Université ABBES LAGHROUR Khenchela
Faculté des Sciences et de la Technologie
Département de Génie Industriel
جامـــعة عبـــاس لـــغرور خـنـشـلة
كليـــة العلـــوم والتكنـــولـــوجيـا
قسم الهنـدسة الصنـاعية

N° Série :.....

Mémoire de fin d'étude

Pour l'obtention du diplôme de Master

Filière : Télécommunications

Spécialité : Systèmes des Télécommunications

THEME

UTILISATION DU COMPORTEMENT CHAOUTIQUE POUR LE CRYPTAGE DES SIGNAUX

Réalisé par : - ***BOUTOBBA Mehdi***
- NESRAOUI Raouf-Eddin

Soutenu le 30 /06/2019 Devant le jurycomposé de:

Mr. Mohamed Saigaa	***Président***	***Université Abbes Laghrour-Khenchela***
Mm.Maamri Fouzia	***Encadreur***	***Université Abbes Laghrour-Khenchela***
Mm.SalimaAourar	***Examinatrice***	***Université Abbes Laghrour-Khenchela***

Promotion : 2018-2019

Remerciements

Je tiens à remercier Madame : Maameri Fouzia, professeur à l'université de AbbessLaghrour - Khenchela qui a accepté de m'encadrer, et je lui exprime particulièrement toute ma reconnaissance pour m'avoir fait bénéficier de ses compétences scientifique ces qualités humaines et sa constante disponibilité.

Je tiens à remercier aussi :

*Monsieur: Laanani

Et à tous ceux qui ont contribué de près ou de loin à la réalisation de ce travail.

Dédicace

Je dédie ce modeste travaille à :

- ***Mes très cher parents pour leur dévouement et leur soutien au long de mes étude. MERCI mon*Père*MERCI ma* Mère.**
- ***A mes frères:*Khalil et Iyad, *mes sœurs:*Hana, Manar*et a toute ma famille.***
- ***Je dédie aussi ce mémoire à tous mes amis pour ne citer que quelque uns:*DakkicheAbba, Hamid Tallous, HoussamBoussalem, AyoubLaassisse, BilalHassnaoui*… et beaucoup d'autres qui m'excuseront de pas les avoir cités.***
- ***Aussi mon binôme :*NesraouiRaouf – Eddine.**
- ***Sans oublié les enseignants et enseignantes, et toute la promotion de :Système des télécommunications* 2019.**

Boutobba Mehdi

Promotion 2019

Dédicace

Je dédie ce modeste travaille à:

- ***Mes très cher parents pour leur dévouement et leur soutien au long de mes étude. MERCI mon*** **Père** ***MERCI ma*** **Mère.**
- ***A mes frèreset a toute ma famille.***
- ***Je dédie aussi ce mémoire à tous mes amis pour ne citer que quelque uns***
- ***Aussi mon binôme :*** **Boutobba Mehdi.**
- ***Sans oublié les enseignants et enseignantes, et toute la promotion de :Système des télécommunications*** **2019.**

NesraouiRaouf – Eddine

Promotion 2019

Résumé:

L'objectif de ce travail dans le cadre du mémoire est de présenter une étude des systèmes dynamiques chaotiques, en commençant par des généralité sur le chiffrement, les définitions et les concepts généraux du chaos, En simulant le modèle célèbre système Chua, basé sur la méthode RungKetta du programme Matlab, nous avons utilisé les caractéristiques du chaos: sensibilité aux conditions initiales, et enfin étude mathématique détaillée du système chaotique en recherchant ses points d'équilibre Avec sa vision de la stabilité et du développement vers le chaos. La troisième partie concerne l'application du système chaotique au Matlab pour des communications sécurisées.

Mots-clés: Cryptage, Chaos, chua, Simulation, RungKetta, Mtalab.

الملخص:

الغرض من هذا العمل في سياق أطروحة الماستر هو تقديم أولي كتحليل للأنظمة الديناميكية الفوضوية، بدأنا مع عموميات حول التشفير و تعاريف ومفاهيم عامة عن الفوضى، و نمذجة الحالات **المستمرة أو المقطعة للفوضى**. من خلال محاكاة نموذج نظام شيا الشهير، على أساس طريقة رونج كيتا **ببرنامج الماتلاب، فإننا أعدنا اكتشاف** خصائص الفوضى هي: الحساسة للشروط الأولية، و تأثير مهلة المحاكاة وأخيرا دراسة لنظام الفوضى العشوائي من خلال البحث عن نقاط توازنه مع رؤية استقراره و **تطوره نحو الفوضى**. الجزء الثالث يعلق بتطبيق **نظام الفوضى العشوائي على الماتلاب في الإتصالات المؤمنة**.

كلمات مفتاحية : التشفير، الفوضى، شيا، المحاكاة، رونج كيتا، ماتلاب.

Abstract :

The purpose of this work in the context of the Master thesis is to present an analysis of the chaotic dynamic systems. We begain with definitions and general concepts of chaos, And its applications. By simulating the model of the famous Chua system, based on the Rung Ketta method of the Matlab program, we re-discovered the characteristics of the chaos: sensitive to initial conditions, the study of the chaotic system by searching for its equilibrium points With its vision of stability and the application of the random mess system to the Matlab in secure communications.

Keywords: Encryption, Chaos, chua, Simulation, RungKetta, Matlab

Liste des figures :

Figure 1.1 : Principe générale d'un algorithme de chiffrement 06

Figure 1.2 : Principe d'un système cryptographique 08

Figure 1.3 : Interception du message par un pirate 10

Figure 1.4 : Principe de cryptage symétrique 11

Figure 1.5 : Cryptographie asymétrique 12

Figure 1.6:Principe de cryptage Asymétrique 13

Figure 1.7:cryptage par DES 14

Figure 1.8 : Le schéma général d'AES 15

Figure 1.9 : Principe général de chiffrement RSA 16

Figure 1.10 : Signature numérique 18

Figure 2.1: Trajectoire dans le voisinage des singularités dans un espace des phases à 2 dimensions. a) et b) valeurs propres négatives nœud stable. c) et d) valeurs propres positives, nœud instable. 25

Figure 2.2 : Trajectoire dans le voisinage des singularités dans un espace des phases à 2 dimensions. a) et b) valeurs propres doubles négatives étoile stable. c) et d) valeurs propres doubles positives, étoile instable 25

Figure 2.3 : Trajectoire dans le voisinage des singularités dans un espace des phases à 2 dimensions.a) et b) valeurs propres de signe opposés, col 26

Figure 2.4 : Trajectoire dans le voisinage des singularités dans un espace des phases à 2 dimensions. Deux valeurs propres complexes conjuguées. (^{a}=σ+jω) 26

Figure 2.5 : Portrait des phases du système avec deux foyers stables, un cycle limite et un point selle 27

Figure 2.6 : Section de Poincaré 29

Figure 2.7 : Diagramme de bifurcation pour la fonction logistique 31

Figure 2.8 : Comportement dynamique de la fonction logistique pour a) r=2, b) r=3, c) r=3.45, d) r=3.8 32

Figure 2.9 : a) Section de Poincaré de l'attracteur de Henon, b) son agrandissement 33

Figure 2.10 : Attracteur de Lorenz 34

Figure 2.11 : Attracteur de Rössler 35

Figure 2.12 : Evolution de la trajectoire en Noir pour les conditions initiales (x_0=2.18; x_1=5.15; x_2=10.20) et la trajectoire en Bleu pour les conditions initiales (x_0=2.17; x_1=5.14; x_3=10.21) 36

Figure 2.13 : La courbe de Koch 38

Figure 2.14 : Masquage additive ……..……..39

Figure 2.15 : Modulation chaotique ……..……..40

Figure 3.1 : Principe de Chiffrement par Chaos 44

Figure 3.2 : Le Circuit de Chua, Diagramme électrique 45

Figure3.3 : L'espace de phase 47

Figure 3.4 : Trajectoire chaotique du circuit de Chua 47

Figure 3.5: L'espace de phase 48

Figure 3.6 : Trajectoire chaotique du circuit de Chua 48

Figure 3.7 : Signal chaotique en fonction de t 49

Figure 3.8 : Chiffrement de l'image par chaos ……50

Liste des Tableaux

Tableau 1.1: substitution mono-alphabétique 09

Tableau1.2: Comparaison entre cryptographie asymétrique et symétrique 17

Tableau 2.1 : Classification des régimes permanents en fonction des exposants de Lyapunov…….37

Sommaire

Remerciements **2**

Dédicace **3**

Dédicace **4**

Résumé: **5**

الملخص: **6**

Abstract : **7**

Liste des figures : **8**

Liste des Tableaux **10**

Introduction générale **1**

CHAPITRE I : La cryptographie **4**

1.1 Introduction **4**

1.2 Historique **4**

1.3 Terminologies **5**

1.4 Objectifs de la cryptographie **6**

1.5 Mécanismes de lacryptographie **7**

1.6 Les déférents algorithmes de cryptage et décryptage **8**

1.7 La cryptographie symétrique **10**

1.8 La cryptographie asymétrique **11**

1.9 Exemples d'algorithmes de cryptage symétriques et asymétriques **13**

1.10 Cryptage symétrique vs cryptage asymétrique **17**

1.11 La cryptographievisuelle **18**

1.12 Conclusion **19**

Chapitre II : Système Dynamique et Chaos **21**

2.1 Introduction **21**

2.2 Définition des systèmes dynamiques **21**

2.3 Attracteurs des systèmes dynamiques 28

2.4 Chaos 28

2.5 Exemples de systèmes chaotiques 30

2.6 La sensibilité aux conditions initiales 35

2.7 Stabilité des systèmes dynamiques 36

2.8 Les fractales 38

2.9 Masquage chaotique 39

2.10 Modulation chaotique 40

2.11 Application du comportement chaotique 41

2.12 Conclusion 42

Cryptage par chaos 21

Chapitre III : Cryptage par chaos 44

3.1 Introduction 44

3.2 Communications Sécurisées par chaos 44

3.3 Comparaison entre chaos et cryptographie 45

3.4 Le circuit de Chua: 45

3.5 Résultats de simulation 47

3.6 Conclusion 51

Conclusion générale 52

Bibliographie : 53

Introduction générale

Depuis l'extraordinaire révolution dans les domaines des technologies de communication ces dernières années, de nombreux informations sont devenus de plus en plus en circulation à travers les réseaux de communication.

La sécurité de ces informations échangées est devenue une nécessité primordiale dans beaucoup d'applications, en la trouve par exemple en biomédical, en imagerie satellitaire et astronomique, en production cinématographique, ou encore en informatique industrielle. Afin d'assurer la confidentialité et d'empêcher toute modification ou exploitation non autorisée des données, une méthode connues et adoptée pour la réalisation efficace de cet objectif, c'est la cryptographie visuelle. C'est une branche de la cryptographie qui sert à transformer une image en d'autres images complètement cryptées ou partiellement illisible et incompréhensible.

La révolution numérique a engendré des moyens plus faciles pour le traitement, le stockage et la transmission des images numériques. Cependant, elle a aussi engendré des moyens de falsification, de contrefaçons et d'espionnage très avancés. Le risque est encore plus grand dans un environnement ouvert tel que la transmission des images satellitaires. C'est à cause de ça, il est devenu nécessaire et impératif de crypter les images numériques avant de les transmettre afin de fournir la sécurité et l'authenticité aux données transmises sur des systèmes de communications.

Pour protéger et préserver l'intimité de l'information personnel contre les attaques et pour réduire les vulnérabilités des systèmes, plusieurs solutions ont été proposées, telles que les pare-feu et la cryptographie. Cette dernière englobe plusieurs techniques et méthodes telles que la cryptographie à clé publique, la cryptographie à clé privée, la cryptographie quantique et la cryptographie basée sur chaos.

L'histoire de la cryptographie est déjà longue. Les méthodes utilisées étaient restées souvent très primitives. D'autre part, sa mise en œuvre était limitée aux besoins de l'armée et de la diplomatie. Ainsi, les méthodes de cryptographie et de cryptanalyse ont connu un développement très important au cours de la seconde guerre mondiale et ont eu une profonde influence.

Depuis quelques années, les chercheurs s'intéressent à la possibilité d'utiliser des signaux chaotiques dans les systèmes de transmission de données, en particulier pour transmettre des quantités importantes d'informations sécurisées. L'intérêt d'utiliser des signaux chaotiques réside dans deux propriétés du chaos :

Un signal chaotique est un signal à large spectre et permet donc de transmettre des signaux très variés, d'autre part, un signal chaotique est obtenu à partir d'un système déterministe, il est donc possible de le reconstituer en se plaçant dans les mêmes conditions que celles qui ont contribué à le créer et, ainsi, de récupérer l'information de départ [48].

L'objectif de notre travail consiste à utiliser un signal chaotique généré par un circuit électrique à élément non linéaire pour crypter des informations.

Ce mémoire est divisé en trois chapitres :

Le premier chapitre présente des généralités, sur les concepts fondamentaux et les notions de base relié à la cryptographie, la cryptographie desimages.

Le second chapitre donne, après quelques généralités sur les systèmes dynamiques linéaires et non linéaires, une introduction au chaos en explicitant des notions primordiales pour l'étude des systèmes dynamiques non linéaires, tels que les attracteurs étranges, et les fractales. Ainsi que l'étude de la stabilité au sens de Lyapunov avec une simulation des exemples chaotiques célèbres tels que la fonction logistique, le modèle de Lorenz et le modèle de Hénon.

Le troisième chapitreprésente une simulation du signal chaotique fourni par un circuit électrique de Chua et son utilisation pour le cryptage.

Enfin, **Une conclusion générale** incluant le bilan des résultats des travaux de ce mémoire.

CHAPITRE I :

La cryptographie

CHAPITRE I : La cryptographie

1.1 Introduction

La sécurité informatique est devenue un défi majeur, et les travaux dans cet axe de recherche sont de plus en plus nombreux. Divers outils et mécanismes sont développés afin de garantir un niveau de sécurité à la hauteur des exigences de la vie moderne. Permis eux, la cryptographie.

La cryptographie est l'art du secret désignant l'ensemble des techniques permettant de chiffrer des messages, c'est-à-dire permettant de les rendre illisible. Dans ce chapitre, nous allons présenter des généralités, sur les concepts fondamentaux et les notions de base reliées à la cryptographie.

1.2 Historique

- En 48 avant J.C., les grecs employaient un dispositif appelé la "scytale". C'est un bâton autour duquel une bande longue et mince de cuir était enveloppée et sur laquelle on écrivait le message. Le cuir était ensuite porté comme une ceinture par le messager. Le destinataire avait un bâton identique permettant d'enrouler le cuir afin de déchiffrer le message [1].
- En 50 avant J.C., le premier système de cryptographie à base mathématique fut inventé par Jules César. C'est un chiffrement par substitution mono-alphabétique basé sur un décalage des lettres [2].
- En 1970 : Horst Feistel a mené un projet de recherche à IBM Watson ResearchLab qui a développé le chiffre Lucifer, qui inspira plus tard le chiffre DES et d'autres chiffres. Un avantage de ce type d'algorithmes est que chiffrement et déchiffrement sont structurellement identiques|[3].
- En 1976 :WhitfieldDiffie et Martin Hellman ont publié « new direction in cryptography», introduisant l'idée de la cryptographie à clé publique.
- En 1978:l'algorithme RSA a été publié dan les communications l'Association for Computing Machinery ACM [2]
- En 1990 :Xuejia Lai et James Massey en Suisse ont publié un algorithme international de cryptage des données (IDEA) qui utilise une clé de 128 bits et utilise des opérations qui sont pratiques pour les ordinateurs à usage général.
- 1985 : Victor Miller et Neal Koblitz utilisent les courbes elliptiques pour la cryptographie [3].

1.3 Terminologies

- **Texte en clair :** est le message à protéger.
- **Texte chiffré :** est le résultat du chiffrement du texte en clair.
- **Chiffrement :** est la méthode ou l'algorithme utilisé pour transformer un texte en clair en texte chiffré.
- **Déchiffrement :** est la méthode ou l'algorithme utilisé pour transformer un texte chiffré en texte en clair.
- **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.
- **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.
- **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.
- **Cryptologie :** il s'agit de la science qui étudie les communications secrètes. Elle est décomposée de deux domaines d'étude complémentaires, la cryptographie et la cryptanalyse.
- **Décrypter :** c'est l'action de retrouver le texte en clair correspondant à un texte chiffré sansposséder la clé qui a servi au chiffrement. Ce mot ne devrait donc être employé que dans le contexte de la cryptanalyse.
- **Coder, décoder :** c'est une méthode ou un algorithme permettant de modifier la mise enforme d'un message sans introduire d'élément secret[4].

