République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
UNIVERSITE ABOU BEKR BELKAID TLEMCEN
FACULTE DE TECHNOLOGIE

DEPARTEMENT DE TELECOMMUNICATIONS

MEMOIRE

Pour l'obtention du diplôme de
MASTER en

Réseaux mobiles et services de télécommunications

Réalisé par

BOUCHENAK Nabahat

THEME

Transmissions sécurisées en utilisant un cryptosystème numérique par CHAOS

Soutenu en Juin 2015 devant le Jury :

Mr KAMECHE Samir	M.C.A à l'Université de Tlemcen	Président
Mr MERZOUGUI Rachid	M.C.A à l'Université de Tlemcen	Examinateur
Mme BENMANSOUR F.Zohra	M.C.B à l'Université de Tlemcen	Encadreur

Année universitaire : 2014-2015

Dedicace

Avec un énorme plaisir, un Coeur ouvert et une immense joie,

que je dédie mon travail à mes trés chers, respectueux

Mari, Parents, Grande mère et Belle mère,

Ainsi a ma soeur et mon frère,

et en particulier à mon fils "Omar".

A toute personnes qui m'ont encouragé ou aidé tout au long de mes études.

Remerciements

Je remercie avant tout DIEU Allah tout puissant pour la volonté, la santé et la Patience qu'il m'a donné afin de réaliser ce modeste travail.

J'exprime ma plus grande reconnaissance à mon encadreur Madame **BENMANSOUR Fatima Zohra** pour avoir accepté de diriger ce travail, de m'avoir guidé et
soutenu avec patience et indulgence, pour ses lectures enrichissantes de mon mémoire.

J'exprime ma plus grande gratitude et respect à Monsieur **KAMECHE Samir**, Maitre de conférences à l'université deTlemcen, pour l'honneur qu'il me fait en president le Jury, ainsi qu'à Monsieur **MERZOUGUI Rachid**, Maitre de conférences à l'université de Tlemcen,
Pour l'honneur qu'ils me font en participant à mon jury.
Je les remercie sincèrement pour le temps qu'ils ont consacré à la lecture et à l'évaluation de ce travail.

Je tiens également à remercier Monsieur CHERKI Brahim, pour son aide, sa culture scientifique, et son incroyable modestie et
disponibilité

Mes sincères remerciements s'adressent aussi à mes parents qui m'ont soutenus tout au long de ma vie.

Un grand merci à mon mari pour son encouragement et sa confiance .

Sommaire

CHAPITRE II: TRANSMISSIONS SECURISEES PAR CHAOS

Chapitre III. Simulation et Résultats

Table des figures :

Liste des tableaux:

Table des abréviations :

AES : **A**dvanced **E**ncryption **S**tandard

DES : **D**ata **E**ncryption **S**tandard

RSA: Ron **R**ivest, Adi **S**hamir et Leonard **A**dleman

DSA: **D**igital **S**ignature **A**lgorithm

RC5 **: R**ivest's **C**ipher

ECB : **E**lectronic **C**ode **B**ook

CFB : **C**ipher **F**eed**b**ack

QKD: **Q**uantum **K**ey **D**istribution

INTRODUCTION GÉNÉRALE

INTRODUCTION GÉNÉRALE

Le besoin de dissimuler les informations préoccupe l'homme depuis le début de la civilisation [1]. La confidentialité apparait notamment nécessaire lors des luttes pour l'accès au pouvoir. Puis elle se développe énormément à des fins militaires et diplomatiques. Aujourd'hui, de plus en plus d'applications dites civiles nécessitent la sécurité des données transitant entre deux interlocuteurs ou plusieurs, via un canal de transmission d'information comme les réseaux de télécommunications actuels et futurs. Ainsi, les banques utilisent ces réseaux pour assurer la confidentialité des opérations avec leurs clients ; les laboratoires de recherche s'en servent pour échanger des informations dans le cadre d'un projet d'étude commun ; les chefs militaires pour donner leurs ordres de bataille, etc.

De nos jours, la nécessité de cacher ou de casser une information rentre dans un vaste ensemble appelé cryptologie. Toutefois, étymologiquement, la cryptologie apparait comme la science du secret. Elle n'est cependant considérée comme une science que depuis peu de temps ; depuis qu'elle allie l'art du secret à celle de la piraterie. Cette discipline est liée à beaucoup d'autres, par exemple la théorie des nombres, l'algèbre, ou encore la théorie de l'information. Cette science comporte deux branches: la cryptographie et la cryptanalyse.

La cryptographie traditionnelle est l'une des méthodes permettant de transmettre les données de manière confidentielle. Afin de protéger un message, on lui applique une transformation qui le rend incompréhensible : c'est ce qu'on appelle le chiffrement. Le chiffrement permet donc à partir d'un texte en clair, d'obtenir un texte chiffré ou cryptogramme. Inversement, le déchiffrement est l'action qui permet de reconstruire le texte en clair à partir du texte chiffré. Dans la cryptographie moderne, les transformations en question sont des fonctions mathématiques, appelées algorithmes cryptographiques, qui dépendent d'un paramètre appelé clé.

La cryptanalyse à l'inverse, est l'étude des procédés cryptographiques dans le but de trouver des faiblesses et en particulier, de pouvoir décrypter des textes chiffrés [2]. Le décryptage est l'action consistant à retrouver le texte en clair sans connaître la clé de déchiffrement.

L'information transmise n'est pas exclusivement sous forme de données textuelles mais également audio, images numériques et autres multimédia. Les images sont très largement utilisées dans notre vie quotidienne et, plus leur utilisation est croissante, plus leur sécurité est vitale. Par exemple, il est primordial de protéger les plans de bâtisses militaires, plans de constructions d'une banque ou bien les images captées par des satellites militaires. En plus avec la progression continue de la cybercriminalité, la sécurité des images numériques est devenue un thème important dans le monde des communications.

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.

Dans de telles circonstances, il est devenu nécessaire et impératif de crypter les images numériques avant de les transmettre. Les algorithmes de chiffrement traditionnels tels que le DES (Data Encryption Standard) et la RSA (RonRivest, Adi Shamir et Leonard Adleman) ne sont pratiquement pas appropriés au chiffrement d'images dû à quelques caractéristiques intrinsèques des images comme la taille (image de grande taille), la redondance élevée, la forte corrélation entre les pixels adjacents .

Pour fournir une meilleure solution aux problèmes de sécurité d'images, un certain nombre de techniques de chiffrement d'images ont été proposées telles que les techniques basées sur les systèmes chaotiques qui fournissent une bonne combinaison entre la vitesse d'exécution et la haute sécurité. Les signaux chaotiques peuvent être analogiques ou numériques, continus ou discrets. Les cryptosystèmes analogiques basés sur le chaos font intervenir la technique de synchronisation chaotique, et ceux numériques font intervenir un ou plusieurs système(s) chaotique(s) de telle manière que la clé secrète soit donnée soit par les paramètres de contrôle, soit par les conditions initiales. Les signaux chaotiques continus non linéaires sont en général apériodiques et bornés. Ceci permet de les utiliser comme des séquences pseudo-aléatoires qui ont l'avantage d'être productibles à l'identique en émission réception. Les séquences chaotiques numérisées peuvent alors être utilisées comme clés secrètes dans un cryptosystème basé sur le chaos. La sécurité obtenue est maximale, car la connaissance d'un cryptogramme «message chiffré connu» ne donne aucune indication sur le message clair correspondant. Toutefois, l'espace des clés et l'échange des clés demeurent une préoccupation. L'espace des clés doit être la plus large possible pour augmenter la sécurité

des cryptosystèmes. L'échange des clés doit se faire de la manière la moins complexe possible. La clé sécrète étant générée par un système chaotique de Lorenz de haute dimensionnalité afin de renforcer la sécurité du cryptosystème.

Le travail présenté dans ce mémoire s'organise autour de trois chapitres :

Le premier chapitre aborde les généralités sur les systèmes cryptographiques. Les deux principaux schémas de chiffrement en cryptographie standard, le chiffrement asymétrique ou à clé publique et le chiffrement symétrique sont décrits. Ensuite, des modes de chiffrement de l'information incluant une dynamique chaotique proposés dans la littérature sont détaillés dans l'optique de mettre en évidence la puissance de cet outil dans la cryptographie par rapport aux méthodes existantes.

Le second chapitre présente la théorie du chaos, ses modes de chiffrement et déchiffrement puis on aborde les méthodes de chiffrement par chaos numérique par la récurrence logistique puis par la récurrence Skew tent.

Dans le dernier chapitre, on a réalisé une chaine de transmission sous simullink de MatLab les résultats sont après résumé dans une interface graphique qui nous permet de visualiser les différentes conversions, ainsi le chiffrement et le déchiffrement d'une image par le chaos.

Le travail ainsi mené s'achève par une conclusion générale.

Chapitre I

Généralités sur les cryptosystemes

Introduction :

L'origine de la cryptologie mot réside dans la Grèce antique. La cryptologie est un mot composé de deux éléments : «cryptos », qui signifie caché et « logos » qui signifie mot. La cryptologie est aussi vieille que l'écriture elle-même, et a été utilisée depuis des milliers d'années pour assurer les communications militaires et diplomatiques. Par exemple, le célèbre empereur romain Jule César utilisait un algorithme de chiffrement pour protéger les messages à ses troupes. La cryptologie est composée de deux éléments : la cryptographie et la cryptanalyse. Le cryptographe cherche des méthodes pour assurer la sûreté et la sécurité des conversations alors que le Crypto analyse tente de défaire le travail ancien en brisant ses systèmes.

I. Généralité sur la cryptographie :

I.1. Définitions :

La cryptographie est une science mathématique qui comporte deux branches : la cryptographie et la cryptanalyse.

Le mot cryptographie est un terme générique désignant l'ensemble des techniques permettant de chiffrer des messages, c'est-à-dire permettant de les rendre inintelligibles sans une action spécifique. Le verbe crypter est parfois utilisé mais on lui préférera le verbe chiffrer.

La cryptanalyse, à l'inverse, est l'étude des procédés cryptographiques dans le but de trouver des faiblesses, en particulier, de pouvoir décrypter des messages chiffrés. Le décryptement est l'action consistant à trouver le message en clair sans connaitre la clef de déchiffrement.

La cryptologie, étymologiquement « la science du secret », ne peut être vraiment considérée comme une science que depuis peu de temps. Cette science englobe la cryptographie (l'écriture secrète) et la cryptanalyse (l'analyse de cette dernière).

