République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Dr Moulay Tahar de Saida
Faculté de Technologie
Département d'Electronique
Spécialité : Télécommunication

Mémoire de fin d'études pour l'obtention du diplôme de master en Télécommunication
Option : Réseaux et télécommunication

**Thème :**

# Cryptographie chaotique : application sur les images

**Présenté par :**
Haddi Asmaa
Guesmia soumeya

**Membres de jury :**
Président: Dr Cherifi Abdelhamid
Examinateur : Dr Bouyeddou Benamer
Encadreur: Dr Benyahia Kadda

**Promotion : Septembre 2020**


بسم الله الرحمن الرحيم

# Remerciement

Nous rendons grâce à notre Dieu, le tout puissant et miséricordieux, pour nous avoir donné le courage et la patience pour mener à bout ce modeste travail.

Nous voulons exprimer par ces quelques lignes de remerciements
Notre gratitude.

Envers tous ceux en qui par leur présence, leur soutien, leur disponibilité et leurs conseils, nous avons eu courage d'accomplir mémoire.

Nous commençons par remercier à notre encadreur Monsieur Benyahia kadda
Pour son encouragement continue et aussi d'être toujours la pour nous écouter, nous aider et nous guider a retrouver le bon chemin par sa sagesse et ses précieux conseils.

Nous tenons également à remercier tous les membres du jury ont fait l'honneur d'accepter de lire et de juger ce mémoire.

Un grand merci à tous les enseignants qui ont contribués à nos formation depuis l'école primaire jusqu'aux études universitaires.

Nous exprimons notre gratitude à tous les enseignants du département d'électronique qui n'ont pas ménagé leurs efforts pour nous assurer une bonne formation.

Enfin un grand merci à nos familles, et surtout nos parents pour leur soutien permanent et indéfectible qui nous ont permis de chercher au plus profond fond de nous même la force, la volonté et la persévérance à même d'arriver à cet instant des plus important de notre vie. Qu'à nos sœurs et frères et à nos amis et tous ceux qui ont contribué de près ou de loin à la concrétisation de cette œuvre.

Nous remercions tous les collègues de la promotion 2020.


Je dédie ce modeste travail à

Ma très chère mère qu'Allah la protège, qui ma offert depuis toujours le plus belle cadeau de l'univers, le cœur d'une mère et à qui je serais éternellement reconnaissant pour son aide moral et son soutient matériel et affectif.

La mémoire de mon père qu'Allah lui accorde ses miséricordes et son vaste paradis.

Merci mes chers parents, je vous dis merci parce que tout simplement sans vous, sans votre Conseils et amour, rien de tout cela n'aurait pu être réalisé.

A ma chère et adorable sœur «manel »

La prunelle de mes yeux, source de la joie et du sourire pour son encouragement.

A mes chers frères : Réda et Oussama pour leur présence dans ma vie.

A mes chères tentes.

A mes chers oncles.

A mes chères cousines : kawtar Louisa, Nadine

A mes enseignants ;

Leur générosité et leur soutien m'oblige de leurs témoigner mon profond respect et ma loyale considération.

A toute les étudiant master 2 Réseaux Télécommunications (promotion 2020).

A mes chers amis de toujours.

Enfin je dédie ce travail à spécialement mes collègues de L'université docteur Moulay Tahar, et à tous ceux qui m'ont aidé de près ou de loin et tous ceux que j'ai oubliés que mon cœur n'oubliera jamais.

Haddi Asmaa


Je dédie ce mémoire :

A mes très chers parents pour leur amour inestimable, leur confiance, leur soutien, leurs sacrifices et toutes les valeurs qu'ils ont su m'inculquer. Je vous remercie pour tout ce que vous avez fait pour moi. Que ce modeste travail soit l'exaucement de vos vœux tant formulés que dieu vous accorde santé, bonheur et longue vie.

A toute ma famille, à tous mes cousins & cousines.

A mes amis (e) qui m'ont soutenue de près ou de loin.

A tous les étudiants avec qui j'ai parcouru mon cursus universitaire.

Guesmia soumeya

# Résumé

La Cryptographie est l'art de chiffrer qui permettant de pallier les menaces pour assurer sigle de sécurité **CAIN** (**C**onfidentialité **A**uthentification **I**ntégrité **N**on-répudiation).D'autre part, Le chao est un système non linéaire déterministe sensible a la condition initiale peut donc être utilisé pour masquer ou mélanger les informations dans une transmission sécurisée**.** Donc les deux mécanismes permettent de garantir la sécurité.

Le but principal de ce mémoire est d'assurer la cryptographie par chao. Nous proposons un algorithme pour crypter et décrypter une image via un système chaotique. Les expérimentations et les tests effectués ont donné des bons résultats qui prouvent la robustesse de l'algorithme.

**Mots clés :** chao, cryptage, décryptage, pixel, image, clé.

# Abstract

Cryptography is the art of encryption which makes it possible to overcome threats to ensure CAIN (Confidentiality Authentication Integrity Non-repudiation) security code. On the other hand, chaotic is a non-linear deterministic system sensitive to the initial condition.
used to hide or mix information in a secure transmission. So the two mechanisms make it possible to guarantee security.

The main purpose of this dissertation is to provide chaotic cryptography. We propose an algorithm to encrypt and decrypt an image via a chaotic system. The experiments and tests carried out have given good results which prove the robustness of the algorithm.



**Keywords:** chaotic, encryption, decryption, pixel, image, key.

## ملخص

التشفير هو فن التشفير الذي يجعل من الممكن التغلب على التهديدات لضمان كود أمان CAIN(مصادقة تكامل مصادقة عدم التنصل ) من ناحية أخرى، النظام الفوضوي هو نظام حتمي غير خطي حساس للشرط الأولي. تستخدم لإخفاء أو خلط المعلومات في عملية نقل آمنة. لذا فإن الآليتين تجعل من الممكن ضمان الأمن.

الغرض الرئيسي من هذه الرسالة هو توفير تشفير البيانات الفوضوية. نقترح خوارزمية لتشفير وفك تشفير صورة عبر نظام فوضوي. وقد أعطت التجارب والاختبارات التي تم إجراؤها نتائج جيدة تثبت متانة الخوارزمية.



**الكلمات المفتاحية:** أنظمة الفوضى ، تشفير ، فك تشفير ، بكسل ، صورة ، مفتاح.

## Chapitre 01 : Généralité sur la cryptographie



## Chapitre 02:Systèmes dynamiques et chaotiques



## Chapitre 03 : Les Techniques de chiffrement chaotiques

**chapitre 04 : Implémentations et Résultats**

## Chapitre 03 : Les Techniques de chiffrement chaotiques



## Chapitre 04 : Implémentations et Résultats

## Liste des Acronymes

**DES** Data Encryption Standard.

**IDEA** international Data Encryptions Algorithm.

**AES** Advanced Encryptions Standard.

**RSA** (Rivest Shamir Adleman).

**CAIN** Confidentialité, Authentification, Intégrité, Non-répudiation.

**GF(28)** groupe de Galois ou corps fini.

**DSA** Digital Signature Algorithm.

**NIST** National Institute of Standards and Technology.

**SCI** sensibilité aux conditions initiales.

**PSNR** Peak Signal to Noise Ratio.

**MSE** Erreur quadratique moyenne.

**M** message clair.

**K** clé chiffrement.

**C** message chiffré**.**

**n** module de chiffrement.

***e*** la clé publique.

**d** la clé privée.

# Introduction Générale

## Introduction Générale:

Depuis l'antiquité le problème de l'homme est la sécurité. Le développement de l'informatique et des télécommunications ainsi que la généralisation élargie des communications par internet ont accentué la complexité des problèmes de sécurité et de leurs solutions. En et de nouveaux phénomènes en résultant telles les virus informatiques, accès non autorisés aux données, fausses informations, engendrent un besoin impérieux de sécurisation des informations et des technologies associées. A l'heure actuelle, nous assistons à une évolution constante des techniques visant à sécuriser l'échange de données pour faire face aux différentes menaces. Pour répondre aux exigences de la politique de sécurité, il faut mettre en œuvre des systèmes de sécurité adéquats et robustes. La construction d'un système de sécurité fait appel inévitablement aux notions de cryptologie qui recouvrent la cryptographie et la cryptanalyse. Les crypto systèmes modernes reposent sur le principe de Kirchhoff, qui arme que le secret ne doit pas résider dans l'algorithme mais plutôt dans la clé. De nombreux systèmes de codage qui répondent à ce principe ont été proposés. Parmi les classes de ces systèmes nous pouvons citer les algorithmes de chiffrement symétrique (**DES, IDEA, AES**, ...) qui reposent sur le secret de la clé et les algorithmes de chiffrement asymétriques (**RSA**, ...) qui se basent sur la difficulté de factoriser les grandes nombres. L'émergence des nouvelles technologies de l'information, de la télécommunication et de la mondialisation des échanges ont donné naissance à de nouvelles approches pour subvenir aux contraints de sécurité.[1] Nous pouvons citer les types et les techniques de chiffrement quantique ,dérivées des prédicats de la mécanique**[2]**et le chiffrement chaotique qui ce repose sur la maitrise de phénomène chaotique.

Les systèmes dynamiques chaotiques sont des systèmes déterministes non linéaires qui montrent souvent un comportement non divergent, apériodique et éventuellement borné. Les signaux qui évoluent dans ces systèmes sont en général, à large bande, ce qui fait apparaître leur trajectoire comme du bruit pseudo aléatoire. En raison de ces propriétés et à cause de la fragilité des crypto systèmes classiques, les signaux chaotiques fournissent potentiellement une classe importante des signaux qui peuvent être utilisés pour masquer les informations dans une transmission sécurisée, il suffit donc de les mélanger de manières appropriées aux messages en clair qu'on souhaite transmettre confidentiellement. [3]

## Organisation de mémoire

Notre mémoire est scindé en **4 chapitres :**

**Le premier chapitre :** décrit la notion de base de cryptographie et son but dans la communication pour assurer la sécurité, ainsi que les différentes techniques de chiffrement.

**Le deuxième chapitre :** Présent les systèmes dynamiques et chaotiques.

**Le troisième chapitre :** Un état de l'art autour de la cryptographie chaotique.

**Le quatrième chapitre :** L'ensemble des expérimentations et tests effectués.

# Chapitre 01 :

# Généralité sur la cryptographie

## 1.1. Introduction :

Les besoins de sécurité de la vie réelle restent toujours en augmentation. Pour Cette raison plusieurs personnes ont développé des systèmes cryptographiques pour réaliser ces besoins.

Quand on parle de la cryptographie plusieurs interprétations se réveille. En générale la cryptographie a été dans la plupart des cas perçu comme une chimie noire qui est seulement utilisée par les états et les gouvernements reflétant la complexité et la difficulté et parfois l'impossibilité de la décrypter que par des mathématiciens brouillons. [4]

L'objectif fondamental de la cryptographie est de permettre à deux personnes de communiquer à travers un canal peu sûr de telle sorte qu'un opposant, une troisième personne, qui a accès aux informations qui circulent sur le canal de communication, ne puisse pas comprendre ce qui est échangé. Le canal peut être par exemple une ligne téléphonique ou tout autre réseau de communication.[5]

## 1.2. Historique :

Ceux-ci sont les périodes les plus importantes :

**.**Age artisanal :( **1900**)

.César : chaque lettres est remplacée par celle située 3 positions plus loin dans l'alphabet.

.systèmes de substitutions et de permutations basiques

**.** Age technique (**190-1970**) :

.substitutions et permutations utilisant des machines mécaniques ou électro mécanique :

Hagelin, Enigma (2eme guerre mondiale)

**.** Age paradoxal (**depuis 30 ans**) : nouveaux mécanismes répondant à des questions a priori hors d'attente.

.comment assurer un service de confidentialité sans avoir établi une convention secrète commune sur un canal qui peut être écouté par un attaquant?

**.**comment assurer un service d'authenticité-basé sur la possession d'un secret sans révéler la moindre information sur le secret? [6]

## 1.3. Cryptographie :

Le terme "cryptographie " vient du grec "*kriptós*" (**caché**) et "*gráphein*" (**écrite**).
La cryptographie est l'art de cacher l'information afin de la rendre incompréhensible aux yeux des autres ; à l'exception de celui à qui elle est destinée. Celui-ci lui rendra son aspect initial grâce au secret qu'il détient qui est la clé. Dans la cryptographie moderne, les transformations en question sont les fonctions mathématiques, appelées algorithmes cryptographiques (crypto systèmes), qui dépendent de la taille de la clé utilisée.

La sécurité d'un crypto système dépend de deux paramètres : la sûreté de l'algorithme et la longueur de la clé utilisée.[7]

La cryptographie consiste notamment en l'élaboration de schémas de chiffrement/déchiffrement ou crypto-systèmes et pratiquée par des cryptographes. Le chiffrement (”encryption”, en anglais) est l'opération qui consiste à transformer un message afin d'en cacher le sens à tous ceux qui ne sont pas autorisés à le connaître. Le déchiffrement (“decryption”, en anglais) est l'opération inverse du chiffrement. Il a pour but de récupérer l'information masquée. Un crypto-système est l'ensemble des deux méthodes de chiffrement et de déchiffrement. En cryptographie, l'information à masquer est également appelée message ou texte clair (“plaintext”, en anglais). Le résultat du chiffrement d'un texte clair est appelé texte chiffré (“Ciphertext”, en anglais). Le texte chiffré est le résultat d'une transformation dépendant du message et d'une clé.

Le texte en clair est noté M. Ce peut être une suite de bits, un fichier de texte, un enregistrement de voix numérisé, ou une image numérique. Du point de vue de l'ordinateur, M n'est rien d'autre que de l'information binaire. Le texte en clair peut être transmis ou stocké. Dans tous les cas, M est le message à chiffrer. Le texte chiffré est noté C, C'est aussi de l'information binaire, parfois de la même taille que M et parfois plus grande. La fonction de chiffrement, notée E, transforme M en C. Ce qui en notation mathématique s'écrit:

E (M) = C. (1.1)

La fonction inverse, notée D, de déchiffrement transforme C en M:

D(C) = M. (1.2)

Comme le but de toutes ces opérations n'est rien d'autre que de retrouver le message en clair à partir de la version chiffré de ce même message, l'identité suivante doit être vérifiée:

D(E (M)) = M. (1.3)

Parmi une grande variété de mécanismes de chiffrement, les deux algorithmes principaux en cryptographie standard sont le chiffrement à clé publique (antisymétrique) et le chiffrement à clé secrète (symétrique), présentés dans la section suivante.[8]

### 1.3.1. Terminologies :

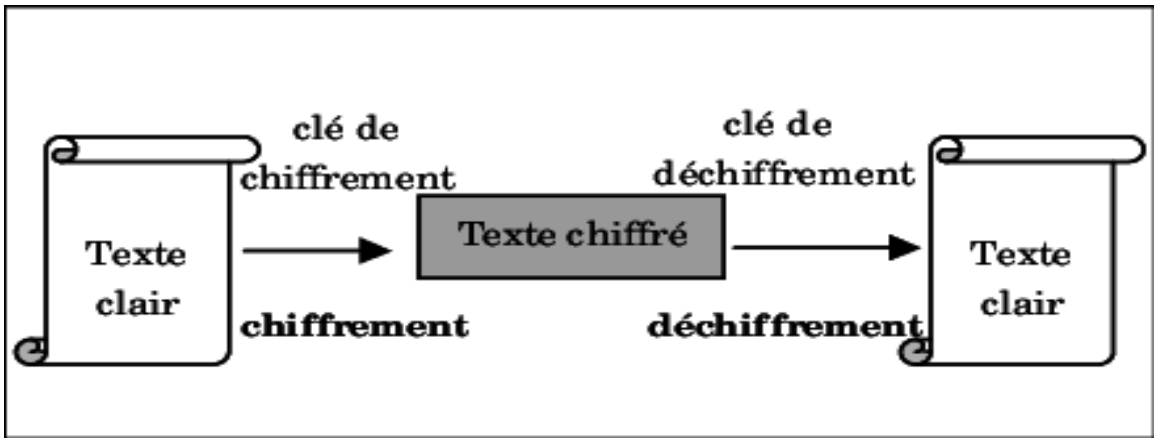



**Figure 1.1: principe de chiffrement et déchiffrement.**

• **Texte en clair** : est le message à protéger.[9]

• **Texte chiffré** : est le résultat du chiffrement du texte en clair [9].

• **Chiffrement** : est la méthode ou l'algorithme utilisé pour transformer un texte en clair en texte chiffré [4].