Le principe général d’un algorithme de chiffrement est illustré par la figure suivante :

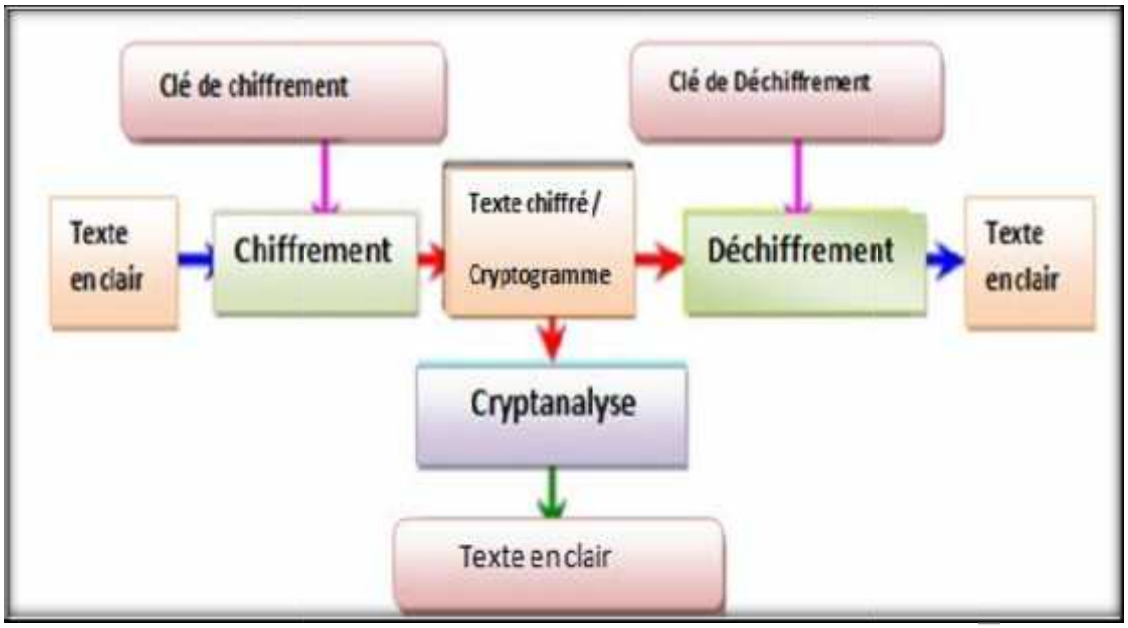


Figure 1.1: Principe générale d'un algorithme de chiffrement[4]

1.4 Objectifs de la cryptographie

Il existe quatre grands objectifs pour le cryptage des données numériques[3] :

1.4.1 Confidentialité

La confidentialité ou masquage des données, le contenu des données va être sauvé de toutes les personnes, machines et systèmes à l'exception de ceux qui ont le droit d'accès.

1.4.1.1 Authentification

Permet à l'émetteur de signer son message, ainsi, le récepteur n'aura pas de doute sur l'identité du premier.

1.4.1.2 Intégrité

Les données vont être protégées du changement (suppression, ajout, mise à jour) de la personne non autorisé.

1.4.1.3 Non-répudiation

C'est la garantie qu'aucun des deux individus ayant effectué une transaction ne pourra nier avoir reçu ou envoyé les messages.

1.4.2 Définition de la cryptographie

La cryptographie est un ensemble de techniques permettant de chiffrer des messages (textes ou images), c'est-à-dire permettant de les rendre inintelligibles. Le fait de coder un message de telle façon à le rendre secret s'appelle chiffrement. La méthode inverse, consistant à retrouver le message original, est appelée déchiffrement. Le chiffrement se fait généralement à l'aide d'une clef de chiffrement, le déchiffrement nécessite quant à lui une clef de déchiffrement. On distingue généralement deux types de clefs :

- **Les clés symétriques** : il s'agit de clés utilisées pour le chiffrement ainsi que pour le déchiffrement. On parle alors de chiffrement symétrique ou de chiffrement àclé secrète.
- **Les clés asymétriques :** il s'agit de clés utilisées dans le cas du chiffrement asymétrique (aussi appelé chiffrement à clé publique). Dans ce cas, une clé différente est utilisée pour le chiffrement et pour ledéchiffrement.

1.4.3 Définition de laclé

La clé est une valeur d'entrée utilisée dans un algorithme de cryptographie. Cette valeur est un nombre complexe dont la taille se mesure en bits. Plus la taille de la clé est grande, plus elle contribue à élever la sécurité. Les clés doivent être stockées de manière sécurisée et de manière à ce que seul leur propriétaire soit en mesure de les atteindre et de lesutiliser.

1.5 Mécanismes de lacryptographie

Un système de chiffrement ou encore crypto système désignera la description d'un procédé de chiffrement / déchiffrement. Il consiste à transmettre un message qui ne soit compréhensible que par le destinataire. Pour cela, celui-ci partage un secret avec l'émetteur du message. Le message "en clair" est transformé à l'aide d'une "*fonction de chiffrement*" paramétrée par une "clé" en un message codé "*texte chiffré*" et le message codé est transformé à l'aide d'une "*fonction de déchiffrement* " paramétrée par une "clé" en un message clair [6**]**.

1.5.1 Chiffrement

Le chiffrement est le processus de transformation d'un message M de telle manière à le rendre incompréhensible. Il est basé sur une fonction de chiffrement E et de la clef k de chiffrement.

$$C= E\ k(M)$$

1.5.2 Déchiffrement

Le déchiffrement est l'opération inverse permettant de récupérer le message clair à partir du message C chiffré.

$$M= DK'(C)$$

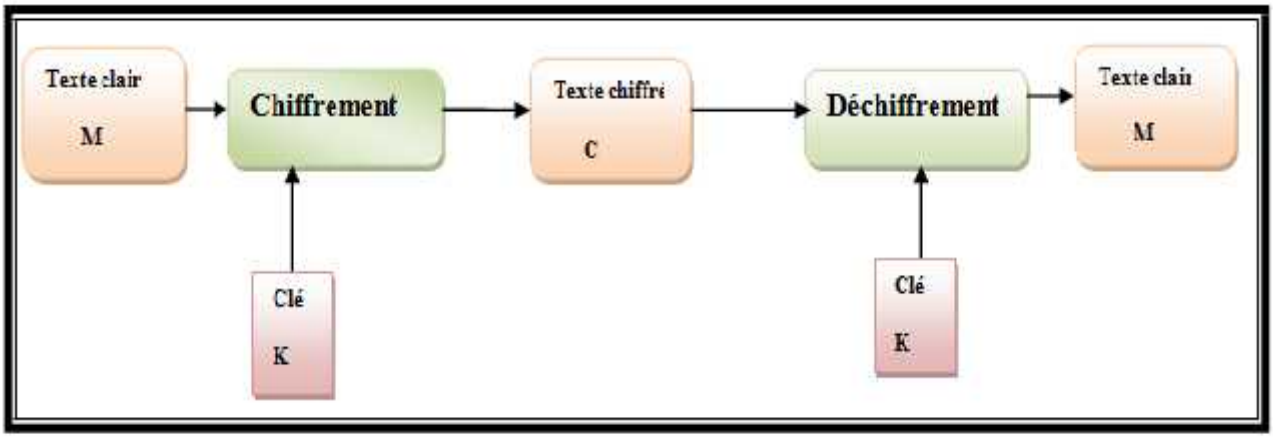


Figure1.2: Principe d'un système cryptographique

1.6 Les déférents algorithmes de cryptage et décryptage

On distingue les méthodes de cryptage classiques et les méthodes de cryptage modernes.

1.6.1 Méthodes de cryptage Classiques

1.6.1.1 Cryptage par substitution [2]

Les substitutions consistent à remplacer des symboles ou des groupes de symboles par d'autres symboles ou groupes de symboles dans le but de créer de la confusion. On distingue deux méthodes de substitution, la substitution mono-alphabétique et la substitution poly-alphabétique.

- **Substitution mono-alphabétique :** consiste à remplacer chaque alphabet clair par un autre alphabet codé.

Texte clair	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Texte codé	W	X	E	H	Y	Z	T	K	C	P	J	I	U	A	D	G	L	Q	M	N	R	S	F	V	B	O

Tableau 1.1 : substitution mono-alphabétique

- **Exemple :**

Texte claire« la cryptographie »

Texte Crypté« iweqbgndtqwgkcy »

- **Substitution poly-alphabétique**

le principe consiste à remplacer chaque lettre du message en clair par une nouvelle lettre prise dans plusieurs alphabets aléatoires associés. Par exemple, on pourra utiliser n substitutions mono-alphabétiques ; celle qui est utilisée dépend de la position du caractère à chiffrer dans le texte en clair. On choisit une clé qui sert d'entrée dans la grille poly alphabétique incluant autant de symboles qu'il y a de lettres différentes à chiffrer. Chaque caractère de la clé désigne une lettre particulière dans la grille de codage. Pour coder un caractère, on doit lire le caractère correspondant du texte en clair en utilisant la grille poly alphabétique et le mot clé associé dans l'ordre séquentiel (on répète la clé si la longueur de celle-ci est inférieure à celle du texte de départ). L'exemple le plus célèbre est l'algorithme de VIGENERE et de BEAUFORT. L'illustration la plus simple qui corresponde à ce principe est l'utilisation d'une fonction à base de ou exclusif (XOR).

1.6.1.2 Cryptage par transposition [2]

Les transpositions consistent à mélanger lessymboles ou les groupes de symboles d'un message clair suivant des règles prédéfinies pour créer de la diffusion. Ces règles sont déterminées par la clé de chiffrement. Une suite de transpositions forme une permutation.

1.6.1.3 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.

1.6.2 Méthodes de cryptage Modernes

On distingue deux méthodes majeures de cryptage modernes :

- Les méthodes à clef secrète (symétriques).
- Les méthodes à clef publique/clef privée (asymétriques).

1.6.2.1 La méthode symétrique

La méthodesymétriqueutiliseuneclésecrètepourcrypter un message,etcette mêmeclé pour ledécrypter.

1.7 La cryptographie symétrique

Dans l'exemple qui suit, on suppose que le client et le serveur connaissent tous deux la clé[7] :

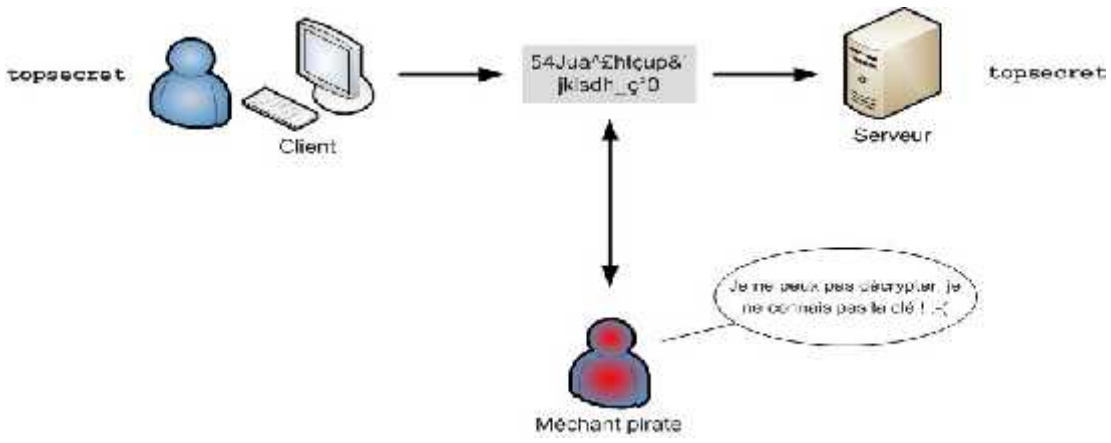


Figure1.3: Interception du message par un pirate

Le cryptage symétrique fonctionne selon deux procédés différents :

- le cryptage par flot : le cryptage s'effectue en continu, bit par bit
- le cryptage par bloc : le cryptage s'effectue sur des blocs de bits

- **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...)
- Clés relativement courtes.

- **Inconvénients du cryptage symétrique :**

- 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.[7]

Figure1.4: Principe de cryptage symétrique

1.8 La cryptographie asymétrique

- Le cryptage asymétrique, se base sur l'utilisation des 2 clés : publique (Pour crypter, elle est accessible publiquement) et privée (pour décrypter le message, elle est gardée secrète). Ce type de cryptage élimine la problématique de la transmission de la clé, Ce mode de cryptage est également nommé le cryptage à clé Publique. Il est essentiel Que l'on ne puisse pas déduire la clé privée de la clé publique. Pour bien comprendre le

principe, on peut l'illustrer avec l'échange d'une lettre entre un émetteur et un destinataire:

- l'émetteur possède deux clés : privé et publique. Il envoie sa lettre contenant la clé publique audestinataire.
- le destinataire utilise la clé publique pour décrypter son message, il envoie tout à l'émetteur initial
- le récepteur utilise sa clé privée pour décrypter lemessage.

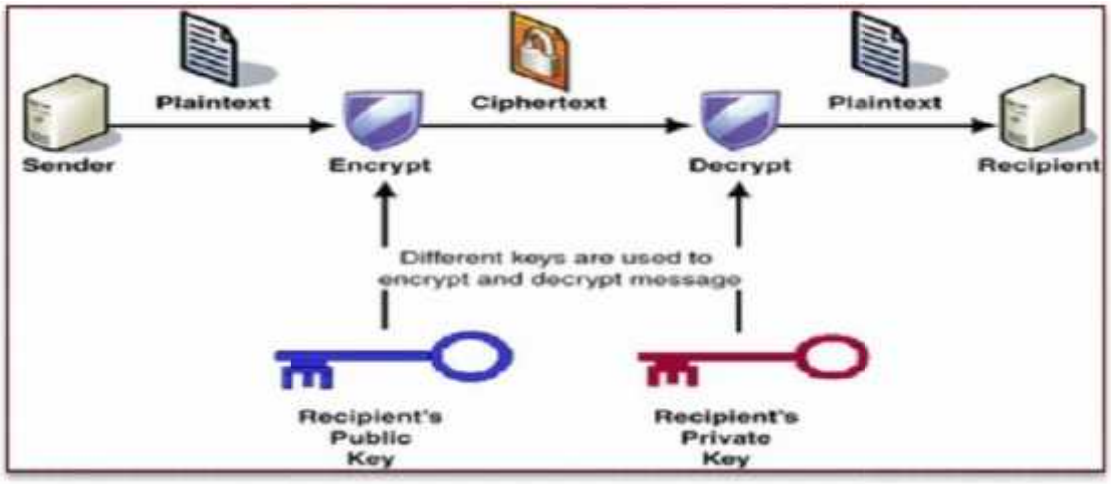


Figure 1.5: Cryptographie asymétrique

➢ 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.

➢ Inconvénients du cryptage asymétrique :

- Un 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. [7]

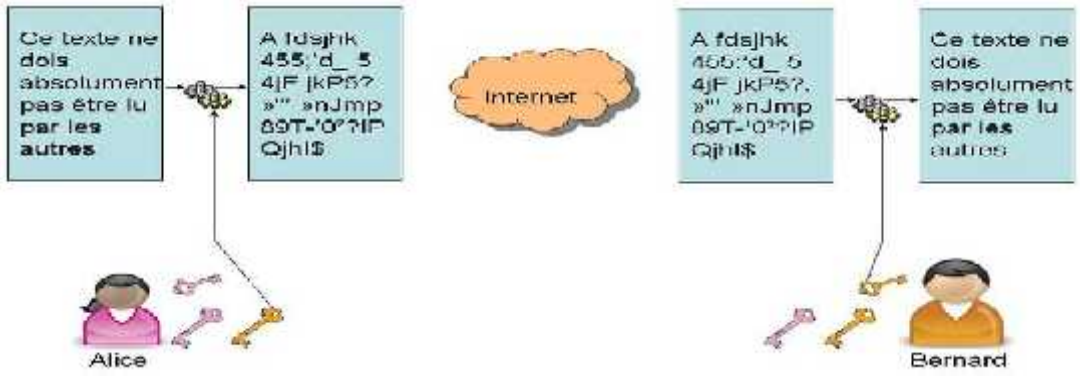


Figure 1.6:Principe de cryptage Asymétrique

1.9 Exemples d'algorithmes de cryptage symétriques et asymétriques

1.9.1 Data Encryptions Standard (DES):

Le DES a été approuvé en 1978. 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 56bits 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 k0 à k16. Etant donné que« seuls » 56 bits servent effectivement à chiffrer.

