurisée, sachant que seul le destinataire possédant la clé privée correspondante pourra les récupérer. **[30]**

II.4.1.4/ Propriétés des systèmes de stéganographie :

Une technique de stéganographie possède trois propriétés qui répondent à des objectifs différents. On peut représenter la relation entre ces trois propriétés comme suit :

- **La capacité :**

La capacité d'insertion en stéganographie représente la quantité d'informations du message secret pouvant être incorporée dans un média spécifique, mesurée en bits. La capacité d'insertion relative quantifie cette capacité en comparant la taille du message secret à la taille du média utilisé. Il s'agit d'un rapport entre les deux mesures, exprimant combien d'informations peuvent être dissimulées dans le média par unité de taille. **[31]**

- **Sécurité :**

En stéganographie, toutes les exigences de sécurité des systèmes cryptographiques sont également applicables. La sécurité repose sur le caractère secret de la clé plutôt que sur l'algorithme, qui peut être public. L'objectif est de rendre indiscernable une image d'origine d'une image stéganographique sans la connaissance de la clé. De plus, les modifications apportées à l'image ne doivent pas altérer ses propriétés statistiques. La stéganalyse est la technique utilisée pour évaluer la sécurité des systèmes de stéganographie en cherchant à détecter les messages dissimulés sans la clé. **[31]**

- **Robustesse :**

Elle quantifie la résistance du message dissimulé aux diverses attaques (transformations) apportées au médium stégo. **[31]**

II.4.2/ La stéganographie informatique :

La stéganographie informatique offre une grande liberté créative pour dissimuler des informations de manière discrète. Grâce aux outils informatiques à notre disposition, il est possible de manipuler les données numériques et de les compresser tout en minimisant les signes apparents de dissimulation.

Le principe de base de la stéganographie est de remplacer les données inutiles ou le bruit de fond par des données que vous voulez cacher. Par exemple, dans une image, on peut utiliser les bits de moindre importance des pixels pour intégrer des informations secrètes. De cette manière, l'image semble inchangée pour un observateur non averti, mais les données cachées peuvent être récupérées par le destinataire approprié.

Il est possible d'utiliser différents types de fichiers numériques comme support pour la stéganographie, tels que des images, des fichiers audio ou des vidéos. Chaque type de fichier offre des opportunités uniques pour dissimuler des informations, en exploitant les caractéristiques spécifiques du format. **[16]**

II.4.3/ La stéganographie ADN :

La stéganographie de l'ADN est une branche spéciale et la plus récente de la stéganographie qui couvre simplement écriture utilisant des méthodes biologiques. La stéganographie ADN est une technique qui utilise l'ADN comme support pour cacher des informations secrètes. L'ADN est une molécule présente dans tous les organismes vivants,

Grâce à ses propriétés de stockage de données extrêmement élevées, l'ADN est devenu un support potentiel pour la stéganographie.

La stéganographie a été utilisé par les rois et le personnel de l'armée de l'époque médiévale et quelques exemples communs inclus utilisation d'encre invisible pendant la Révolution américaine, messages tatoués sur la tête rasée et attendus la repousse des cheveux avant d'envoyer un esclave pour provoquer une rébellion, et Léonard de Vinci messages secrets dans ses peintures.

Plus tard, avec les progrès technologiques, les méthodes de stéganographie ont également varié comme la méthode la plus courante est de convertir les données en binaire et improviser dans le moins significatif Bit (LSB) de l'image de couverture. Bien que ces changements sont significatifs, mais à peine perceptible par l'œil humain**. [32]**

La stéganographie ADN fonctionne en encodant les données secrètes sous forme de séquences d'ADN, qui sont ensuite insérées dans une séquence d'ADN existante. Ces séquences d'ADN supplémentaires, appelées "marqueurs" ou "insertions", sont généralement conçues de manière à ne pas perturber le fonctionnement normal de l'ADN hôte.

II.5/ conclusion :

Dans ce chapitre, nous avons présenté de manière plus ou moins approfondie les concepts de base de la molécule d'ADN, et ses concepts ainsi que sa structure et ses caractéristiques, passant à la cryptographie à base d'ADN, nous avons voire que cette approche a connu des avancées significatives. Bien que ce domaine soit extrêmement complexe et que les recherches actuelles soient encore en phase de développement, il existe un fort optimisme quant à l'utilisation de l'informatique de l'ADN comme technique prometteuse pour assurer la sécurité des informations.

Nous avons aussi discuté de la stéganographie, tout d'abord nous avons donnés le concept de la stéganographie et son objectif principal, après nous avons parlé sur la stéganographie ADN qui offre une approche alternative à la cryptographie pour assurer la confidentialité des informations. Cependant, il est essentiel de prendre en compte les limites et les défis liés à cette technique lors de sa mise en œuvre.

Dans le chapitre suivant, nous proposons notre sméthode et notre algorithme de chiffrement qui utilise les séquences d'ADN et la stéganographie.