• **Déchiffrement** : est la méthode ou l'algorithme utilisé pour transformer un texte chiffré en texte en clair.[4]

• **Clé** : est le secret partagé utilisé pour chiffrer le texte en clair en texte chiffré et pour déchiffrer le texte chiffré en texte en clair. On peut parfaitement concevoir un algorithme qui n'utilise pas de clé, dans ce cas c'est l'algorithme lui-même qui constitue la clé, et son principe ne doit donc en aucun cas être dévoilé.[4]

• **Cryptographie** : cette branche regroupe l'ensemble des méthodes qui permettent de chiffrer et de déchiffrer un texte en clair afin de le rendre incompréhensible pour qui conque n'est pas en possession de la clé à utiliser pour le déchiffrer [4]

• **Cryptanalyse** : c'est l'art de révéler les textes en clair qui ont fait l'objet d'un chiffrement sans connaître la clé utilisée pour chiffrer le texte en clair.[4]

• **Cryptologie** : il s'agit de la science qui étudie les communications secrètes. Elle est composée de deux domaines d'étude complémentaires, la cryptographie et la cryptanalyse.[4]

•**Décrypter**: rendre le message compréhensible.[9]

• **Crypter** : brouiller l'information, la rendre "incompréhensible"[9].

• **Coder, décoder** : c'est une méthode ou un algorithme permettant de modifier la mise en forme d'un message sans introduire d'élément secret. Le Morse est donc un code puisqu'il transforme des lettres en trait et points sans notion de secret. L'ASCII est lui aussi un code puisqu'il permet de transformer une lettre en valeur binaire [4].

• **Crypto système** : Il est défini comme l'ensemble des clés possibles (espace de clés), des textes clairs et chiffrés possibles associés à un algorithme donné.[10]

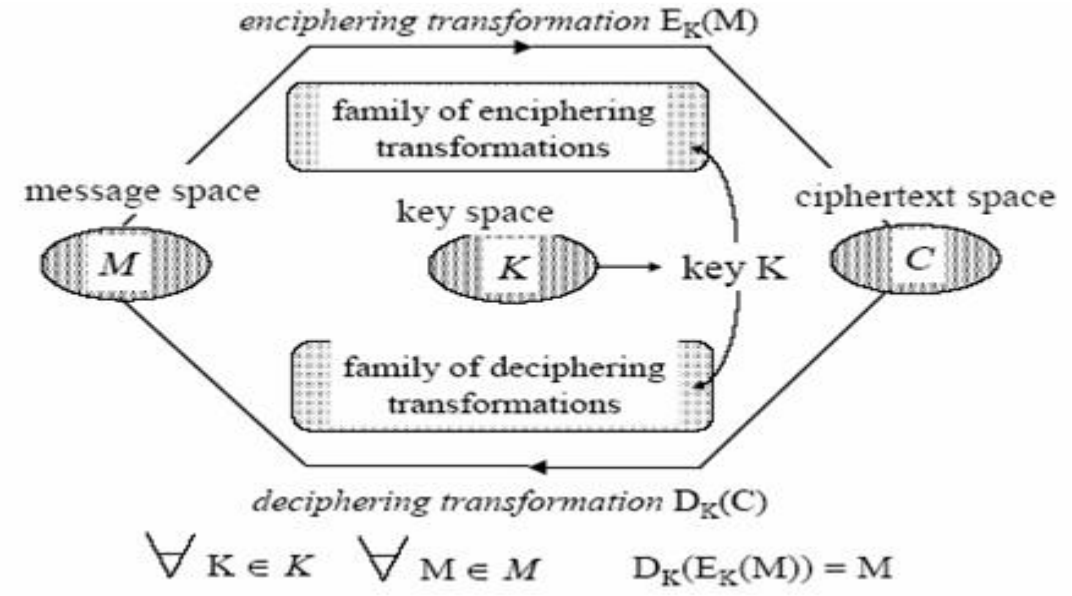



**Figure 1.2:schéma d'un cryptosystème.**

L'algorithme est en réalité un triplet d'algorithmes : [10]
– l'un générant les clés K,
– un autre pour chiffrer M, et
– un troisième pour déchiffrer C.

### 1.3.2. Principes de Kerckhoffs pour la cryptographie :

Les crypto systèmes civils utilisés actuellement, sont basés sur le principe fondamental suivant :

La sécurité du chiffre ne doit pas dépendre de ce qui ne peut être facilement changé [10]. En d'autres termes, aucun secret ne doit résider dans l'algorithme mais plutôt dans la clé. Sans celle-ci, il doit être impossible de retrouver le texte clair à partir du texte chiffré. Par contre, si on connaît la clé, le déchiffrement est immédiat [3]
Ce principe est l'un des six principes publiés par Kerckhoffs dans son traité de cryptographie militaire et dont l'énoncé est **: [11]**

- Une information codée ne doit en aucun cas pouvoir être déchiffrée sans la connaissance de sa clé.
- Les interlocuteurs ne doivent pas subir de dégâts au cas où le système de codage serait dévoilé.
- La clé doit être simple et modifiable à souhait.
- Les cryptogrammes doivent être applicables à la correspondance télégraphique.
- L'appareil de codage et les documents doivent être transportables.
- Le système doit être simple d'utilisation.

L'interprétation de ces principes est que le secret d'un message crypté doit se reposer sur le paramètre le moins cher à changer si celui-ci est dévoilé , c'est-à-dire la clé de déchiffrage.

## 1.4. But de la cryptographie : [1]

On désigne par la sécurité informatique l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. La notion de la sécurité fait référence à la propriété d'un système, d'un service, d'une entité. Elle s'exprime par les objectifs de sécurité résumés dans le sigle **CAIN**, pour Confidentialité, Authentification, Intégrité, Non-répudiation.

### 1.4.1. Confidentialité :

Seuls les utilisateurs autorisés peuvent accéder à l'information. Pour assurer la confidentialité des données, deux actions complémentaires sont à appliquer :

- ✓ Limiter et contrôler l'accès aux données.
- ✓ Transformer les données par des techniques de chiffrement pour qu'elles deviennent intelligibles. Dans le cas du chiffrement à clé privée, une même clé est utilisée pour le chiffrement et le déchiffrement, Dans le cas d'un chiffrement à clé publique, chaque entité à sa propre paire de clés et Dans le chiffrement hybride, on utilise le chiffrement à clé privée pour chiffrer le message. Par l'intermédiaire du système à clé publique, on sécurise l'échange de la clé.[1]

### 1.4.2. Intégrité :

Seuls les utilisateurs autorisés peuvent modifier l'information. D'où la nécessité de vérifier si le message n'a pas subit de modifications durant la communication. [1].

### 1.4.3. Authentification :

C'est la propriété qui consiste à vérifier l'identité d'une entité avant de lui donner l'accès à une ressource. L'entité doit prouver son identité. Tous les mécanismes de contrôle d'accès logiques aux ressources informatiques nécessitent de gérer l'identification et l'authentification. [1]

### 1.4.4. Non-répudiation : [1]

C'est le fait de ne pas pouvoir nier qu'un évènement (action, transaction) a eu lieu. Elle contient :

**1.4.4.1. -Non-répudiation d'origine :** L'émetteur ne peut nier avoir écrit le message et il peut prouver qu'il ne l'a pas fait si c'est effectivement le cas.

**1.4.4.2. -Non-répudiation de réception :** Le receveur ne peut nier avoir reçu le message et il peut prouver qu'il ne l'a pas réutilisé si c'est effectivement le cas.

**1.4.4.3.-Non-répudiation de transmission :** L'émetteur du message ne peut nier avoir envoyé le message et il peut prouver qu'il ne l'a pas fait si c'est effectivement le cas.

## 1.5. Classification des algorithmes : [12]

Les crypto systèmes peuvent être classé conformément à différentes caractéristiques :

- selon les types de clefs : symétrique, asymétrique ou hybride ;

- selon les techniques de chiffrement : par bloc ou par flot ;

- ou selon les corrélations entre le flux de clefs (Key, Stream) et les textes clairs et chiffrés : synchrone ou asynchrone.

**Le chiffrement symétrique** : l'émetteur et le destinataire partagent une clef unique.

**Le chiffrement asymétrique** : également appelé chiffrement à clef publique est un système où chaque interlocuteur dispose d'un couple de clefs, la clef publique pour crypter et la clef privée pour décrypter.

**Le chiffrement hybride** : fait appel aux deux techniques en même temps, symétrique et asymétrique.

## 1.6. Chiffrement moderne :

la cryptographie moderne s'intéresse en fait plus généralement aux problèmes de sécurité des communications [**13].**

### 1.6.1. Chiffrement asymétrique (à clefs publiques) :

La cryptographie asymétrique se base sur des problèmes mathématiques complexes (factorisation de grands nombres entiers ou équation de logarithme discrète). La cryptographie asymétrique se base sur le principe de **deux** clés: **clé publique**, **clé privée**. La clé publique est mise à la disposition de quiconque désirant chiffrer un message (cette clé peut être connue par tout le monde). Ce dernier ne pourra être déchiffré qu'avec la clé privée, qui doit être confidentielle et connue seulement par son propriétaire. [6]

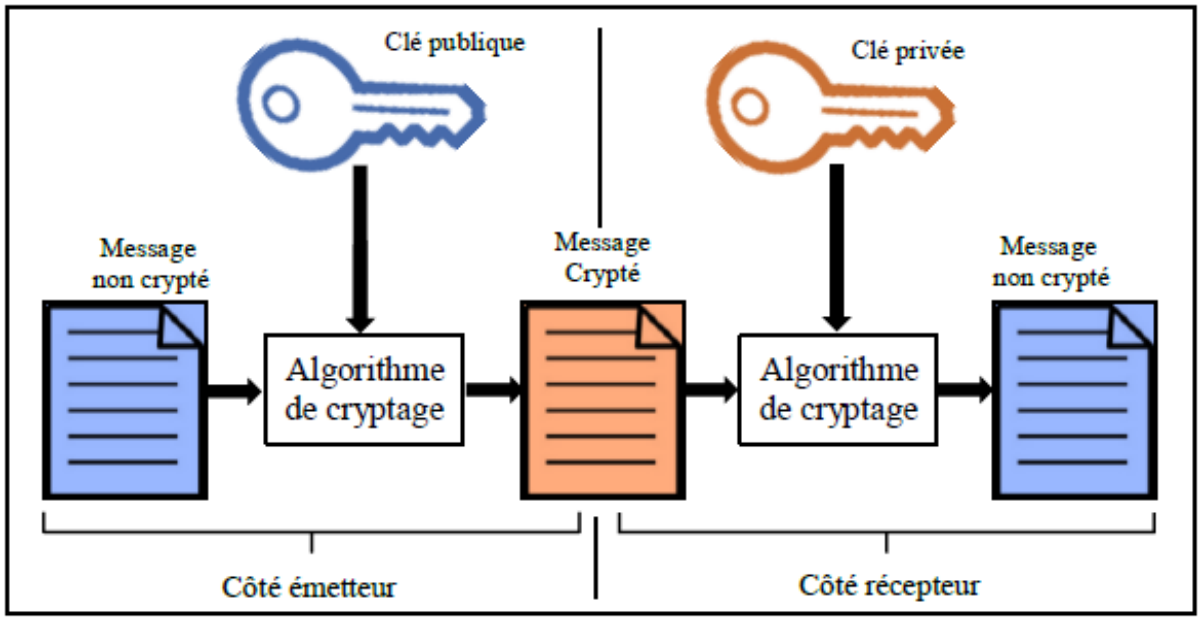



**Figure 1.3:cryptographie asymétrique.**

### a)Les avantages du cryptage asymétrique :

- l'élimination de la problématique de la transmission de clé
- la possibilité d'utiliser la signature électronique
- l'impossibilité de décrypter le message dans le cas de son interception par une personne non autorisé.
-Une paire de clés (publique/secrète) peut être utilisée plus longtemps qu'une clé Symétrie.[5]

### b) Les inconvénients du cryptage asymétrique :

- le temps d'exécution : plus lent que le cryptage symétrique
- le danger des attaques par substitution des clés (d'où la nécessité de valider les émetteurs des clés)
-Taille des clés, plus grand que celle des systèmes symétriques.[5]

### 1.6.2. Fonction de hachage :

C'est une fonction mathématique à sens unique qui permet de chiffrer un message dont son déchiffrement est impossible dont l'objectif est de fournir un résultat représentatif du contenu d'un message d'une taille restreinte à la taille initiale et ainsi de garantir l'intégrité de ce dernier. Les propriétés de ces fonctions de hachage sont :

**1/**la fonction de hachage doit être qu'elle associe un et un seul haché à un texte en clair.

**2/**un résultat sur un nombre limité d'octets.

**3/**l'impossibilité de retrouver le message original à partir de condensé (sens unique).[14]

### 1.6.3.Crypto système à Clé Symétrique :

Dans le chiffrement symétrique les deux entités qui communiquent utilisent un algorithme de chiffrement/déchiffrement symétrique basé sur une même clé secrète k. Les algorithmes de chiffrement symétrique sont divisés en deux classes principales : algorithmes de chiffrement par bloc et algorithmes de chiffrement par flux.[15]

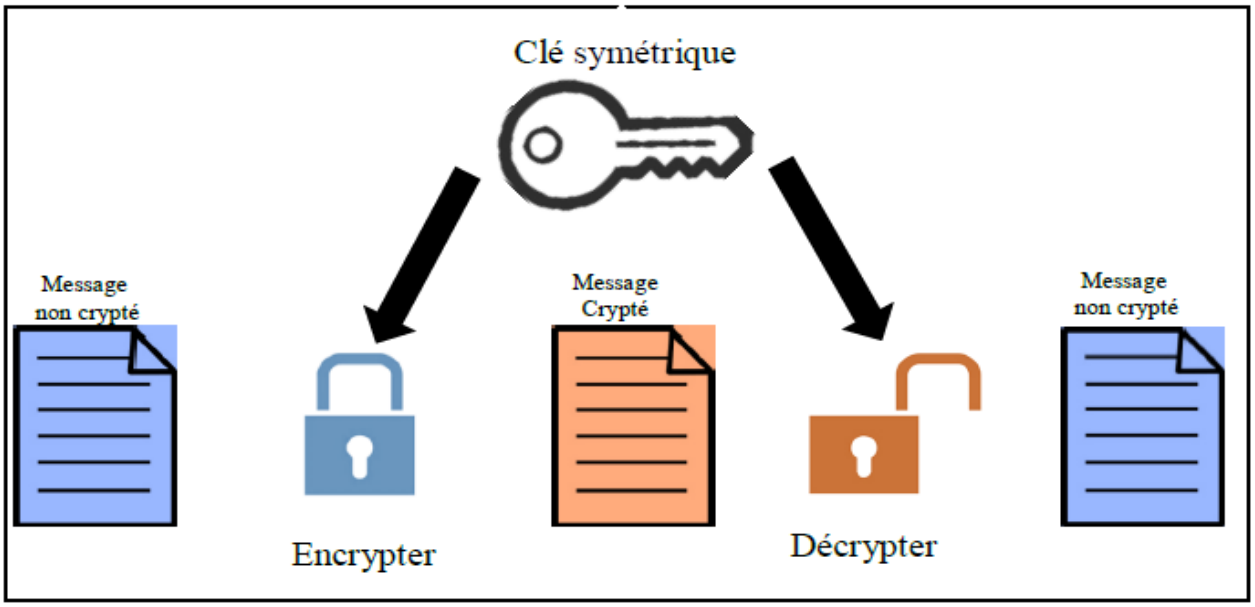



**Figure 1.4: cryptographie symétrique.**

### 1.6.3.1.le chiffrement par bloc:

dans un algorithme de chiffrement par bloc, chaque message clair est découpé en blocs de taille fixe de même longueur et chiffrer à l'aide d'une clé unique. Ces algorithmes sont en général construits sur un modèle itératif. Il utilise une fonction F qui prend une clé secrète k et un message M de n bits. La fonction F est itérée un certain nombre de fois (nombre de tours). Lors de chaque tour, la clé k est différente et on chiffre le message qui vient d'être obtenu de l'itération précédente. Les différentes clés k(i) qui sont utilisées sont déduites de la clé secrète k. Les algorithmes les plus connus des systèmes cryptographique symétriques sont : le DES et l'AES .[7]

**1.6.3.2. Chiffrement par flot:** dans un crypto système par flots, le cryptage des messages se fait caractère par caractère ou bit par bit, au moyen de substitutions générées aléatoirement, la taille de la clé est donc égale à la taille du message**.[13]**

### a)Les avantages du cryptage symétrique :

-la rapidité d'exécution (une seule clé utilisée).
-la simplicité d'implémentation (gestion d'une seule clé).
- Permet de concevoir différents mécanismes cryptographiques (fonctions de hachage, etc.)[5]

### b) Inconvénient :

- Clés relativement courtes.
- la complexité de fonctionnement : une obligation d'avoir le nombre de clés privées égal au Nombre de destinataires.
- la sécurisation de la chaîne de transmission de la clé.
- Impossibilité de garantir la propriété de non-répudiation dans les schémas de signature électronique. **[5]**

## 1.7. Chiffrement hybride :

La cryptographie asymétrique est intrinsèquement lente à cause des calculs complexes qui y sont associés, alors que la cryptographie symétrique brille par sa rapidité. Toutefois, cette dernière souffre d'une grave lacune, qui est celle de transmettre les clés de manière sécurisée. Pour pallier à ce défaut, on a recourt à la cryptographie asymétrique qui travaille avec une paire de clés : privée et publique. La cryptographie hybride combine les deux systèmes afin de bénéficier de la rapidité de la cryptographie symétrique pour le contenu du message et de l'utilisation de la cryptographie asymétrique uniquement pour la clé.