1.9.2 Les grandes lignes de l'algorithme sont les suivantes :

- ✓ Fractionnement du texte en blocs de 64 bits (8 octets)
- ✓ Permutation initiale des blocs
- ✓ Découpage des blocs en deux parties : gauche et droite, nommées G et D

- ✓ Etapes de permutation et de substitution répétées 16 fois (appelées rondes)
- ✓ Recollement des parties gauche et droite puis permutation initialeinverse

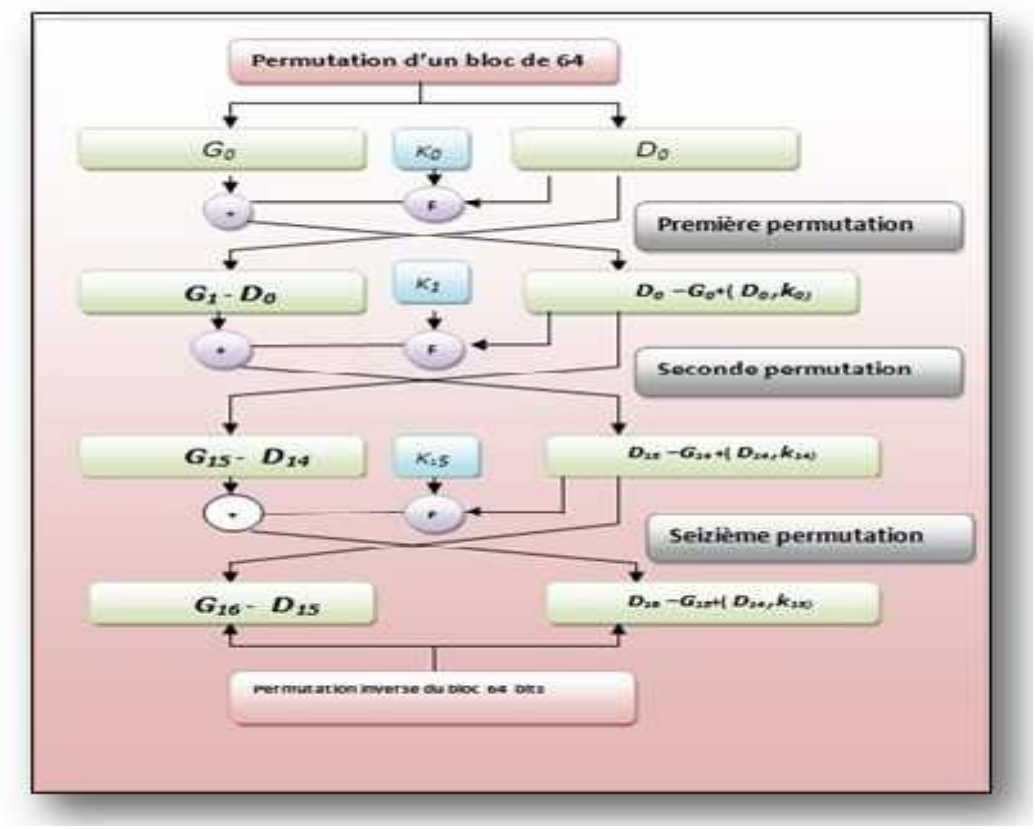


Figure 1.7: Cyptage par DES [5]

1.9.3 Advanced Encryptions Standard (AES) :

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 transformationlinéaire 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[8].

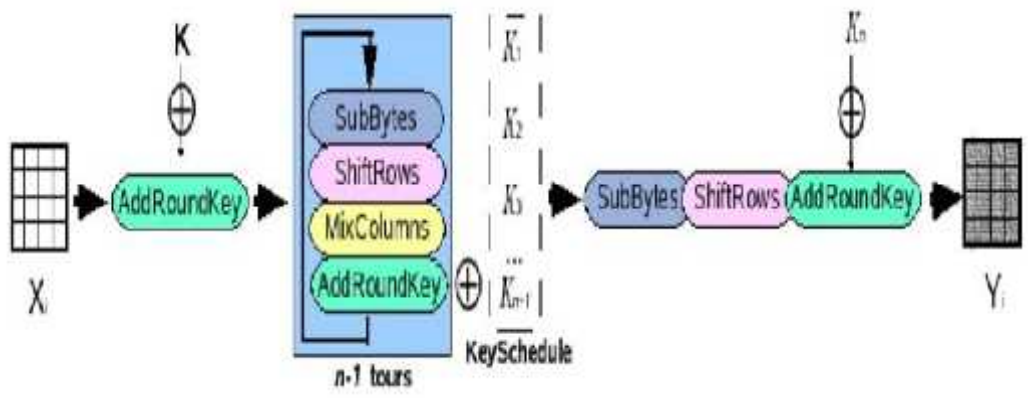


Figure 1.8 : Le schéma général d'AES[1]

1.9.4 RivestShamirAdleman (RSA) :

RSA est un algorithme asymétrique, très utilisé dans le commerce électronique, et plus généralement pour échanger des données confidentielles sur Internet. Cet algorithme a été inventé en 1977 par Ron Rivest, Adi Shamir et Len Adleman. Il est basé sur la difficulté de factoriser un grand nombre en produit de deux grands facteurs premiers.

RSA fonctionne de la manière suivante :

- **Création des clés:**
  - ✓ Générer deux grands nombres premiers p et q au hasard par un algorithme de Test de primalité probabiliste, noter n =p*q.
  - ✓ Choisir un nombre entier premier avec (p-1)(q-1). Deux nombres sont premiers entre eux s'ils n'ont pas d'autre facteur commun que1.
  - ✓ L'entier d est l'entier de l'intervalle [2, (p-1)(q-1)] tel que e*d soit congrue à 1modulo (p-1)(q-1)[9].

- **Distribution des clés** :

Le couple (n, e) constitue la clé publique du destinataire, et il a rend disponible à l'émetteur. Le couple (n, d) constitue la clé privée dudestinataire.

- **Chiffrement du message** :

L'émetteur représente le message sous la formede plusieurs entiers M compris entre 0 etn-1,

- **Déchiffrement du message** :

le destinataire reçoit C et le calcule par sa clé privée pour obtenir le message initial M[10].

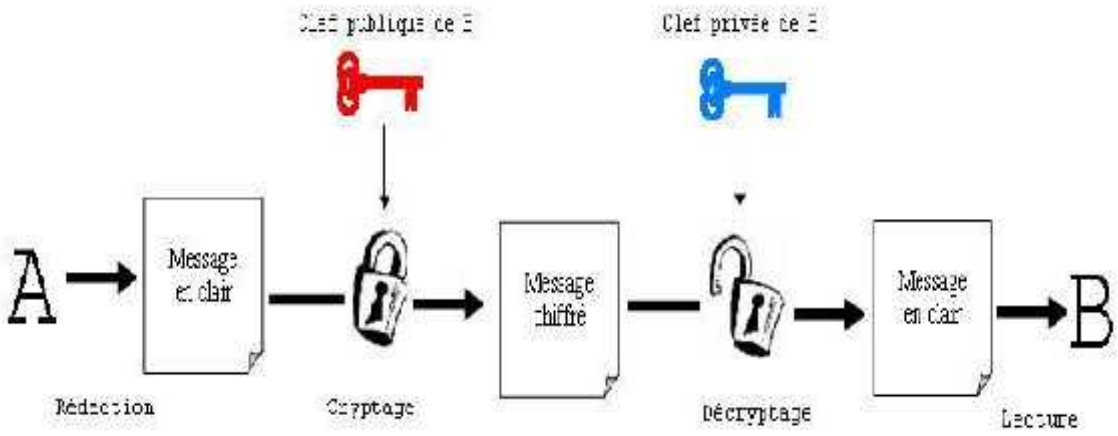


Figure 1.9: Principe général de chiffrement RSA

1.9.5 Chiffrement par flots

Les algorithmes de cryptage par flot peuvent être définis comme étant des algorithmes de chiffrement par bloc, où chaque bloc est de dimension unitaire (1 bit, 1 octet, etc.) ou relativement petit. Leurs principaux avantages sont leur extrême rapidité et leur capacité à changer à chaque symbole du texte clair. avec un algorithme de chiffrement par flot, il est possible de crypter séparément chaque caractère du message clair un par un, en utilisant une fonction de cryptage qui varie à chaque fois (ces algorithmes ont donc besoin de mémoires). Généralement, les algorithmes de chiffrement par flot sont composés de deux étapes :
La génération d'une clef dynamique et la fonction de cryptage de sortie dépendant de la clef dynamique.

Le principe de ce système consiste à générer une clé aléatoire avec la même taille du message et de le combiner avec le message bit à bit par l'opération XOR. Le récepteur applique le même mécanisme.

1.9.6 Fonction de hachage

Cette fonction permet à partir d'un texte de longueur quelconque, de calculer une chaîne de taille inférieure et fixe appelée condensé ou empreinte (message digest ou hash en anglais). Ce dernier permet d'assurer l'intégrité des données, authentification de la source et la non-répudiation de la source.

Une fonction de hachage doit être à sens unique, c'est à dire qu'il doit être impossible étant donné une empreinte de retrouver le message original, et sans collisions, ça veut dire l'impossibilité de trouver deux messages distincts ayant la même valeur de condensé. La moindre modification du message entraîne la modification de l'empreinte.
MD5 (Message Digest 5 - Rivest1991-RFC 1321) et SHA sont deux exemples de fonctions de hachage.

1.10Cryptagesymétriquevscryptageasymétrique

Cryptage symétrique	Cryptage asymétrique
Gestion des clés difficiles (nombreuses clés)	Pas de secrète à transmettre
Point faible = l'échange de la clé secrète	Très utile pour échanger les clés
Clés relativement courtes (128 ou 256 bits)	Des clés plus longues (1024 à 4096 bits)
Système rapide du chiffrement/déchiffrement	Lenteur de calcul
Facile	Difficile

Tableau1.2: Comparaison entre cryptographie asymétrique et symétrique

D'après ce tableau, le cryptage symétrique est le plus utilisé car il est plus simple est plus1 rapide que le cryptage asymétrique.

1.11 La cryptographievisuelle

1.11.1 Définition:

- ✓ Le cryptage dans le domaine de l'imagerie est une technique courante pourmaintenir la sécurité de l'image. Cette technique essaie de convertir l'image originale en une autre image qu'il est impossible de comprendre. En d'autres termes, elle assure qu'aucune personne ne peut connaitre le contenu sans une clé pour ledécryptage.
- ✓ Le cryptage d'image a des applications dans divers domaines, y compris la Communication par Internet, l'imagerie médicale et la communicationmilitaire.

1.11.2 Signature numérique :

La signature numérique est définit comme des données ajoutées à un message ou une transformation cryptographique d'un message permettant à un destinataire.

- D'authentifier l'auteur d'un document électronique de garantir son intégrité.
- De se protéger contre la contrefaçon (seul l'expéditeur doit être capable dégénérer la signature) non-répudiation.
- La signature électronique est basée sur l'utilisation conjointe d'une fonction de hachage et de la cryptographie asymétrique.

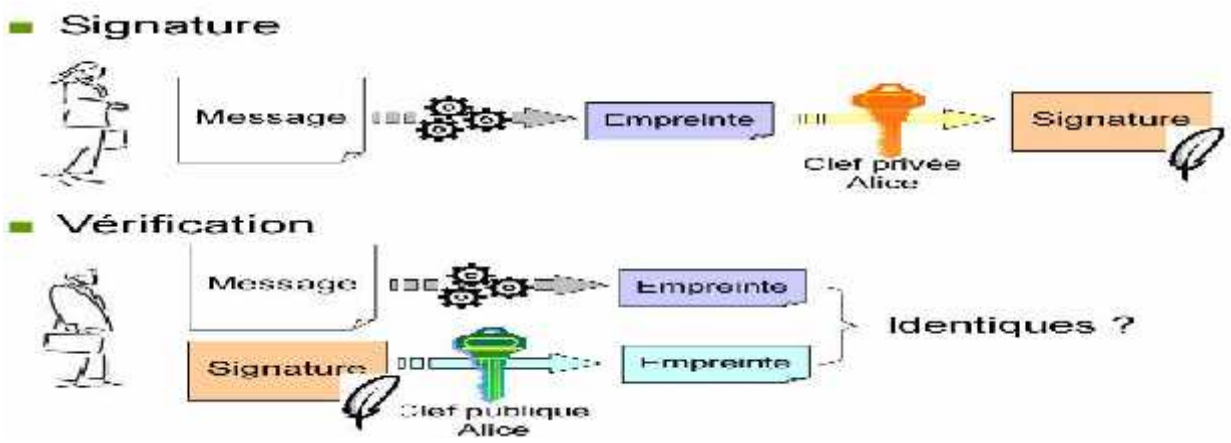


Figure 1.10: Signature numérique

1.11.3 Certificat électronique :

Un certificat numérique est un bloc de données contenant, dans un format spécifié, les parties suivantes[11] :

- La clé publique d'une paire de clés asymétriques,

- Des informations identifiant le porteur de cette paire de clés (qui peut-être une personne ou un équipement), telles que son nom, son adresse IP, son adresse de messagerie électronique, son URL, son titre, son numéro de téléphone, etc...
- L'identité de l'entité ou de la personne qui a délivré ce certificat (autorité de certification),
- La signature numérique des données générée par la personne ou l'entité prenant en charge la création ou l'authentification de ce certificat et servant d'autorité de certification. Usuellement, on distingue deux familles de certificats numériques :
- Les certificats de signature, utilisés pour signer des e-mails ou s'authentifier sur un site web. les certificats de chiffrement : les gens qui vous envoient
- Des e-mail utilisent la partie publique de votre certificat pour chiffrer le contenu que vous serez seul à pouvoir déchiffrer. Il existe deux façons distinctes de créer des certificats électroniques :
- Le mode décentralisé (le plus courant) qui consiste à faire créer, par l'utilisateur (ou, plus exactement par son logiciel ou carte à puce) la biclef cryptographique et de remettre la partie publique à l'AC qui va y adjoindre les informations de l'utilisateur et signer l'ensemble (information + clé publique)
- Le mode centralisé qui consiste en la création de la bi clef par l'AC, qui génère le certificat et le remet avec la clé privée à son utilisateur.

Les certificats électroniques respectent des standards spécifiant leur contenu de façon rigoureuse. On trouve parmi les plus connus et les plus utilisés :

- La norme X.509 en version 1, 2, et 3, sur lequel se fondent certaines infrastructures à clés publiques.

1.12 Conclusion

Dans ce chapitre, nous avons donné un aperçu sur le vaste monde de la cryptographie, ainsi que le principe de l'algorithme de cryptage symétrique et asymétrique, Puis nous avons cité les différents algorithmes de cryptage classiques et modernes. Enfin, nous avons abordé la notion de signature numérique et certificat électronique.

Dans le chapitre suivant, nous allons présenter les différentes méthodes de cryptage chaotiques.

CHAPITRE II :

Système dynamique

etchaos

Chapitre II : Système Dynamique et Chaos

2.1 Introduction

Ce chapitre a pour objectif de présenter quelques généralités et définitions des systèmes dynamiques, nous allons introduire les propriétés de base d'un système chaotique telles que le concept de la bifurcation, les attracteurs étranges et nous terminerons par la définition de exposants de Lyapunov qui peuvent servir à étudier la stabilité (l'instabilité) des systèmes chaotiques ainsi que la sensibilité aux conditions initiales [44].

L'emploi du chaos pour la sécurité des systèmes de communications a été considéré dans les dernières années comme une solution très attirante pour augmenter les performances des systèmes de transmission actuels [12].

Dans la littérature on trouve une multitude d'applications et d'études réalisés concernant plusieurs aspects de la transmission. Puisque le chaos à des caractéristiques quasi-stochastiques permettant d'offrir une solution possible pour les systèmes à probabilités réduites de détection et d'interception ainsi que des applications dans l'accès multiple [13].
En contradiction avec ces aspects positifs qui font du chaos une solution très attirante, il faut préciser que l'optimisation d'un système utilisant un système non linéaire chaotique nécessaire à la récupération de l'information transmise, est difficile à réaliser [14]. Beaucoup de travaux utilisent des algorithmes d'optimisation des systèmes non linéaire [15-16] et identifier les paramètres de contrôle tant pour la cryptographie que pour la stabilité d'un oscillateur utilisé en microprocesseur, dans un RADAR, à bord des satellites GPS. La stabilité de tels systèmes est cruciale pour leurs fonctionnements.

2.2 Définition des systèmes dynamiques

Un système dynamique consiste en un ensemble d'états possibles, avec une loi qui détermine de façon unique l'état présent du système en fonction de ses états passés [17]. Les systèmes dynamiques (chaotiques) non-linéaires remontent aux travaux sur la mécanique céleste et la mécanique statistique par Henri Poincaré, vers 1900, ils sont très connus dans le domaine des mathématiques mais c'est seulement au cours de ces deux dernières décennies que les applications concrètes se sont multipliées [18].