Chapitre III

Implémentation et résultats

III.1/ Introduction :

Les techniques de stéganographie LSB sont les techniques les plus simples et les plus connues. Les techniques LSB sont très vulnérables à diverses attaques stéganalytiques. La stéganographie LSB a donc besoin d'être améliorée. Dans ce chapitre, nous avons discuté une technique améliorée par rapport à la substitution LSB.

Nous proposons un algorithme cryptographique à base d'ADN pour le chiffrement/déchiffrement et une technique de substitution LSB avec clé secret pour la stéganographie.

III.2/ La stéganographie à base d'ADN :

Notre technique de stéganographie illustré dans la **Figure III.1**, repose sur deux grandes phases : **(1)** le chiffrement du texte et **(2)** cacher ce texte dans une image couleur par LSB.

+

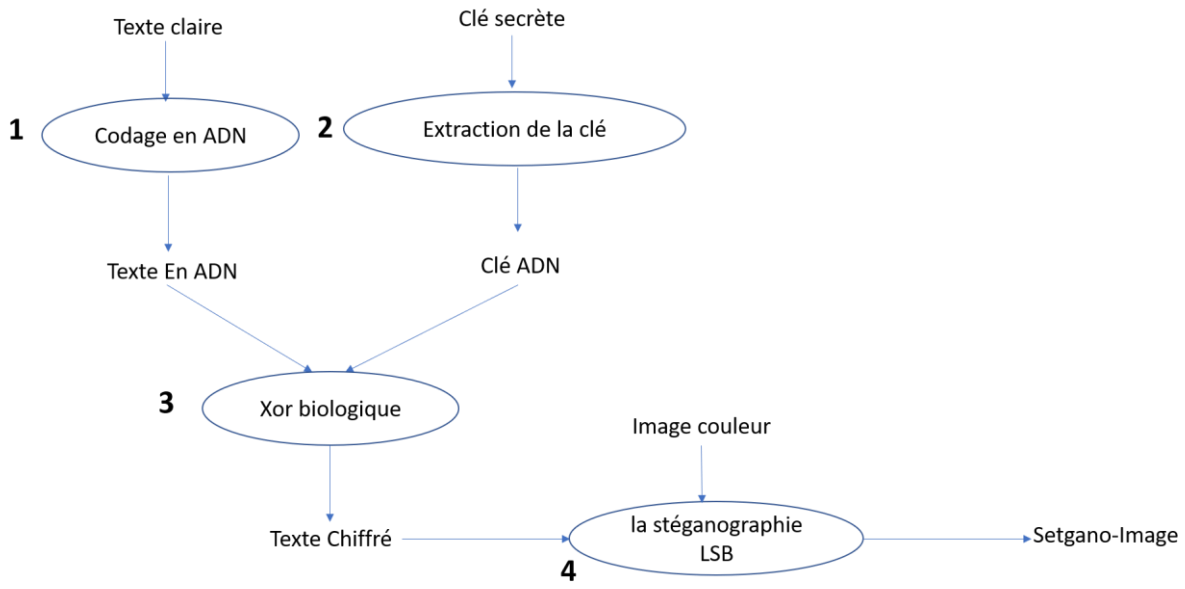


Figure III.1 : La technique de la stéganographie

Nous détaillons dans la suite les phases de notre technique :

III.2.1/ chiffrement du texte :

III.2.1.1/ Codage en ADN :

Le texte claire sera nous représentons le texte en claire en binaire permet, notamment des nombres ou des caractères textuel en suite de bits (0et 1). En utilisant, le code ASCII où chaque caractère est représenté par un code qui sera convertit en binaire.

0	NUL	16	DLE	32	SPC	48	0	64	@	80	P	96	`	112	p
1	SOH	17	DC1	33	!	49	1	65	A	81	Q	97	a	113	q
2	STX	18	DC2	34	"	50	2	66	B	82	R	98	b	114	r
3	ETX	19	DC3	35	#	51	3	67	C	83	S	99	c	115	s
4	EOT	20	DC4	36	$	52	4	68	D	84	T	100	d	116	t
5	ENQ	21	NAK	37	%	53	5	69	E	85	U	101	e	117	u
6	ACK	22	SYN	38	&	54	6	70	F	86	V	102	f	118	v
7	BEL	23	ETB	39	'	55	7	71	G	87	W	103	g	119	w
8	BS	24	CAN	40	(	56	8	72	H	88	X	104	h	120	x
9	HT	25	EM	41	)	57	9	73	I	89	Y	105	i	121	y
10	LF	26	SUB	42	*	58	:	74	J	90	Z	106	j	122	z
11	VT	27	ESC	43	+	59	;	75	K	91	[	107	k	123	{
12	FF	28	FS	44	,	60	<	76	L	92	\	108	l	124	|
13	CR	29	GS	45	-	61	=	77	M	93	]	109	m	125	}
14	SO	30	RS	46	.	62	>	78	N	94	^	110	n	126	~
15	SI	31	US	47	/	63	?	79	O	95	_	111	o	127	DEL

Figure III.2 : Le code ASCII

Nous transformons le texte binaire en brin d'ADN qui contient les quatre bases azotées A, C, G et T selon le **Tableau III.1** :

Code binaire	Code ADN
00	A
01	C
10	G
11	T

Tableau III.1 : Conversion Binaire / ADN

III.2.1.2/ Génération de la clé :

La chaine secrète introduite par l'émetteur/ récepteur sera convertit à un nombre entier qui sert comme une position de départ à partir de laquelle en commence à générer la clé de chiffrement/déchiffrement à partir de la séquence ADN qui est généralement un ou une partie de chromosome. La taille de la clé à extraire dépend de la taille du texte claire.