La plupart des systèmes hybrides procèdent de la manière suivante :

Une clé aléatoire, appelée clé de session, est générée pour l'algorithme symétrique. Ce dernier est ensuite utilisé pour chiffrer le message. La clé de session quant à elle, se voit chiffrée grâce à la clé publique du destinataire, c'est ici qu'intervient la cryptographie asymétrique, Comme la clé est courte, ce chiffrement prend peu de temps. Chiffrer l'ensemble du message avec un algorithme asymétrique serait bien plus coûteux, c'est pourquoi on préfère passer par un algorithme symétrique. Il suffit ensuite d'envoyer le message chiffré avec l'algorithme symétrique et accompagné de la clé chiffrée correspondante. Le destinataire déchiffre la clé symétrique avec sa clé privée et via un déchiffrement symétrique, retrouve le message.[16]

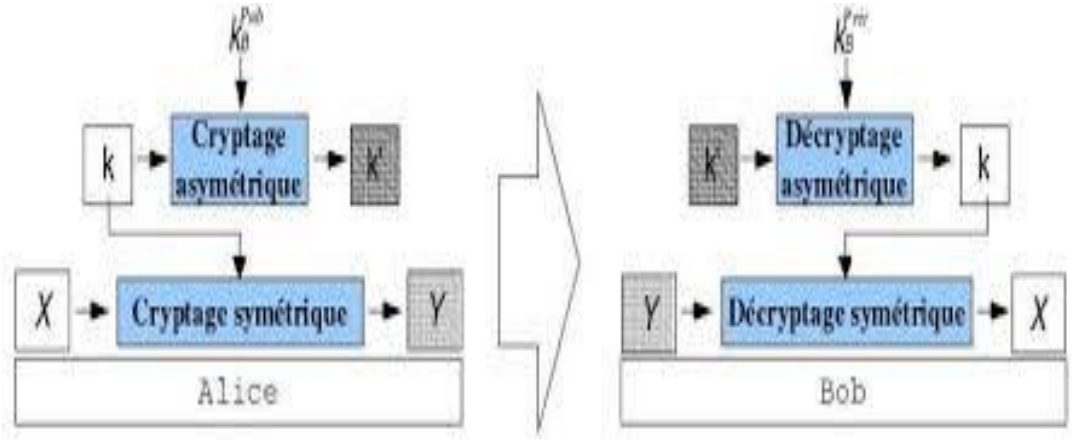



**Figure 1.5 : cryptage hybride.**

## 1.8. Exemples d'algorithmes de cryptage symétriques et asymétriques :

### ➢ Data Encryption Standard (DES) :

Il s'agit d'un système de chiffrement symétrique par blocs de 64 bits, dont 8 bits (un octet) servent de test de parité (pour vérifier l'intégrité de la clé). Chaque bit de parité de la clé (1 tous les 8 bits) sert à tester un des octets de la clé par parité impaire, c'est-à-dire que chacun des bits de parité est ajusté de façon à avoir un nombre impair de '1' dans l'octet à qui il appartient. La clé possède donc une longueur « utile » de 56 bits, ce qui signifie que seuls 56 bits servent réellement dans l'algorithme.

L'algorithme consiste à effectuer des combinaisons, des substitutions et des permutations entre le texte à chiffrer et la clé, en faisant en sorte que les opérations puissent se faire dans les deux sens (pour le déchiffrement). La combinaison entre substitutions et permutations est appelée code produit.

La clé est codée sur 64 bits et formée de 16 blocs de 4 bits, généralement notés k1 à k16 Etant donné que « seuls » 56 bits servent effectivement à chiffrer, il peut exister 256 (soit 7.2*1016) clés différentes.[**17]**

L'algorithme repose principalement sur 3 étapes, en plus de la gestion spécifique de la clé :

1. Permutation initiale.
2. Calcul médian (16 fois) : application d'un algorithme complexe appliqué en fonction de la clé.
3. Permutation finale.

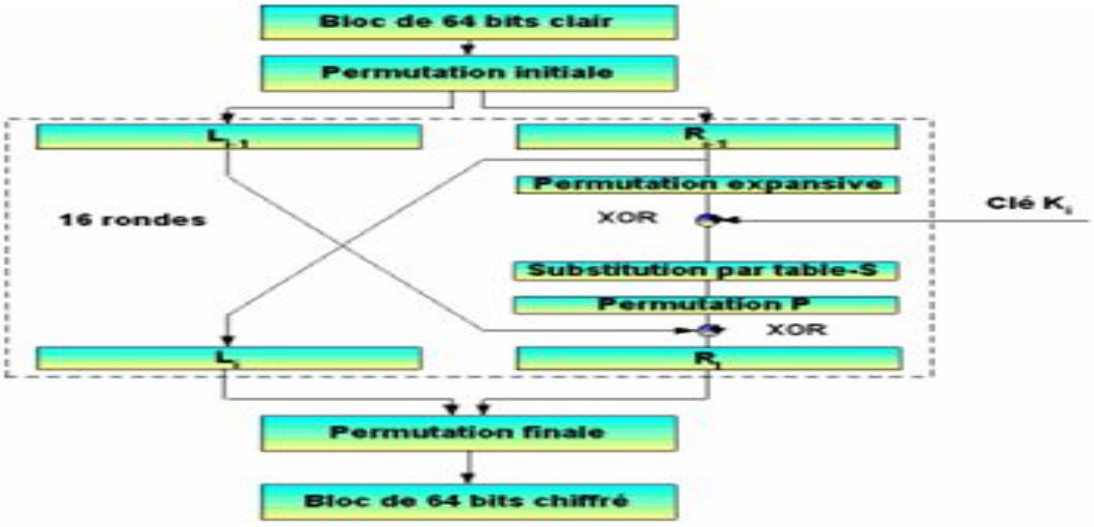



**Figure 1.6 : algorithme principale du DES.**

## ➢ Cryptage AES (Advanced Encryption Standard) :

L'algorithme prend en entrée un bloc de 128 bits (16 octets), la clé fait 128, 192 ou 256 bits. Les 16 octets en entrée sont permutés selon une table définie au préalable. Ces octets sont ensuite placés dans une matrice de 4x4 éléments et ses lignes subissent une rotation vers la droite. L'incrément pour la rotation varie selon le numéro de la ligne. Une transformation linéaire est ensuite appliquée sur la matrice, elle consiste en la multiplication binaire de chaque élément de la matrice avec des polynômes issus d'une matrice auxiliaire, cette multiplication est soumise à des règles spéciales selon GF(28) (groupe de Galois ou corps fini). La transformation linéaire garantit une meilleure diffusion (propagation des bits dans la structure) sur plusieurs tours.

Finalement, un XOR entre la matrice et une autre matrice permet d'obtenir une matrice intermédiaire. Ces différentes opérations sont répétées plusieurs fois et définissent un « tour ». Pour une clé de 128, 192 ou 256, AES nécessite respectivement 10, 12 ou 14 tours [17].

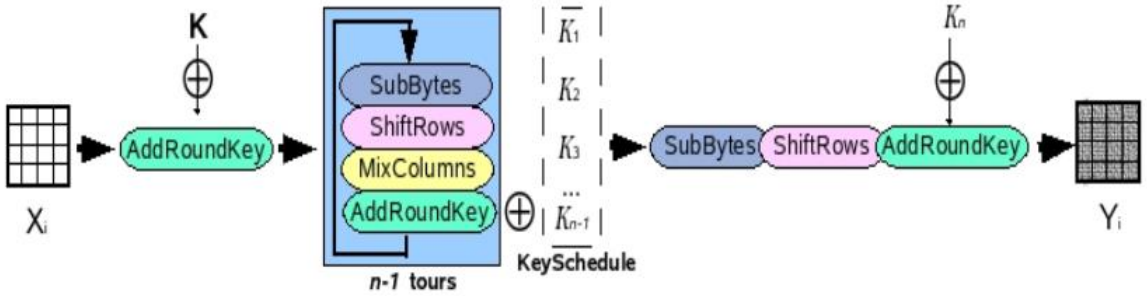



**Figure 1.7 : le schéma général d'AES.**

- **RSA :**

**L'algorithme RSA** a été inventé par Rivest Shamir et Adleman en 1977. Cet algorithme est un chiffrement à clé publique (ou chiffrement asymétrique)**.[18].**Il est basé sur le fait qu'il est facile d'effectuer la multiplication entre deux grands nombres premiers mais difficile de factoriser ce produit. Ce standard est basé sur le calcul de l'exponentiation modulaire pour le chiffrement et le déchiffrement. Une technique asymétrique ne peut être considérée comme sûre que si la taille de la clé utilisée est grande
(de l'ordre de 2048 bits actuellement) alors qu'un algorithme symétrique avec une clé de taille128 bits peut être considéré suffisamment sûr. [19]

Le chiffrement se fait selon [2]

$$C=M^e \bmod n$$

Et le déchiffrement par :

$$M=C^d \bmod n$$

Cet algorithme est utilisé pour le cryptage et la signature électronique.

- **DSA (Digital Signature Algorithm) :**

Le système DSA a été créé et certifié par le NIST, et a été spécifié comme algorithme de signature digitale. DSA sert uniquement comme système de signature et ne permet pas de chiffrer un message (inventé par David Kravitz)**.[2]**

## 1.8.1Signatures numériques :

Les signatures digitales (ou numériques) sont utilisées pour assurer l'authentification signataire, l'intégrité du message signé et la non répudiation. Pour signer un message le signataire utilise sa clé privée pour générer la signature et la signature sera vérifiée par la clé publique correspondante. Tout le monde peut vérifier la signature en utilisant la clé publique du signataire.**[15]**

## 1.9. Chiffrement classique :

La cryptographie classique concerne la période de l'antiquité jusqu'à l'apparition des Ordinateurs. Elle inclut tous les mécanismes et algorithmes basés sur des fonctions mathématiques ou logiques (exemple: César, Vigenère) .[20]

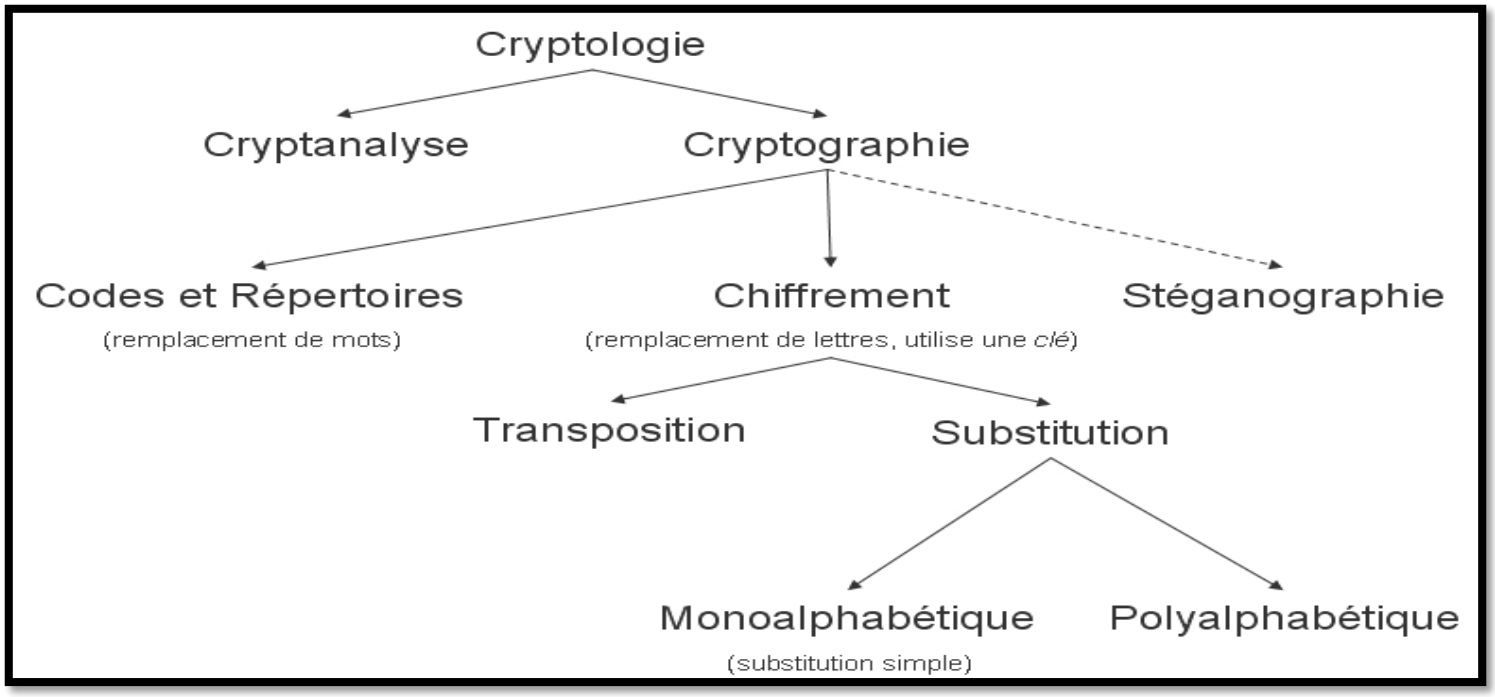



**Figure 1.8 : domaine inclus dans la cryptographie.**

### 1.9.1. Chiffrement par substitution :[21]

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

On distingue généralement plusieurs types de crypto systèmes par substitution :

- **La substitution mono alphabétique :** consiste à remplacer chaque lettre du message par une autre lettre de l'alphabet.

  .

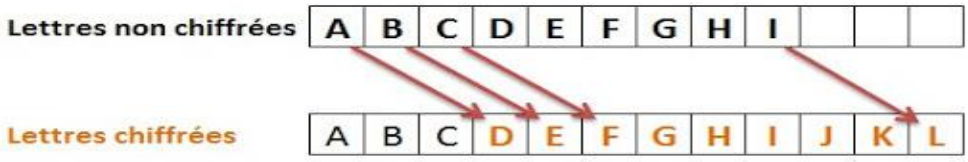



**Figure 1.9 : substitution mono alphabétique.**

**Exemple :**

Texte claire« la cryptographie »

Texte Crypté «iweqbgndtqwgkcy »

- **La substitution poly alphabétique :** consiste à utiliser une suite de chiffres mono alphabétique réutilisée périodiquement.

- **La substitution homophonique :** permet de faire correspondre à chaque lettre du message en clair un ensemble possible d'autres caractères.

- **La substitution de poly grammes :** consiste à substituer un groupe de caractères (poly gramme) dans le message par un autre groupe de Caractères.

## 1.9.2. Chiffrement par transposition :

Les méthodes de chiffrement par transposition consistent à réarranger les données à chiffrer de façon à les rendre incompréhensibles. Il s'agit par exemple de réordonner géométriquement les données pour les rendre visuellement inexploitables.[22]

**Exemple :** la scytale utilisée par les spartiates pour la transmission sécurisée.


**Figure 1.10 : scytale.**

Plusieurs variations de transposition sont utilisées, parmi eux on trouve :

- **Transposition simple (à base matricielle) :**

Elle consiste à écrire le texte en clair dans une matrice de n colonnes (une lettre dans chaque case), et ensuite de construire le texte chiffre en prenant les lettres à partir de cette matrice colonne par colonne. La clé dans ce cas est le nombre n.[23]

- **Transposition avec substitution simple :**

L'idée dans ce cas est de combiner la transposition avec une substitution simple.
Il s'agit ainsi de chiffrer le message clair par une méthode de substitution simple, et en suite d'en appliquer une transposition. Une autre astuce est souvent utilisée qui consiste à appliquer une fonction de permutation sur l'ordre d'arrangement des colonnes. [23]
On cite à titre d'exemple : le chiffre de DELASTELLE.

**1.9.3. Cryptage par produit :** C'est la combinaison de chiffrement par substitution et chiffrement par transposition. La plupart des algorithmes à clés symétriques utilisent le chiffrement par produit. On dit qu'un « round » est complété lorsque les deux transformations ont été faites une fois (substitution et transposition). Ces successions des rondes portent également le nom de réseaux S-P de Shannon.[4].

## 1.10. Conclusion :

Dans ce chapitre, nous avons présenté l'historique et la généralité de cryptographie .Nous avons débuté par terminologie et le but de la cryptographie, ainsi que la classification des crypto systèmes de chiffrement et de déchiffrement. Nous avons aussi abordé des exemples d'algorithmes de cryptage symétrique et asymétrique citons quelques avantages et inconvénients du chaque cryptage.

Dans le chapitre suivant, nous allons étudier les systèmes dynamiques et chaotiques.