En 1963, le météorologue Edward Lorenz prouve le caractère chaotique des conditions météorologiques, un infime changement de l'état initial pouvant entraîner une trajectoire complètement différente « attracteurs étranges ». Avec cette découverte les travaux d'Henri Poincaré connurent un élargissement d'intérêt et en 1975 le mathématicien James

Yorkeemploie pour la première fois le terme de « chaos » Plusieurs domaines d'applications variés utilisent les principes de la théorie du chaos pour étendre et mieux comprendre les phénomènes liés à ses applications, ainsi les études se sont ensuite enchainées [19].

Du point de vue mathématique la notion générale de système dynamique est défini à son tour à partir d'un ensemble de variables qui forment le vecteur d'état:
$x\{x_i \in \mathbb{R}\}, i = 1..n$, où n représente la dimension du système. En associant en plus un système de coordonnées on obtient l'espace d'état qui est appelé également *l'espace des phases*. Parallèlement avec l'espace d'état un système dynamique est défini aussi par une loi d'évolution, qui caractérise l'évolution de l'état du système en temps. La notion de déterminisme provient du fait que le système considéré est complètement caractérisé par son état initial et sa dynamique [17].

L'évolution d'un système dynamique peut être [20] :

- **causale :** c'est-à-dire que son avenir ne dépend que de phénomènes du passé ou du présent
- **déterministe :** c'est-à-dire qu'à une condition initiale donnée à l'instant présent va correspondre à chaque instant ultérieur 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. C'est à priori la plus naturelle physiquement, puisque le paramètre temps nous semble continu.

  Un système dynamique continu peut être vu comme un système multi variables caractérisé par un vecteur d'état réel de dimension finie [29].
- une évolution discrète dans le temps. Ce second cas est souvent le plus simple à décrire mathématiquement, même s'il peut sembler à priori moins réaliste physiquement. Cependant, 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.

2.2.1 Temps continu

Un système dynamique en temps continu est décrit par un système d'équations différentielles [21] :

$$\dot{x} = F(x(t), t) \tag{2.1}$$

Où F : $\mathbb{R}^n$ x $\mathbb{R}^+ \rightarrow \mathbb{R}^n$ désigne la dynamique du système.

Si on associe à cette dynamique un état initial $x_0 = x(t_0)$, pour chaque couple choisi (x_0, t_0) on peut identifier une solution unique $\Phi(.; x_0, t_0)$: $\mathbb{R}^+ \rightarrow \mathbb{R}^n$ telle que [44]:

$$\Phi_F(t_0; x_0, t_0) = x_0 \ldots . \text{et} \ldots . \dot{\Phi}_F(t; x_0, t_0) = F(\Phi_F(t; x_0, t_0), t) \tag{2.2}$$

Cette solution unique déterminée avec l'aide des équations (2.2), et qui fournit l'ensemble d'états successifs occupés par le système à chaque instant *t*, s'appelle généralement trajectoire.

Pour calculer l'évolution future d'un tel système, il faut connaitre les grandeurs $t \mapsto u(t)$ ainsi que la condition initiale de l'état. On dit que l'état $x$du système représente sa mémoire.

On dira qu'un tel système est stationnaire (par opposition au cas (2.2) instationnaire lorsque F ne dépend pas explicitement du temps [30-31]. Dans ce cas l'équation s'écrit

$$\dot{x} = F(x) \tag{2.3}$$

2.2.2 Temps discret

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. Le système dynamique est dans ce cas représenté par des équations aux différences finies, avec le modèle général suivant[44] :

$$x(k+1) = G(x(k), k) \tag{2.4}$$

Où G : $\mathbb{R}^n$ x $\mathbb{Z}^+ \rightarrow \mathbb{R}^n$ désigne la dynamique du système discret.

Si on associe à cette dynamique un état initial $x_0 = x(k_0)$, pour chaque couple choisi (x_0, k_0) on peut identifier une solution unique $\Phi_G(.; x_0, k_0)$: $\mathbb{Z}^+ \rightarrow \mathbb{R}^n$ telle que :

$$\Phi_G(k_0; x_0, t_0) = x_0 \text{et} \dot{\Phi}_G(t; x_0, t_0) = G(\Phi_G(k; x_0, k_0), k) \tag{2.5}$$

En temps discret le système autonome est définit comme une dynamique qui ne dépend pas de l'instant k :

$$\boldsymbol{x(k+1) = G(x(k))} \tag{2.6}$$

La trajectoire d'un système dynamique atteint une région limitée de l'espace des phases à partir d'un état initial $\mathbf{x}_0$ et après un régime transitoire. Ce comportement asymptotique obtenu pour $t,\ k \to \infty$ est une des caractéristiques les plus intéressantes à étudier pour les systèmes dynamique. Lorsque l'indice k ou le temps t n'apparaît pas dans les relations (2.1) ou (2.4), on parle alors de système autonome.

2.2.3 Dynamique linéaire en dimension 2

Paul Manne ville à donner les différents cas possibles pour le système différentiel $\dot{X} = LX$ qui s'écrivent de la forme suivante [22] :

$$\dot{X} = l_{11}\dot{X_1} + l_{12}X_{2_1} \tag{2.7}$$

$$\dot{X}_2 = l_{21}X_1 + l_{22}X_2 \tag{2.8}$$

Si on cherche les solutions de la forme $X = \hat{X}\exp(\lambda t)$, on obtient

$$^{a}\hat{X}_1 = l_{11}\hat{X}_1 + l_{12}\hat{X}_2 \tag{2.9}$$

$$^{a}\hat{X}_2 = l_{21}\hat{X}_1 + l_{22}\hat{X}_2 \tag{2.10}$$

Où $\hat{X}_1$ et $\hat{X}_2$ sont les deux composantes du mode propre $\hat{X}$. Ce système de deux équations à deux inconnues n'a de solution non triviale que si λ est valeur propre de l'opérateur linéaire L représenté par la matrice $[l]$ dans la base canonique, soit :

Cette équation du second degré admet deux racines $^{a}_{1}$ et $^{a}_{2}$ soit réelles distinctes ou confondues, soit complexes conjuguées[44].

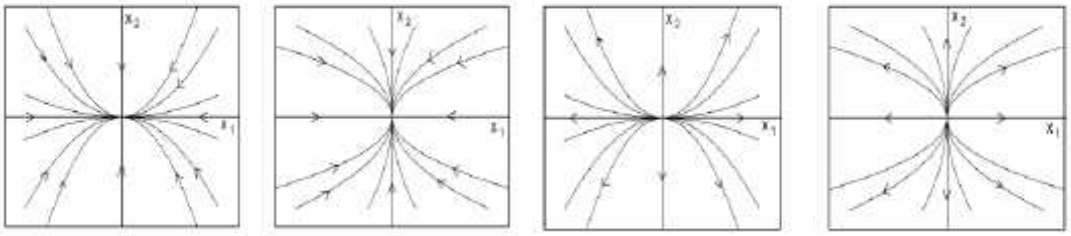
Les composantes du vecteur X représentant l'état du système dans la base propre étant appelées $\tilde{X}_i$:

$$\dot{\tilde{X}}_1 = \lambda_1\tilde{X}_1 \tag{2.11}$$

$$\dot{\tilde{X}}_2 = \lambda_2\tilde{X}_2 \tag{2.12}$$

- valeurs propres λ_1 et λ_2 réelles distinctes

Lorsque les valeurs propres λ_1 et $\lambda_2$de même signes, on a affaire à un point fixe de type nœud. Si les deux valeurs propres sont négatives le nœud est stable, sinon, il est instable. Les trajectoires ont une allure parabolique, la parabole s'ouvrant dans la direction de la valeur propre la plus grande en module. Cette situation est illustrée par la Figure 2.1.

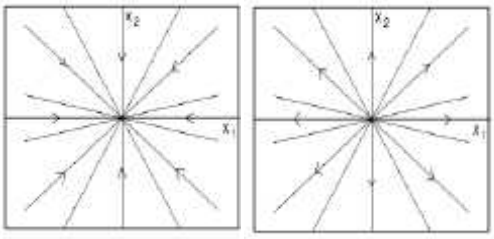


a) $\lambda_2 < \lambda_1 < 0$ b) $\lambda_1 < \lambda_2 < 0$ c) $\lambda_2 > \lambda_1 > 0$ d) $\lambda_1 > \lambda_2 > 0$

Figure 2.1 : Trajectoire dans le voisinage des singularités dans un espace des phases à 2 dimensions. a) et b) valeurs propres négatives nœud stable. c) et d) valeurs propres positives, nœud instable.

- valeurs propres λ_1 et λ_2 réelles doubles

La figure 2.2 illustre le cas où $\lambda_1 = \lambda_2$. Les trajectoires s'approchent ou s'éloignent de l'origine suivant le signe des valeurs propres formant une étoile [22]



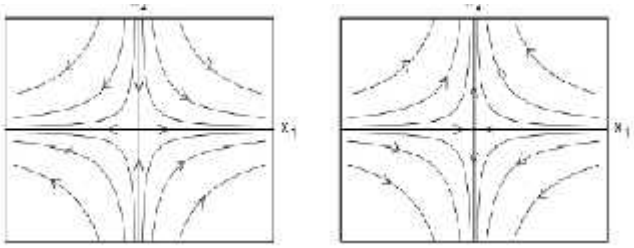
a) $\lambda_1 = \lambda_2 < 0$ b) $\lambda_1 = \lambda_2 > 0$

Figure 2.2 : Trajectoire dans le voisinage des singularités dans un espace des phases à 2 dimensions. a) et b) valeurs propres doubles négatives étoile stable. c) et d) valeurs propres doubles positives, étoile instable.

- valeurs propres λ_1 et λ_2 réelles de signes opposées

Lorsque les valeurs propres λ_1 et $\lambda_2$sont de signe opposées, le point fixe est un col. Les trajectoires, d'allure hyperbolique, s'approchent du point fixe dans la direction du vecteur

propre associe à la valeur propre négative (direction stable) puis s'en écartant le long de l'autre direction propre.

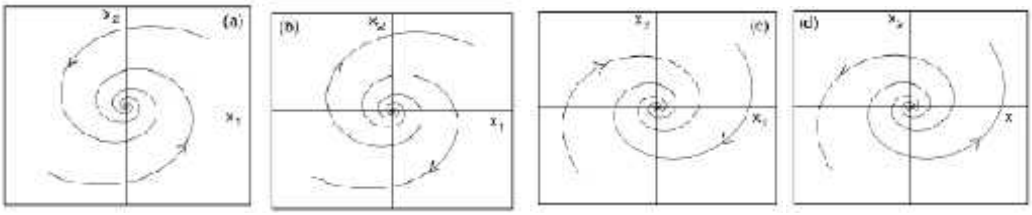


a) $\lambda_2 < 0 < \lambda_1$ b) $\lambda_1 < 0 < \lambda_2$

Figure 2.3 : Trajectoire dans le voisinage des singularités dans un espace des phases à 2 dimensions.a) et b) valeurs propres de signe opposés, col.

- valeurs propres λ_1 et λ_2 complexes conjuguées

Foyer stable ou instable selon le signe de la partie réelle des valeurs propres.

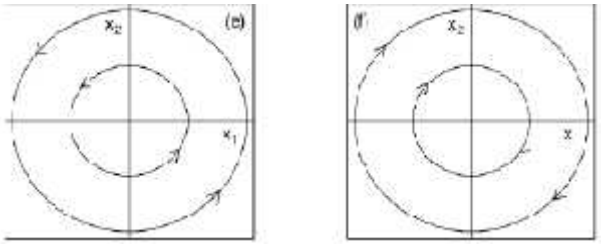


a) Foyer stable $\sigma < 0$ et $\omega > 0$ b) Foyer stable $\sigma < 0$ et $\omega < 0$

c) Foyer instable $\sigma > 0$ et $\omega < 0$ d) Foyer instable $\sigma > 0$ et $\omega > 0$

- Cas particulier $\sigma = 0$

Un cas marginal de valeurs propres imaginaires pures: Centre. La partie imaginaire des valeurs propres est responsable de la rotation des trajectoires autour de l'origine [22].



$\sigma = 0$, avec $\omega > 0$ $\sigma = 0$, avec $\omega < 0$

Figure 2.4 : Trajectoire dans le voisinage des singularités dans un espace des phases à 2 dimensions. Deux valeurs propres complexes conjuguées. (^{a}=σ+jω)

L'utilisation des modèle linéaires est pertinente dans le domaine de linéarité ; en dehors de cette zone, les capacités de prédiction d'une solution peuvent devenir réduites ou nulles [23-24].

2.2.4 Systèmes dynamiques non linéaires

Un système dynamique non linéaire peut avoir plusieurs points d'équilibre isolés. Autour de chacun de ces équilibres, les équations peuvent admettre des systèmes linéarités tangents très différents et donc localement des propriétés différentes. Une particularité importante d'un système non linéaire réside dont le fait qu'il peut également posséder un ou plusieurs cycles limites [25]. Pour illustrer ce concept, on se reporte à l'exemple suivant :

$$\dot{x}_1 = -a_1 x_1 - x_2 x_1 + a_2 \tag{2.13}$$

$$\dot{x}_2 = -x_2 + x_1^2 \tag{2.14}$$

Ce système possède, suivant les valeurs des paramètres a_1 et a_2, un portrait des phases très intéressant, autour de chacun de ces équilibres, les équations peuvent admettre des systèmes linéarisés tangents très différents et donc localement des propriétés différentes [26].

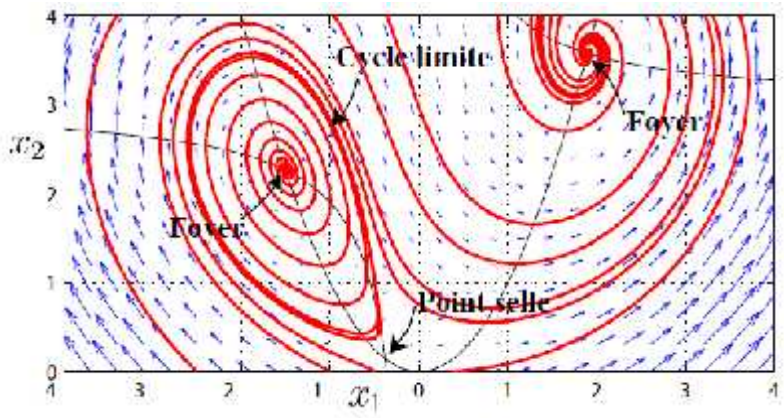


Figure 2.5 : Portrait des phases du système avec deux foyers stables, un cycle limite et un point selle.

L'intérêt du portrait de phase est qu'il permet d'identifier des classes de trajectoires et par conséquent de caractériser des comportements spécifiques du système dynamique. Le portrait de phase d'un système subi des changements qualitatifs lorsqu'il est structurellement instable [27].

2.3Attracteurs des systèmes dynamiques

Un attracteur du système dynamique est une région de l'espace de phase vers laquelle converge toute trajectoire de phase passant à son voisinage. Le voisinage en question est appelé bassin d'attraction de l'attracteur [28].

Dans le cas d'un système linéaire la solution asymptotique est indépendante de la condition initiale et unique, pour les systèmes non linéarités il existe une plusieurs variété de régimes permanents, parmi lesquelles on trouve, par ordre de complexité

On classe les attracteurs en fonction de leur complexité:

• point fixe : les points fixes sont des points singuliers du système dynamique.

• cycle limite : attracteur formant une courbe fermée.

• régime quasi-périodique : correspond à une somme de solutions périodiques dont le rapport des périodes est un nombre irrationnel ce régime peut être représenté dans l'espace d'état par un tort.

• Un attracteur étrange ou chaotique, cette fois le comportement développé par un système dynamique particulier est fortement dépendant de la condition initiale choisie [28].

2.4 Chaos

Lorenz donna en 1972 une conférence devant le grand public du congrès de l'Association américaine pour l'avancement des sciences. Cette conférence « grand public » était intitulée : « Prédictibilité : le battement des ailes d'un papillon au Brésil peut-il déclencher une tornade au Texas ? » En termes de marketing, ce titre était plus alléchant que « Déterministe non périodique flow ». Et la suite l'a prouvé. Quant au terme « chaos », il a été proposé par le mathématicien Yorke, deux ans plus tard, en 1975 [29].

Le chaos est défini généralement comme un comportement particulier d'un système dynamique non-linéaire [21]. Le chaos se produit quand le comportement du système, n'est pas un point d'équilibre, n'est pas périodique, n'est pas quasi-périodique [30-31].

Les systèmes chaotiques contrairement aux comportements purement aléatoires obéissent à des lois déterministes, parfois assez simples dans leur représentation mathématique, caractérisés par la sensibilité aux conditions initiales et aux paramètres du système et possèdent une certaine régularité qui se traduit par le fait que les points périodiques sont denses. La densité des points périodiques exprime l'infinité des comportements dynamiques que prodigue le chaos.