Un cryptosystème est l'ensemble des deux méthodes de chiffrement et de déchiffrement. En cryptographie, l'information à masquer est également appelée message ou texte clair

(«plaintext», en anglais). Le résultat du chiffrement d'un texte clair est appelé texte chiffré («ciphertext», en anglais). Le texte chiffré est le résultat d'une transformation dépendant du message et d'une clé.

- *La confidentialité* : consiste à rendre l'information intelligible à d'autres personnes que les acteurs de la transaction.
- *L'intégrité* : vérifier l'intégrité des données consiste à déterminer si les données n'ont pas été altérées durant la communication.
- *L'authentification* : consiste à assurer l'identité d'un utilisateur, c.-à-d de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être un contrôle d'accès peut permettre (par exemple par le moyen d'un mot de passe qui devra être crypté) l'accès à des ressources uniquement aux personnes autorisées.
- *La non répudiation de l'information* : est la garantie qu'aucun des correspondants ne pourra nier la transaction [8].

Figure I.1 : Processus de chiffrement et déchiffrement

I.2. Cryptanalyse

La cryptanalyse s'oppose en quelque sorte à la cryptographie, c'est l'étude des faiblesses des systèmes cryptographiques, elle est effectuée généralement par un intrus qui met en œuvre des méthodes afin de retrouver des informations secrètes tel que la clé, message en clair à partir d'informations considérées comme publique (cryptogramme, algorithmes), la cryptanalyse est une des disciplines de la cryptologie.

Dans la cryptanalyse on part du principe que l'homme est faible et facilement soudoya le, ainsi la force d'un système doit reposer sur la force du principe utilisé.

Si le but de la cryptographie est d'élaborer des méthodes de protection, le but de la cryptanalyse est au contraire de casser ces protections. Une tentative de cryptanalyse d'un système est appelé une attaque, et elle peut conduire à différents résultats :

- *Cassage complet*: le cryptanalyse retrouve la clef de déchiffrement.
- *Obtention globale*: le cryptanalyse trouve un algorithme équivalent à l'algorithme de déchiffrement, mais qui ne nécessite pas la connaissance de la clef de déchiffrement.
- *Obtention locale*: le cryptanalyse retrouve le message en clair correspondant à un message chiffré.
- *Obtention d'information*: le cryptanalyse obtient quelque indication sur le message en clair ou la clef (certains bits de la clef, un renseignement sur la forme du message en clair).

D'une manière générale, on suppose toujours que le cryptanalyste connait le détail des algorithmes, fonctions mathématiques ou protocoles employés. Même si ce n'est pas toujours le cas en pratique, il serait risqué de se baser sur le secret des mécanismes utilisés pour assurer la sécurité d'un système, d'autant plus que l'usage grandissant de l'informatique rend de plus en plus facile la reconstitution de l'algorithme à partir du programme.

En revanche, on distingue deux classes d'attaques : les attaques actives et les attaques passives.

Dans les attaques actives, l'adversaire agit sur l'information. Il altère l'intégrité des données, l'authentification et la confidentialité. Il peut chercher à altérer la transmission du message sur le canal, par exemple, en modifiant le message (suppression, ajout, modification des séquences du message), en retardant (ou empêchant) sa transmission, en répétant son envoi.

Dans les attaques passives, l'adversaire observe des informations qui transitent sur le canal sans les modifier. Il cherche à récupérer des informations sur le cryptosystème sans l'altérer, telles que le message, la clé secrète, etc. Dans ce cas, l'adversaire touche à la confidentialité des données.

L'objectif commun de toutes les attaques est de systématiquement retrouver le texte clair à partir de texte chiffré ou de déduire la clé secrète.

I.3. Différentes classes d'attaques :

L'intrus peut effectuer quatre niveaux d'attaques, l'attaque est une tentative de cryptanalyse.

- ***L'attaque par cryptogramme*** **(par message chiffré seulement)** : ou le cryptanalyste ne connait qu'un ensemble de messages chiffrés, il peut soit retrouver seulement les messages en clair, soit retrouver la clef. En pratique, il est très souvent possible de deviner certaines propriétés du message en clair (format ASCII, présence d'un mot particulier, …), ce qui permet de valider ou non le décryptement.
- ***L'attaque à message en clair connu***: ou le cryptanalyste connait non seulement les messages chiffrés mais aussi les messages en clair correspondants, son but est alors de retrouver la clef. Du fait de la présence, dans la plupart des messages chiffrés, de parties connues (en-têtes de paquets, champs communs à tous les fichiers d'un type donné,…).
- ***L'attaque à message en clair choisi***: ou le cryptanalyste peut, de plus choisir des messages en clair à chiffrer et donc utiliser des messages apportant plus d'informations sur la clef. Si le cryptanalyste peut de plus adapter ses choix en fonction des messages chiffrés précédents, on parle d'attaque adaptative.
- ***L'attaque à message chiffré choisi***: qui l'inverse de la précédente, le cryptanalyste peut choisir des messages chiffrés pour lesquels il connaitra le message en clair correspondant ; sa tâche est alors de retrouver la clef. Ce type d'attaques est principalement utilisé contre les systèmes à clef publique, pour retrouver la clef privée [9].

II. Chiffrement en cryptographie standard :

II.1. Chiffrement à clé publique :

II.1.1 Principe ;

Le chiffrement à clé publique, ou chiffrement asymétrique, a été proposé par Diffie et Hellman [4], en 1976. Dans un tel schéma, la clé de chiffrement est différente de celle de déchiffrement. N'importe qui peut utiliser la clé de chiffrement, ou clé publique, pour chiffrer un message, mais seul celui qui possède la clé de déchiffrement, ou clé privée, peut déchiffrer le message chiffré résultant

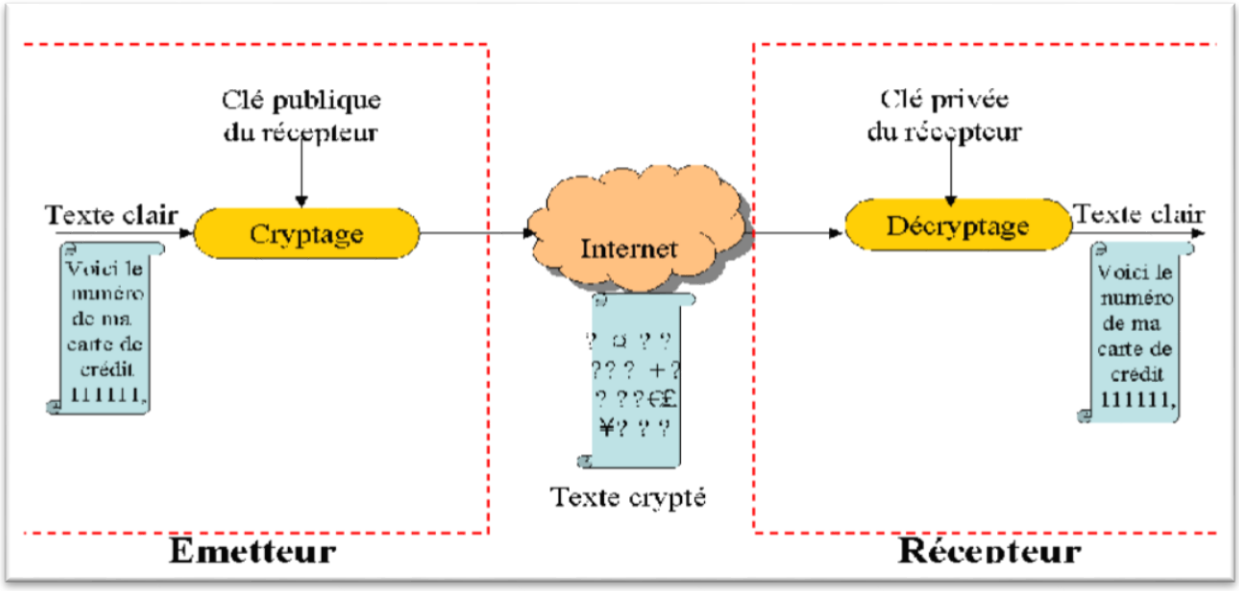


Figure I.2 : Cryptographie asymétrique

Les principaux algorithmes asymétriques à clé publiques sont :

- **RSA** (chiffrement et signature)
- **DSA** (signature)
- **Diffie-Hellman** (échange de clé).

II.1.2. RSA :

Le premier système à clé publique solide à avoir été inventé, et le plus utilisé actuellement, est le système RSA. Publié en 1977 par Ron Rivest, Adi Shamir et Leonard Adleman de

l'Institution de technologie du Massachusetts [5], le RSA est fondé sur la difficulté de factoriser des grands nombres, et la fonction à sens unique utilisée est une fonction "puissance".

II.1.3. Avantages et inconvénients du chiffrement à clé publique :

L'atout principal de la cryptographie à clé publique réside dans la facilité de gestion du parc des clés des utilisateurs. En effet, l'augmentation du nombre d'utilisateurs ne rend pas complexe le protocole. De plus, l'arrivée de nouveaux utilisateurs et leur intégration demande très peu d'efforts et ne modifie en rien les paramètres des autres. Pour le groupe d'utilisateurs il suffit, de manière simplifiée, de :

- choisir un administrateur digne de confiance qui sera chargé de gérer les clés.
- chaque utilisateur demande à l'administrateur son inscription
- pour chaque utilisateur, l'administrateur crée une paire de clés (clé privée / clé publique)
- l'administrateur informe secrètement chaque utilisateur de sa clé privée
- il publie toutes les clés publiques dans un annuaire

Si un nouvel utilisateur arrive, il suffit de lui créer une paire de clés et de la distribuer.

Tableau I.1 : Problèmes complexes et principaux cryptosystèmes asymétriques [3 - 4]

Cryptosystème asymétrique	Problème complexe
RSA	Factorisation des grands entiers
El Gamal	Logarithme discret Problème de Diffie-Hellmann
Rabin	Factorisation des grands entiers
Blum-Goldwasser	Factorisation des grands nombres

II.1.2. Chiffrement à clé privée :

II.1.2.1. Principe :

La cryptographie à algorithmes symétriques utilise la même clé pour les processus de codage et de décodage ; cette clé est le plus souvent appelée « secrète ». Le chiffrement consiste à appliquer une opération (algorithme) sur les données à chiffrer à l'aide de la clé privée, afin de les rendre inintelligibles. Ainsi, le moindre algorithme peut rendre le système quasiment inviolable (la sécurité absolue n'existant pas).