# Chapitre 02 :

# Systèmes dynamiques et chaotiques

## 2.1. Introduction :

Depuis fort longtemps, la science a été dominée par le déterminisme et la prévisibilité. L'apparition de la théorie du chaos, qui a vu le jour dans les travaux d'Henri Poincaré, a poussé l'horizon des recherches scientifiques plus loin. Le chaos a fait l'objet de beaucoup d'études approfondies qui ont permis de l'introduire dans divers domaines. N'ayant pas de définition au sens universel, le chaos est décrit comme étant un cas particulier d'un système non linéaire déterministe, caractérisé par son comportement très sensible aux conditions initiales et bien qu'il soit déterministe, il est imprédictible à long terme, et présente un aspect aléatoire, sans pour autant faire partie des phénomènes aléatoires. [24]

## 2.2. Sémantique de la théorie du chaos :

Le mot chaos n'a pas ici le même sens que l'usage dans la vie courante. On retrouve trace de ce mot du grec Khaos dans les écrits de **Christine de Pisan** (Chemin de long estude) qui définit le chaos comme un

" État de confusion des éléments ayant précédé l'organisation du monde "

Au XVIème siècle Desportes, le décrit dans ses Elegies comme

" Toute sorte de confusion, de désordre "

Le chaos, dans son sens familier aujourd'hui, c'est le désordre et la violence, mais aussi l'inintelligibilité. Loin de ces considérations historiques et mythologiques, Chaos : un terme souvent utilisé comme métaphore du désordre. Et la théorie du Chaos a vu le jour dans les travaux d'Henri Poincaré à la fin du XIXe siècle et c'est dans les années soixante qu'elle fut redécouverte après la publication d'un article qui allait révolutionner le monde des sciences. Le chaos est devenu un champ d'exploration de la science,[25]

## 2.3. Historique du chaos :

-1890 Le Roi Oscar II de Suède octroie un prix au premier chercheur qui pourrait déterminer et résoudre le problème des n-corps des orbites des corps célestes et ainsi prouver la stabilité du système solaire. Jusqu'à ce jour, le problème n'a pas été résolu.

- 1890 Henri Poincaré gagne le premier prix du Roi Oscar II. Etant le plus proche à résoudre le problème de n-corps, il a découvert que l'orbite de trois corps célestes agissantes l'une sur

l'autre peut engendrer un comportement instable et imprévisible. Ainsi, le chaos est naît (mais pas encore mentionné !).

- 1963 Edward Lorenz découvre le premier système chaotique dans la météo ou encore appelé attracteur étrange.

- 1975 Tien-Yien Li et James A. Yorke ont présenté pour la première fois le terme "chaos" dans un article intitulé "Period three implies chaos".

- 1978 Mitchell Feigenbaum introduit un nombre universel associé au chaos.

- 1990 Edward Ott, Celso Grebogi et James A. Yorke. Introduisent la notion de contrôle du chaos.

- 1990 Lou Pecora. Synchronisation des systèmes chaotiques. [26]

## 2.4. Définition du chao :

Le terme chaos a été introduit avec sa signification actuelle en 1976 par Jim Yorke, un mathématicien de l'université du Maryland, mais le début des études du chaos peut être imputé a Henri Poincaré au début du XXe siècle, puis elles ont été ressuscitées en 1961 par le météorologue américain Edward Lorenz , professeur de mathématiques au MIT (Massachusetts Institute of Technology) qui est considéré après ses recherches sur le chaos , en tant que père officiel. Et depuis, ce concept a envahi beaucoup de domaines qu'ils soient physiques, mathématiques, politiques ou religieux [27].

Le phénomène du chaos est un phénomène complexe non linéaire, qui dépend de plusieurs paramètres et qui est caractérisé par une extrême sensibilité aux conditions initiales. Les systèmes chaotiques sont des systèmes dont les trajectoires évoluent dans une région bornée présentant un caractère stable mais sans toute fois converger vers un point fixe ou un cycle limite. Ces trajectoires qui restent denses dans cette région sont très sensibles aux conditions initiales. Les solutions des équations différentielles non linéaires ne peuvent pas être calculées avec exactitude analytiquement car il n'existe pas de méthode de résolution analytique pour ces équations, sauf pour certaines classes particulières. Elles sont alors déterminées numériquement et le comportement du système est analysé par simulation [28].

## 2.5. La différence entre le chaos et l'aléatoire :

La différence entre le chaos et l'aléatoire nous a paru le point le plus important de la compréhension du chaos. En effet, on a toujours tendance à considérer qu'un phénomène tire son imprédictibilité du nombre trop important de paramètres en jeu dans sa description. Ce qui nous pousse à en donner une approche probabiliste qui peut être parfaitement satisfaisante, garde par définition une certaine marge d'aléatoire. En ce qui concerne le chaos, il n'en est rien, les systèmes Chaotiques se comportent, en effet, d'une manière qui peut sembler aléatoire. Mais ce comportement est en fait décrit de manière déterministe par des équations non linéaires parfaitement déterministes, c'est-à-dire en particulier avec des outils mathématiques qui permettant une approche précise et certaine. Pour paraphraser une

publicité célèbre, on pourrait écrire : “Ça ressemble à du hasard, ça a le goût du hasard,...mais ce n’est pas du hasard !”.[8]

## 2.6. Condition obtention chaos :

Le chaos est défini généralement comme un comportement particulier d’un système dynamique qui inclut :

**a)la non-linéarité :** l’évolution irrégulière du comportement d’un système chaotique est due aux non linéarités.

**b)le déterminisme :** un système chaotique a des règles fondamentales déterministes et non probabilistes.

**c) la sensibilité :** le système manifeste une très haute sensibilité aux changements de conditions.

**d) l’imprévisibilité :** en raison de la sensibilité aux conditions initiales, qui peuvent être connues seulement à un degré fini de précision.

**e) l’irrégularité :** L’ordre caché comprenant un nombre infini de modèles périodiques instables (ou mouvements). Cet ordre caché forme l’infrastructure des systèmes chaotiques [29].

## 2.7. Les systèmes dynamiques :

### 2.7.1. Définition d’un système dynamique : [30]

Un système dynamique consiste en un espace de phase abstrait ou un espace d’état dont les coordonnées décrivent l’état dynamique du système à n’importe quel moment et dont une règle dynamique spécifie la tendance future immédiate de toutes les variables d’état composant le système, donnée par la valeur présente de ces mêmes variables d’état.

Mathématiquement, un système dynamique est décrit par un problème où seules sont données les valeurs de départ des variables d’état sont données. Il peut y avoir une composante de temps "discrète" ou "continue" Ce système est décrit par un ensemble d’équations différentielles ordinaires du premier ordre du type :

$$\frac{dx}{dt} \stackrel{\text{def}}{=} \dot{x} = \mathrm{f}\,(x,\, t)$$

## 2.7.2. Les systèmes dynamiques :

Un système dynamique est une structure qui évolue au cours du temps de façon à la fois :

– Causale, où son avenir ne dépend que de phénomènes du passé ou du présent.

– Déterministe, c'est-à-dire qu'à partir d'une « condition initiale » donnée à l'instant « présent» va correspondre à chaque instant ultérieur un et un seul état « futur» possible. L'évolution déterministe du système dynamique peut alors se modéliser de deux façons distinctes.

**Une évolution continue dans le temps,** représentée par une équation différentielle ordinaire.

**Une évolution discrète dans le temps,** l'étude théorique de ces modèles discrets est fondamentale, car elle permet de mettre en évidence des résultats importants, qui se généralisent souvent aux évolutions dynamiques continues. Elle est représentée par le modèle général des équations aux différences finies » [31].

## 2.7.3. Représentations mathématiques des systèmes dynamiques :

Un Système dynamique décrit par une fonction mathématique présente deux types de variables : dynamiques et statiques, les variables dynamiques sont les quantités fondamentales qui changent avec le temps, les variables statiques, encore appelés paramètres du système, sont fixes.

Dans le cas où le composant "temps" est **continu** le système dynamique est présenté par un système d'Equations différentielles de la forme :

$$\frac{dx}{dt} = f(x, t, p) \text{ ou } x \in R^n \text{ et } p \in R^r, n \text{ et } r \in N \qquad 2:1$$

Dans le cas où le temps est discret le système dynamique est présenté par une application itérative. $X_{k+1} = f(x_k, p)$, $x_k \in R^n$ et $p \in R^r$, $k = 1; 2; 3;$ 2:2

où p un paramètre, et $t \in T$, le domaine temporel. Lorsque le temps t ou indice k apparaissent explicitement dans les relations (2.1) et (2.2) le systèmes est dit **non-autonome**. En général, c'est un inconvénient majeur pour la résolution numérique et il est préférable de s'en affranchir. Par un changement de variables approprié, on peut transformer un système non autonome avec $X \in R_n$ en système **autonome** avec $X \in R_{n+1}$[32].

## 2.8. Attracteur :

La région de l'espace de phases vers laquelle convergent les trajectoires d'un système dynamique dissipatif s'appelle "attracteur".

Les attracteurs sont des formes géométriques qui caractérisent l'évolution à long terme des systèmes dynamiques.[25]

le bassin d'attraction d'un attracteur est l'ensemble des points de l'espace des phases qui donnent une trajectoire évoluant vers l'attracteurs considéré. On peut donc avoir plusieurs attracteurs dans un même espace des phases [33].

### 2.8.1Les types d'attracteurs :

Il existe deux types attracteurs : Attracteurs réguliers et attracteurs étranges (chaotiques).

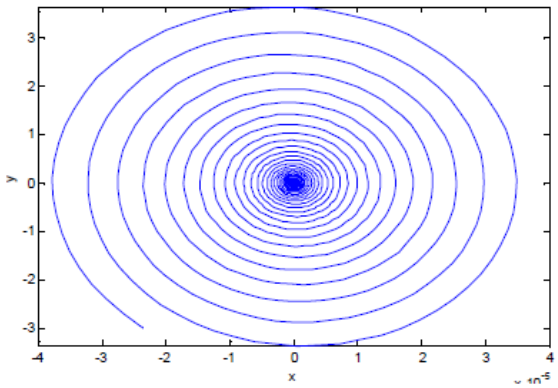
#### 2.8.1.1Attracteurs réguliers :

Un attracteur régulier caractérise les systèmes non chaotiques et peuvent être de 3 sortes :

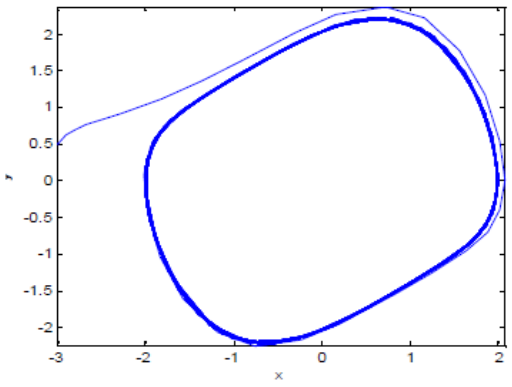
**a. L'attracteur "point fixe"** est un point de l'espace de phase vers lequel tendent les trajectoires, c'est donc une solution stationnaire constante.

**b. L'attracteur "cycle limite"** est une trajectoire fermée dans l'espace des phases vers laquelle tendent les trajectoires. C'est donc une solution périodique du système.

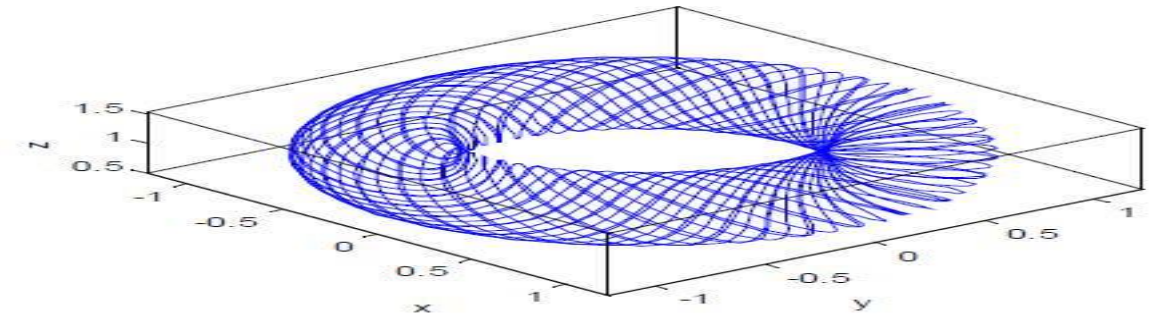
**b. L'attracteur "tore"** représente les mouvements résultant de deux ou plusieurs oscillations indépendantes que l'on appelle parfois "mouvements quasi périodiques".[25] .




(a)point fixe




(b) cycle limite



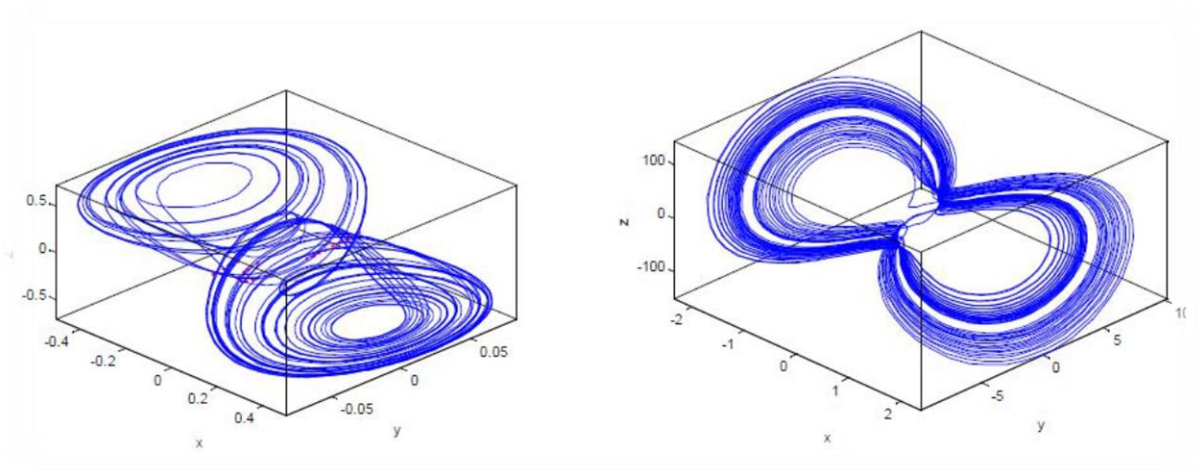

c) Tore

**Figure 11 : différent types d'attracteurs réguliers.**

### 2.8.1.2. Attracteurs étranges :

Le terme attracteur Etrange a été utilisé pour la première fois par David Ruelle et Floris Takens en 1971, afin de décrire l'attracteur obtenu par une série de bifurcations d'un système modélisant le courant d'un liquide. En fait, avant l'article Ruelle et Floris, les attracteurs avaient déjà l'objet de publications mais ils sont restés ignorés. Cette appellation d'attracteur Etrange fait appel à leur propriété peu commune, qui est leur dimension fractale. En effet la structure géométrique des trajectoires générées par un système chaotique est extrêmement complexe à cause des Etirements, repliements et contractions s'opérant dans une région bornée de l'espace d'État. La section de Poincaré d'une trajectoire chaotique est constituée d'une infinité des couches fines, ce qui suppose que les trajectoires tendent à remplir un espace de dimension non entière, c'est-a-dire fractale. Les attracteurs étranges sont l'une des caractéristiques de l'évolution des systèmes chaotiques : au bout d'un certain temps, tous les points de l'espace des phases (et appartenant au bassin d'attraction de l'attracteur) donnent des trajectoires qui tendent à former l'attracteur étrange. [34]

La figure 2.2 représente deux exemples d'attracteurs étranges :




Oscillateur de Chua

Oscillateur de Moore Spiegel

**Figure 12 : attracteurs étrange.**

### 2.8.1.3Quelques exemples d'attracteurs chaotiques :

Les attracteurs chaotiques scinder on deux type :

### 2.8.1.3.1analogique (continu) :

### a)Attracteur de Lorenz : [30]

L'attracteur de Lorenz tient son nom du météorologue Edward Lorenz qui l'a étudié le premier. C'est une simplification à l'extrême d'équations régissant les mouvements atmosphériques. Lorenz les a étudiés afin de mettre en évidence sur un système simple la sensibilité aux conditions initiales qu'il avait observées.

Les équations de ce système sont les suivantes :

$$\begin{cases} \frac{dx}{dt} = a(y - x) \\ \frac{dy}{dt} = bx - y - xz \\ \frac{dz}{dt} = xy - cz \end{cases}$$

On prendra : a= 10, b = 28 et c = 8/3.