2.4.1 L'attracteur étrange

Les systèmes aléatoires évoluent au hasard dans tout l'espace. Les systèmes chaotiques ont un comportement infiniment complexe. Ils sont attirés par une figure géométrique de structure également infiniment complexe sur laquelle ils errent au hasard, mais sans jamais la quitter, ni repasser deux fois par le même point. Les attracteurs étranges semblent inclure à la fois des lois déterministes et des lois aléatoires [32].

Le terme attracteur étrange est introduit pour la première fois par Ruelle et Takensen1971, pour appeler un ensemble limite d'un système dynamique qui n'est pas une variété et par suite il n'est pas un point fixe, un cycle limite, un tore invariant ou autre. La notion de l'attracteur étrange indique la nature du modèle qui est un « objet » mathématique bien défini. Il n'existe pas une définition rigoureuse d'un attracteur étrange ou chaotique mais il existe quelques essais pour définir ce «objet », mais toutes ces définitions sont restrictives9. Par cette définition un attracteur est la limite asymptotique des solutions de l'équation différentielle avec un ensemble des conditions initiales *B* tel que : $A \subset B$, c'est-à-dire *B* est le bassin d'attraction de *A*.

2.4.2 Section de Poincaré

La section de Poincaré est un hyperplan S qui transforme la trajectoire continue (c) en une succession de points (A, B, …) de passages discontinus à travers la section. Un autre aspect de la section de Poincaré est le passage d'une loi dynamique continue à une loi discrète.

La section de Poincaré est un outil très fréquemment utilisé pour étudier les systèmes dynamiques (notamment les trajectoires périodiques). Le principe de construction de cette technique est illustré par la figure suivante [29] :

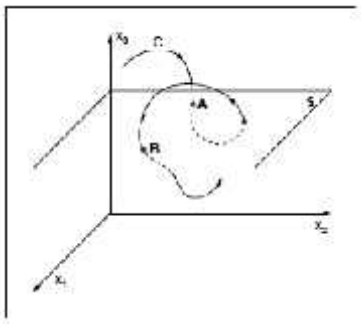


Figure 2.6 : Section de poincaré

2.4.3 Bifurcations

Les systèmes que nous considérons sont en général fonction de paramètres de contrôle. Un point de bifurcation est un point de l'espace de contrôle où le portrait de phase du système change de façon qualitative [33].

- Un système est structurellement stable ou robuste si le portrait de phase ne change pas dans une perturbation de ses paramètres. Par conséquent une bifurcation correspond à une perte de stabilité structurelle. Un « petit » changement quantitatif des paramètres peut induire un changement qualitatif du comportement. Celui-ci peut être local ou global selon qu'il affecte le portrait de phase dans une région localisée autour d'ensembles limites particuliers ou, au contraire, dans son ensemble.
- Une bifurcation locale se produit lorsqu'un ensemble limite change de stabilité. Par exemple, en dimension 2, un nœud bifurque lorsque l'une de ses valeurs propre passe par zéro et change de signe, le transformant en un col, et réciproquement.
- Un foyer bifurque quand la partie réelle de ses valeurs propres s'annule et change de signe.
- Un centre est caractérisé par une paire de valeurs propres imaginaires pures conjuguées est à cet égard structurellement instable car la moindre perturbation apportée au système le transforme en un foyer, stable ou instable.

2.5 Exemples de systèmes chaotiques

Dans la section suivante, nous allons donner quelques exemples de systèmes dynamiques non linéaires.

2.5.1 La fonction logistique

La fonction logistique très connue dans la théorie des systèmes dynamiques sert de modèle universellement utilisé pour l'étude des systèmes discrets. Ce système à une dimension définie par la suite suivante [12] :

$$x_{k+1} = f(x_k) = r x_k(1-x_k) \tag{2.15}$$

La fonction logistique correspond à un comportement intéressant selon la valeur du paramètre r. on trouve un cascade de doublements de période pour décrire la transition entre un comportement périodique et un attracteur chaotique. Une plus grande variété de régimes permanents se présente, parmi lesquelles on trouve :

Pour r < 3, le système possède un point fixe attractif, qui devient instable lorsque r = 3.

Pour r > 3, le système évolue périodiquement de période 2n, (n entier qui tend vers l'infini lorsque r tend vers 4). On obtient donc une succession de bifurcations lorsque r augmente.

Cette courbe présente un diagramme de bifurcation parce que le comportement asymptotique subit, pour des valeurs du paramètre *r* bien déterminées, une bifurcation de l'ensemble des états limitent[44].

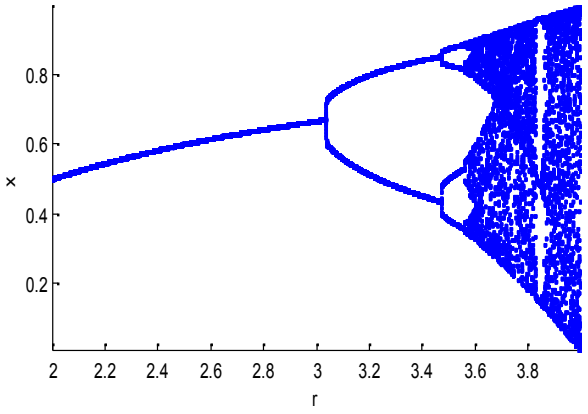


Figure 2.7 : Diagramme de bifurcation pour la fonction logistique

Nous pouvons constater que pour (1 < r < 3), toutes les conditions initiales (0 <x_0 <1) convergent à la position p=a, (a est un point attracteur correspond à l'intersection de la parabole de la fonction logistique avec la droite y = x).

Si r = 2, la trajectoire converge au point p=0.5, à partir de r = 3, après la disparition du comportement transitoire, un changement important est constaté, x prend maintenant deux positions d'équilibre qui se commutent alternativement, p1 = 0.6503 et p2 = 0. 6823 ($x_{0=}$0.3 et x_0=0.4).

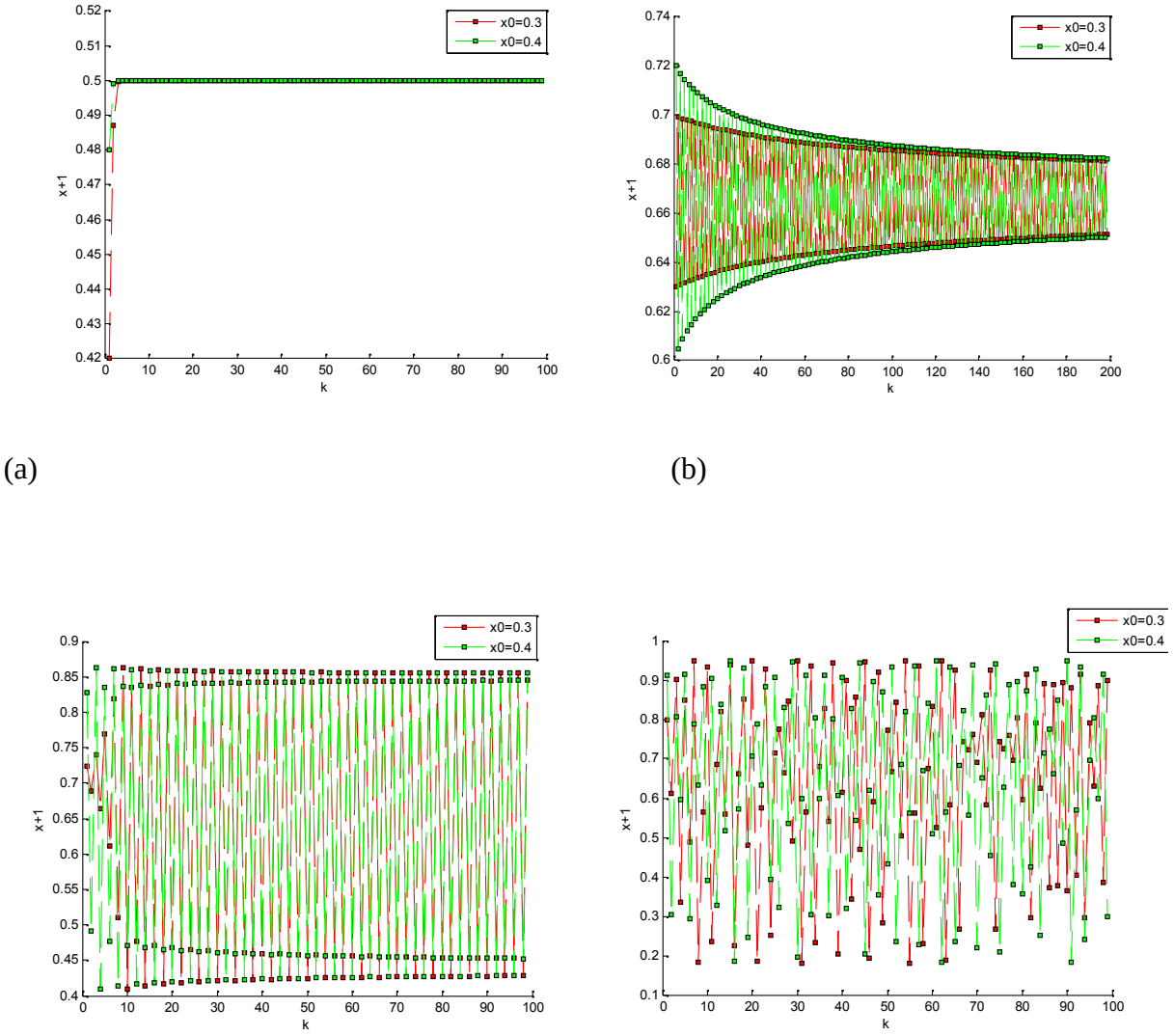


Figure 2.8 : Comportement dynamique de la fonction logistique pour a) r=2, b) r=3, c) r=3.45, d) r=3.8 [44]

Cette variation du régime linéaire (un seul état d'équilibre) en régime non linéaire, passant par une valeur parfaitement définie du paramètre r où il y en a deux états d'équilibre (doublement de période), s'appelle "*bifurcation*".

Lorsque r tend vers 4, on voit clairement que l'évolution de x_{n+1} donne un comportement totalement chaotique du fait de la succession de bifurcation[44].

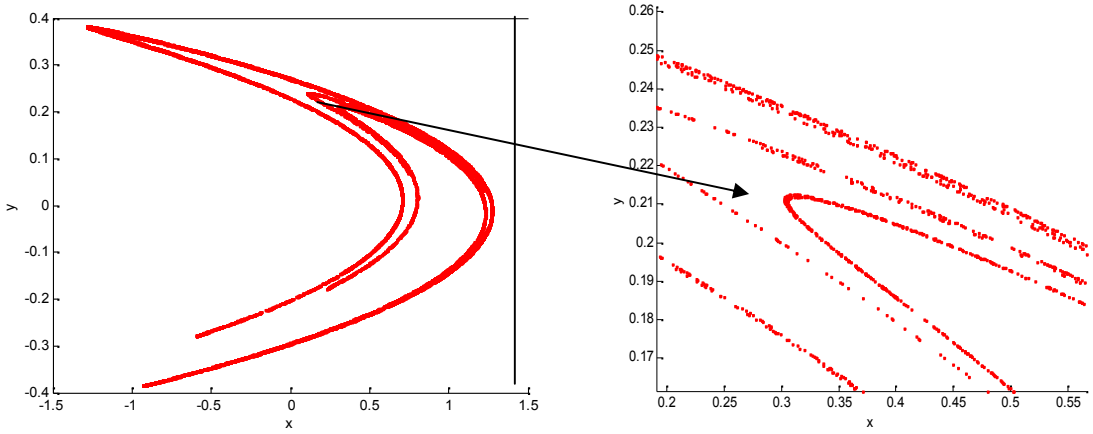
2.5.2 Modèle de Henon

Un autre modèle discret très connu, mais à 2 dimensions, est celui de l'astrophysicien M. Hénon.

$$x_{n+1} = -1.4x_n^2 + y_n + 1 \tag{2.16}$$

$$y_{n+1} = 0.3x_n \tag{2.17}$$

La figure suivante illustre la géométrie discrète de Hénon dans un plan.



(a) (b)

Figure 2.9 : a**) Section de Poincaré de l'attracteur de Henon,**

b**) son agrandissement. [44]**

2.5.3 Attracteurs de Lorenz

Un célèbre système chaotique est celui de Lorenz, qui a prouvé que la difficulté de la prédiction de la météorologie réside dans l'existence du chaos dans les équations climatique :

$$\dot{x} = \sigma\left(-x + y\right) \tag{2.18}$$

$$\dot{y} = rx - y - xz \tag{2.19}$$

$$\dot{z} = xy - bz \tag{2.20}$$

Lorenz a étudié ces équations dans son article en1963 [34] et il a observé l'existence d'un attracteur étrange pour les paramètres σ = 10, r = 28, b = 8/3 [30].L'illustration de l'espace de phase est donnée par la figure suivante (Figure 2.10).

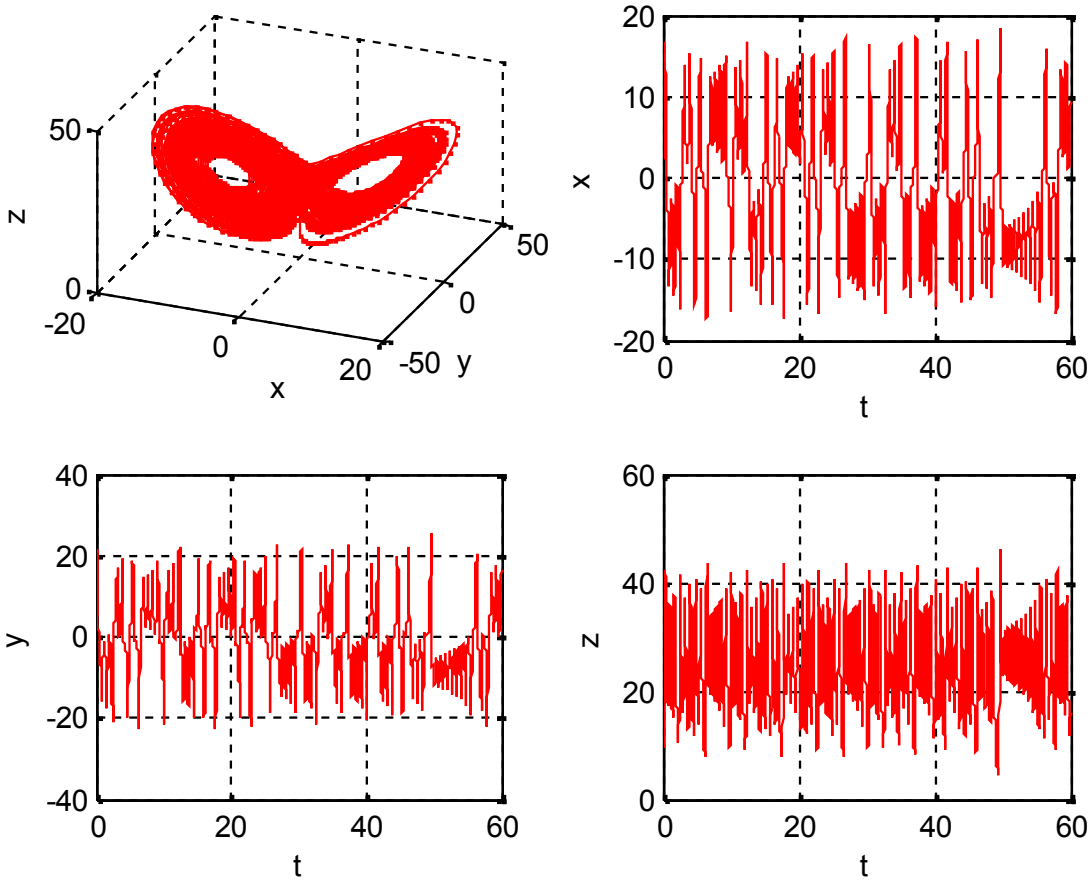


Figure 2.10 : Attracteur de Lorenz [44]

2.5.4 Attracteurs de Rössler

Un autre exemple d'un système dynamique continu et celui de Rössler. Ce système, qui a été proposé par l'Allemand Otto Rössler, est lié à l'étude de l'écoulement des fluides ; il découle des équations de *Navier-Stokes*. Les équations de ce système ont été découvertes à la suite de travaux en cinétique chimique [35].

$$\dot{x} = -y - z \tag{2.21}$$

$$\dot{y} = x + Ay \tag{2.22}$$

$$\dot{z} = B + xz - cz \tag{2.23}$$

Les paramètres de trajectoire illustrée dans la figure (figure 2.11) ont été choisis de la manière suivante : A = 0.3, B=0.3, C = 5 avec la condition initiale (x_0, y_0, z_0) = (1, 1, 0.3). La solution de ce système est un attracteur étrange.