Taille clé = Taille (texte)*2

III.2.1.3/ Xor biologique :

C'est une opération définie entre les bases azotées selon les tables suivantes :

⊕	*A*	*C*	*G*	*T*
A	**A**	**C**	**G**	**T**
C	**C**	**A**	**T**	**G**
G	**G**	**T**	**A**	**C**
T	**T**	**G**	**C**	**A**

Table III.2 : ⊕ biologique

Cette opération qui est définie sur les bases azotique respecte les mêmes critères

Texte ⊕ clé =C **(2)**

C⊕clé = texte **(3)**

- Dans cette phase, on réalise l'opération du ⊕biologique entre le texte ADN et la clé ADN.
- L'équation **(2)** est utilisée dans la phase de chiffrement et l'équation **(3)** est utilisée dans la phase de déchiffrement.

III.2.2/ la sténographie :

Nous avons proposé un algorithme de stéganographie d'image pour cacher le message secret à l'aide d'une clé symétrique dynamique combiné avec le chiffrement par ADN.

- **Description :**

Il s'agit d'un algorithme de la stéganographie d'image pour cacher une donnée secrète dans une image colorée.

1- convertit les valeurs des pixels de l'image en valeurs binaires avec une taille égale à

(M × N × 3 × 8) bits,

Où :

(M) : indique le nombre de lignes dans l'image,

(N) : indique le nombre de colonnes dans l'image,

(3) : fait référence au nombre des trois plans de l'image colorée et

(8) : fait référence au nombre de bits de chaque pixel d'image dans le plan.

2- obtenez les deux bits les moins significatifs de chaque valeur de pixel en fonction de la position, où la position (LSB) est égale à 0 et le bit avant la position LSB (LSB 1) est égal à 1.

3- .Dans un processus parallèle, le secret message (message résultat de la phase 1) est converti en une colonne de valeurs binaires de taille égale à (1×K), où K est le nombre total de bits du message

4- Chaque bit du message secret à partir du premier bit est comparé aux deux bits correspondants du (LSB) et du (LSB-1).

La **Figure III.3** montre l'encodage et le décodage qui ont été effectués.