Toutefois dans les années 40 Claude Shannon démontra qu'être totalement sûre, les systèmes à clefs privées doivent utiliser des clefs d'une longueur au moins égale à celle du message à chiffrer.

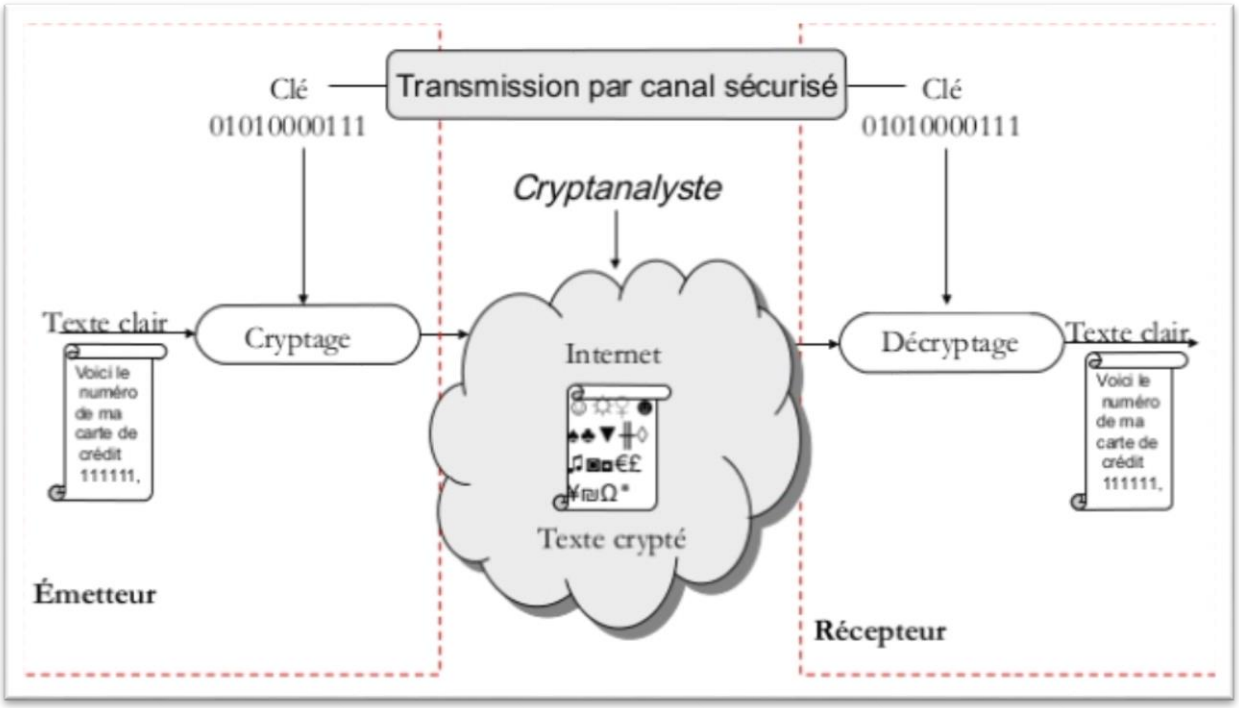


Figure I.3 : Cryptographie symétrique

Quelques algorithmes de chiffrement symétriques très utilisés :

- **Chiffre de Vernam** (le seul offrant une sécurité théorique absolue, à condition que la clé ait au moins la même longueur que le message, qu'elle ne soit utilisée qu'une seule fois à chiffrer et qu'elle soit totalement aléatoire)
- **DES**
- **3DES**
- **AES**
- **RC5**

Les schémas de chiffrement symétrique peuvent être classés en deux catégories, le chiffrement par flot et le chiffrement par blocs.

II.1.2.1.1. Algorithmes de chiffrement par flot

Le chiffrement de flux ou chiffrement par flot (en anglais *stream cipher*) et appelé aussi chiffrement en continu est une des deux grandes catégories de chiffrements modernes en cryptographie symétrique. Il arrive à traiter les données de longueur quelconque et n'a pas besoin de les découper.

Un chiffrement par flot se présente souvent sous la forme d'un générateur de nombres pseudo-aléatoires avec lequel on opère un XOR entre un bit à la sortie du générateur et un bit provenant des données. Toutefois, le XOR n'est pas la seule opération possible. L'opération d'addition dans un groupe est également envisageable (par exemple, addition entre deux octets, modulo 256).

Leur principe est d'effectuer un chiffrement de Vernam en utilisant une clé pseudo-aléatoire, c'est à dire une clé qui ne soit pas choisie aléatoirement parmi tous les mots binaires de longueur *n*. Cette clé (qu'on appellera par la suite pseudo-aléatoire) est générée par différents procédés à partir d'une clé secrète d'une longueur juste suffisante pour résister aux attaques exhaustives.

Exemple : Message en clair: "**SALUT**"

Conversion en binaire :

01010011 01000001 01001100 01010101 01010100

XOR

Clé (générée aléatoirement)

01110111	01110111	00100100	00011111	00011010
		=		
00100100	00110110	01101000	01001010	01001110

Conversion en caractère :

"Message chiffré: **$6jJM**"

Il a été démontré par le mathématicien Claude Elwood Shannon qu'il était impossible de retrouver un message crypté par le principe de Vernam sans connaître la clé. Ce qui ferait en théorie du chiffre de Vernam un cryptosystème incassable ou inconditionnellement sûr.

II.1.2.1.2 Algorithmes de chiffrement par bloc :

Le chiffrement par bloc [12] (en anglais *block cipher*) est une des deux grandes catégories de chiffrements modernes en cryptographie symétrique, La principale différence vient du découpage des données en blocs de taille généralement fixe. La taille de bloc est comprise entre 32 et 512 bits, dans le milieu des années 1990 le standard était de 64 bits mais depuis 2000 et le concours AES le standard est de 128 bits. Les blocs sont ensuite chiffrés les uns après les autres. Il est possible de transformer un chiffrement de bloc en un chiffrement par flot en utilisant un mode d'opération comme ECB (chaque bloc chiffré indépendamment des autres) ou CFB (on chaîne le chiffrement en effectuant un XOR entre les résultats successifs).

Un chiffrement par bloc peut également être utilisé comme une fonction de hachage, c'est-à-dire une fonction à sens unique. Une variante de DES est employée pour le système de mots de passe dans Unix. Une chaîne contenant uniquement des zéros est chiffrée avec une clé correspondant au mot de passe (une composante aléatoire appelée "sel" est encore intégrée à l'algorithme). Ce chiffrement est itératif et se fait 25 fois avant d'obtenir le résultat final.

II.1.2.1.3. Avantages et inconvénients du chiffrement par bloc et par flot :

Avec un algorithme de chiffrement par bloc, on ne peut commencer à chiffrer et à déchiffrer un message que si l'on connaît la totalité d'un bloc. Ceci occasionne naturellement un délai dans la transmission et nécessite également le stockage successif des blocs dans une mémoire tampon. Au contraire, dans les procédés de chiffrement par flot, chaque bit transmis peut être chiffré ou déchiffré indépendamment des autres, en particulier sans qu'il soit nécessaire d'attendre les bits suivants. D'autre part, les chiffrements par flot ne requièrent évidemment pas de padding, c'est-à-dire l'ajout de certains bits au message clair dont le seul objectif est d'atteindre une longueur multiple de la taille du bloc. Ceci peut s'avérer particulièrement souhaitable dans les applications où la bande passante est très limitée ou quand le protocole employé impose la transmission de paquets relativement courts.

Un autre avantage du chiffrement par flot est que contrairement aux chiffrements par bloc, le processus de déchiffrement ne propage pas les erreurs de transmission. Supposons qu'une erreur survenue au cours de la communication ait affecté un bit du message chiffré. Dans le cas d'un chiffrement à flot, cette erreur affecte uniquement le bit correspondant du texte clair, et ne le rend donc généralement pas complètement incompréhensible. Par contre, dans le cas d'un chiffrement par bloc, c'est tout le bloc contenant la position erronée qui devient incorrect après déchiffrement. Ainsi, une erreur sur un seul bit lors de la transmission affecte en réalité 128 bits du message clair. C'est pour cette raison que le chiffrement par flot est également utilisé pour protéger la confidentialité dans les transmissions bruitées.

III. Avantages et inconvénients de la cryptographie standard :

Le tableau ci-dessous résume les avantages et inconvénients rencontrés dans les cryptosystèmes classiques :

Tableau I.2 : Avantages et inconvénients des cryptosystèmes classiques

	Systèmes symétriques	Systèmes asymétriques
Avantages	Algorithmes rapides	Usage à long terme des paires de Clés
	Volumes importants de données à chiffrer	Authentification de la clé publique
	Débit élevé	Signature électronique des messages
Inconvénients	Usage à court terme des clés (One-Time-Pad)	Lenteur des algorithmes de déchiffrement
	Pas de signature électronique	Taille de clé généralement grande

Le problème de découverte de clés reste non résolu par les techniques standards de cryptographie. Pour remédier à cette situation, la cryptographie quantique et la cryptographie chaotique apparaissent comme de bonnes alternatives du fait que les clés proposées par ces dernières n'ont jamais été cassées.

IV. Chiffrement en cryptographie quantique :

La cryptographie quantique, plus correctement nommée distribution quantique de clés (QKD: Quantum Key Distribution), désigne un ensemble de protocoles permettant de distribuer une clé de chiffrement secrète entre deux interlocuteurs distants, tout en assurant la sécurité de la transmission grâce aux lois de la physique quantique et de la théorie de l'information.

Cette clé secrète peut ensuite être utilisée dans un algorithme de chiffrement symétrique, afin de chiffrer et déchiffrer des données confidentielles.

La cryptographie quantique ne constitue donc pas en elle seule un système cryptographique mais en est un élément. Pour avoir un système cryptographique complet, il faudrait associer la QKD à un algorithme de chiffrement conventionnel tel qu'un masque jetable ou code de Vernam.

IV.1 Principe de la cryptographie quantique :

La cryptographie quantique est rendue possible grâce à la lumière. En effet, ce sont les photons qui assurent le transport de l'information à travers une fibre optique, d'un émetteur (Alice) vers un récepteur (Bob).

Chaque photon peut-être polarisé, c'est-à-dire que son champ électrique possède une direction. La polarisation est mesurée par un angle pouvant varier de *0°* à *180°*. Suivant le protocole, ces angles peuvent prendre les valeurs *0°*, *45°*,*90°* et *135°*. On parle de polarisation rectiligne pour les photons polarisés entre *0°* et *90°* et de polarisation diagonale pour les photons polarisés entre *90°* et *135°*.