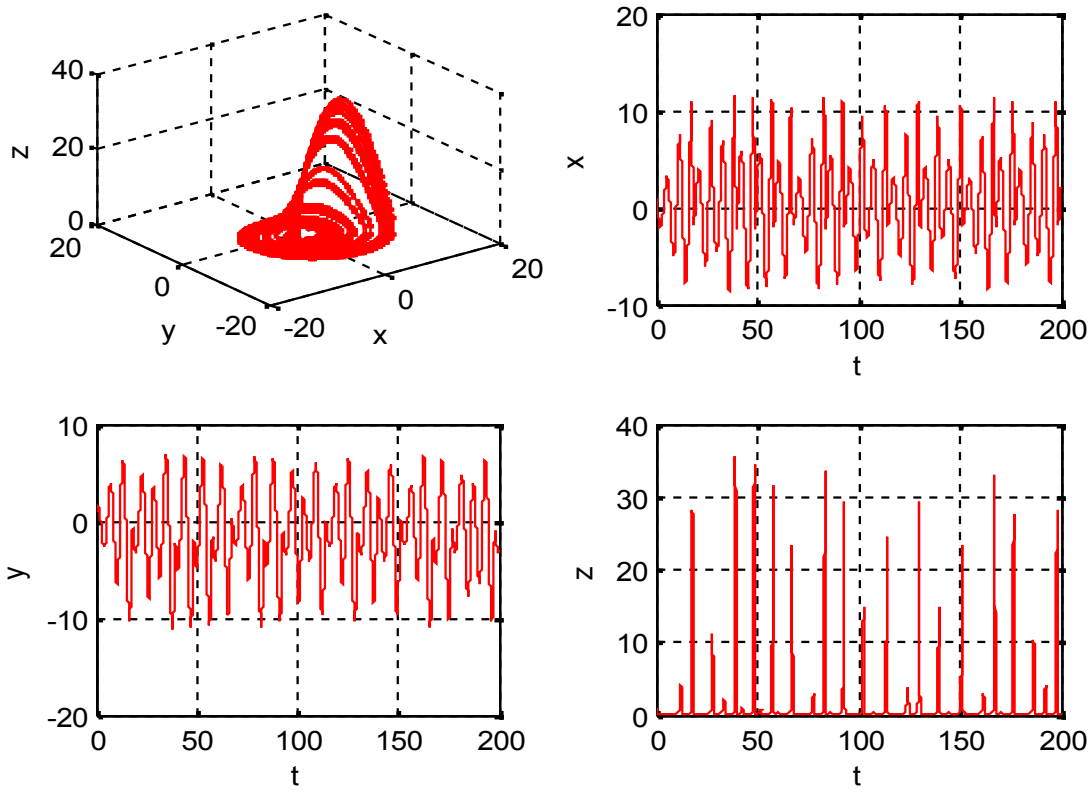


Figure 2.11 : Attracteur de Rössler [44]

2.6 La sensibilité aux conditions initiales

Poincaré a prouvé qu'une petite erreur sur les conditions initiales produirait une erreur énorme sur le résultat final. Cependant, la sensibilité aux conditions initiales constitue la caractéristique essentielle du comportement chaotique d'un système, et la solution devient imprévisible[44].

Quantitativement, une petite erreur à l'entrée va être amplifiée exponentiellement, ainsi toute prédiction devient pratiquement impossible.

Dans la figure suivante, nous pouvons constater que la variation du système de Lorenz à une petite erreur aux paramètres d'entrée s'amplifie d'une manière imprévisible dans l'état final.

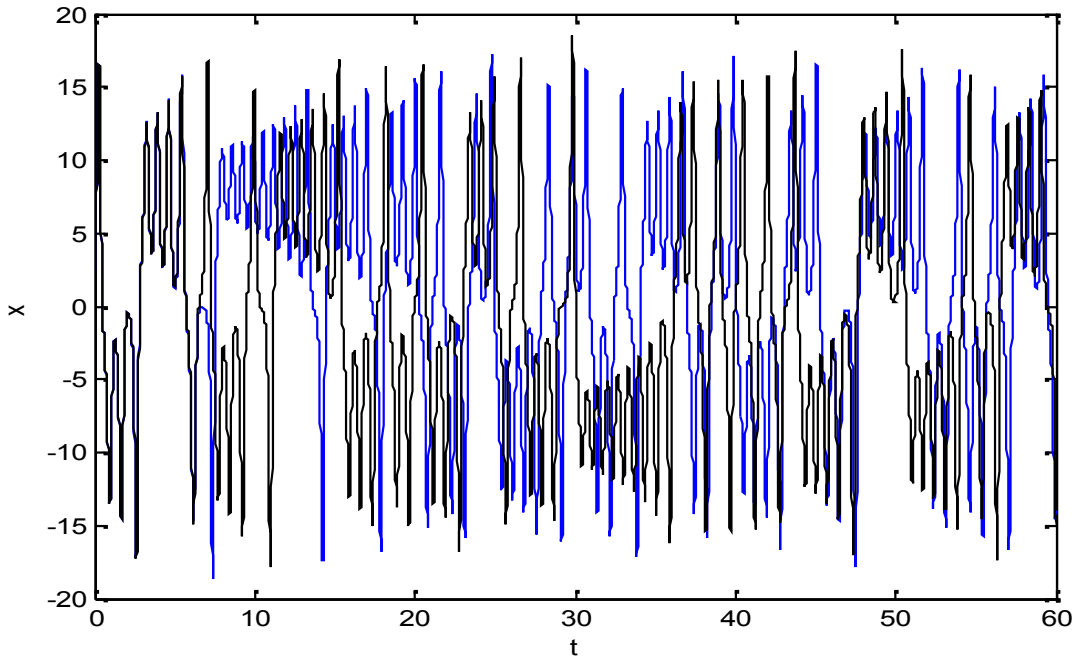


Figure 2.12 :Evolution de la trajectoire en Noir pour les conditions initiales (x_0=2.18; x_1=5.15; x_2=10.20) et la trajectoire en Bleu pour les conditions initiales (x_0=2.17; x_1=5.14; x_3=10.21). [44]

2.7 Stabilité des systèmes dynamiques

L'étude de la stabilité d'un système se réfère souvent à la théorie directe de Lyapunov qui ne nécessite pas la résolution du système [36]. L'exposant de Lyapunov permet de quantifier la stabilité ou l'instabilité des mouvements d'un système dynamique. La fonction de Lyapunov est généralement l'approche la plus utilisée pour garantir la convergence du système.

Le système chaotique est caractérisé par l'existence d'un attracteur étrange, et par suite pour cet attracteur deux points de départ initialement très proches divergent de façon exponentielle, donc au moins un exposent de Lyapunov est positif strictement, ceci élabore la notion appelé sensibilité aux conditions initiales.

Géométriquement, cela se traduit par le fait que si on choisit un ensemble de conditions initiales situées dans une sphère infiniment petite de diamètre δ (0) dans le bassin d'attraction d'un système dynamique de dimension n ; sous l'effet de la dynamique cette sphère va se déformer pour se transformer en ellipsoïde. Le i-ème exposant de Lyapunov se définit alors en fonction de la déformation subie sur la i-ème direction comme [37] :

$$\lambda_i = \lim_{t\to\infty} \frac{1}{t} \ln \frac{\delta_i(t)}{\delta_i(0)}, \quad i = 1..n \tag{2.24}$$

L'ensemble $(\lambda_i)i$=1...*n* constitue le spectre de Lyapunov.

Un exposant de Lyapunov positif indique que selon la direction qu'il représente la divergence entre deux trajectoires voisines augmente exponentiellement avec le temps. Il s'agit donc bien là d'une caractérisation d'un attracteur étrange.

On peut caractériser le mouvement d'un système dynamique selon les signes des exposants de Lyapunov comme suit :

- Un mouvement instable a un exposant de Lyapunov positif
- Un mouvement stable, un exposant de Lyapunov négatif. Alors le système est asymptotiquement stable ; les trajectoires convergent vers le point d'équilibre.
- Les mouvements bornés ont un exposant de Lyapunov négatif ou nul.
- Un mouvement chaotique si l'un des exposants de Lyapunov d'un système non linéaire est positif.

On peut résumer la correspondance entre le type de l'attracteur et le signe des exposants de Lyapunov dans le Tableau suivant [44] :

Régimes permanentes	**Attracteur**	**Exposants de Lyapunov**
Point d'équilibre	Point	$0 > \lambda_1 \geq \ldots\ldots \geq \lambda_n$
Périodique	courbe fermée	$\lambda_1 = 0$ $0 > \lambda_2 \geq \ldots\ldots \geq \lambda_n$
Quasi-périodique	Tore	$\lambda_1 = \ldots\ldots = \lambda_{i=} 0$ $0 > \lambda_{i+1} \geq \ldots\ldots \geq \lambda_n$
Chaotique	Fractale	$\lambda_1 > 0$ $0 \geq \lambda_2 \geq \ldots\ldots \geq \lambda_n$

Tableau 2.1 : Classification des régimes permanents en fonction des exposants de Lyapunov.

2.8 Les fractales

La notion de fractale a été introduite par le mathématicien Benoît Mandelbrot dans les années 1970 pour désigner des ensembles possédant des propriétés géométriques particulières que l'on peut rapidement résumer par les concepts de similitude interne et d'invariance par changement d'échelle : une structure fractale est la même « de près comme de loin » [44][38]. Il est possible grâce aux fractales d'aborder l'étude de phénomènes complexes et chaotiques de façon rationnelle permettant de reconnaître pour ces phénomènes une homothétie interne,
un mécanisme répétitif souvent très simple et une dimension fractale. Ce qui justifie largement le développement que connaît actuellement cette branche des sciences [39].

Exemple : la courbe de Helgevon Koch

Cette courbe de Koch se crée ainsi : au début, c'est-à-dire à l'itération zéro, on dispose d'un « initiateur » (état initial) qui est un segment de droite L (fig. 2.13). À la première itération, ce segment est remplacé par une ligne brisée, formée de 4 segments de longueur L/3, que l'on nomme le « générateur » (startingshape ou seedshape). À la seconde itération, on remplace chacun des 4 segments par le générateur, si bien que chaque nouveau segment mesure L/9. À la fin de chaque étape, la forme résultante (output) est reportée en début d'une nouvelle étape
(input) : ce procédé se nomme « récursivité » (recursion). À la troisième itération, on poursuit le remplacement de chaque segment par une version encore réduite du générateur. En poursuivant de la sorte, on obtient une forme de plus en plus complexe, jusqu'à l'infini [38][44].

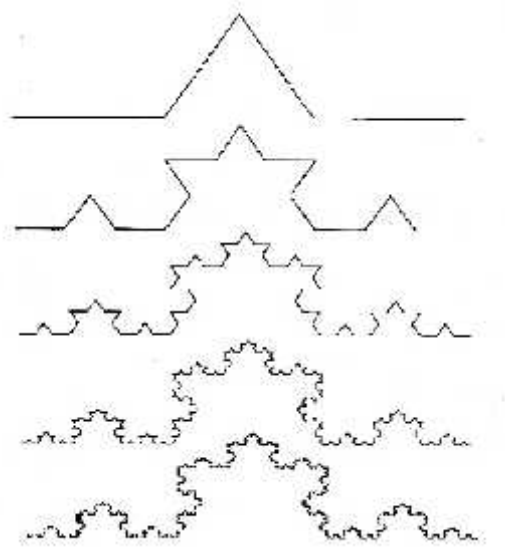


Figure 2.13: La courbe de Koch

2.9 Masquage chaotique

Le principe de ce schéma consiste à effectuer une simple addition entre le signal de sortie de l'émetteur et l'information m_k. L'émetteur (générateur de chaos) et le récepteur ont pour représentation d'état, respectivement[47]:

$$\begin{cases} x_{k+1} = f(x_k) \\ y_k = x_{k+1} + m_k \end{cases} \quad (2.25) \qquad \begin{cases} x'_{k+1} = f(x'_k) \\ y'_k = x'_{k+1} \end{cases} \quad (2.26)$$

Où x_k (resp. x_k') est le vecteur d'état de l'émetteur (resp. du récepteur), y_k (resp. y_k') la sortie de l'émetteur (resp. du récepteur), m_k l'information à masquer. La figure suivante illustre ce mode de masquage.

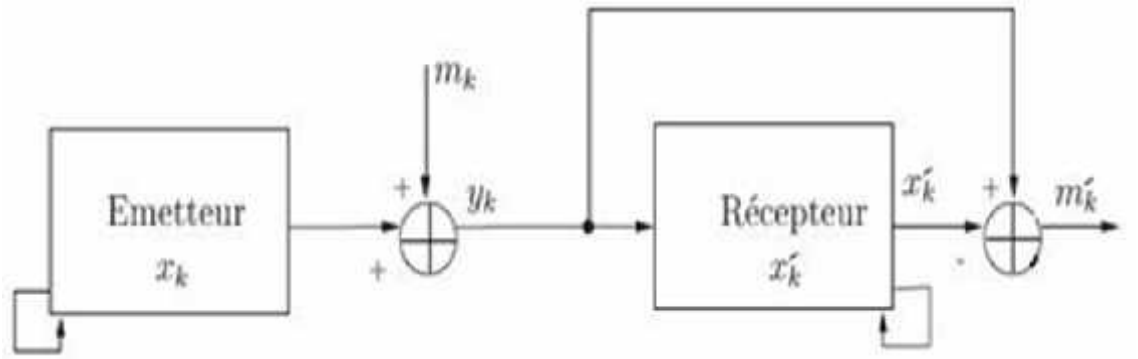


Figure 2.14 : Masquage additif

La reconstruction de l'information nécessite la synchronisation de l'émetteur et du récepteur. L'information est alors récupérée en soustrayant la sortie du récepteur avec celle de l'émetteur [47]:

$$m_k = y_k - x_k \quad (2.27)$$

2.10 Modulation chaotique

La modulation chaotique, est aussi connue sous le nom de “chaos shiftkeying” ou “chaoticswitching”, en anglais. Côté émetteur, à chaque symbole $m_k = m_i$ de l’information, appartenant à un ensemble fini $\{m_k, \dots m_N\}$ correspond un signal y_k issu d’un système chaotique décrit par [47]:

$$\begin{cases} x_{k+1} = f_i(x_k) \\ y_k = x_{k+1} \end{cases} \quad (2.28)$$

Où $i \in \{1, \dots, N\}$, x_k est le vecteur d’état, y_k la sortie. Le cas le plus simple correspond à une information binaire. Dans ce cas, seulement deux systèmes émetteur, avec $i \in \{1,2\}$,, sont nécessaires, l’un correspondant à $m_1 = 0$ et l’autre à $m_2 = 1$. La figure suivante illustre la modulation chaotique [47]:

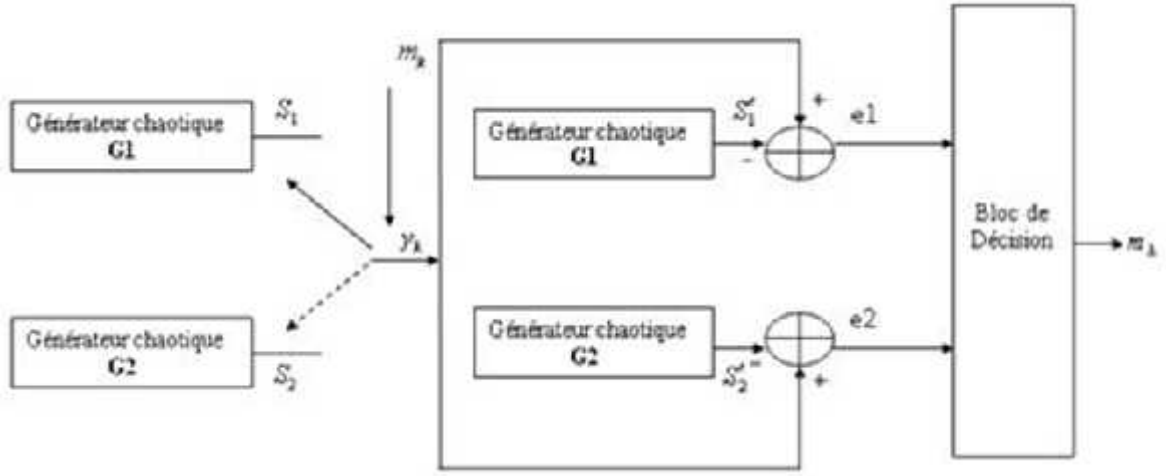


Figure 2.15 : Modulation chaotique

Le rôle du récepteur est de détecter quel émetteur a produit la sortie y_k .Pour cela, le récepteur est composé d’autant de systèmes que l’émetteur, décrits par:

$$\begin{cases} x'_{k+1} = f'_i(x'_k) \\ y'_k = x'_{k+1} \end{cases}, \text{i} = 1, \dots, \text{N} \quad (2.29)$$

2.11 Application du comportement chaotique

L'impact majeur de la théorie du chaos est encore à venir; il ne se limitera pas aux mathématiques, mais se fera sentir sur l'ensemble de la science [40-41]. Dans la littérature on peut trouver plusieurs applications du chaos pour des différents domaines de sciences, telles que [28] :

- **En télécommunication :** L'utilisation du chaos pour masquer ou mélanger les informations dans une transmission sécurisée. L'originalité repose sur la prise en compte des propriétés de signaux chaotiques issus soit d'équations différentielles soit de récurrences discrètes non linéaires.
- **En informatique :** Des procédés de compression d'images ont été mis au point à partir des fractales. Des images de synthèse, au cinéma ou dans le domaine des jeux vidéo, sont rendues de plus en plus réalistes, toujours grâce aux fractales. En effet, les objets fournis par la géométrie euclidienne sont assez peu aptes à représenter fidèlement le monde : les formes de la nature répondent bien plus aisément aux formes fractales.
- **En biologie :** La théorie du chaos permet d'expliquer les variations des populations animales, les oscillations du cerveau. (c'est-à-dire un enregistrement graphique de l'activité électrique du cerveau au moyen d'électrodes placées sur le cuir chevelu, est un attracteur étrange). Ce pourrait donc être en vertu de la théorie du chaos que l'homme est libre et unique[44].
- Les arythmies cardiaques typiques de nombreuses maladies du cœur se trouvent aussi expliquées par la théorie du chaos. Dans un cœur normal, des impulsions électriques se répandent de manière régulière dans les fibres musculaires, qui forcent le ventricule du cœur à se contracter et à pomper le sang. Une fois contractées, les fibres sont insensibles aux signaux électriques ; on parle de période réfractaire. Ce sont ainsi les variations de la durée de la période réfractaire d'une zone du ventricule à un autre qui seraient la cause de la contraction spasmodique à l'origine d'une crise cardiaque[44].
- **En économie :** Les mouvements commerciaux et les marchés financiers, ainsi que les cycles économiques, peuvent être expliqués en partie par la théorie du chaos, où les fractales ont un lien très étroit avec le hasard, et permettent donc de modéliser des expériences aléatoires complexes, d'où l'utilisation en finance, pour modéliser les variations des cours de la Bourse[44].