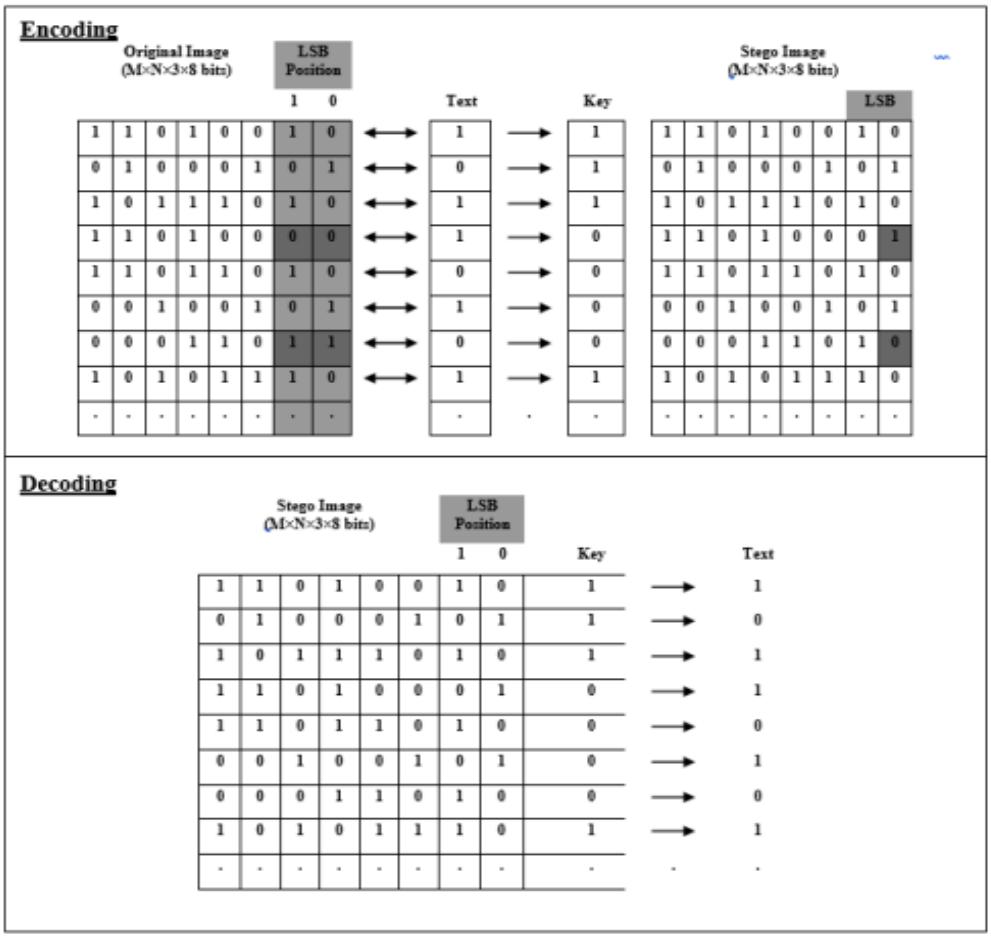


Figure III.3 : la stéganographie LSB

Les sept premiers bits du LSB sont le type de processus de stéganographie. Étant donné que cet algorithme est la quatrième méthode, le type de stéganographie est (4), le nombre (4) est représenté par sept bits sous la forme (0000100). Cette valeur binaire est enregistrée (masquée) dans les sept premiers bits du LSB.

Les vingt bits du message secret après les sept bits du LSB représentent la longueur du message secret (les positions de 8 à 27 du LSB des pixels de l'image).

Après le vingt-septième bit, l'algorithme (LSB+KEY) démarre son processus illustré à la **Figure III.3** Il existe trois instances du processus de mise en correspondance de la stéganographie d'image à l'aide d'une clé symétrique dynamique :

1) Si le bit du message secret correspond à la position 0 du (LSB), la clé sera 0.

2) Si le bit du message secret correspond à la position 1 du (LSB), la clé sera 1.

3) Si le bit du message secret ne correspond pas à la première et à la deuxième position du (LSB) et du (LSB-1), nous changerons la position 0 du (LSB) à la valeur de ce bit du message secret et la clé sera 0.

À la fin de ce processus, nous obtenons une vectrice ligne qui sera au-delà de la clé. La clé indique la position des bits du message secret dans l'image stego. Cette clé est une clé secrète partagée entre l'expéditeur et le destinataire des données. Sans cette clé, le récepteur ne peut pas obtenir le message secret caché de l'image stego. Ainsi, la clé est considérée comme la base de cette méthode.

La taille maximale du message secret qui peut être masqué dans l'image à l'aide de cette méthode est calculée comme l'équation suivante :

S1= M* N *3- 27

Où :

(S1) indique la taille maximale du message secret qui peut cacher dans l'image

(M) fait référence au nombre de lignes dans l'image colorée,

(N) fait référence au nombre de colonnes dans l'image colorée,

(3) indique aux trois plans de l'image colorée et

(27) indique au bit réservé, où les sept premières positions du LSB de l'image sont des positions réservées au type stéganographie, ces bits peut être [1, 2, 3, …, 127] dans le système binaire. Les positions de 8 à 27 représentent 20 bits indiquent la longueur du message secret.

III.3/ Implémentation et résultats :

Pour analyser les performances de la procédure stéganographique prévue, une évaluation des résultats est effectuée. Le système stéganographique a deux caractéristiques essentielles : (1) l'imperceptibilité et (2) la capacité de recouvrement qui sont passées en revue afin d'évaluer la perfection d'une méthode de stéganographie. Les données masquées sont intégrées dans les images, comme indiqué dans l'algorithme proposé. Les expériences ont été menées à l'aide du programme pythons sur la plate-forme Windows 10. Différents paramètres d'exécution tels que MSE et PSNR ont été utilisés pour évaluer l'exécution de l'algorithme en utilisant différentes images qui incorporent à la fois des images standard et naturelles bien connues.

Les messages secrets consistent en des textes intégrés dans les images. Les expériences sont basées sur l'intégration des textes de différentes tailles. Les images originales et les images stego résultantes formées sont illustrées à la **Figure III.4**

(a) image originale

(b) image stego

(c) image originale

(d) image stego

Figure III.4: Images originales et leurs images stego respectives

III.3.1/ L'analyse visuelle :

L'analyse visuelle tente de distinguer la présence de données couvertes par une inspection à l'œil nu ou à l'oreille dans le cas du son.

L'incohérence entre les images originales et les images stego résultantes est imperceptible, comme le montre la **Figure III.4** Par conséquent, les deux images peuvent traverser l'analyse de perceptibilité car il n'y a pas de distorsion visuelle entre eux. Plus le résultat de l'algorithme est comparable à l'image d'origine, et plus la qualité de l'algorithme est détectable. Par la suite, le discernement des informations dissimulées serait plus compliqué. Les images stego créent une découverte telle qu'elles ne contiennent aucun artefact pouvant être reconnu par les yeux humains.

À partir d'yeux normaux, les images originales et les images stego sont indiscernables et il n'y a pas de distinction perceptible entre elles et la complexité de l'image n'est pas perturbée.