Afin de pouvoir détecter les différents états de polarisation d'un photon, on utilise des filtres.

En physique quantique, le théorème dit de «non clonage» assure la confidentialité du message transmis, puisqu'il interdit la copie parfaite de l'information quantique par une tierce personne (Eve). Il lui est impossible de reproduire l'état quantique de la lumière car le simple fait de vouloir observer un photon le dénature complètement à moins de connaître à l'avance l'état quantique du photon. Ainsi, toute tentative d'Eve pour essayer d'espionner la conversation entre Alice et Bob entraînera une modification de l'état quantique des photons (principe d'indétermination d'Heisenberg ou principe de réduction du paquet d'ondes), elle ne pourra, au mieux, qu'essayer de deviner l'état quantique des photons, ce qui introduira inévitablement des modifications qui seront perçues par Alice et Bob [14].

V. Chiffrement basé sur le chaos :

V.1 Principe :

Le chiffrement d'un message par le chaos s'effectue en superposant à l'information initiale un signal chaotique. Nous envoyons par la suite le message noyé dans le chaos à un récepteur

qui 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.

Un système de cryptage par chaos est constitué de deux parties : le brouilleur et le décrypteur. Ceux-ci sont strictement identiques pour assurer de façon optimale le respect des conditions initiales. La synchronisation des dispositifs est établie dans le système récepteur qui amorce le chaos en injectant dans sa boucle à retard l'ensemble de l'information à transmettre superposée à la dynamique chaotique. Cet ensemble constitue un système de cryptage symétrique à clé secrète. L'émetteur et le récepteur possèdent la même clé. La synchronisation va représenter la phase critique de l'opération de décryptage. Du fait de la nature complexe du comportement du signal brouilleur, le moindre écart lors du décodage va entraîner un parasite sur l'information appelé "bruit de déchiffrement".Une mauvaise synchronisation rendra illisible l'information.

La figure I.4 présente les différents éléments d'un système de cryptage symétrique basé sur le chaos.

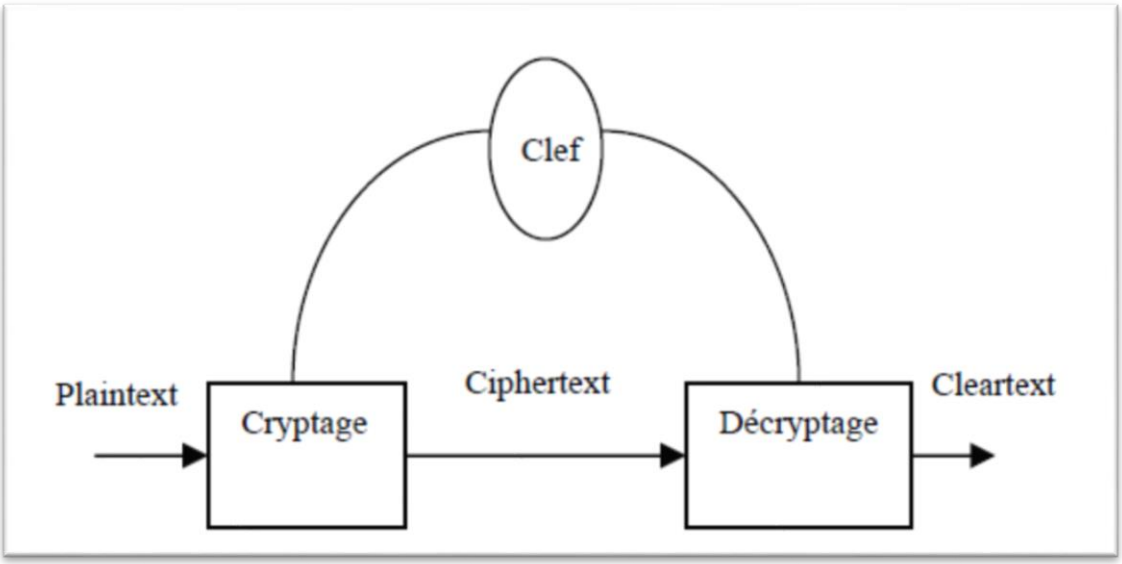


Figure I.4 : Système de cryptage symétrique

L'idée fondamentale exige que l'émetteur produit un signal chaotique pour masquer le message à transmettre, appelé également le "plaintext". À l'extrémité du récepteur, un second système chaotique est induit pour synchroniser avec le signal entrant masqué, également appelé le "ciphertext". Une simple opération de soustraction indiquerait alors le message

(cleartext).

VI. 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. Les tableaux suivants illustrent parfaitement cette correspondance.

Tableau I.3 : Correspondance entre la théorie du chaos et la cryptographie

Théorie du chaos	Cryptographie
Système chaotique	Système pseudo-aléatoire
Transformation non linéaire	Transformation non linéaire
Nombre infini d'états	Nombre fini d'états
Nombre infini d'itérations	Nombre fini d'itérations
État initial	Plaintext
État final	Ciphertext
Condition initiale (s) et/ou paramètre (s)	Clé (s)
Indépendance asymptotique des états initiaux et finaux	Confusion
Sensibilité aux conditions initiales (s) et paramètre (s)	Diffusion

Tableau I.4 : Comparaison entre le chaos et la cryptographie

Propriété du chaos	Propriété de la cryptographie	Description
Ergodicité	Confusion	Le rendement a la même distribution pour n'importe quelle entrée (chaque trajectoire tend à une distribution invariable qui est indépendante de conditions initiales).
Sensibilité aux conditions initiales et aux paramètres du système. Propriété de mélange.	Diffusion avec un petit changement du Plaintext/de la clé secrète	Une petite déviation en entrée peut causer un grand changement au rendement.
Dynamique déterministe	Aspect déterministe pseudo-aléatoire	Un processus déterministe peut causer un comportement pseudo-aléatoire
Complexité de structure	Complexité d'algorithme	Un processus simple a une complexité très élevée.

Donc l'intérêt accordé aux systèmes et aux signaux chaotiques n'est pas fortuit.

Conclusion :

Un concepteur de système cryptographique est toujours en train d'essayer d'élaborer un système de chiffrement plus sure mais en même temps des intrus essayent de casser ce dernier, ils se livrent constamment une bataille mais les enjeux sont énorme : c'est la sécurité de nos transmissions qui est menacée.

La discrétisation des signaux chaotiques, nous offre de nouvelles opportunités pour exploiter les comportements chaotiques dans la cryptographie, avec une synchronisation optimale, assurant le compromis entre la robustesse aux bruits et la protection des informations confidentielles. Ainsi, la compatibilité de cette synchronisation avec l'infrastructure des télécommunications existante, encourage l'intégration des systèmes chaotiques dans les transmissions chiffrées en temps réel, par la création de nouveaux algorithmes de chiffrement par flux.

Chapitre II :

Transmissions sécurisées par chaos

Introduction

Un système de communications utilisant le chaos représente une application prometteuse de l'estimation d'état des systèmes non linéaires.

A partir d'un message contenant l'information, l'émetteur génère un signal qui est transmis au récepteur par l'intermédiaire d'un canal. Le récepteur reconstruit alors le message original, grâce à une "clé" partagée avec l'émetteur.

Nous nous intéressons uniquement aux systèmes de communications à porteuse chaotique.

I. Système chaotique dans les transmissions sécurisées :

L'intérêt d'utiliser les systèmes chaotiques dans les transmissions chiffrées est pour envisager de nouvelles approches dédiées aux transmissions temps réel. Le procédé général de telles approches repose sur trois points principaux :

I.1. La dynamique chaotique :

Doit avoir un comportement particulièrement complexe, généré à l'aide de simples fonctions mathématiques continues et/ou discrètes, sensibles à leurs paramètres critiques. Cette sensibilité encourage l'emploi des paramètres et des états initiaux des systèmes chaotiques comme clé secrète du chiffrement/ déchiffrement.

I.2 La procédure de chiffrement/ déchiffrement :

Désigne la manière employée pour mélanger l'information avec le signal chaotique. Elle s'effectue selon différentes méthodes en mode analogique ou numérique : masquage additif, commutation chaotique ou modulation paramétrique.

Plusieurs algorithmes de chiffrement bases sur ces méthodes ont été proposés dans la littérature, comme il y en a d'autres qui ont été inspires des algorithmes de chiffrements conventionnels, fonctionnant par bloc ou par flux, et adaptes aux différentes données multimédias. Cependant l'originalité du chiffrement par chaos réside principalement dans les systèmes purement analogiques, permettant un chiffrement au niveau composant, qualifie de chiffrement physique.

En ce qui concerne le déchiffrement, le récepteur doit disposer des systèmes chaotiques (la configuration paramétrique adéquate), qui permettent la reproduction du même comportement chaotique utilise pour le chiffrement, afin de pouvoir extraire l'information confidentielle. Cela est possible grâce au caractère déterministe des systèmes chaotiques. Cependant, dans le cas d'une transmission bruitée le contrôle des systèmes chaotiques devient un vrai challenge, a cause de leur forte sensibilité aux variations, et l'application d'un mécanisme de synchronisation est nécessaire pour réussir une bonne réception.

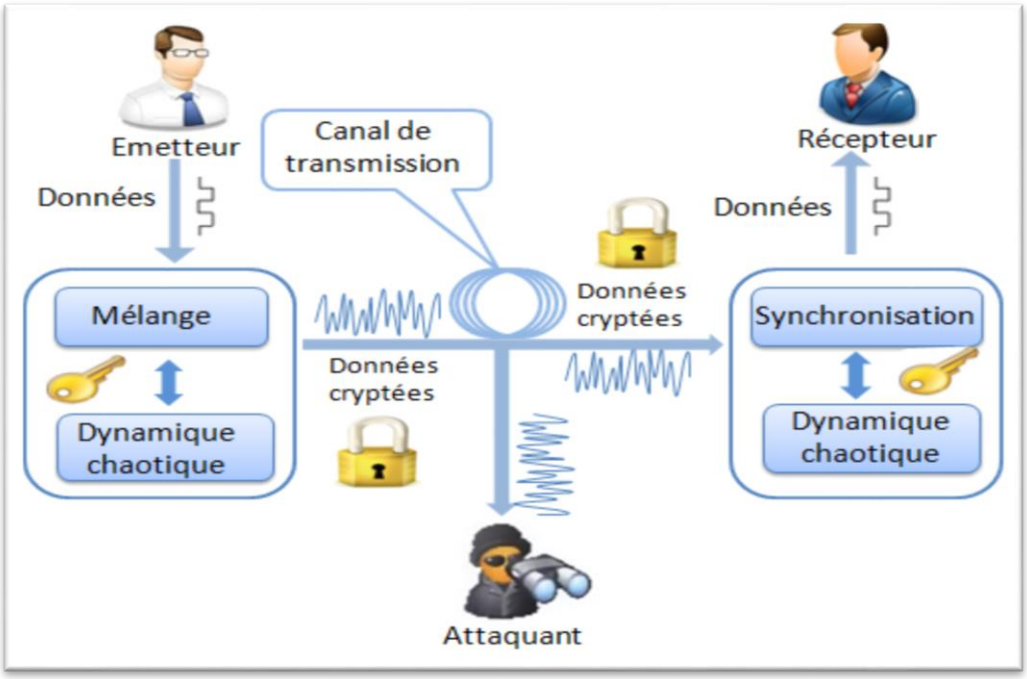


Figure I.1: Principe de chiffrement par chaos.