La figure 2.3 représente l'attracteur étrange de Lorenz :

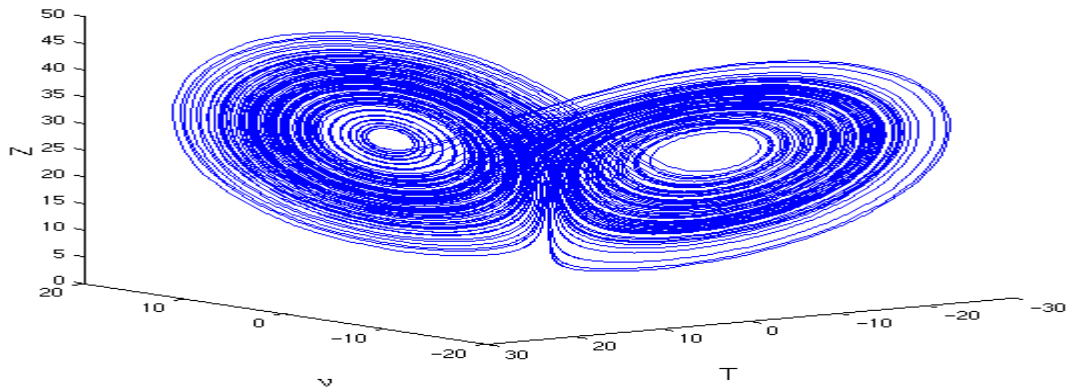



**Figure 13 : attracteurs Lorenz.**

## b) Système de Rössler :[18]

Il a été inventé par Otto Rössler en 1976. Ce simple système chaotique est présenté comme suit :

$$\begin{cases} X = -(y+z) \\ Y = x+ay \\ Z = (x-c)z+b \end{cases}$$

Avec a = 0.2, b = 0.2 et c = 5.7

La figure 2.4 montre l'attracteur de Rössler en 3 dimensions x(t), y(t) et z(t).

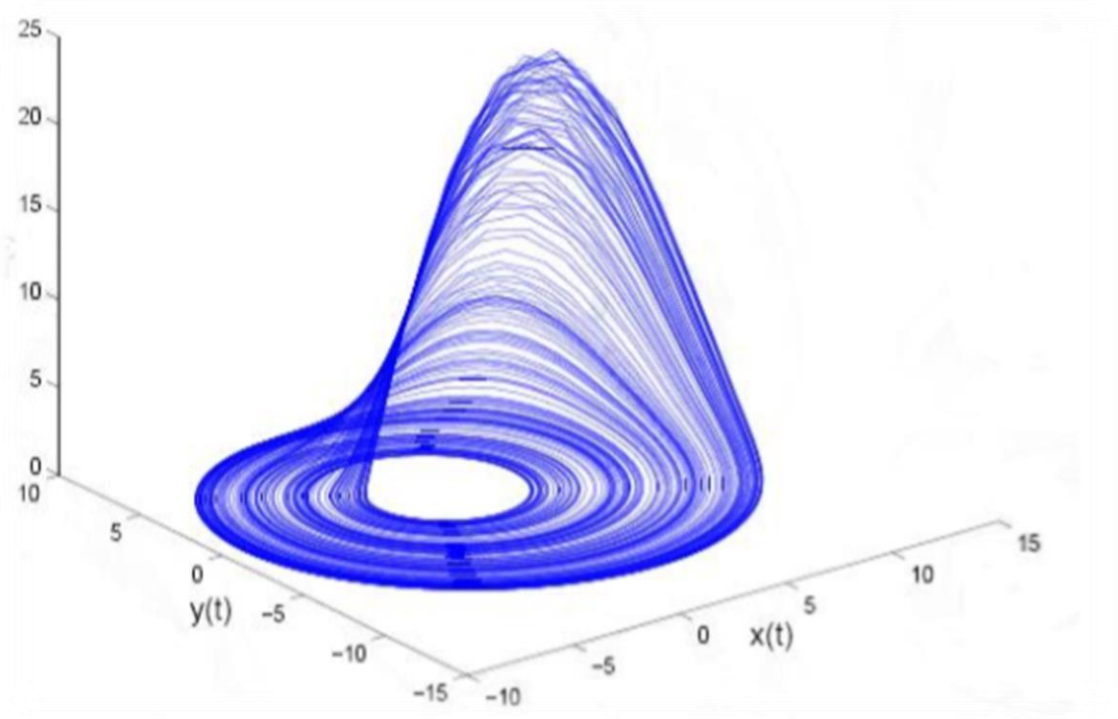



**Figure 14 :attracteurs Rössler.**

## c)Attracteur de Chua : [30]

Proposé par le professeur chinois LeonOng Chua en 1993, cet attracteur provient de l'étude de l'oscillateur chaotique de Chua. Les équations de ce système sont les Suivantes :

$$\begin{cases} \frac{dx}{dt} = \alpha*(y-x-c*x) \\ \frac{dy}{dt} = x-y+z \\ \frac{dz}{dt} = -\beta*y \end{cases}$$

On prendra : $\alpha$=10, $c$=−0.143, $\beta$=16.

La figure 2.5 représente l'attracteur étrange de Chua :

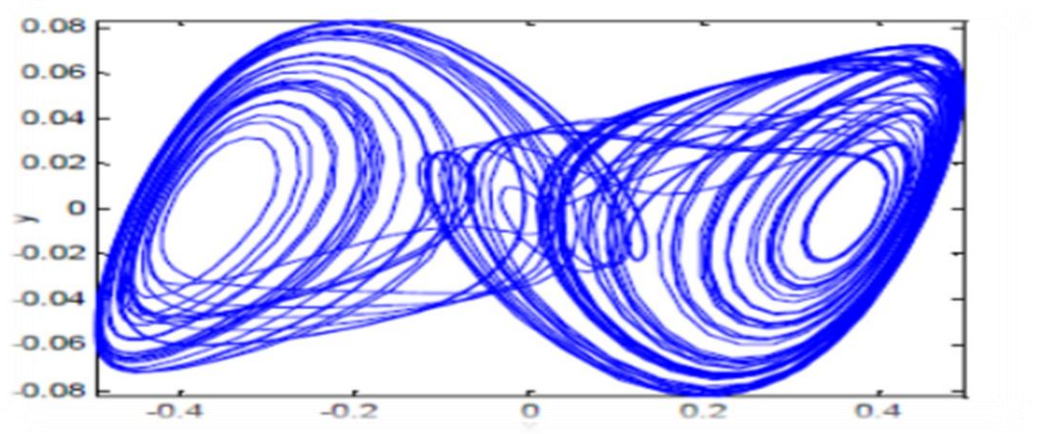



**Figure 15 : attracteurs Chua.**

## d) Système de Chen :[18]

Il est donné par le système d'équations suivant :

$$\begin{cases} \dot{a}=a(y-x) \\ \dot{Y}=(c-a)x-xz+cy \\ \dot{z}=xy-bz \end{cases}$$

La figure 2.6 montre l'attracteur de Chen en 3 dimensions x(t), y(t) et z(t) avec a=35, b=3 et c=28.

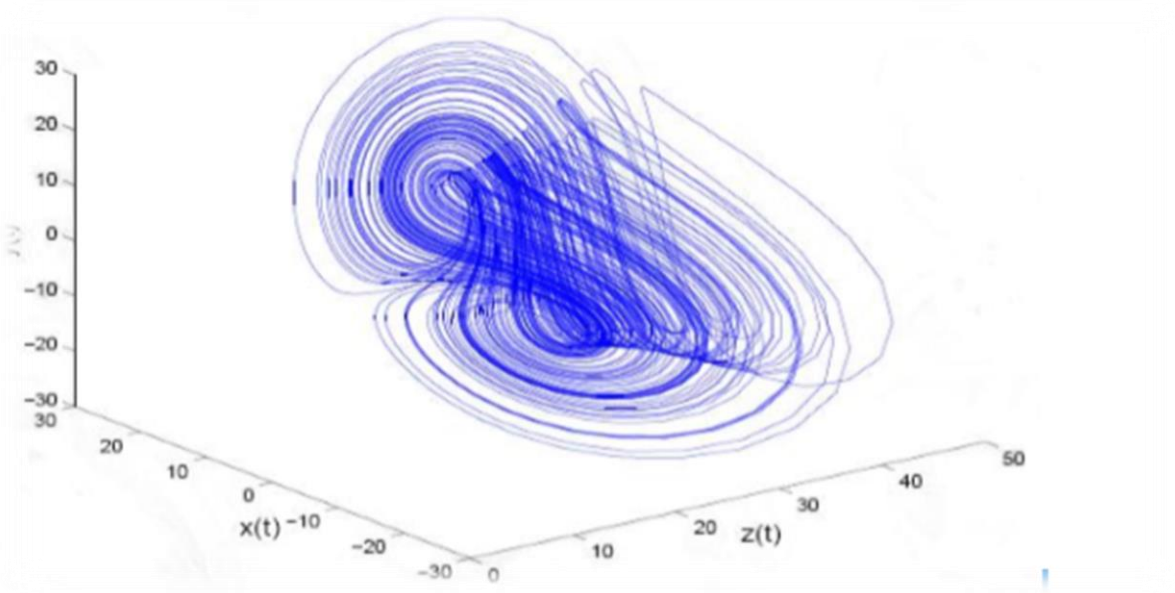



**Figure 16:attracteur chen.**

## 2.8.1.3.2.attracteurs numérique (discret) :

## a)Attracteur de Hénon : [26]

L'attracteur de Hénon est un système dynamique à temps discret. C'est l'un des systèmes dynamiques ayant un comportement chaotique les plus étudiés. L'attracteur de Hénon prend tout point du plan (x, y) et lui associe le nouveau point :

$$\begin{cases} \mathbf{X}n+1 = \mathbf{y}n+1 - \mathbf{a}\mathbf{X}^2n \\ \mathbf{y}n+1 = \mathbf{b}\mathbf{X}n \end{cases}$$

Avec (x, y) le vecteur d'état et a, b les paramètres du système. Le système de Hénon montre un comportement chaotique et génère un attracteur étrange pour a = 1.4, b = 0.3 avec x(0) = 0 et y(0) = 0 les conditions initiales du système.[26]

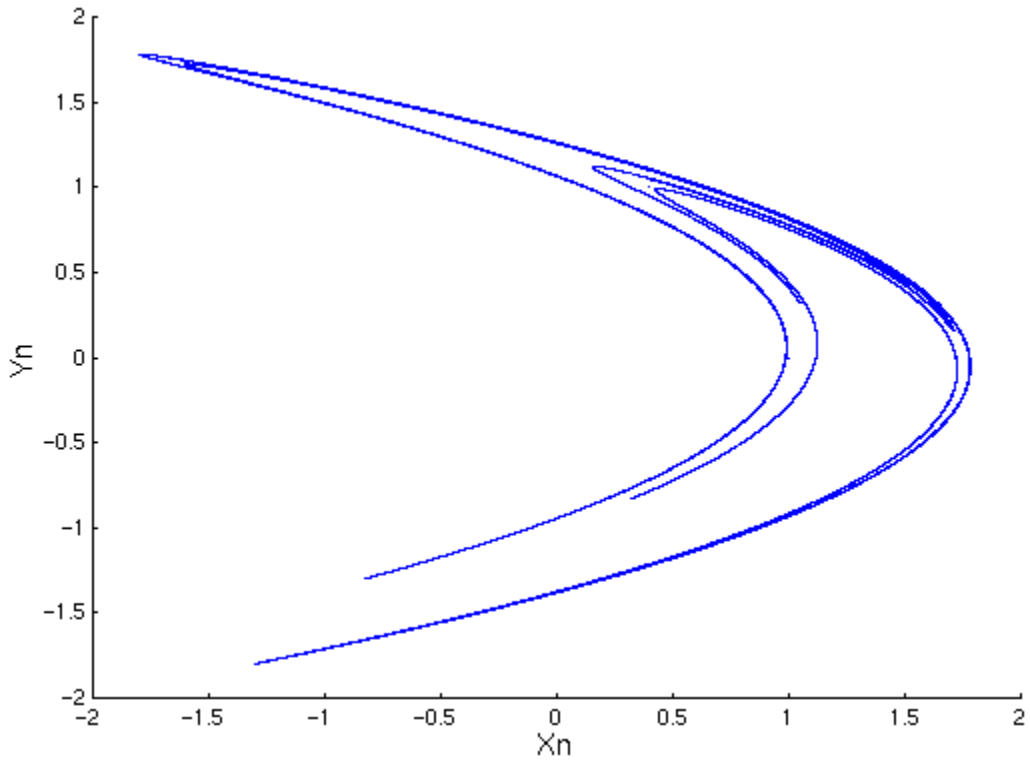



**Figure 17:attracteur de Henon.**

## b)Suite logistique (logistic map) :[2]

Cette fonction est donnée par l'équation suivante :

$x_{n+1=} rx_n(1-x_n)$

$x_n$ est compris entre 0 et 1 et r est un nombre positif compris entre 1 et 4.le comportement est chaotique a partir de r=3.57.

## Suites chaotiques linéaires par morceaux :

## c)Skew tent map :[18]

$$\mathbf{F(x)} = \begin{cases} \frac{x}{r}, & \mathbf{0 \le x < r} \\ (1-x)/(1-r), & \mathbf{r \le x < 1} \end{cases}$$

Il existe d'autres systèmes chaotiques discrets. Nous citons le système de Lozi qui consiste en le système de Henon pour lequel la non-linéarité $x_k^2$ est remplacée par $|x_k|$. **[35]**

## 2.9. Techniques de caractérisation du comportement chaotique :

L'identification des caractéristiques des systèmes non linéaires à partir d'observations peut se faire grâce à des outils issus du domaine des dynamiques non linéaires tels que : la section de Poincaré, l'espace des phases, le diagramme de bifurcation, les exposants de Lyapunov [36].

## 2.9.1. La section de Poincaré :

La section de Poincaré est un outil mathématique simple permettant de transformer un système dynamique **continu** en un système dynamique **discret**. Cette transformation s'opère via une réduction d'une unité de l'ordre du système. Soit un système dynamique continu, décrit dans un espace d'état de dimension n et une surface de dimension (n-1) définie dans cet espace. L'application de Poincaré est le système dynamique en temps discret dont la suite des itérés correspond aux coordonnées des points d'intersection successifs de la trajectoire avec cette surface.

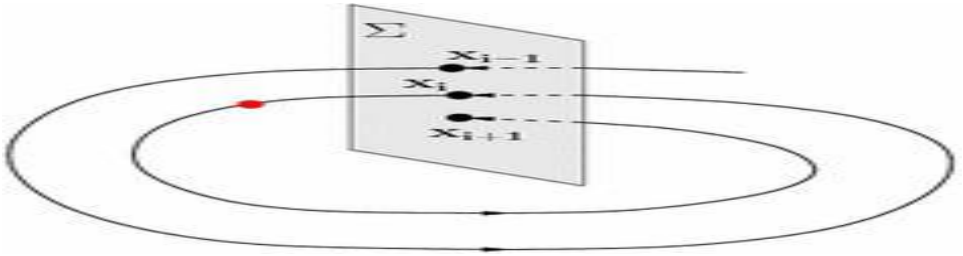



**Figure 18:section Poincaré.**

L'ensemble des points d'intersections, situés sur la surface représente la section de Poincaré. Dans un espace euclidien, le plan de la section doit être choisi de manière à garantir l'existence d'intersections avec la trajectoire Φ et de telle sorte que celle-ci le traverse alternativement dans un sens puis dans l'autre.

On peut définir trois applications différentes de Poincaré.

$\mathbf{p}^+$ décrit les points où **Φ** traverse le plan dans le sens du vecteur normal,

$\mathbf{p}^-$ dans le sens contraire

**p±** décrit la suite des points d'intersection quel que soit le sens de traversée.

Si **Φ** est bornée sans tendre asymptotiquement vers un équilibre et définie sur un espace euclidien, alors il existe toujours une surface pour laquelle les trois applications de Poincaré sont définies. [36]

## 2.9.2. La bifurcation :

La théorie de bifurcation est l'étude mathématique des changements qualitatifs ou topologiques de la structure d'un système dynamique .Une bifurcation survient lorsqu'une variation quantitative d'un paramètre du système engendre un changement qualitatif des propriétés d'un système telles que la stabilité, le nombre de points d'équilibre ou la nature des

régimes permanents. Les valeurs des paramètres au moment du changement sont appelées valeurs de bifurcation. Dans les systèmes dynamiques, un diagramme de bifurcation montre les comportements possibles d'un système, à long terme, en fonction des paramètres de bifurcation [37].

### 2.9.3. Les exposants de Lyapounov :

Le mathématicien Alexander Lyapounov a étudié le phénomène de la sensibilité aux conditions initiales des systèmes chaotiques et a développé un degré permettant de mesurer la vitesse à laquelle ces petites variations peuvent s'amplifier ; cette quantité est appelée « Exposant de Lyapounov ». Autrement dit, l'exposant de Lyapounov est le taux de divergence entre l'évolution des trajectoires issues de conditions initiales proches au sein de l'attracteur étrange [38].

## 2.10. Routes vers le chaos :

Il existe plusieurs types d'évolution possibles d'un système dynamique régulier vers le chaos. Le système peut passer d'un état stationnaire à un état périodique, puis au delà d'un certain seuil, à partir d'un scénario de transition pour devenir chaotique. On distingue trois scénarios théoriques d'évolution vers le chaos. [39]

### 2.10.1. Par intermittences :

Le système conserve pendant un certain laps de temps un régime périodique ou pratiquement périodique, c'est à dire une certaine "régularité", et il se déstabilise, brutalement, pour donner lieu à une sorte d'explosion chaotique. Il se stabilise de nouveau ensuite, pour donner lieu à une nouvelle "bouffée" plus tard. On a constaté que la fréquence et la durée des phases chaotiques avaient tendance à s'accroître plus on s'éloignait de la valeur critique de la contrainte ayant conduit à leur apparition. [8].