III.3.2/ Attaques statistiques :

Outre une véritable analyse statistique, on peut conclure si une image a été modifiée ou non... L'analyse statistique tente de révéler les petites modifications des objets porteurs, une performance statistique produite par l'incorporation stéganographique.

III.3.2.1/ Mesure des performances :

Les paramètres pris en compte pour l'évaluation de la proposition sont donnés comme suit : capacité d'integration (EmbeddingCapacity), erreur quadratique moyenne(MSE) et rapport signal bruit (PSNR).

- **Erreur quadratique moyenne (MSE) :**

Il est défini comme le carré de l'erreur entre l'image originale et l'image stego. La distorsion de l'image peut être mesurée à l'aide de MSE.

- **Rapport signal-bruit de crête (PSNR) :**

Il est défini comme le rapport de la valeur carrée maximale des pixels par MSE. Elle est exprimée en décibel. Il mesure la différence statistique entre l'image originale et l'image stego.

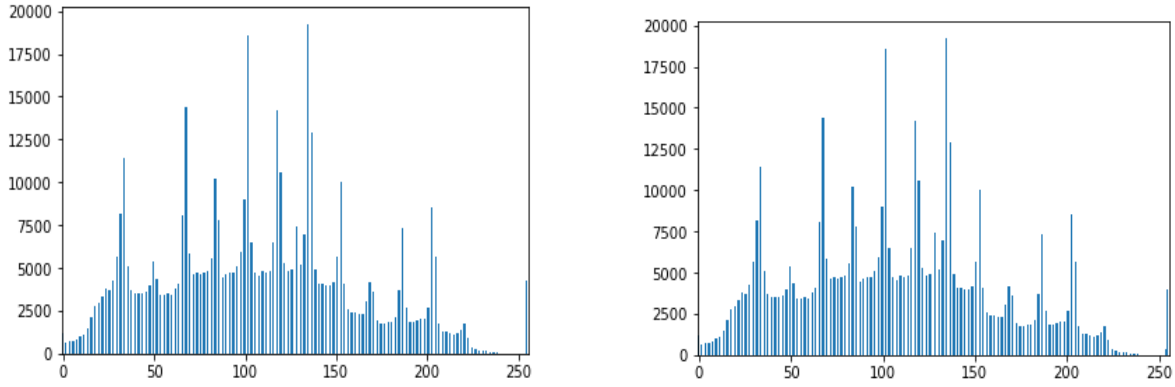
III.3.2.2/ Résultats expérimentaux :

Deux types d'images sont considérés pour mener une expérience ; des images en niveaux de gris et des images en couleur.

III.3.2.2.1/ Images niveaux Gris

- **Histogrammes :**

Si nous observons le diagramme à barres dans les différentes **Figures III.5** (a), (b) et (c), (d), il n'y a pas de différence entre les diagrammes à barres d'images originales et les diagrammes à barres de stego-images.



(a) **(b)**

Figure III.5 : les histogrammes

Le premier scénario défini est mis en œuvre sur des images en niveaux de gris pour trouver le MSE et le PSNR en faisant varier la taille du texte secret intégré, comme indiqué dans le **Tableau III.3 :**

Taille de texte	MSE	PSNR
2.4	0.028	66.24
4.9	0.037	64.85
7.4	0.058	63.31
9.6	0.079	61.56
13.2	0.092	62.34

Tableau III.3 : Les mesures pour les images en niveaux gris

Une valeur inférieure pour MSE implique une erreur mineure, et les images avec un MSE inférieur sont fabuleuses. Cependant, la plus petite valeur de MSE définit l'excellente propriété de l'image résultante. D'après le **Tableau III.3**, il est confirmé que la distorsion est minimale.

Une valeur PSNR plus élevée indique le fait que l'écart entre l'image de couverture et la stégo-image n'est pas perceptible à l'œil humain et qu'il peut remplacer certaines des mesures statistiques de détection des données secrètes. Comme on le voit le **Tableau III.3** la méthode prévue obtient une valeur PSNR moyenne de 63.66.

Lors de l'évaluation de la qualité de l'image, de mystérieux messages de cinq tailles sont insérées dans les images de couverture. Il est à noter que la valeur du PSNR diminue progressivement avec l'augmentation de la capacité du message. Les résultats confirment que la stéganographie d'image basée sur l'ADN proposé donne une meilleure valeur PSNR.

III.3.2.2.2/ Images RGB

- **Histogrammes :**

Si nous observons le diagramme à barres dans les différentes **Figure III.6** (a), (b) et (c), (d), il n'y a pas de différence entre les diagrammes à barres d'images originales et les diagrammes à barres de stego-images.