II. Systèmes dynamiques chaotiques :

Les systèmes dynamiques chaotiques sont les systèmes dynamiques satisfaisant aux conditions suivantes:

- *La non-linéarité* : un système chaotique est un système dynamique non linéaire. Un système linéaire, ne peut pas être chaotique.
- *Le déterminisme* : un système chaotique a des règles fondamentales déterministes et non probabilistes. L'évolution irrégulière du comportement d'un système chaotique est due aux non linéarités.
- *La sensibilité aux conditions initiales* : de très petits changements sur l'état initial peuvent mener à des comportements radicalement différents dans son état final.
- *L'imprévisibilité* : en raison de la sensibilité aux conditions initiales.

III. Quelques outils pour caractériser le chaos :

III.1. Espace des phases:

Il est possible de suivre l'évolution de l'état d'un système physique dans le temps. Pour cela, on construit d'abord un modèle avec les lois physiques et les paramètres nécessaires et suffisants pour caractériser le système. Ce modèle est bien souvent constitué par des équations différentielles. On définira, à un instant donné, un point dans un « repère ». Ce point caractérisera l'état du système dans l'espace à cet instant. Cet espace est appelé « l'espace des phases ».

L'espace des phases est une notion purement mathématique qui comporte autant de dimensions qu'il y a de paramètres dans le système dynamique étudié. Ainsi on pourrait très bien imaginer se retrouver à manipuler un espace de phases à 216 dimensions, si le système dynamique analysé implique 216 paramètres (toute difficulté géométrique mise à part...).

En considérant un espace des phases à 3 dimensions, on ne peut tracer qu'un graphique.

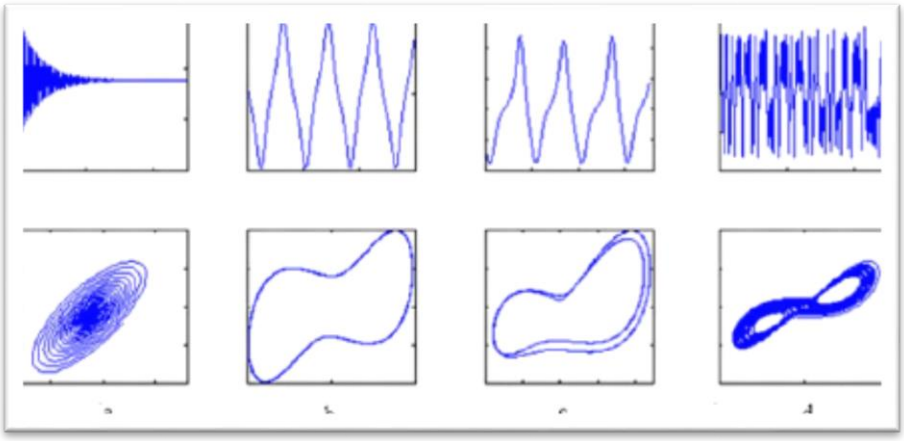


Figure II.2 : Séries temporelles et espaces de phase de quelques oscillateurs

Le système (A) converge vers un état d'équilibre après maintes oscillations, ce qui correspond dans l'espace des phases à des boucles qui convergent vers un point.

Le système (B) se répète périodiquement, ce qui correspond dans l'espace des phases à une orbite cyclique.

Le système (C) a également un mouvement périodique mais plus complexe ; il se répète seulement après deux oscillations différentes : on dit qu'il possède un cycle de période 2. Cela correspond à des boucles plus compliquées dans l'espace des phases.

Le système (D) est chaotique, et dans l'espace des phases, il possède la forme en aile de papillon de l'attracteur étrange de Lorenz.

III.2. Attracteurs :

Un attracteur est un objet géométrique vers lequel tendent toutes les trajectoires des points de l'espace des phases, c'est à dire une situation ou un ensemble de situations vers lesquelles évoluent un système, quelles que soient ses conditions initiales. Le bassin d'attraction d'un attracteur est l'ensemble des points de l'espace des phases qui donnent une trajectoire évoluant vers l'attracteur considéré. On peut donc avoir plusieurs attracteurs dans un même espace des phases. Il existe deux types d'attracteurs : les attracteurs réguliers et les attracteurs étranges ou chaotiques. Les attracteurs étranges semblent inclure à la fois des lois déterministes et des lois aléatoires, ce qui rend impossible toute prévision à long terme.

III.2.1. Attracteurs étranges :

Ils sont les caractéristiques de l'évolution des systèmes chaotiques c'est-à-dire qu'au bout d'un certain temps, tous les points de l'espace des phases (et appartenant au bassin d'attraction de l'attracteur) donnent des trajectoires qui tendent à former l'attracteur étrange [20].

À grande échelle, un attracteur étrange n'est pas une surface lisse, mais une surface repliée plusieurs fois sur elle-même. En effet, les trajectoires des points divergent (puisque, par définition deux points ne peuvent avoir la même évolution), mais comme l'attracteur a des dimensions finies, l'attracteur doit se replier sur lui-même. Le processus d'étirement-repliement se répète à l'infini et fait apparaître un nombre infini de « plis » imbriqués les uns dans les autres qui ne se recoupent jamais. Ainsi, deux points très proches au départ (conditions initiales) peuvent se retrouver à deux extrémités opposées de l'attracteur (conditions finales). Cela traduit le comportement divergent des phénomènes chaotiques.

On obtient ainsi des attracteurs différents, qui présentent des formes diverses et surprenantes.

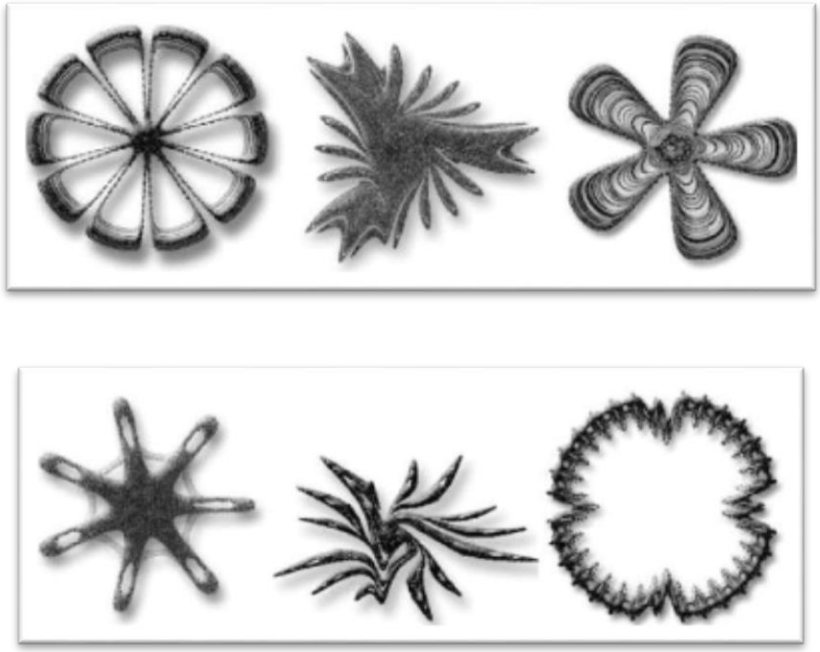


Figure II.3 : Attracteurs étranges

IV. Générateurs chaotiques :

Les générateurs chaotiques peuvent être utilisés, entre autres, dans les applications touchant à la sécurité de l'information, pour la génération de clés secrètes dynamiques dans les algorithmes de chiffrement. Rappelons, que le chaos peut être généré par tout système dynamique non linéaire. En effet, des simples équations de récurrence sont capables de générer des dynamiques chaotiques riches, si les paramètres de contrôle sont bien positionnés. Dans beaucoup d'équations de récurrences simples, le bon choix de ces paramètres se fait grâce au diagramme de bifurcation.

IV.1. Récurrences chaotiques :

Les récurrences chaotiques sont des systèmes dynamiques définis en réel par la relation [10]:

$$x_i(n) = f(x_1(n-1), x_2(n-1), \dots, x_m(n-1)), \qquad \text{i} = 1,2,..\text{m} \qquad \text{(II.1)}$$

où $x \in S, f: S^m \to S^m$ est une fonction de m-dimensions, $S^m \subset [0,1]^m \; ou \; [-1,1]^m$.

Les générateurs chaotiques (ainsi que les différents crypto-systèmes) proposés, sont totalement numériques et sont constitués à partir des récurrences chaotiques de bases suivantes : Logistique, Skew tent,mais sous forme discrétisée, utilisant une précision finie N=32 bits.

IV.1.1. Etude des performances des récurrences chaotiques de base :

Seulement, dans le cas de la récurrence Logistique, le diagramme de bifurcation sont donnés en réel. En effet, dans le cas discret, le paramètre de contrôle est fixé à sa valeur optimale.

L'équation sous sa forme générale en réels des cartes chaotiques monodimensionnelles s'écrit:

$$x(n) = f(x(n-1), p), \;\; n = 1,2,\dots, \qquad x(0) \in S, \qquad p \in S_p \qquad \text{(II.2)}$$

$$f: S \to S, \;\; S \subset \mathbb{R} \qquad \text{avec } S = [0,1] \; ou \; S = [-1,1]$$

, et S_p est l'intervalle de variation du paramètre de contrôle.

Partant d′une valeur initiale $x(0) \in S$, nous obtenons, en réitérant la carte n fois, la séquence suivante :

$$x(1) = f(x(0), p), \quad x(2) = f(f(x(0), p), p), \dots , \qquad x(n) = f(\dots f(f(x(0), p), p) \dots , p)$$

Pour n′importe quelle valeur initiale $x(0) \in S$, la séquence de valeurs x(0),x(1),…,x(n) est appelée l′orbite (ou la trajectoire) de la récurrence, produite à partir de l'état initial x(0), et pour la valeur p donnée du paramètre du contrôle.