### 2.10.2. Par doublement de la période :

Par augmentation du paramètre de contrôle de l'expérience, la fréquence du régime périodique double, puis est multipliée par 4, par 8, par 16 < etc. Les doublements étant de plus en plus rapprochés, on tend vers un point d'accumulation auquel on obtiendrait hypothétiquement une fréquence infinie. C'est à ce moment que le système devient chaotique. [8]

### 2.10.3. La quasi-périodicité :

Qui intervient quand un deuxième système perturbe un système initialement périodique. Si le rapport des périodes des deux systèmes en présence n'est pas rationnel, alors le système est dit quasi périodique. Ce scénario un peu compliqué est relié à la théorie des nombres, notamment aux travaux de Jean Christophe Yoccoz, lauréat de la Médaille Fields en 1994, pour ses travaux sur les systèmes dynamiques [32].

## 2.11. Propriétés systèmes chaotiques :

### 2.11.1. Sensibilité aux conditions initiales (SCI) :

Tout d'abord, les systèmes chaotiques sont extrêmement sensibles aux perturbations. On peut illustrer ce fait par l'effet papillon, popularisé par le météorologue Edward Lorenz. L'évolution d'un système dynamique chaotique est imprédictible dans le sens qu'elle est sensible aux conditions initiales. Ainsi, deux trajectoires de phases initialement voisines s'écartent toujours l'une de l'autre, et ceci quelle que soit leur proximité initiale. Il est clair que la moindre erreur ou simple imprécision sur la condition initiale empêche de décider à tout temps qu'elle sera la trajectoire effectivement suivie et, par conséquence, de faire une prédiction autre que statistique sur le devenir à long terme du système. Ainsi, bien que l'on traite de systèmes déterministes, il est impossible de prévoir à long terme leurs comportements. La seule manière est d'opérer effectivement l'évolution du système. Si cette simulation se fait informatiquement, un problème de précision sur les conditions initiales se pose alors : de petites erreurs d'arrondissement dues à la précision du type de la variable codant ces conditions initiales peuvent exponentiellement s'amplifier de telle sorte que la trajectoire de phases obtenue n'est pas représentative de la réalité. Illustrons ce phénomène de SCI par une simulation numérique. On affecte à un système chaotique deux conditions initiales très proches. Dans un premier temps, les deux systèmes évoluent de la même manière; mais, très vite, leur comportement devient différent. Ceci est illustré dans la figure suivante. [35]

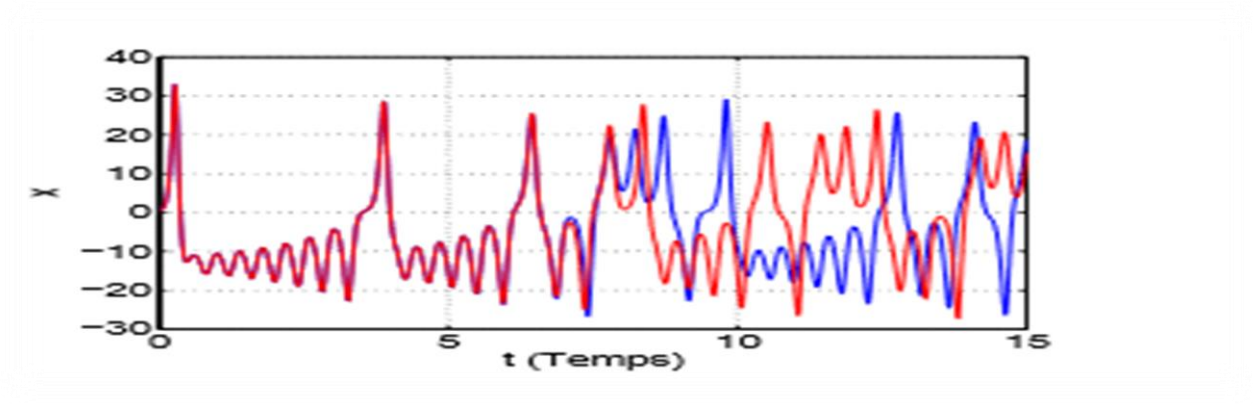



**Figure 19:évaluation dans le temps pour deux conditions initiales très proches.**

## 2.11.2. Aspect aléatoire :

Les courbes précédentes (Figure 2.10) illustrent la sensibilité aux conditions initiales. Cependant, une autre caractéristique des systèmes chaotiques peut être observée sur les courbes précédentes. En effet, un système chaotique évolue d'une manière qui semble aléatoire. La courbe suivante permet de comparer une évolution simple, périodique et donc prédictible d'un système classique avec l'évolution plus complexe, non périodique et non prédictible d'un système chaotique.

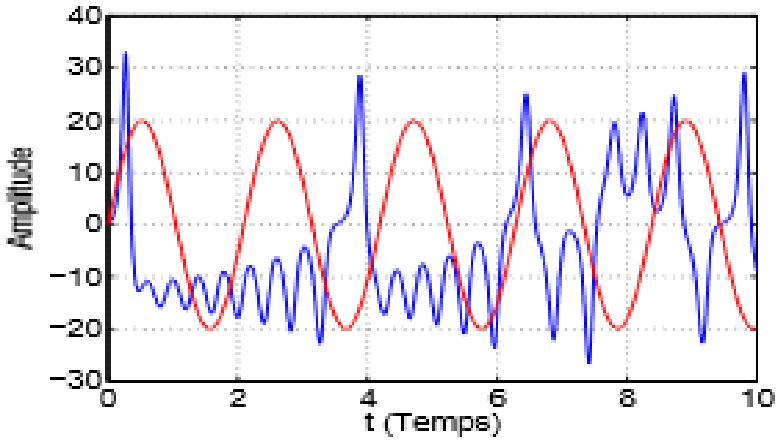



**Figure 20:évolution dans le temps d'un système chaotique, comparé a une sinusoïde.**

Ainsi, les systèmes chaotiques semblent évoluer de manière aléatoire. En tout cas, on ne peut prévoir facilement quelle sera leur évolution dans le temps.

Notons que les systèmes chaotiques obéissent tout de même aux lois de la physique. Si on se place dans l'approximation de la physique classique, on peut affirmer que le système est totalement déterministe. Il ne faut donc pas se laisser abuser par le caractère a priori aléatoire qui ne dénote qu'une complexité du système.[35]

### 2.11.3. Degré de liberté :

L'étude du chaos nécessite de travailler dans l'espace des phases du système. C'est un espace mathématique contenant N dimensions, où N est le nombre de variables physiques nécessaires pour décrire la dynamique du système. Chaque

variable doit être indépendante des autres, dans le sens qu'il est possible de fixer les (N-1) tout en la faisant varier. On dit alors que le système possède N degrés de liberté.

Si on considère par exemple une roue, fixée à un axe, lui-même fixé dans le sol, le tout dans un matériau rigide, le seul "paramètre" qui peut changer d'un point de vue mécanique, c'est la vitesse angulaire de la roue. Ce paramètre est appelé degré de liberté. On dit alors qu'il s'agit d'un système à un degré de liberté.

Maintenant, si cette roue a la possibilité de se déplacer le long d'un axe, on a deux nouveaux "paramètres" : l'abscisse et la vitesse le long de l'axe. Ce sont deux degrés de liberté de plus. Il s'agit donc d'un système à 3 degrés de liberté. [2]

### 2.11.4. Espace de phase :

La sensibilité aux conditions initiales est le problème majeur du chaos, elle empêche Toute prédiction sur l'évolution du système au delà d'un certain temps. Une erreur $\varepsilon 0 > 0$ sur la condition initiale va évoluer exponentiellement. L'erreur à un instant *t*, aura l'expression suivante:
On peut calculer la valeur de λ, appelé *exposant de Lyapunov*, grâce aux méthodes $|\varepsilon(t)| = \varepsilon e^{\lambda t}$ développées par Alexandre Lyapunov. Une façon de contourner ce problème est d'éliminer le temps entre les équations. C'est le rôle de *l'espace des phases* (ou espace des états), il s'agit d'un espace de dimension 2 ou 3 dans lequel chaque coordonnée est une variable d'état du système considéré.**[40]**

## 2.12. Conclusion :

Dans ce chapitre, et après avoir abordé l'historique du chao, on a présenté les principaux notions de système dynamique et chaotique, on a étudié les attracteurs en temps continu et discret. Ainsi que les scénarios de passage du point fixe vers le chaos .Puis la technique du comportement chaotique tel que la section de Poincaré, l'espace des phases, bifurcation, les exposants de Lyapunov.

Et finalement, nous avons vu des propriétés et caractéristique du système chaotique.

Dans le prochain chapitre, nous allons passer à la technique de chiffrement chaotique.

# Chapitre 03 :

# Les Techniques de chiffrement chaotiques

## 3.1. Introduction :

La fonction de sécurité la plus répandue de nos jours, est le chiffrement, mais la plupart des algorithmes de chiffrement actuels ont déjà été cassés et sont donc devenus sans garantie. La cryptographie chaotique est récente et a démontré une fiabilité de la sécurité tant bien qu'elle a démontré une grande résistance à la cryptanalyse. [**24]**
Dans ce chapitre, nous allons étudier les techniques de chiffrement par chao et les différentes attaques cryptanalytique.

## 3.2. Cryptographie Chaotique :

### 3.2.1. Principe :

La cryptographie chaotique est l'une des alternatives développées durant cette dernière décennie. Elle répond non seulement aux exigences de la sécurité mais elle a démontré une grande résistance à la cryptanalyse, comme elle est parfaitement combinée avec le maintien des attributs nécessaires aux algorithmes de chiffrement. Sachant qu'il y a deux types de fonctions chaotiques, part celles qui ont un comportement purement chaotique et qui ne sont pas modélisables, et d'autre part les fonctions chaotiques déterministes qui sont modélisables par des systèmes d'équations qu'on nomme « systèmes dynamiques non linéaires », et ce sont ces dernières qui sont utilisées dans le chiffrement chaotique car leurs attracteurs sont sous forme fractale et rendent l'évolution des trajectoires totalement dépendantes des conditions initiales, et il est donc impossible de prédire ces trajectoires sans connaitre leurs états initiaux, ce qui rend le comportement chaotique imprévisible, et leur sécurité quasi totale. Et pour les introduire dans le chiffrement il faut d'abord choisir une fonction chaotique, ensuite il faut superposer le signal chaotique au flux de données à transmettre selon l'une des techniques choisies pour le cryptage par chaos.[24].

## 3.3. Méthode de transmission chaotique :

La méthode de cryptage chaotique a été la première solution proposée dans la littérature comme application du chaos aux communications.il est possible d'employer des signaux chaotiques continus comme porteur d'information. Dans le cas le message est codé par l'émetteur et il décodé et extrait du signal chaotique par le récepteur [38]
Parmi les méthodes de transmission chaotique, on peut citer : Méthode par addition, par commutation, par modulation par inclusion et cryptage mixte.

### 3.3.1. Méthode d'inclusion :

Cette technique consiste à injecter le message dans la dynamique de l'émetteur, sans toutefois réaliser une modulation de paramètre. La restauration de l'information se fait principalement par 2 techniques, reposant soit sur les observateurs ont entrées inconnues, soit sur l'inversion du système émetteurs. **[41]**

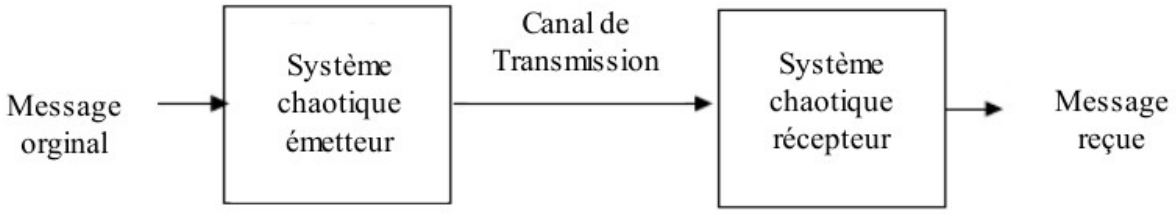



**Figure 21:cryptage par inclusion.**

### 3.3.2. Cryptage par décalage chaotique (CSK) :( commutation)

La méthode de décalage illustrée par la figure 3.2 a été réservée à la transmission de messages numériques [**42**]. Dans ce schéma de communication, le message d'information est utilisé pour commuter le signal transmis entre deux attracteurs chaotiques statistiquement similaires, qui sont utilisés respectivement pour coder le bit 0 et le bit 1 du message d'information numérique.
Ces deux attracteurs sont générés par deux systèmes chaotiques de même structure et de paramètres différents. A la réception, le signal reçu est utilisé pour produire un système chaotique identique à ceux de l'émetteur. Le message d'information est restitué par application d'un filtre passe-bas et ensuite un seuillage de l'erreur de synchronisation e(t).

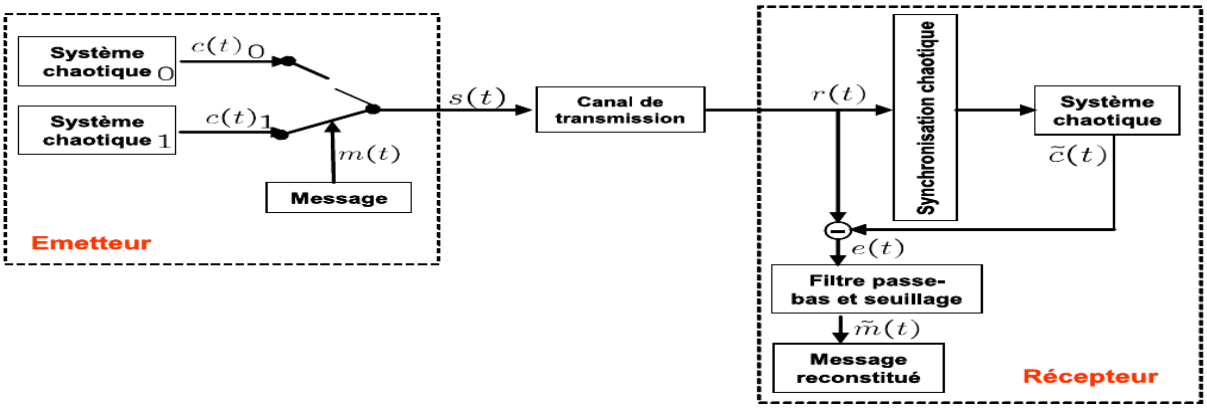



**Figure 22:cryptage CSK.**

### 3.3.3. Cryptage par modulation paramétrique :

L'approche par modulation utilise le message contenant l'information pour moduler un ou plusieurs paramètres θ de l'émetteur chaotique. Un contrôleur adaptatif est chargé de maintenir la synchronisation au niveau du récepteur, tout en suivant le changement du paramètre modulé. Le schéma correspondant est présenté par la figure 3.3 Au niveau de l'émetteur, le fait de moduler un ou plusieurs paramètres impose à la trajectoire un changement continu de l'attracteur et de ce fait, le signal transmis est plus complexe qu'un signal chaotique normal. Cependant, la façon d'injecter le message et donc la fonction démodulation des paramètres ne doivent pas supprimer le caractère chaotique du signal envoyé au récepteur. [41]

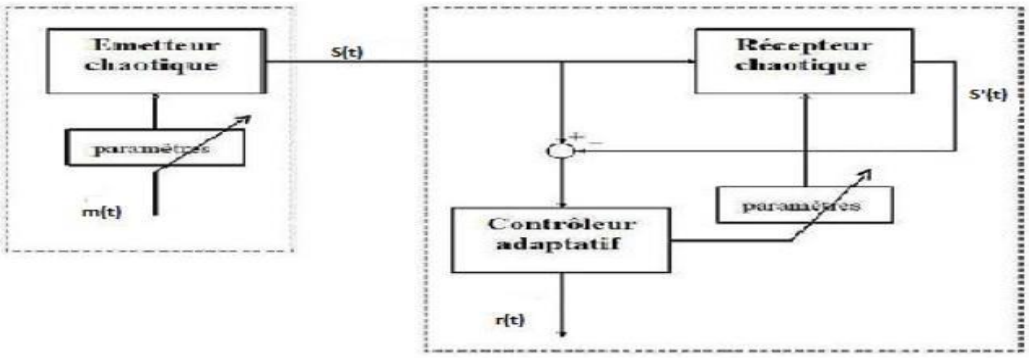



**Figure 23:cryptage par modulation paramétrique.**

### 3.3.4. Masquage par addition (The additive chaos masking scheme) :

Cette technique développée en 1993 [**43**] est illustrée par la figure 3.4 Elle consiste en deux systèmes chaotiques identiques, l'émetteur et le récepteur. Le signal chaotique c(t) est l'une des variables d'état du système dans l'émetteur. Le message d'information (le signal utile qui doit être crypté) m(t), qui est typiquement très faible devant c(t), est ajouté au signal c(t) et donne le signal transmis s(t). Comme c(t) est très complexe et m(t) est beaucoup plus petit que c(t), alors il est difficile de séparer m(t) du signal s(t) sans connaître c(t).