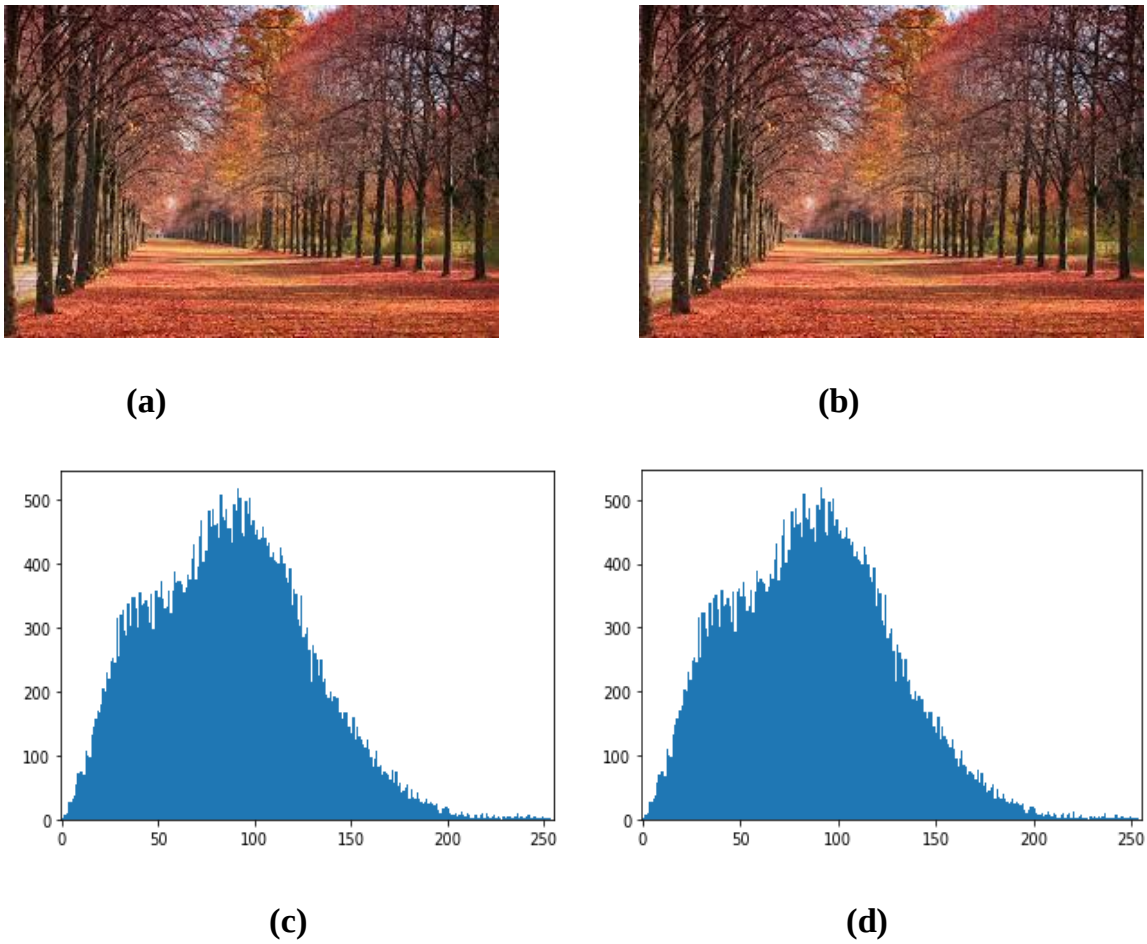


Figure III.6 : les histogrammes

Le deuxième scénario défini est mis en œuvre sur des images RGB pour trouver le MSE et le PSNR en faisant varier la taille du texte secret intégré, comme indiqué dans le **Tableau III.4** :

Taille de texte	MSE	PSNR
2.4	0.026	71.12
4.9	0.034	69.85
7.4	0.054	68.25
9.6	0.078	67.51
13.2	0.088	65.98

Tableau III.4 : Les mesures pour les images en niveaux gris

D'après les résultats expérimentaux du **Tableau III.4,** lors de l'augmentation des tailles des textes insérés, la valeur MSE évaluée est étendue de 0,026 à 0,088, ce qui décide qu'il n'y a pas de différence exceptionnelle entre l'image de couverture et l'image stego après l'implantation.

Dans l'évaluation de la qualité de l'image, des messages mystérieux de cinq tailles allant de 2.4Kb à 13.2 Kb sont insérés dans les images de couverture et présentés dans le tableau 3.4. Cette expérience vise à évaluer l'impact de l'expansion de la taille du message sur le PSNR pour une image de couverture individuelle. Il est à noter que la valeur du PSNR diminue progressivement avec l'augmentation de la capacité du message. Les résultats confirment que la stéganographie d'image basée sur l'algorithme proposé donne une valeur PSNR plus élevée.

III.3.3/ Le temps de chiffrement /déchiffrement

Dans ce test, en faisant varier la taille du texte secret intégré, comme indiqué dans le **Tableau III.5** et on fait le calcul du temps de chiffrement et déchiffrement

Taille	Temp de Chiffrement (Ms)	Temps de Déchiffrement (Ms)
50	0,921	0,930
100	1,008	1,012

150	1,422	1,430
200	2,092	2,130
250	2,255	2,367
300	2,751	2.801
350	3,936	4,082

Tableau III.5 : temps de chiffrement/déchiffrement en fonction de la taille du texte en claire

On remarque que le temps de chiffrement (respectivement déchiffrement) augmente linéairement avec l'augmentation de la taille de texte en clair (respectivement texte chiffré).