IV.1.1.1. Récurrence Logistique :

A l'origine, la récurrence logistique est un modèle de croissance démographique publié par

Pierre Verhulst en 1845. A cause de la simplicité de son équation de récurrence, en 1947 Ulam et Von Neumann l'ont utilisé en tant que générateur de nombre pseudo-aléatoire. Depuis, c'est l'une des récurrences les plus utilisées dans les applications cryptographiques, l'histogramme des séquences générées n'est pas uniforme. Son équation de récurrence est donnée par :

$$x(n) = f(x(n-1), p) = p \times x(n-1) \times (1 - x(n-1)) \qquad \textit{(II.3)}$$

$avec \;\; f : S \to S, S = [0,1] \quad x(n) \in S, et\; p \in [1,4]$.

Dans la figure II.4, Nous présentons le diagramme de bifurcation de la récurrence en réel.

Comme attendu, la région du chaos est obtenue pour ≥ 3.57 . Cependant, la valeur p= 4, est optimale, car dans ce cas, l'amplitude x(n), n= 1,2, … couvre toute la dynamique $\in [0,1]$ de la récurrence. Pour cette raison, dans la version discrète de la récurrence, nous fixons la valeur du paramètre de contrôle à la valeur correspondant à p= 4.

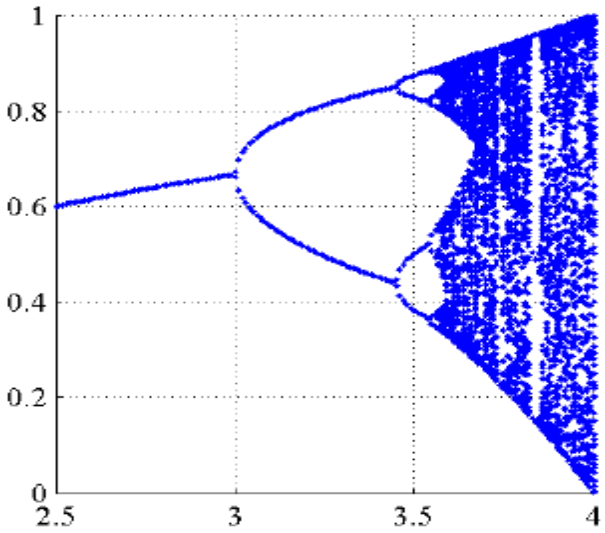


Figure II.4 : Evolution du diagramme de bifurcation de la récurrence logistique en fonction de p.

IV.1.1.2. Récurrence Logistique discrétisée :

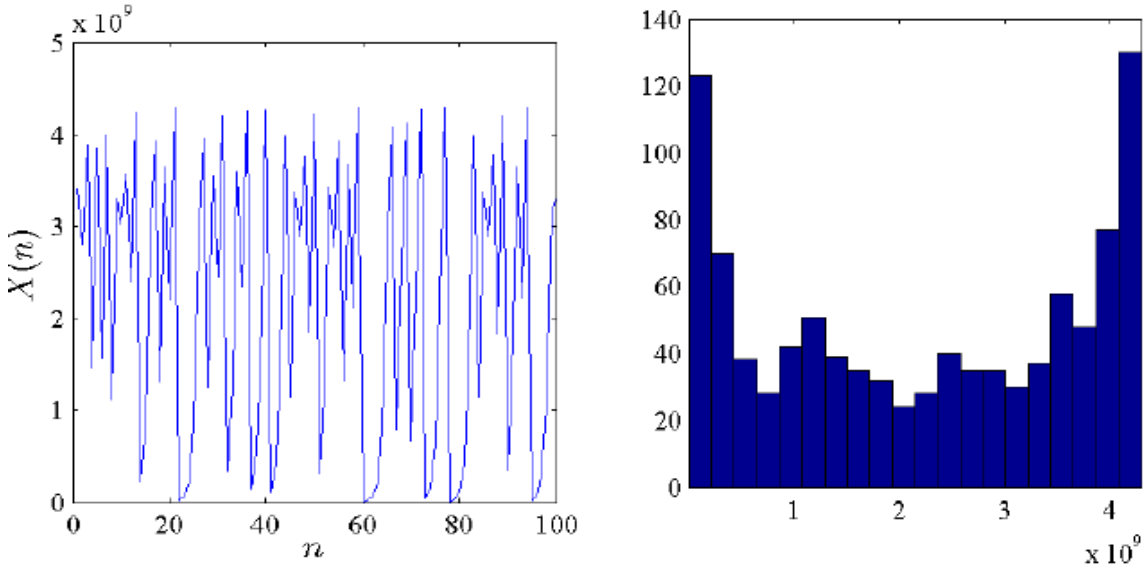
L'équation de la récurrence Logistique discrétisée, pour le paramètre de contrôle p fixé à 4, est donnée par la relation suivante:

$$X(n) = F\big(X(n-1)\big) = \begin{cases} \left\lfloor \dfrac{X(n-1)\times\left(2^N - X(n-1)\right)}{2^{N-2}} \right\rfloor & \text{si } X(n-1)\neq\{0,3\times2^{N-2},2^N\} \\ 2^N - 1 & ailleurs \end{cases} \qquad \text{(II.4)}$$

$\lfloor Z \rfloor$ (fonction Floor), dénote le plus grand entier inférieur à la valeur Z.

X(n) prend une valeur entière$\in [0,2^N - 1]$, et N=32 bits est la précision utilisée.

Notons que le processus de discrétisation dégrade les propriétés chaotiques de la récurrence chaotique originale (en représentation réelle).



(a) **(b)**

Figure II.5 : Exemple de résultats de la récurrence logistique discrète :

a) variation discrète de *X(n)* en fonction de *n*, b) histogramme.

IV.1.1.3. Récurrence Skew Tent :

La récurrence Skew tent est une récurrence linéaire par morceaux, décrite en réel par l'équation suivante :

$$x(n) = f(x(n-1), p) = \begin{cases} \frac{x(n-1)}{p} & si\ 0 \leq x(n-1) \leq p \\ \frac{1-x(n-1)}{1-p} & si\ p < x(n-1) \leq 1 \end{cases} \qquad \text{(II.5)}$$

avec $f: S \to S,\ S = [0,1]\,, x(n) \in S$ et p est le paramètre de contrôle qui varie dans l'intervalle suivant : $0 < p < 1$

L'histogramme de cette récurrence est pratiquement uniforme comparé à celle de la récurrence Logistique .

IV.1.1.4. Récurrence Skew Tent discrétisée:

La récurrence Skew tent discrétisée est définie par la relation suivante :

$$X(n) = F(X(n-1), P) = \begin{cases} \left\lfloor \frac{2^N \times X(n-1)}{P} \right\rfloor & si\ 0 \leq X_n \leq P \\ \left\lfloor 2^N \times \frac{2^N \times X(n-1)}{2^N - P} \right\rfloor + 1 & si\ P < X_n \leq 2^N \end{cases} \qquad (II.6)$$

Où $\lfloor Z \rfloor$(fonction ceil) dénote l'entier supérieur à Z, X(n) prend une valeur entière appartenant à $[0,2^N - 1]$, et P le paramètre de contrôle discret est tel que : 0 < P < $2^N - 1$.

Dans la figure II.6, nous présentons le diagramme de bifurcation de la récurrence Skew tent discrète, pour X(0)=3890346746

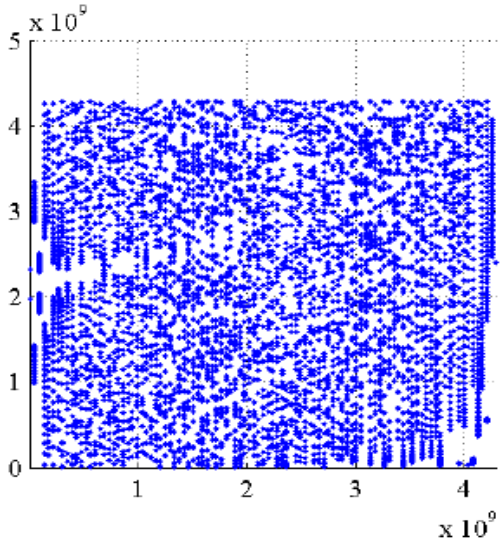


Figure II.6: Evolution du diagramme de bifurcation de la carte Skew tent discrète en fonction de P.

Le diagramme de bifurcation, nous montre que le meilleur intervalle pour le paramètre de contrôle est : $0.6 \times 10^9 \leq P \leq 3.7 \times 10^9$. Donc, il est préférable d'utiliser les valeurs de cet intervalle pour former la valeur de la clé secrète.

V. Cryptographie chaotique

Le chiffrement d'un message par le chaos s'effectue 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, autrement dit son principe de fonctionnement est le même que celui du chiffrement continue (stream cipher).

V.1. Différents modes de cryptages [11] :

V.1.1. Chiffrement par addition :

Dans cette méthode appelée, masquage chaotique, l'émetteur est un système chaotique autonome dont le signal de sortie y(t) est ajouté au signal du message m(t). La somme de deux signaux est transmise au récepteur à travers le canal de transmission, qui est un canal public. Le récepteur est constitué d'un système chaotique identique à l'émetteur et un simple soustracteur. Ainsi, après la synchronisation des deux systèmes chaotique (émetteur et récepteur), le message est extrait a l'aide d'une opération de soustraction.

La figure suivante illustre ce mode de cryptage :

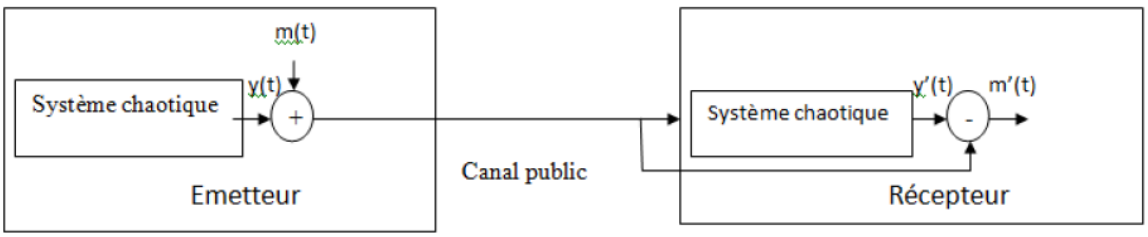


Figure II.7 : Principe du chiffrement chaotique par addition

V.1.2. Chiffrement par commutation :

Cette méthode (en anglais Chaos Shift Keying, CSK) est utilisée pour transmettre un message binaire (voir figure II.6). L'émetteur est composé de deux systèmes chaotiques et pour chaque niveau de message m(t) (0 ou 1), l'un des systèmes envoi sa sortie sur la ligne de transmission. Ainsi, le signal transmis commute entre deux attracteurs étrange.