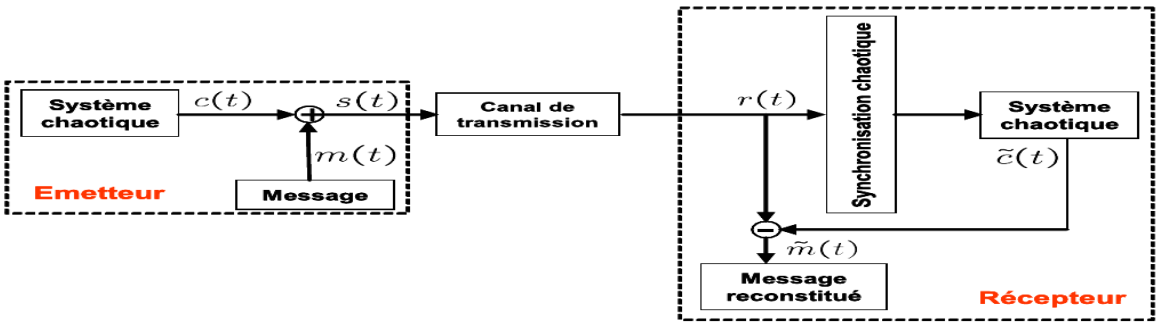



**Figure 24:cryptage par addition.**

### 3.3.5. Cryptage Mixte :

Afin de faire face aux problèmes de sécurité des méthodes précédentes, une nouvelle technique combinant les principes de la cryptographie standard et la synchronisation chaotique a été proposée. Le message *u(t)*contenant l'information est crypté grâce à une clé, *c(t)*, générée par l'émetteur chaotique.

Le message crypté est alors injecté dans la dynamique du système chaotique, pour la rendre plus complexe. Ensuite, un signal y(t) fonction des variables d'état de l'émetteur est transmis au récepteur, qui établit une synchronisation avec l'émetteur. La clé est alors reconstruite par le récepteur, qui peut finalement décoder le message. Le principe général de cette méthode est illustré par la figure (3.5).[28]

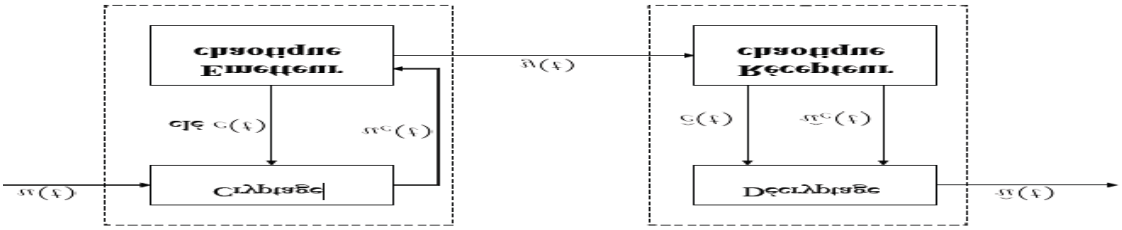


**Figure 25:cryptage mixte.**

## 3.4. Comparaison entre la cryptographie classique et chaotique : [38]

| **Cryptographie classique** | **Cryptographie chaotique** |
|---|---|
| Valeurs entières sur un corps fini | Valeurs continues en utilisant une représentation en virgule fixe ou flottante |
| Méthodes algébriques | Méthodes analytiques |
| Méthodes analytiques<br>Réalisation numérique en arithmétique entière | Réalisation numérique en arithmétique non entière |

**Tableau 3.1:la comparaison entre le cryptage chaotique et classique.**

## 3.5. La cryptanalyse :

Il s'agit de l'étude des mécanismes théoriques ou techniques visant à briser (casser) un algorithme de chiffrement, c'est-à-dire le fait de retrouver le message M à partir de C, sans connaître la clé K a priori.
Dans certains cas, il s'agira également de retrouver cette clé K.
On parlera d'"attaque" cryptanalytique [10] . Les attaques sont classifiés en deux types :
**Un attaquant passif** : qui surveille seulement la communication et essaie de casser la confidentialité.
**Un attaquant actif** : qui ajoute, supprime et modifie des messages. Il essaie de casser la confidentialité et aussi d'autres fonctions de sécurité. **[15]**

Il en existe 4 grands types, chacun pouvant utiliser différentes techniques. Ce chapitre présentera ensuite quelques attaques souvent évoquées dans la littérature spécialisée dans le domaine de la cryptologie.[10]

### 3.5.1. Les différentes attaques cryptanalyse :

- **Attaque sur le texte chiffré uniquement (ciphertext-only) :**

L'attaquant a connaissance du texte chiffré de plusieurs messages [12]

- **Attaque à texte clair connu (known-plain text attack) :** disposition de couple de message (clairs, chiffrés).[13]

- **Attaque sur un texte clair sélectionné (chosen-plain text attack) :**

l'attaquant peut choisir le texte en clair et obtient aussi le texte chiffré correspondant (et essaye à nouveau de trouver la clé de déchiffrement**).[15]**

- **Attaque à texte en clair choisi adaptative : (Adaptive chosen plain text attack) :**

c'est l'attaque la plus facile à mettre en œuvre. En effet, l'attaquant peut choisir les textes en clair qu'il donne à chiffrer au système et il peut les adapter (modifier) en fonction du résultat du chiffrement. Ceci permet au cryptanalyste (l'attaquant qui pratique la cryptanalyse) de modifier son texte en clair en fonction du résultat du chiffrement correspondant et d'arriver ainsi assez vite à déchiffrer tout texte, si l'algorithme de chiffrement utilisé n'est pas assez robuste.

Parmi ces modèles, seulement les deux premières attaques sont disponibles pour un attaquant passif. Dans ce cas l'attaquant doit essayer toutes les combinaisons des clés possibles pour le

déchiffrement. Cette attaque est connue sous le nom de l'attaque par **force brute** ou **par recherche exhaustive.**

Par conséquent, la taille des clés secrète doit être assez importante pour que cette attaque ne soit pas techniquement faisable
Ces modèles d'attaques s'appliquent également pour les attaques contre la protection de l'intégrité et de l'authentification.[15]

### 3.5.2. Cryptanalyse différentielle :

Elle a été proposée par Eli Biham et Adi Shamir en 1991. Elle permet de trouver la clef en utilisant une quantité de textes clairs. L'idée est de fournir comme entrée des textes clairs avec de légères différences (un bit par exemple). Ensuite, on analyse statistiquement le comportement des sorties selon les entrées pour retrouver la clef. En regardant comment les différences en entrée affectent les sorties, on peut établir des règles statistiques. Il existe plusieurs variantes des cryptanalyses différentielles, nous distinguons : différentielle tronquée, différentielle d'ordre supérieur et différentielles impossibles.[12]

### 3.5.3. Cryptanalyse linéaire :

Elle a été inventée par Mitsuru Matsui en 1993. Elle nécessite une quantité n de couples (texte clair, texte chiffré), tous chiffrés avec la même clef. Le principe est que le même message soit chiffré plusieurs fois avec des clefs différentes pour construire une immense table (téraoctet) qui contient toutes les versions chiffrées de ce message. Lors d'une interception d'un message chiffré, on peut le retrouver dans la table et obtenir la clef qui avait été utilisée pour le cryptage. Cette attaque n'est bien sûr pas faisable car nous aurions besoin d'une table trop importante. Le génie d'Hellman a été de trouver un moyen pour réduire cette table, processus réalisable. Celui-ci consiste à faire une approximation linéaire de l'algorithme pour le simplifier.[12]

## 3.6. Conclusion :

Dans ce chapitre on a introduit le principe de cryptographie par chaos. Nous avons expliqué les différentes méthodes de transmission chaotique tels que : cryptage par modulation, par inclusion par décalage CSK et cryptage additif et mixte.
On a définit la cryptanalyse et les attaques cryptanalytique, et nous avons fait une petite étude comparative entre le chao et cryptographie.

# Implémentations et Résultats

## 4.1. Introduction :

Nous avons présenté dans le chapitre précédent, une vue sur le chiffrement à base de chao , dans ce chapitre nous présentons un algorithme basé sur la technique de chao , une description de l'algorithme est suivie par les expérimentations réalisées font l'objet des différents sections.

## 4.2. Principe de l'algorithme de cryptage et de décryptage proposé :

Le nouveau algorithme de cryptage d'image basé sur les étapes suivant :

**Étape 1.** Lisez une image simple A et obtenez sa taille m × n.

**Étape 2.** Générez deux séquences chaotiques H, L avec clés$\bar{x}$, $\hat{x}$et p, q. Effectuez brouillage des lignes et des colonnes de image A, et obtenez une image permutée B.

Nous supposons que l'image brute originale A de taille m × n doit être chiffrer. Ensuite, deux séquences chaotiques doit être générer dans un processus de substitution.

les valeurs initiales H et L sont choisies pour être itérées en fonction de Chebyshev discrète $x_i = T_k(x_i - 1), \forall k \geq 2, i = 1, 2, ,$ nous choisissons k = 4 pour petit calcul et bonne propriété de Chebyshev, , l'équation d'itération est :

$xi = 8x^4_{i-1} - 8x^2_{i-1} + 1, i = 1, 2,....$

**Étape 3.** Créer une séquence pseudo-aléatoire {μi} de mn valeurs avec les touches x0, y0 et le paramètre de contrôle r.

**Étape 4**. Organisez B en un vecteur b de gauche à droite et de haut en bas.

**Étape 5.** Effectuez le processus de diffusion suivant pour b avec {μi}:

$$c_i = \text{round}(\mu i \times 255) \otimes c_{i-1}.$$

ou :

$\oplus$ : xor bit par bit

$c_{i-1}$ : représente la valeur actuelle du pixel

$c_{i-1}$ : la nouvelle valeur de le pixel après son chiffrement.

**Étape 6 :** Réarranger le vecteur c en image C pour obtenir l'image crypté**.**

## 4.3. Expérimentations et résultats :

Nous avons implémenté l'algorithme en langage python , pour tester ses performances. Cette section présente et discute les résultats obtenus.

### 4.3.1. Environnement de travail :

Nous avons implémenté l'algorithme sur un pc Hp I5 , ram 4G , DD 500 Go , sous le système d'exploitation Windows 10.

### 4.3.2Langage de programmation :

Python est un langage de programmation, dont la première version est sortie en **1991.** Créé par Guido van Rossum, il a voyagé du Macintosh de son créateur, qui travaillait à cette époque au Centrum voor Wiskunde en Informatica aux Pays-Bas, jusqu'à se voir associer une organisation à but non lucratif particulièrement dévouée, la Python Software Foundation, créée en 2001.
Python est un langage puissant, à la fois riche en possibilités. Dès l'instant où vous l'installez sur votre ordinateur, vous disposez de nombreuses fonctionnalités intégrées au langage. Ainsi, il existe ce qu'on appelle des bibliothèques qui aident le développeur à travailler sur des projets particuliers.[44]


**Figure 4.1 : logo de python.**

Python est un langage de programmation de haut niveau interprété (il n'y a pas d'étape de compilation) et orienté objet avec une sémantique dynamique. Il est très sollicité par une large communauté de développeurs et de programmeurs. Python est un langage simple, facile à apprendre et permet une bonne réduction du cout de la maintenance des codes. Les bibliothèques (packages) python encouragent la modularité et la réutilisabilité des codes. Python et ses bibliothèques sont disponibles (en source ou en binaires) sans charges pour la majorité des plateformes et peuvent être redistribués gratuitement.[45]

3. Corpus de test

## 4.4.Discussion des résultats

### 4.4.1Analyse de la sécurité :

Un bon algorithme de chiffrement devrait être robuste contre les attaques issues. Dans cette partie, nous discutons de l'analyse de sécurité de l schéma de cryptage d'image proposé. Les méthodes de l'analyse statistique telles que : l'histogramme, la corrélation entre deux pixels adjacents voisins, l'analyse de sensibilité à la clé, et l'analyse différentielle, sont évaluées pour prouver que l'algorithme proposé offre une grande sécurité contre les attaques les plus connues.

Les expérimentations sont faites avec les paramètres suivant :

$\bar{x}$= 0.393, $\hat{x}$=−0.644, $p$ = 21, $q$ = 43, $x0$ =−0.236, $y0$ = 0.522, $r$ = 16

- Cryptage puis décryptage de l'image avec l'algorithme proposé :

**(a)** **(b)**

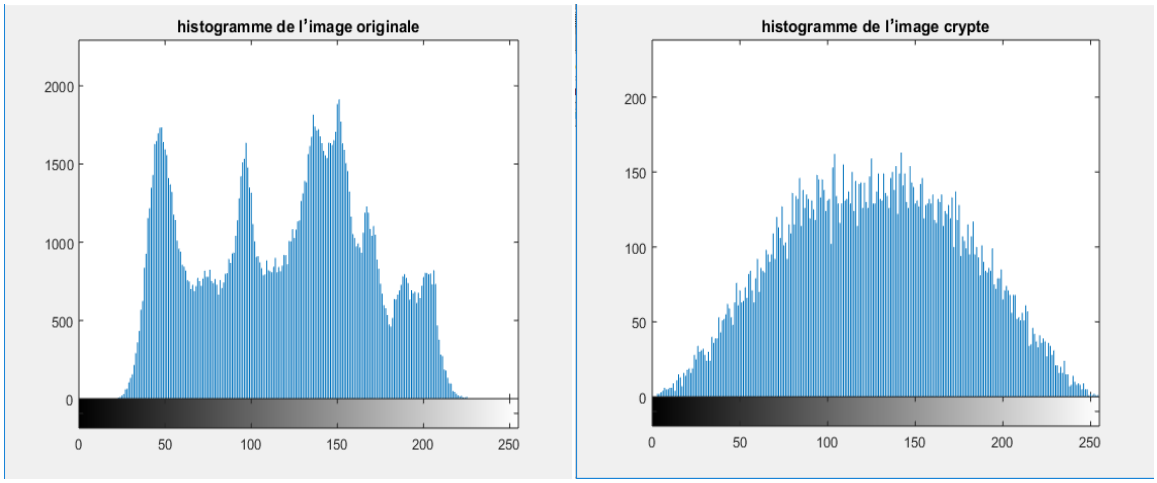
**(c)**

**Figure 4.2:(a)image originale (b) image cryptée,(c) image décryptée.**

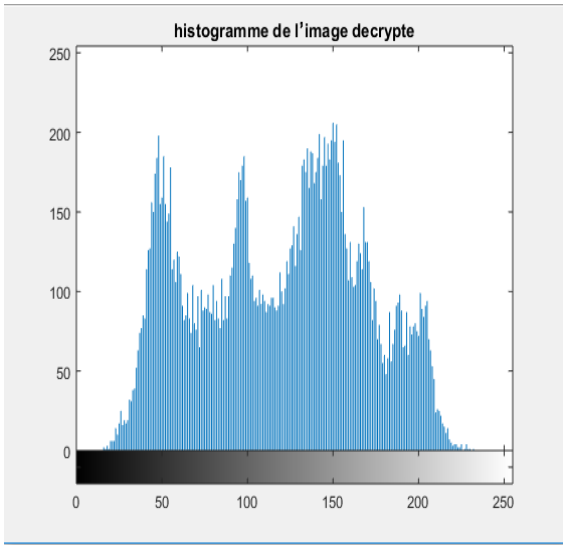
### 4.4.1.1 L'histogramme :

L'histogramme d'une image désigne un histogramme des valeurs d'intensité des pixels. Cet histogramme est un graphique illustrant le nombre de pixels dans une image à chaque valeur d'intensité trouvée dans cette image. Pour une image grise il y a 256 intensités différentes possibles, ainsi, l'histogramme s'affiche graphiquement en utilisant 256 chiffres indiquant la distribution des pixels entre ces valeurs de niveaux de gris.[46]

- Affichage des histogrammes de l'image originale, cryptée et décryptée.