III.3.4/ La taille de la clé :

Nous utilisons une chaine qui sera convertit par la suite à un entier, qui sert comme position de départ de l'extraction de la clé :

La clé de chiffrement /déchiffrement utilisé dépond de la taille du texte clair, elle est composé des bases azotique et de taille égale à 4 * taille du texte.

Ce qui montre que notre clé est robuste contre l'attaque de force brute. Car la séquence ADN contient au minimum 1000000 positions de départ. Et la taille de l'ensemble des séquences existantes sur (Genbank) dépasse les 135440924 bases azotiques donc 135440924 positions de départ possible.

III.4/ Conclusion :

En proposant un algorithme de stéganographie basé sur l'ADN, l'image stégo est formée efficacement sous notre technique. L'algorithme est appliqué pour intégrer les données secrètes et l'obstacle de l'asymétrie entre l'image originale et l'image stégo dans les procédés existants est minime. Notre Algorithme est utilisé pour intégrer le code en DNA dans l'image et contribue à augmenter le niveau de sécurité. De plus, le texte brut n'est pas masqué ; il est chiffré est caché, ce qui ajoute un autre niveau de sécurité. L'algorithme de chiffrement est un

chiffrement par ADN qui utilise une clé extraite à partir d'une séquence adn, donc un algorithme plus fort.

Conclusion Générale

La sécurité de l'information devient particulièrement authentique puisque les données se trouvent complètement à différents endroits du globe et Internet est un environnement ouvert et les probabilités sont plus d'extraire les informations secrètes par une intervention non autorisée. C'est la raison pour laquelle de nouvelles technologies ont été développées pour prévenir les failles de sécurité dans le service de transmission de données.

La stéganographie, la cryptographie sont parmi les technologies utilisées pour dissimuler les données le but de la technologie de cryptage conventionnelle est de dissimuler le contenu, et donc les documents cryptés sont difficiles à lire. La stéganographie est une technique de sécurité qui cache des données parmi les bits d'un fichier de couverture, où le message secret est inséré dans un autre support afin que l'existence même du message secret ne soit pas détectable. Le fichier de couverture peut être une image, un son ou une vidéo ; la forme la plus couramment utilisée est le fichier image, dans lequel les bits inutilisés ou insignifiants sont remplacés par les données secrètes.

Dans ce mémoire nous avons présenté un algorithme qui utilise les deux techniques : cryptographie et stéganographie. (1) La cryptographie lorsqu'on chiffre un texte clair à base d'ADN qui utilise les séquences ADN comme source de génération de clé à partir d'une position secrète échangée entre l'émetteur et le récepteur, et (2) la sténographie lorsque en cache ce texte résultant dans une image en appliquant la technique LSB.

Trois niveaux de sécurité y sont atteints, (i) au niveau de la cryptographie, (ii) au niveau de la stéganographie et (iii) au niveau de la clé définie par l'utilisateur.

Comme futur recherche, nous envisageons d'améliorer notre technique par l'application des différentes techniques de stéganographie et de choisir la meilleure combinaison avec notre algorithme de chiffrement.

Références Bibliographiques

Référence :

[1] : Dr. Mohamed Amine FERRAG, « Sécurité Informatique Cours et TD », 3ème année Licence - SI, Université 8 mai 1945 - Guelma Faculté des mathématiques, de l'informatique et des sciences de la matière, 2018.

[2] : Jean-Marie Flaus, « cyber sécurité des systèmes industriels », livre, ISTE Edition Ltd, 27-37 ST George Road, London SW 19 4EU, 2019.

[3] :« Développement des applications Web sécurisées », cour, Master 01 sécurité informatique et cryptographie, Université Dr. Moulay Taher- Saïda Faculté des technologies Département d'informatique, 2021-2022.

[4] : Pascal Urien, «Introduction à la Cyber Sécurité », Telecom ParisTech Edition, Londres, 2017.

[5] :« Maîtrisez le concept de sécurité », cour, Master 01 sécurité informatique et cryptographie, Université Dr. Moulay Taher- Saïda Faculté des technologies Département d'informatique, 2021-2022.

[6] : LESCOP Yves, « LA SÉCURITÉ INFORMATIQUE », Post BTS R2, 2002.

[7] : Laure Petrucci, « Cours de Sécurité et Surveillance des Réseaux », IUT de Villetaneuse-Licence Professionnelle ASUR, 6 mars 2011.

[8] : Mr Kamel SADDIKI, « Denial of service attack in wireless networks », Thèse de Doctorat 3 èmeCycle, université Djillali Liabes Domaine : LMD Mathématiques informatique Filière : Informatique Spécialité : Technologies des réseaux sans fi, 2018 – 2019.

[9] : Dr. Raphael Grevisse Yende, «SUPPORT DE COURS DE SÉCURITÉ INFORMATIQUE ET CRYPTO », Cours dispensé aux Facultés Africaine BAKHITA en Première Licence : Réseaux informatiques, YENDE R.G., 2018.