Le récepteur est constitué de deux systèmes chaotiques identiques à ceux de l'émetteur et un bloc de comparaison permet de relever la valeur du message noté m'(t).

La figure ci-dessous illustre cette méthode de cryptage.

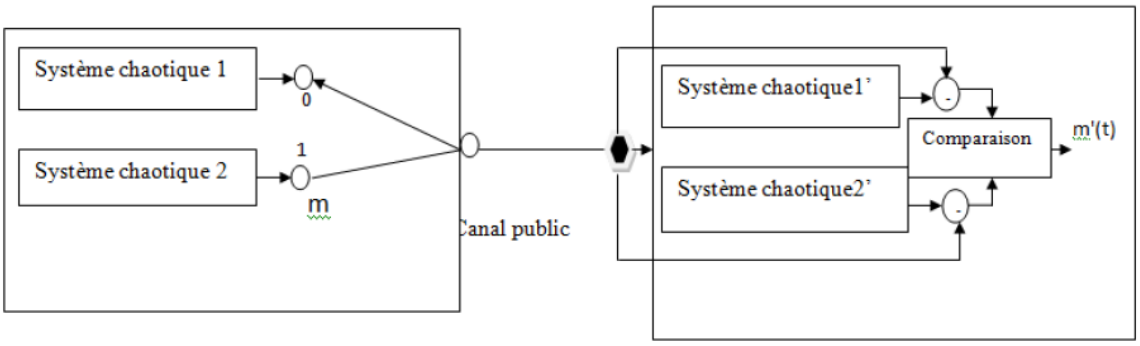


Figure II.8 : Principe du chiffrement chaotique par commutation

V.1.3. Chiffrement par modulation :

Cette technique utilise le message contenant l'information pour moduler un paramètre de l'émetteur chaotique. Un contrôleur adaptatif est chargé de maintenir la synchronisation au niveau du récepteur, tout en suivant les changements du paramètre modulé. Le schéma correspondant est présenté à la figure.

Au niveau de l'émetteur, le fait de moduler un (ou plusieurs) paramètre(s) impose à la trajectoire de changer continûment d'attracteur, et de ce fait, le signal transmis est plus Complexe qu'un signal chaotique normal. Cependant, la façon d'injecter le message et donc la

fonction de modulation des paramètres ne doivent pas supprimer le caractère chaotique du signal envoyé au récepteur. Il est important de souligner que cette technique exploite pleinement les qualités des systèmes chaotiques.

Elle n'a pas d'équivalent parmi les systèmes de communication classique. Cependant, le cryptage par modulation s'est avéré sensibles à certaines attaques.

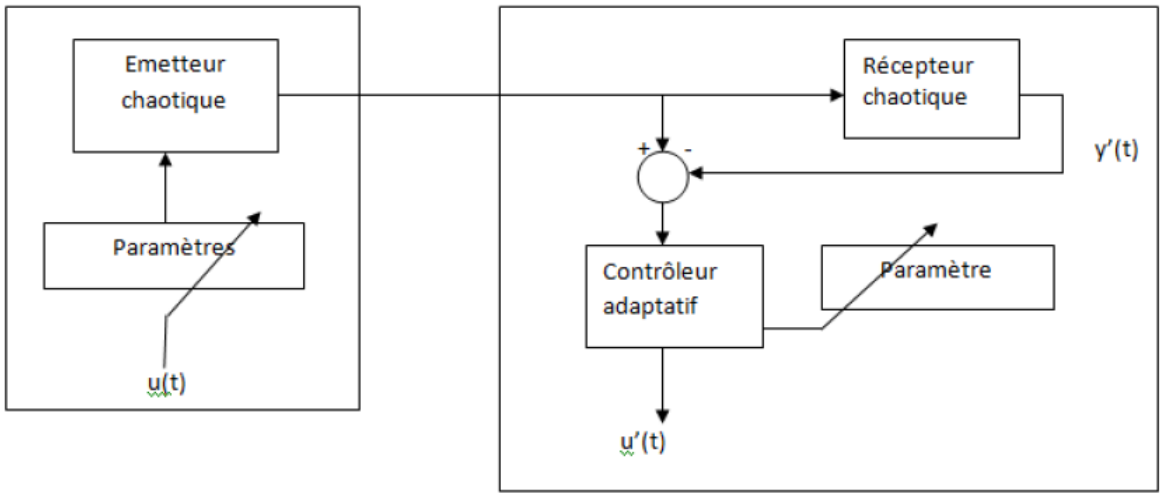


Figure II.9 : Principe du chiffrement chaotique par modulation

V.1.4. Cryptage par inclusion :

Cette technique de cryptage consiste à injecter le message dans la dynamique de l'émetteur.

La restauration de l'information se fait principalement par deux techniques, reposant soit sur les observateurs à entrées inconnues, soit sur l'inversion du système émetteur .Cette méthode présente beaucoup d'avantages et reste très utilisée en pratique.

Conclusion :

L'utilisation du chaos dans les télécommunications est étudiée depuis plusieurs années. Le chaos est obtenu à partir de systèmes non linéaires; il correspond à un comportement borné de ces systèmes, ce qui le fait apparaître comme du bruit pseudo aléatoire. Il peut donc être utilisé pour masquer ou mélanger les informations dans une transmission sécurisée.

L'originalité de cette communication repose sur la prise en compte des propriétés de signaux chaotiques issue soit d'équations différentielles soit de récurrences discrètes non linéaire.

Chapitre III

Simulation et résultats

Introduction :

Ce chapitre est dédié à l'analyse d'un système de transmission basé sur le chaos. Notre chaine a été modélisée sous Simulink de Matlab. L'interface graphique qui résume le fonctionnement de cette chaine sera abordée en fin de chapitre.

I. Implémentation sous Simulink :

Notre système de transmission utilise un générateur de chaos numérique dont les séquences de sortie sont combinées à l'information par un algorithme avant d'être transmise. A la réception le même générateur sert à déchiffrer le signal obtenu pour extraire l'information.

I.1. Chaine de transmission :

La configuration de cette chaine de transmission a été réalisée sous Simulink de Matlab :

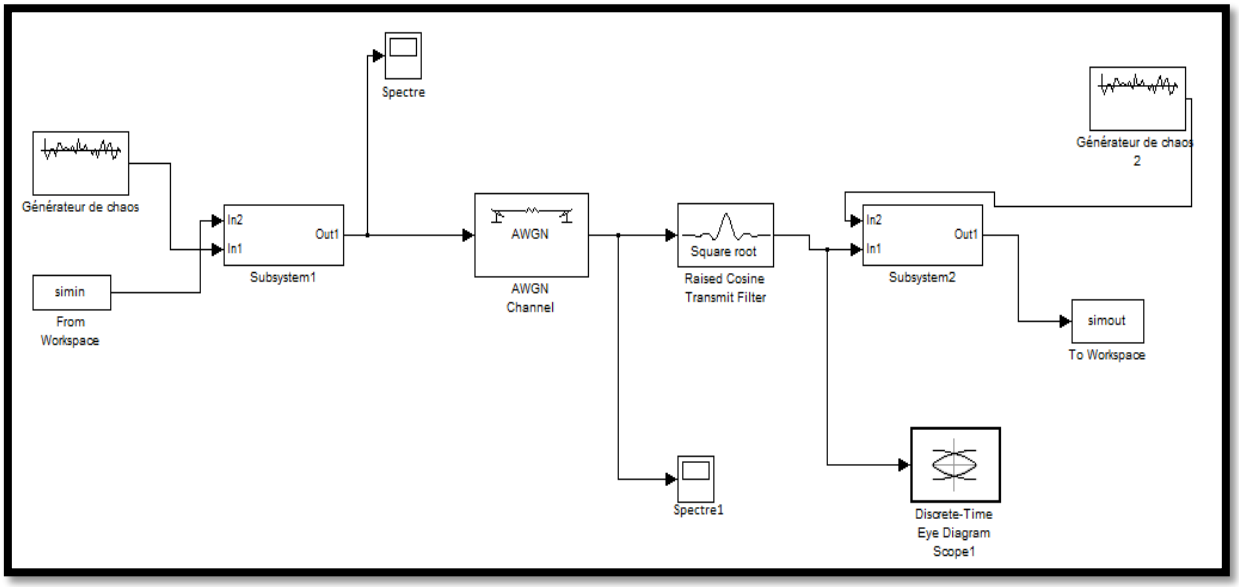


Figure III.1: Transmission sécurisée par chaos.

II. Générateur de chaos :

Le générateur de séquences chaotiques réalisé à partir d'une récurrence logistique nous délivre des suites chiffrantes de grande taille remplissant les critères suivants :

- Les suites chiffrantes doivent êtres, sur le plan statistique, en apparence aléatoires ;
- Les suites chiffrantes doivent êtres imprévisibles au sens où il doit être impossible de prédire la prochaine séquence.

La sortie de ce générateur est utilisée pour chiffrer les données qui sont stockées dans des fichiers adéquats pouvant être appelé par MatLab.
Nos données (image ou texte) ont été enregistrées dans un fichier pour être appelé dans la chaine par Workspace.

Dans le bloc subsystemon a intégré notre modèle de chiffrement. Le résultat c'est-à-dire l'information chiffrée est transmise par le canal de transmission au récepteur

Le récepteur contient lui aussi le même générateur de chaos qui a servi au chiffrement pour nous permettre de revenir à l'information initiale sans pour cela être obligé de transmettre la clé de chiffrement.