**(a)** **(b)**




**(c)**

**Figure 4.3:histogrammes:(a)image original,(b) image crypté,(c) image décryptée avec algorithme proposé.**

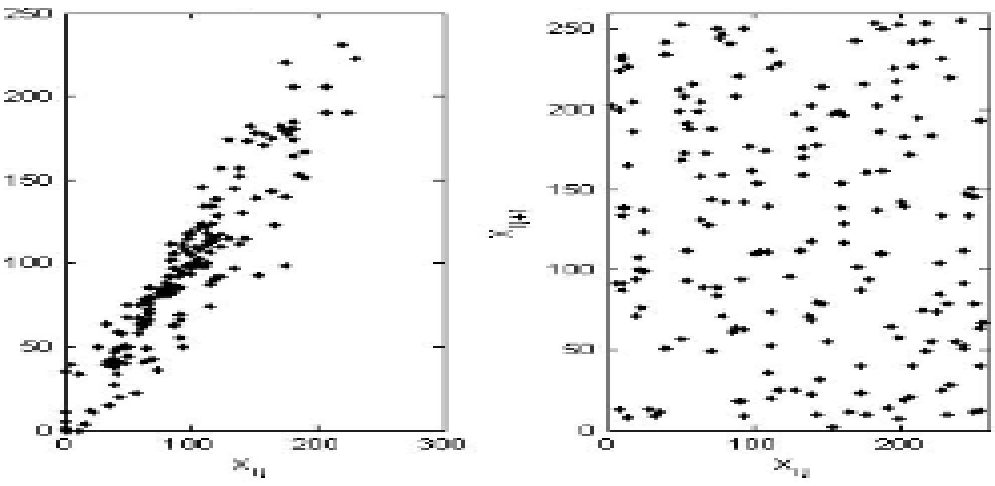
Il ressort des figures a,b et c que les histogrammes de l'images chiffré sont uniformément distribuées par rapport aux histogrammes des images d'origines. qui sont expliquées par le rôle de l'algorithme de chiffrement utilisé qui assure que la dépendance des propriétés statistiques des images chiffrées et des images originales soit quasi aléatoire afin de rendre la Cryptanalyse de plus en plus difficile en plus que l'image chiffrée ne fournit aucun élément reposant sur l'exploitation de l'histogramme et permettant de concevoir une attaque statistique sur le procédé de chiffrement des images proposées.

### 4.4.1.2. L'analyse de corrélations :

L'analyse de corrélations entre pixels adjacents, est la phase de test permettant d'analyser la robustesse de l'algorithme de chiffrement, Nous avons analysé les corrélations des pixels adjacents horizontaux, verticaux et diagonaux voisins dans le cadre des images originales et cryptées.

Les figures a et b, montrent les distributions de deux pixels adjacents horizontaux pour l'image originale et chiffrée de Lena respectivement.

Nous remarquons que dans le cas de l'image originale, les pixels adjacents horizontaux ont des corrélations fortes et s'alignent sur la première bissectrice. Par contre, dans le cas de l'image chiffrée, les pixels adjacents horizontaux sont disséminés presque de manière aléatoire. Ce qui nous montre que l'algorithme est robuste à toute attaque statistique.




(a) (b)

**Figure 4.4:corrélation horizontale.**

Nous avons aussi calculé le coefficient de corrélation entre deux pixels adjacents verticaux, diagonaux et horizontaux aussi bien de l'image originale et chiffrée. Pour ce calcul, nous avons utilisé la formule suivante :

$$C(r) = \frac{\sum m \sum n (x_{mn} - \bar{x})(y_{mn} - \bar{y})}{\sqrt{(\sum m \sum n (x_{mn} - \bar{x})^2)(\sum m \sum n (y_{mn} - \bar{y})^2)}}$$

Le tableau suivant montre les résultats obtenus

| Sens | Originale | Chiffrée |
|---|---|---|
| Horizontal | 0.9732 | -0.1891 |
| Vertical | 0.9865 | -0.0029 |
| Diagonal | 0.9603 | -0.0052 |

**Tableau 4.1 : Coefficients de corrélation entre l'image originale et l'image chiffrée.**

Nous remarquons les coefficients de corrélation pour l'image originale sont voisins de 1 ce qui montre que les pixels sont fortement corrélés, tandis que pour l'image chiffrée les coefficients de corrélation sont voisins de *0* ce qui prouve qu'il n'y a pas de corrélation entre les images originales et chiffrées. L'image chiffrée est donc totalement différente de l'image originale.

### 4.4.1.3 Analyse différentielle :

Cette analyse sert à calculer le nombre de taux de change des pixels pour voir l'influence de la modification d'un seul pixel dans l'image originale sur l'image chiffrée.

Nous définissons deux calculs :

### a)Erreur quadratique moyenne (MSE) :[47]

L'image dégradée Î est toujours comparée à l'originale I pour déterminer son rapport de ressemblance. Ce critère est le plus utilisé. Il est basé sur la mesure de l'erreur quadratique moyenne (MSE) calculée entre les pixels originaux et dégradés:

$$\mathbf{MSE} = \frac{1}{M*N} \sum_{m=1}^{M} \sum_{n=1}^{N} (I(m.n) - \hat{I}(m.n))^2$$

Où (M × N) est la taille de l'image, et I p et Î p sont respectivement les amplitudes des pixels sur les images originale et dégradée. Il est vraisemblable que l'œil tienne beaucoup plus compte des erreurs à grandes amplitudes, ce qui favorise la mesure quadratique.

## b)Rapport crête signal sur bruit (PSNR) :[47]

Au lieu de mesurer la distorsion, cette valeur (Peak Signal to Noise Ratio, PSNR) mesure la fidélité, puisqu'elle est proportionnelle à la qualité. Tout de même, elle est une fonction de MSE ; sa définition et son utilisation proviennent du domaine du traitement de signal:

$$\mathbf{PSNR=10log}_{10}\left(\frac{Imax^2}{MSE}\right)$$

Pour une image à niveau de gris, Imax désigne la luminance maximale possible. Une valeur de PSNR infini correspond à une image non dégradée. Et cette valeur décroît en fonction de la dégradation. Le PSNR relie donc le MSE à l'énergie maximale de l'image.

Le tableau suivant montre les résultats obtenus

| La valeur de MSE | La valeur de PSNR |
|---|---|
| 93.95 | 28.40 |

**Tableau 4.2: les valeurs de MSE et PSNR.**

De l'analyse **Tableau 03** du, Nous remarquons que les valeurs des PSNR et du MSE restent à l'échelle des valeurs espérées. ce qui démontre la robustesse de l'algorithme proposé

## 4.4.1.4. Sensibilité à la clé :

Un bon algorithme de chiffrement doit être sensible à la clé secrète, c'est-à-dire un légère changement dans la clé produira une image totalement différente.

Nous avons fait des changements dans la clé avec des modifications légères

Les résultats obtenus

| La clé | Corrélation |
|---|---|
| X=0.393 , r=16 | 0.68 |
| X=0.3931 , r=17 | 0.25 |
| X=0.392 , r=10 | 0.091 |

**Tableau 2.3 : les valeurs de sensibilité à la clé.**

Il y’a pas de corrélation entre les trois images chiffrées malgré que la modification dans la clé était très légère. Nous constatons que l’algorithme de chiffrement proposé est sensible à la clé secrète.

## 4.5. Conclusion :

Dans ce chapitre, nous avons présenté un algorithme de chiffrement chaotique d'image. Un ensemble de tests ont été effectués afin de prouver la sécurité de la procédure de chiffrement proposée. Les résultats obtenus montrent la robustesse de l’algorithme proposé.

# Conclusion Générale

## Conclusion Générale :

Aujourd'hui, La protection et la sécurité des données et des informations (image, texte, etc…..) sont toujours en augmentation car le réseau de communication connu un grand développement. De cette raison nous avons étudié la cryptographie chaotique.

La cryptographie est un moyen efficace permette de cacher l'information transmise pour assurer la sécurité. Nous distinguons trois catégories de technique cryptographique : cryptographie symétrique (a clé secrète) asymétrique (a clé public) et chiffrement hybride relier les deux techniques (Symétrique et asymétrique) .d'autre part, Le phénomène de chaos est un système dynamique déterministe non linéaire, sensible à la condition initiale qui est l'aspect fondamental est la caractéristique propre de tout système chaotique.

Dans ce mémoire, nous avons proposé et examiné un algorithme cryptage décryptage des images chaotique qui a été implémenté via python. Cet algorithme utilise une carte chaotique de Tchebychev pour générer une séquence de nombres qui sont ensuite utilisés pour brouiller les positions des pixels dans l'image.

Les résultats expérimentaux montrent que des histogrammes de l'image chiffrée sont uniformément distribués par rapport aux histogrammes des images d'origines. Cela signifie que l'algorithme est bon et sécurisé contre les attaques issues. Nous avons analysé la robustesse de l'algorithme de chiffrement grâce au coefficient corrélations. Les tests de la sensibilité de la clé ont montré que l'algorithme de chiffrement proposé est sensible à la clé secrète.

Enfin, tous les résultats expérimentaux tels que les tests statistiques, différentielle et l'analyse de sensibilité à la clé montrent l'efficacité et la robustesse de notre algorithme.

Comme perspectif, nous envisageons de tester notre algorithme dans un environnement IOT.

# Références bibliographiques

## Références bibliographiques :


[1] Mohand-Amokrane BIR Lyes DAHMOUNI, « Etude et implémentation d'algorithmes de chiffrement à clé secrète et à clé publique : Application au cryptage de la parole », Université Mouloud Mammeri De Tizi-Ouzou, 4 juillet 2018.

[2] Benzerrouki Aïcha Essedikia et Guemidi Zoulikha, « Application des systèmes chaotiques à la cryptographie », MEMOIRE DE MASTER, UNIVERSITE Dr. TAHAR MOULAY SAIDA, 2018.

[3] Mme AZIB née BENZEMAM Djamila, « Systèmes chaotiques et hyper chaotiques pour la transmission sécurisée de données », UNIVERSITE ABOU BEKR BELKAID TLEMCEN, 2009-2010.

[4 ] Mr Medjahdi NASREDDINE, « Cryptage Chaotique Basé Sur l'Attracteur Clifford » , Université Abou Bakr Belkaïd– Tlemcen,02 Juillet 2017.

[5] Kebir Bahia et Rahmouni Samia, « Développement d'une application pour l'échange des messages sécurisés », université Abou Bakr Tlemcen, 27 Mai 2015.

[6] Belkadi imane et Amiar narimen , « Cryptage d'image par considération des plans de bits des pixels séparément par ordre de leurs poids avec une clé publique de taille libre »,Master en informatique , 2018.

[7] Melle BOUSALAH Malika Melle TIFOUR Yamina « Contribution à la conception d'un crypto système symétrique flexible sur circuit FPGA », UNIVERSITE M'HAMED BOUGARA DE BOUMERDES, 2015/2016.

[8] Djamal Eddine, « Fonction logistique et standard chaotique pour le chiffrement des images satellitaires », Goumidi Djamal Eddine 2010 Université Mentouri de Constantine (UMC) 2010.

[9] B. DEBBAGH, N. BOUNEGEB, « Etude de comparaison de principaux systèmes crypto fournis par le package de Bouncy Castel plat forme Java SDK ", Mémoire de Master académique, Université KASDI MERBAH OUARGLA (Algérie) ,05.Juin.2016.

[10] R. Dumont .Introduction a la cryptographie et a la sécurité informatique. Note de cours, université de Liége, 2006-2007.

[11] A.Kerckhoffs "La cryptographie militaire "Journal des sciences militaires.

[12]M. BOUKHATEM Mohammed Belkaïd, « Application des techniques de cryptage pour la transmission sécurisée d'images MSG », UNIVERSITE MOULOUD MAMMERI, TIZI-OUZOU, 2015.

[13] Ben Ammar Asma, Haddouche khalissa, « Amélioration de la génération des sous clés de l'algorithme cryptographique DES », UNIVERSITE Akli Mohand Oulhadj —Bouira, 2017.

[14] MlleATTAF Nassima & Mlle CHERFA Hamida, « Etude sur l'Applicabilité de la Cryptographie Asymétrique aux Réseaux de Capteurs sans Fil », Université Abderrahmane Mira de Bejaïa, Juin 2012.

[15] Kassem AHMAD, «Protocoles, gestion et transmission sécurisée par chaos des clés secrètes. Applications aux standards :TCP/IP via

DVB-S, UMTS, EPS ».École doctorale Sciences et Technologies, Liban juillet 2013.

[16] YAGOUB Imad Eddine, « Systèmes dynamiques discrets et chaos », université du havre, Année 2010/2011.

[17] : DAEMEN J., RIJMEN. V., AES, Proposal: The Rijndael Block Cipher. Technicalreport, Proton World Int.l, Katholieke Universiteit Leuven, ESAT-COSIC, Belgique, 2002.

[18] Ghada Zaïbi, « Sécurisation par dynamiques chaotiques des réseaux locaux sans fil au niveau de la couche MAC », Université de Toulouse, 30/09/2013.

[19] AZZOUZI Oussama, HADDADI Ferhat : « Plateforme de chiffrement/déchiffrement pour la sécurisation du stockage et de la transmission de l'information », thèse d'ingéniorat, école nationale supérieur de l'informatique, 2012.

[20] Alice Lan, Benoit Vandevelde, cours: « Panorama des algorithmes de Cryptographie », université de Nantes, 13 mars 2011.

[21] https://www.commentcamarche.com/contents/213-chiffrement-parsubstitution;11-05-2018)

[22] https://www.commentcamarche.com/contents/216-cryptage-par-transposition

[23] ELHACHI HANA, « Sécurisation de la Couche Physique OFDM Dans un Réseau de Capteurs : Application sur les Images Médicales », Université 8 Mai 1945 – Guelma, 2019.

[24] ARBANE Dehbia ARAB Katia, « Conception de crypto-systèmes à base de systèmes chaotiques d'ordre fractionnaire : Application au cryptage de la parole», Université Mouloud Mammeri De Tizi-Ouzou, 09 juillet 2018.

[25] Tayeb Hamaizia Systèmes Dynamiques et Chaos « Application à l'optimisation a l'aide d'algorithme chaotique », université Constantine ,2013.

[26]M.AIT HAMMI, Abdelfateh, « ÉTUDE ET RÉALISATION D'UN SYSTEME CHAOTIQUEBASÉ SUR LE CIRCUIT DE CHUA », UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU, 2013-2014.

[27]J.Gleick. La théorie du chaos – vers une nouvelle science. Albin Michel, Paris, 1989.

[28]Melle Megherbi Ourdia. « Etude et réalisation d'un système sécurisé a base de Systèmes chaotiques », Mémoire de Magister, Université Mouloud Mammeri de Tizi-Ouzou, (2013).

[29] Adel Ouannas, « Intitulée Sur La Synchronisation Des Systèmes Chaotiques Discrets », Université Frères Mentouri à Constantine, 07/12/2015.

[30 ]OUKSOUM Ryma&BOUMESSID Hanane, « Transmission sécurisée par modulation CSK (Chaos Shift Keying) », Université SAAD DAHLAB de BLIDA, 2015-2016.

[31]BENHABIB Chouaib, « ETUDE D'UN SYSTEME CHAOTIQUE POUR LASECURISATION DES COMMUNICATIONS OPTIQUES » mémoire master, L'UNIVERSITEDE TLEMCEN, 2014.

[32]Ibtissem TALBI, « système dynamique non linéaires et phénomène chao », Université Mentouri de Constantine Faculté des Sciences Exactes, 29 / 06 / 2010.

[33]Jean Marc GINOIX, « le chaos en quelques mots », Université de Toulon, 07/01/2006.

[34]Tidjani Menacer « synchronisation des systèmes dynamique a dérivées fractionnaires », UNIVERSITE CONSTANTINNE1, 26/05/2014.

[35]A. Zemouche. "Sur l'observation de l'état des systèmes dynamiques non linéaires." Thèse de Doctorat, Université Louis Pasteur Strasbourg I, 2007.

[36]IKHLEF Ameur, « Synchronisation, Chaotification et Hyperchaotification des Systèmes Non-linéaires : Méthodes et Applications », Université Mentouri de Constantine,2010/2011.

[37]Maizi marwa« Etude et contrôle du chao dans des systèmes physiques », université Larbi Tébessi –Tébessa, 2016.

[38]Bouaiache Amina&Djezairi chaima, « IMPLEMENTATION FPGA D'UNE TRANSMISSION SECURISE PAR CHAOS DE L'ECG (électrocardiogramme) », Université SAAD DAHLAB de BLIDA 1,2017/2018.
.

[39] BELLAHBIB Hadhoum Nadjet, ABDELLI Ikram, « L'EXPLOITATION DU CHAOS NUMERIQUE DANS LES TRANSMISSIONS SECURISEES », Univ Abou Bakr Tlemcen ,2017.

[40]ODEN. « Le chaos dans les systèmes dynamiques ».2007.

[41]Chikhi L., « Application des systèmes dynamiques chaotiques en transmission de données ».Thèse de magister de l'université de Blida 1, 2012.

[42]p. Dedieu, M. P. Kennedy, and M. Hasler. Chaos shift Keying : modulation and demodulation of a chaotic carrier using self-synchronizing chua's circuits. IEEE Trans. Circuits Syst.II, 40(10) :634–642, 1993.

[43]K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz. Synchronization of lorenz-based chaotic circuits with applications to communications. IEEE Trans. Circuits Syst. II, 40(10) :626–633, 1993

[44]Mr: BOUHARAOUA Abderrahim et Mr: BOUKLI HACENE Mohammed Imad, « Automatisation d'une maison intelligente via une application Android », Université Aboubakr Belkaïd – Tlemcen –,11 / 06 /2017.

[45]Daha Boubaker et Medileh Mounir, « Un miroir intelligent interactif basé sur Raspberry Pi » UNIVERSITÉ ECHAHID HAMMA LAKHDAR EL OUED, 24-09-2018

[46]HADJI Faiçal, «conception et réalisation d'un système de cryptage pour les images médicales » université Msila, 2017 2018.

[47] AHMED SEGHIR Zianou, « Evaluation de la qualité d'image », Université de Mentouri – Constantine, 2012.