[10] : DOGNION Tiphaine, VANDAMME Julien, «Le piratage informatique », Rapport de mini projet, 6, bd maréchal Juin F-14050 Caen cedex 4, 2005-2006.

[11] : Mme Labraoui N. « Sécurité Informatique Chapitre 1: Notions Fondamentales », Master 1 Réseaux et systèmes distribués, Université Abou Bakr Belkaid Faculté des sciences Département d'Informatique, 2019-2020.

[12] : Hamouda Djallel, « Un système de détection d'intrusion pour la cybersécurité », Mémoire de Fin d'études Master, Université de 8 Mai 1945 – Guelma - Faculté des Mathématiques, d'Informatique et des Sciences de la matière Département d'Informatique, Octobre 2020.

[13] : Klaus Müller, « IDS - Systèmes de Détection d'Intrusion, Partie I », LinuxFocus article number 292, 2005-01-14, generated by lfparser_pdf version 2.51.

[14] : Dr. Nesrine KHERNANE, « Chapitre 5 : Les SystèmeS de Détection/Prévention D'Intrusion (IDS/IPS) », Université Batna 2 Facultédesmathématiquesetde l'informatique Département d'informatique, Master 1 ISIDS Année 2021/2022.

[15] : Nathalie Dagorn1, « Détection et prévention d'intrusion : présentation et limites », Rapport de recherche, 1 Université de Nancy1 Laboratoire Lorrain de Recherche en Informatique et ses Applications (LORIA) Campus Scientifique BP 239, F-54506 Vandœuvre-lès-Nancy Cedex, France.

[16] : Mlle BELKHATMI Keltouma ; Mlle BENAMARA Ouarda, « Mise en place d'un système de détection et de prévention d'intrusion », Mémoire de fin d'étude Master, Université A/Mira de Bejaïa Faculté des Sciences Exactes Département d'Informatique, 2015/2016.

[17] : Amirta Pathak, « IDS vs IPS : un guide complet des solutions de sécurité réseaux », site, 31 aout 2021, IDS vs IPS : un guide complet des solutions de sécurité réseau (geekflare.com).

[18] : M. Bigarré ; D. Leroy ; L. Valat, « Cryptographie : système RSA ».

[19] : XIAO Guozhen, LU Mingxin, QIN Lei & LAI Xuejia, « New field of cryptography: DNA cryptography », article, Chinese Science Bulletin Vol. 51 No. 12 June 2006.

[20] : E. G. Berger, T. Hennet, « Le Génome Humain: Principes fondamentaux sur l'ADN », Forum Med Suisse No 23 6 juin 2001.

[21] : « Cibler l'ADN : pour la compréhension du vivant », Carine Giovannangeli Cibler l'ADN : pour la compréhension du vivant.

[22] : Isabelle Quinkal, INRIA Rhône-Alpes, « Quelques termes-clef de biologie moléculaire et leur définition », Septembre 2003.

[23] : Mme BELKHEIR, « Structure et organisation de l'ADN (Acide désoxyribonucléique) : », Module de génétique, Faculté de médecine d'Alger

[24] : Raphael Coqouz ; Jennifer Comte ; Diana Hall ; Tacha Hicks ; Franco Taroni, « Preuve par l'ADN, la génétique au service de la justice », collections sciences forensiques, Livre, troisième édition revue et augmentée.

[25] : Jean François Mattei, « Regard éthique : le génome humain », livre, Council of Europe Publishing Editions Council of Europe.

[26] : Djenidi Habiba, « La génétique cellulaire, Code génétique et traduction », Université Batna 2.

[27] : Damien Imbs ; Mohamed Sayed Hassan, « Bioinformatique », Travail d'étude, Université de Nice Sophia Antipolis

[28] : M. Ludovic Haye, sénateur, « Le stockage de donnée s sous la forme d'ADN », Note n° 29, Décembre 2021.

[29] : Patrick Bas ; Rémi Cogranne ; Marc Chaumont, Cristal Lille, « stéganographie : insertion d'information dans des contenue multimédia », Cristal Lille,CNRS, Univ. Technologique Troyes, Troyes, LIRMME, Université Montpellier, CNRS.

[30] : Dalia Battikh, « Sécurité de l'information par stéganographie basée sur les séquences chaotiques », Thèse soutenue doctorat, l'Université européenne de Bretagne, Institut National des Sciences Appliquées de Rennes, 18.05.2015.

[31] : KAMIL MOHOBOOB, « État de l'art des techniques de stéganographie audio », École Nationale Supérieure d'Ingénieurs de Bretagne Sud, 1 Mai 2020.

[32] : A. ALI-PACHA ; N. HADJ-SAID ; A. BELGORAF ; A. M'HAMED, « Stéganographie : Sécurité par Dissimulation », Université des Sciences et de la Technologie d'Oran –USTO, Institut National des Télécommunications Evry- Paris, RIST Vol, 16 n°01, 2006.