- **En art :** Dans le domaine de l'*art*, depuis les années 1980, la beauté des fractales est exploitée et appréciée, et on voit des expositions se multiplier avec pour thème ces images fascinantes. Les images fractales ont un intérêt esthétique certain, mais on peut se demander si elles ont une autre utilité. On peut remarquer certaines fonctions remarquables des fractales dans différents domaines[44].

2.12 Conclusion

Dans ce chapitre, nous avons défini les différents termes des systèmes dynamiques non linéaires, le chaos, les attracteurs ainsi que la stabilité…etc. nous avons aussi présenté quelques exemples célèbres continus et discrets illustrent la route vers le chaos après un cascade de bifurcation allant d'un état stable à un état chaotique.

Nous avons montré également que les systèmes dynamiques non linéaires pouvaient adopter des comportements dynamiques complexes, sensibles aux conditions initiales et à la valeur des paramètres. Et nous finirons ce chapitre par quelques domaines d'application du chaos. Les notions introduites dans ce chapitre vont être utilisées par la suite. Dans le chapitre suivant, nous allons nous intéresser aux non linéarité dans le résonateur piézoélectrique présentant un comportement chaotique sous de fortes excitations.

Chapitre III

Cryptage par chaos

Chapitre III : Cryptage par chaos

3.1 Introduction

Dans ce chapitre on va s'intéresser à l'étude de quelques exemples théorique et pratiques des systèmes qui sont sources de chao .on va commencer par l'analyse du circuit de Chua qui est un simple circuit électronique montrant un comportement chaotique et cepar l'exploration numérique des équations tirées du circuit par simulation sous MATLAB pour voir l'influencesdesdifférentparamètressurlecomportementchaotique.

3.2 Communications Sécurisées par chaos

Dans les différentes applications actuellement envisagées, les signaux chaotiques servent soit à véhiculer l'information soit à réaliser le cryptage de données.

Nous intéressons au cryptage de données à transmettre et plus particulièrement dans un contexte de transmission sécurisée.

Comme il a été déjà mentionné dans ce chapitre, le chaos déterministe peut générer des comportements dynamiques d'apparences aléatoires. Il serait donc intéressant d'utiliser ces derniers comme porteuses d'informations en télécommunication.

Le diagramme principal de la communication sécurisée par le chaos est montré sur la **Figure3.1**. Le principe est de masquer une information par des signaux chaotiques et de l'envoyer vers le récepteur sur un canal public. L'information cryptée est récupérée au niveau du récepteur.

La clé du système de transmission est l'ensemble des paramètres des deux générateurs chaotiques à l'émission et à la réception qui doivent être synchronisés

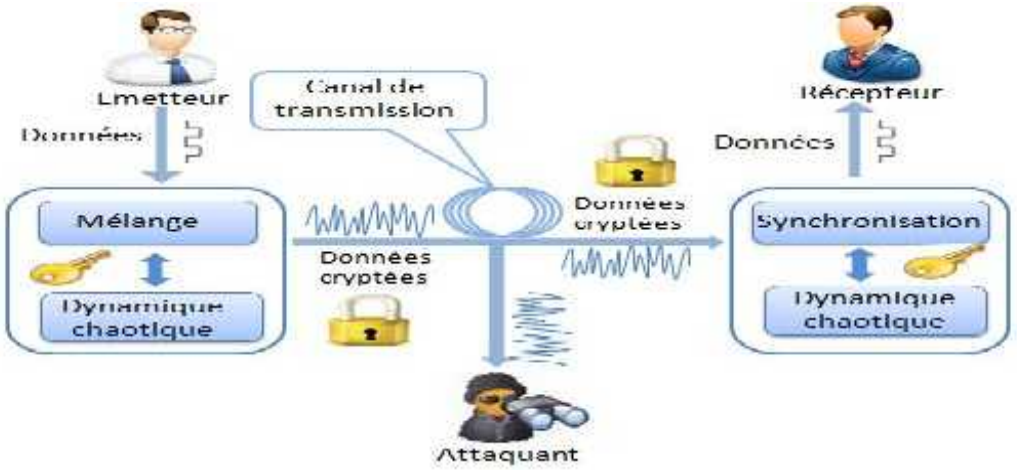


Figure 3.1: Principe de Chiffrement par Chaos.

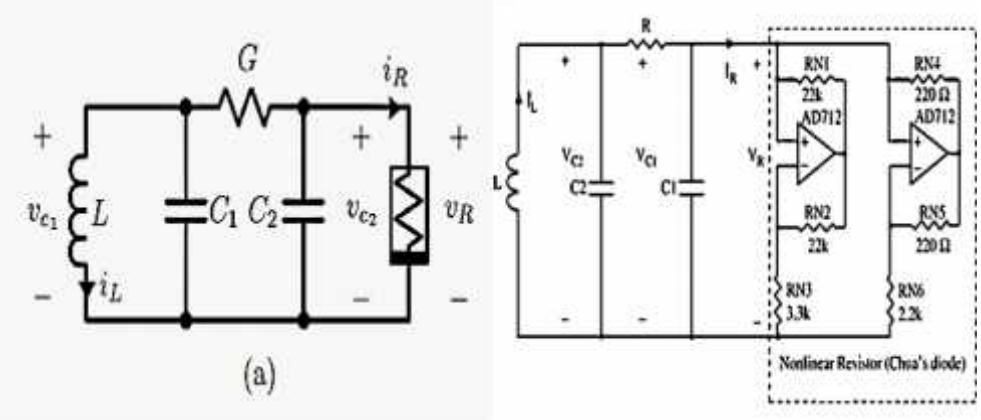
Le chiffrement d'un message par le chaos s'effectue donc en superposant à l'information initiale un signal chaotique. On envoie par la suite le message noyé dans le chaos à un récepteur qui lui connaît les caractéristiques du générateur de chaos. Il ne reste alors plus au destinataire qu'à soustraire le chaos de son message pour retrouver l'information..[42][43]

3.3 Comparaison entre chaos et cryptographie

Les techniques de chiffrage basées sur le chaos, fournissent une bonne combinaison de vitesse, de haute sécurité, de complexité, de frais généraux raisonnables de calcul et de puissance de calcul, etc. Plusieurs propriétés font des systèmes chaotiques, des candidats attrayants pour la sécurité des communications. Nous pouvons citer entre autres un spectre à large bande, des trajectoires qui ne repassent jamais par le même état, un aspect pseudo-aléatoire (comme du bruit par exemple), une implémentation relativement simple des systèmes chaotiques. De plus, depuis les années 90, plusieurs chercheurs ont noté qu'il existe un rapport intéressant entre le chaos et la cryptographie. En effet, plusieurs propriétés des systèmes chaotiques présentent des correspondances similaires ou presque, avec des systèmes cryptographiques traditionnels.

3.4 Le circuit de Chua:

Le circuit de Chua est un circuit électronique simple, c'est un type spécifique des circuits électronique utilisé pour générer les signaux stochastiques et chaotiques. Ce circuit à des applications importantes en communication. Il est constitué par deux capacités C1 et C2 and une inductance L, placés parallèlement en trois branches.
L'élément NR est une diode à résistance négative[44].



.Figure3.2: Le Circuit de Chua, Diagramme électrique

Le circuit de Chua est défini par les équations d'états suivants [44]:

$$\begin{aligned}\frac{dV_1}{dt} &= \frac{G}{C_1}(V_2 - V_1) - \frac{1}{C_1}g(V_1)\\ \frac{dV_2}{dt} &= \frac{G}{C_2}(V_1 - V_2) + \frac{1}{C_2}i_3\\ \frac{di_3}{dt} &= -\frac{1}{L}(V_2 - R_0 i_3)\end{aligned} \qquad (3.1)$$

Ces équations peuvent être écrites par l'ensemble des équations suivantes généralement utilisé dans la littérature [45-46].

$$\begin{aligned}\dot{x} &= \sim(y - x - g(x))\\ \dot{y} &= x - y + z\\ \dot{z} &= -\ y - ¥z\end{aligned} \qquad (3.2)$$

L'élément non linéaire du circuit g(x) est donné par :

$$g(V_1) = G_b V_1 + \frac{G_a - G_b}{2}\left(|V_1 + 1| - |V_1 - 1|\right) \qquad (3.3)$$

3.5 Résultats de simulation

3.5.1 Signal chaotique du circuit de Chua

Le système non linéaire de Chua présente un comportement chaotique. Nous avons obtenu les figures suivantes par l'utilisation de l'Algorithme de Runge Kutta par MATLAB .La figure (3.3) et la figure (3.4) montres deux trajectoires du circuit électriques de Chua pour deux valeurs des paramètres du circuit (a=-2.5, b=-0.9 2, α =-4.89, β =-3.62, γ=-0.016).

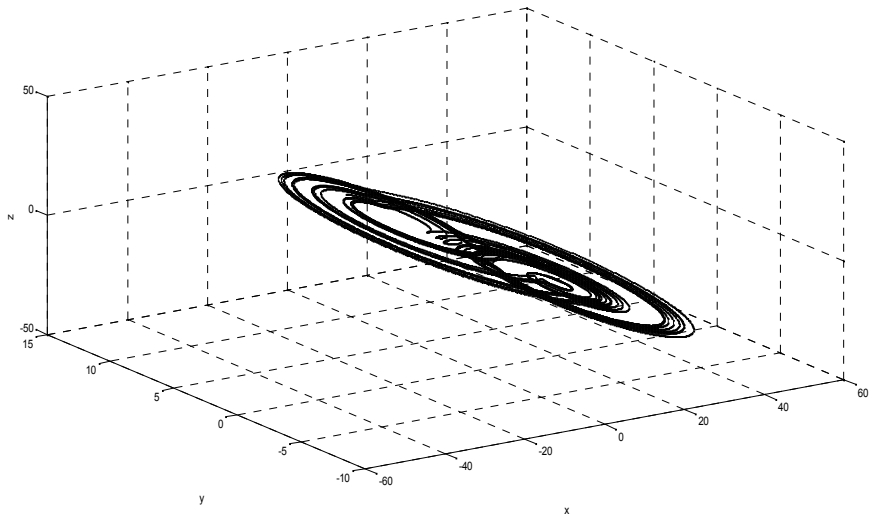


Figure3.3: L'espace de phase

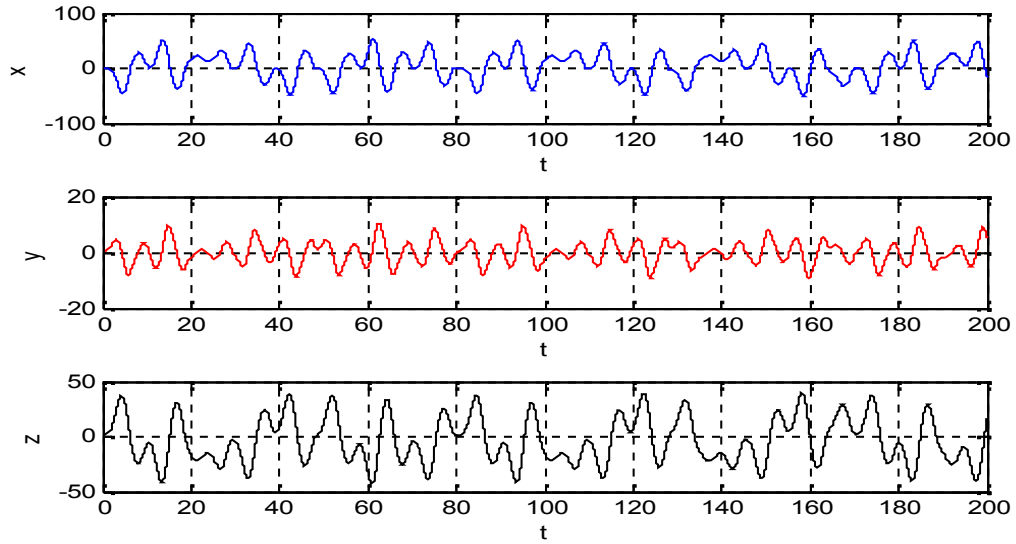


Figure 3.4 : Trajectoire chaotique du circuit de Chua

a=-2.5, b=-0.9 2, α =-4.89, β =-3.62, γ=-0.016

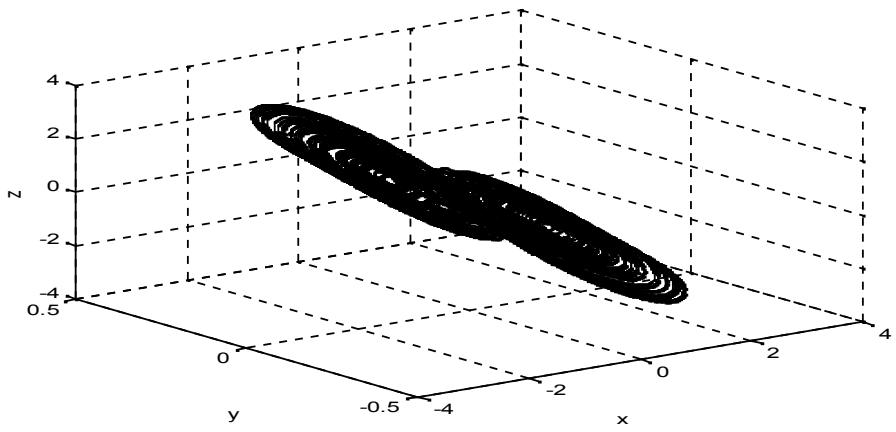


Figure3.5: L'espace de phase

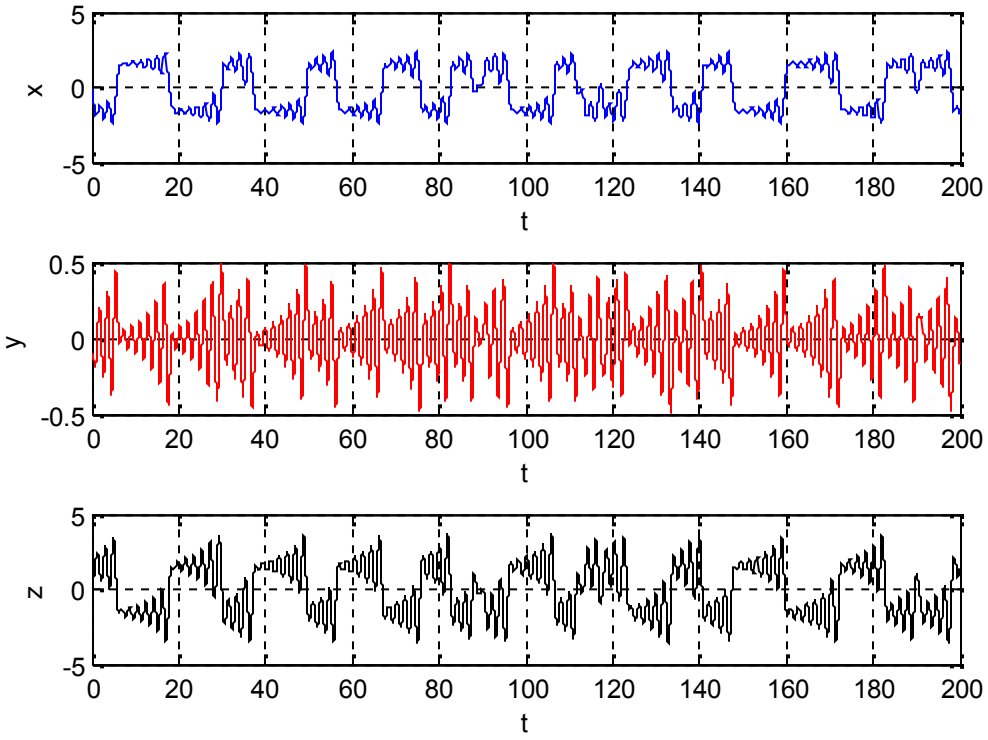


Figure 3.6 : **Trajectoire chaotique du circuit de Chua**

a= -1.20, b= -0.65, alpha1= -0.1,alpha2= -0.1, alpha3= -0.1 α =10, β =16, γ=0.

3.5.2 Chiffrement d'un signal en temps continu par chaos

La figure (3.7) donne le chiffrement d'une information par le chaos. Cette technique s'effectue en superposant à l'image originale un signal chaotique. Il ne reste alors plus au destinataire qu'à soustraire le chaos de son message pour retrouver l'information. Pour montrer l'efficacité de la technique, nous avons utilisé comme donnée un signal sinusoïdal.

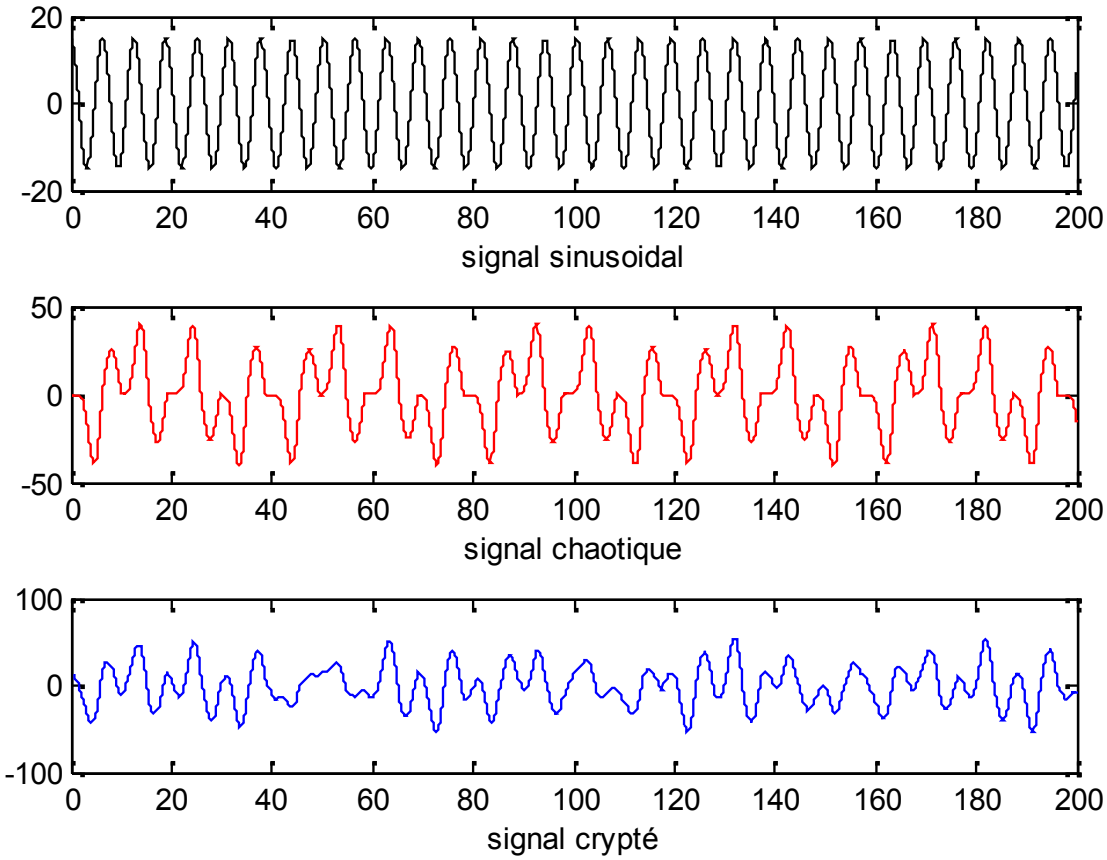


Figure 3.7 : Signal chaotique en fonction de t

Cette figure montre bien que le signal sinusoïdal est devenu un signal crypté et il est difficile à le décrypter sans connaitre la clé de chiffrement.

3.5.3 Chiffrement d'une image

Dans notre travail nous avons utilisé l'algorithme de Runge Kutta pour simuler le modèle de Chua afin de donner un signal chaotique. ce signal est mélangé par le signal ou l'image à crypter.

(A)

(B)

Figure 3.8: Chiffrement de l'image par chaos

(A) : image originale

(B) : image chiffrée

Le type de chiffrement est un chiffrement symétrique puisque la clé de chiffrement est la même que celle du déchiffrement.

Dans cette figure nous avons réussi à crypter l'image originale (A) par un signal chaotique

généré de l'oscillateur chaotique de Chua. La clé de cryptage est l'utilisation des conditions initiales du système et les paramètres de circuit.

3.6 Conclusion

A travers cette étude nous avons défini le circuit de Chua qui permet de générer un signal chaotique déterministe à large spectre. Ce signal permet de crypter des informations avec une clé bien déterminée. Nous avons commencé notre application par le cryptage d'un signal en temps continue et le deuxième exemple c'est le cryptage d'une image.

Les résultats obtenus ont montré l'efficacité des signaux chaotiques pour crypter les informations en temps continu ainsi que les images.

Conclusion générale

Ce mémoire consiste à réaliser un système de transmission de données basée sur le chaos. Le principe s'appuie sur une dynamique chaotique non linéaire.

Au début, le chaos a été considéré comme dangereux ou indésirable par la communauté scientifique, mais

Dans le premier chapitre de ce mémoire, nous avons présenté les différentes méthodes cryptographiques existent dans la littérature. On a des méthodes symétriques et d'autres asymétriques, ces deux méthodes sont généralement utilisées conjointement. Bien que ces méthodes ont fait leurs preuves, la puissance croissante des moyens de calcul menace leur confidentialité. Les ordinateurs puissants sont certes capables de crypter et de décrypter rapidement l'information, mais leur vitesse de calcul autorise parallèlement la cryptanalyse, qui a pour objectif de casser un code en découvrant la clé.

Dans le deuxième chapitre, nous avons évoqué d'abord quelques notions sur les systèmes dynamiques qu'ils soient en temps continu où en temps discret. Par la suite, nous sommes intéressés à une classe particulière de système non linéaire qui est dit chaotique.

Ces systèmes présentent plusieurs caractéristiques dont l'exploitation serait intéressante pour la transmission des données. Parmi ces caractéristiques que nous avons utilisé avec plus de détails, nous pouvons citer le déterminisme qui signifie que ces systèmes sont régis par des règles fondamentales non probabilistes. Il est alors possible de reproduire le comportement chaotique. Une autre propriété intéressante de ces systèmes est la sensibilité aux conditions initiales.

Dans le troisième chapitre du mémoire, nous avons fait une simulation qui nous a permis de simuler notre cryptage chaotique, en utilisant le langage de programmation MATLAB pour l'insertion de quelques fonctions.

Dans ce mémoire, nous avons utilisé un système de cryptage chaotique. L'opération de chiffrement a été réalisée avec succès. Les données du signal chaotique ont été obtenues sous logiciel MATLAB.

Bibliographie :

[1] :L. H. Minh, Modélisation et Optimisation non convexe basées sur la programmation DC et DCA pour la résolution de certaines classes des problèmes en Fouille de Données et Cryptologie, Thèse de Doctorat de l'université de Paul Verlaine-Metz, 2007

[2] :R. Dumont, Cryptographie et Sécurité informatique, Cours de l'université de Liège, 2009 – 2010.

[3] :N.Mahammedi et H.Mahdadi, Implémentation de benchmark d'opérations crypto basées ECC pour l'étude et comparaison de courbes elliptiques, Mémoire MASTERACADEMIQUE de l'université KasdiMerbah, Ouargla, 2013.

[4] :http://ram0000.developpez.com/tutoriels/cryptographie/?page=page_2#L2. <visité le :28/04/2019>

[5] :Medjahdi NASREDDINE, Cryptage Chaotique Basé Sur l'Attracteur Clifford, mémoire Master, Faculté des Sciences Département d'Informatique, Tlemcen 2017

[6] :G. Florin, S. Natkin, 'LES TECHNIQUES DE CRYPTOGRAPHIE', mars 2002.

[7] :http://www.bart-konieczny.com/fr/blog/securite-des-applications-web/cryptage-symetrique-et-asymetrique.< visité le :05/04/2019>

[8] :R.Dumont, Cryptographie et Sécurité informatique, Cours de l'université de Liège, 2009 – 2010.

[9] :L. H. Minh, Modélisation et Optimisation non convexe basées sur la programmation DC et DCA pour la résolution de certaines classes des problèmes en Fouille de Données et Cryptologie, Thèse de Doctorat de l'université de Paul Verlaine-Metz, 2007

[10] :Z. Amrani, S Chitroub et A. Boukhari , Cryptage d'Images par Chiffrement de Vigenère Basé sur le Mixage des Cartes Chaotiques, International Conférence on Computer IntegratedManufacturing ,2007.

[11] :P. Loidreau, Introduction à la cryptographie, , 2005

[12] :A. Ouannas. Sur La Synchronisation Des Systèmes Chaotiques Discrets. Thèse de Doctorat en science, Université de Constantine.

[13] :I.Zelinka. M. Chadli. An investigation on evolutionary reconstruction of continuous chaotic systems. Mathematical and Computer Modelling. Vol 57, pp 2–15,2013.

[14] :L. Wang, Y. Xu, L. Li, Parameter identification of chaotic systems by hybrid Nelder–Mead simplex search and differential evolution algorithm, Expert Systems with Applications. Vol 38, pp 3238–3245, 2011

[15] :J. Sun, J. Zhao, X. Wu , W.Fang, Y. Cai, W. Xu, Parameter estimation for chaotic systems with a Drift Particle Swarm Optimization method, Physics Letters A. Vol 374,pp 2816–2822, 2010.

[16] :J. J. Bricmont. Introduction à la dynamique non linéaire. Phys 2111, Unité de Physique théorique & mathématique. 2009-2010.

[17] :M.L. Bogdan. Apports du chaos et des estimateurs d'états pour la transmission sécurisée de l'information. PhDthesis, Université de Bretagne occidentale, 2006.

[18] :D. Battikh. Sécurité de l'information par stéganographie basée sur les séquences chaotiques. Thèse INSA Rennes, Université européenne de Bretagne, 2015.

[19] :H.K. Lam W-K. Ling, H.H-C. Lu; SS.H. Ling, Synchronization of Chaotic Systems Using Time-Delayed Fuzzy State Feedback Controller, IEEE Transactions on Circuits and Systems I, Vol. 55, No, 3, pp. 893 – 903, 2008.

[20] :A. Mitsiouk Contribution a l'Optimisation des Systemes Dynamiques :Application au Genie des Procedes.thèse de doctorat, Institut national Polytechnique de Toulouse.2007.

[21] :M.L. Bogdan. Apports du chaos et des estimateurs d'états pour la transmission sécurisée de l'information. PhDthesis, Université de Bretagne occidentale, 2006.

[22] :I. Mareels,S . Van Gils,J . W. Polderman and A. Ilchmann. Asymptotic Dynamics in Adaptive Gain Control. Advances in Control. London: Springer-Verlag, pp 29-63. 1999.

[23] :Unité de Physique théorique & mathématique. Phys 2111.Université de catholique de Louvain. 2009-2010.

[24] :I. Mareels, S. Van Gils, J. W. Polderman, and A. Ilchmann. Asymptotic dynamics in adaptive gain control. In P. M. Frank, editor, Advances in Control, Highlights of ECC'99, pages 391_449. Springer, 1999.

[25] :A. Serbanescu. Electronique, physique et signal pour les telecommunications, chapterSystèmes et signaux face au chaos. Ed. Tehnica, 1997.

[26] :D. G. Luenberger. Introduction to Dynamic Systems : Theory, Models, and Applications. John Wiley& Sons, 2 edition, 1979.

[27] :Z. Elhadj, etude de quelques types de systèmes chaotiques : Generalisation d'un modele issu du modele de Chen, thése de doctorat, université de constantine. 2006.

[28] :K. T. Alligood, T. D. Sauer, J. A. Yorke, CHAOS: An Introduction to dynamical Systems. Springer, 2000.

[29] :J. M. Ginoux. Stabilité des systèmes dynamiques chaotiques et variétés singuliéres. Phden sciences. Mathématique appliquée. Systèmes dynamiques. Université du Sud Toulon-Var. 2005.

[30] :M. P. Kennedy. Basic concepts of nonlinear dynamics and chaos. *Tutorials (IEEE)*, pages 289–313, 1994.

[31] :E. N. Lorenz. Deterministic nonperodic flow. *J. Atmos. Sci.*, Vol 20, pp130–141, 1963.

[32] :A. H. Gandomi, G. J. Yun, X.-S. Yang & S. Talataharix, Chaos-enhanced accelerated particle swarm optimization, Communications in Nonlinear Science and Numerical Simulation, 18, 327-340, 2013.

[33] :C.C. Wang, and J.P. Su, "A novel variable structure control scheme for chaotic synchronization," Chaos SolitonsFract., vol. 18, pp. 275-287, 2003.

[34] :P. Gaspard. Rossler systems. Encyclopedia of NonlinearScience, Alwyn Scott, Editor. Pp808-811, New York, 2005.

[35] :A. Wolf, J. B. Swift, H. L. Swinney, and J. A. Vastano. Determining lyapunovexponentsfroma time series. Physica D, Vol 16, pp 285–317, 1985.

[36] :D. Dehouve, La notion de fractale en anthropologie, Ethonographique.org, Revue en ligne de sciences humaines et sociales.2014.

[37] :J. Lajoa. La géométrie fractale. Mémoire en maitrise en mathématique et informatique appliquées. Université de Quebec. Juin 2006.

[38] :O. chabour. Stabilisation des systèmes non linéaires. Thése de doctorat, Université De Metz. 2003.

[39] :U.E. Vincent, R. Guo. Adaptive synchronization for oscillators in 6 potentials, Nonlinear Dyn. Syst. Theory, Vol. 13(1), pp. 93–106, 2013.

[40] :C. Li, J. Zhou, J. Xiao, H. Xiao, Hydraulic turbine governing system identification using T–S fuzzy model optimized by chaotic gravitational search algorithm, Engineering Applications of Artificial Intelligence, Vol. 26, No. 9, pp. 2073-2082, 2013.

[41] :A. Clairet. Modélisation et analyse numérique de résonateurs à quartz à ondes de volume. Electronique. Université de Franche-Comté, 2014.

[42] :G. Florin, S. Natkin, 'LES TECHNIQUES DE CRYPTOGRAPHIE', mars 2002.

[43] :Pierre-Louis Cayrel, 'Chiffrement par blocs', Université de limoges, France.

[44] :F.Maamri, Contribution à la modélisation et à l'identification des systèmes chaotiques par les méta-heuristiquesMéthodes méta-heuristiques - Stabilité par la méthode de Lyapunov. Thése de Doctorat. Univérsité d'Oum el Boighi. 2019

[45] :V. Siderskiy, Parameter matching Adaptive Synchronization of Chua's Circuit, Thesis Submitted in Partial Ful_llment of the Requirements for the Degree of Bachelor of science, New York university, 2014.

[46] :G-Q Zhong, Implementation of Chua's Circuit with a Cubic Nonlinearity. IEEE Transaction On Circuits and Systems—I: Fundamental Theory And Applications, Vol. 41,NO. 12, 1994.

[47] :NKouadriMoustefia, Teste de validation pour les crypto-systèmes chaotiques, Thése de magister, université de science et technologie d'oran, 2013-2014.

[48] :Adda Ali Pacha, Abdallah M'Hamed Chaos Crypto-Système basé sur l'Attracteur de Hénon-Lozi. ConferencePaper · January 2009.