III. Simulation :

III.1. Caractérisation du chaos :

- **Attracteur de Lorenz :**

Afin de confirmer la première théorie du chaos, on a voulu refaire la représentation graphique du modèle de Lorenz pour cela on a tracé en premier lieu l'attracteur à partir d'un programme écrit sous MatLab, puis le diagramme de bifurcation

Le script Matlab pour la détermination d'attracteur de Lorenz est le suivant :

```
function lorenz
global A B R
A = 10; B = 8/3; R = 28;
u0 = 100*(rand(3,1) - 0.5);
[t,u] = ode45(@lor2,[0,100],u0);
N = find(t>10);
v = u(N,:);
plot3(v(:,1),v(:,2),v(:,3))
title('The Lorenz attractor')
xlabel('x'), ylabel('y'), zlabel('z')
grid, shg
function uprime = lor2(t,u)
global A B R
uprime = zeros(3,1);
uprime(1) = -A*u(1) + A*u(2);
uprime(2) = R*u(1) - u(2) - u(1)*u(3);
uprime(3) = -B*u(3) + u(1)*u(2);
```

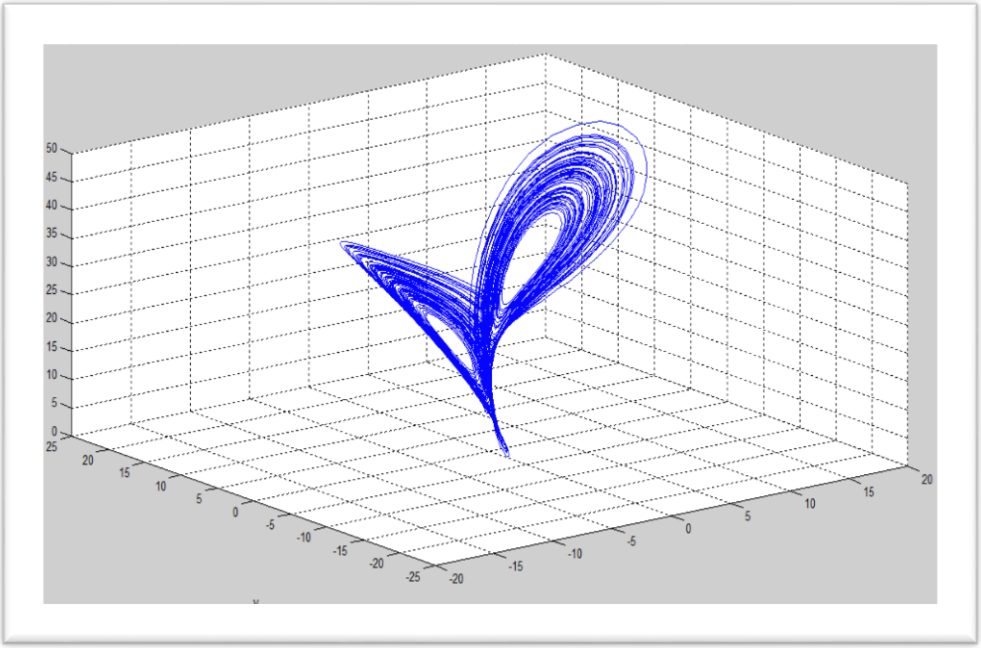


Figure III.2 : Attracteur de Lorenz

- **Diagramme de Bifurcation** :

Une bifurcation survient lorsqu'une variation quantitative d'un paramètre du système engendre un changement qualitatif des propriétés d'un système telles que la stabilité, le nombre de points d'équilibre ou la nature des régimes permanents. Les valeurs des paramètres au moment du changement sont appelées *valeurs de bifurcation*.

Dans les systèmes dynamiques, un diagramme de bifurcation montre les comportements possibles d'un système, à long terme, en fonction des paramètres de bifurcation

Le script Matlab pour la détermination du diagramme de bifurcation est le suivant :

```
Npre = 200; Nplot = 100;
x = zeros(Nplot,1);
for r = 2.5:0.005:4.0,
  x(1) = 0.5;
  for n = 1:Npre,
x(1) = r*x(1)*(1 - x(1));
  end,
  for n = 1:Nplot-1,
    x(n+1) = r*x(n)*(1 - x(n));
  end,
  plot(r*ones(Nplot,1), x, '.', 'markersize', 2);
  hold on;
end,
title('Bifurcation diagram of the logistic map');
xlabel('r');  ylabel('x_n');
set(gca, 'xlim', [2.5 4.0]);
hold off;
```

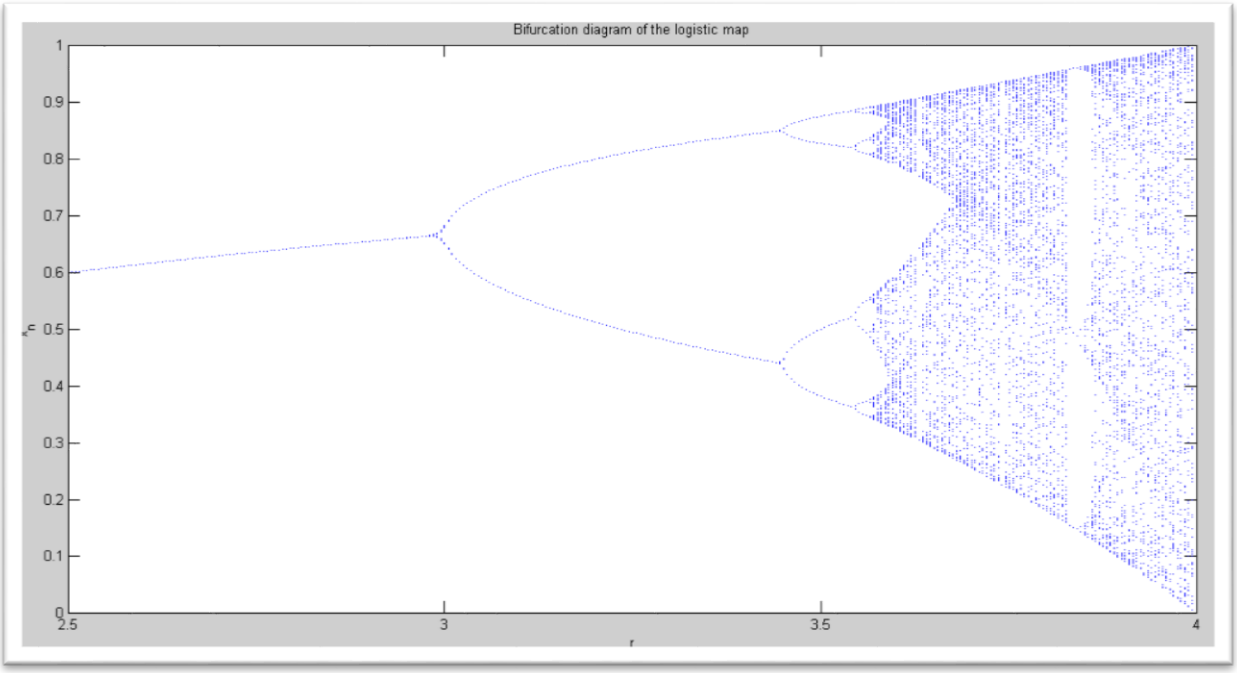
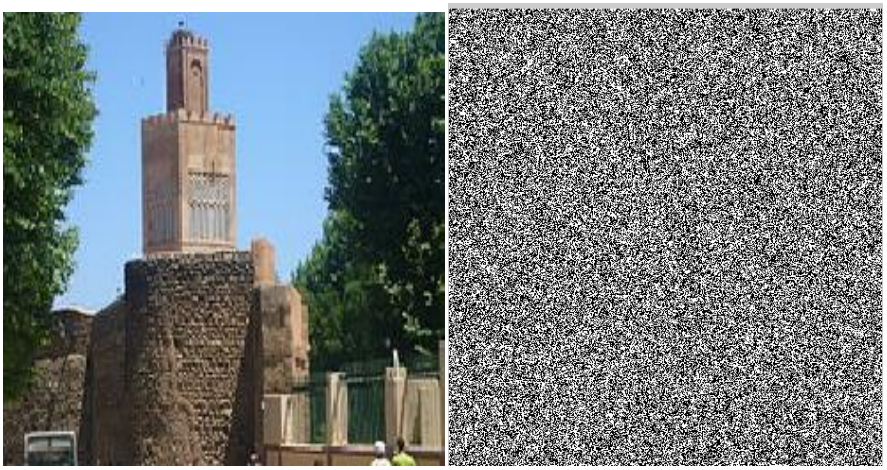


Figure III.3 : Diagramme de Bifurcation

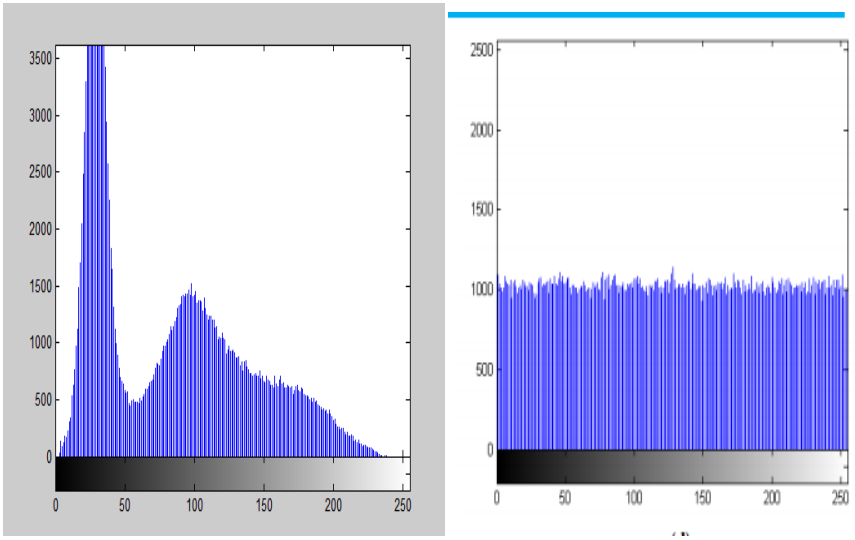
IV. Chiffrement – Déchiffrement :

Dans cette section on s'intéresse aux techniques de transmission sécurisée d'informations qui reposent sur le principe de synchronisation chaotique. Le point commun constate dans la majorité des techniques développées dans la littérature est l'utilisation de la configuration maitre-esclave pour laquelle on dispose d'un émetteur chaotique qui génère le signal du texte chiffré transmis dans le canal de communication vers un système récepteur qui a pour objectif de synchroniser avec le système et de restaurer le signal.

Parmi les techniques de communications traditionnelles a base du chaos, on cite : le masquage chaotique la commutation chaotique le cryptage par injection la transmission à deux voies.



(a) (b)



(c) (d)

Figure III.4 : Chiffrement et Déchiffrement

(a) Image en clair (b) Image crypté

(c) Histogramme de l'image clair (d) Histogramme de l'image cryptée

V. Réalisation pratique :

Le fonctionnement de la chaine de transmission est résumé dans une interface graphique.

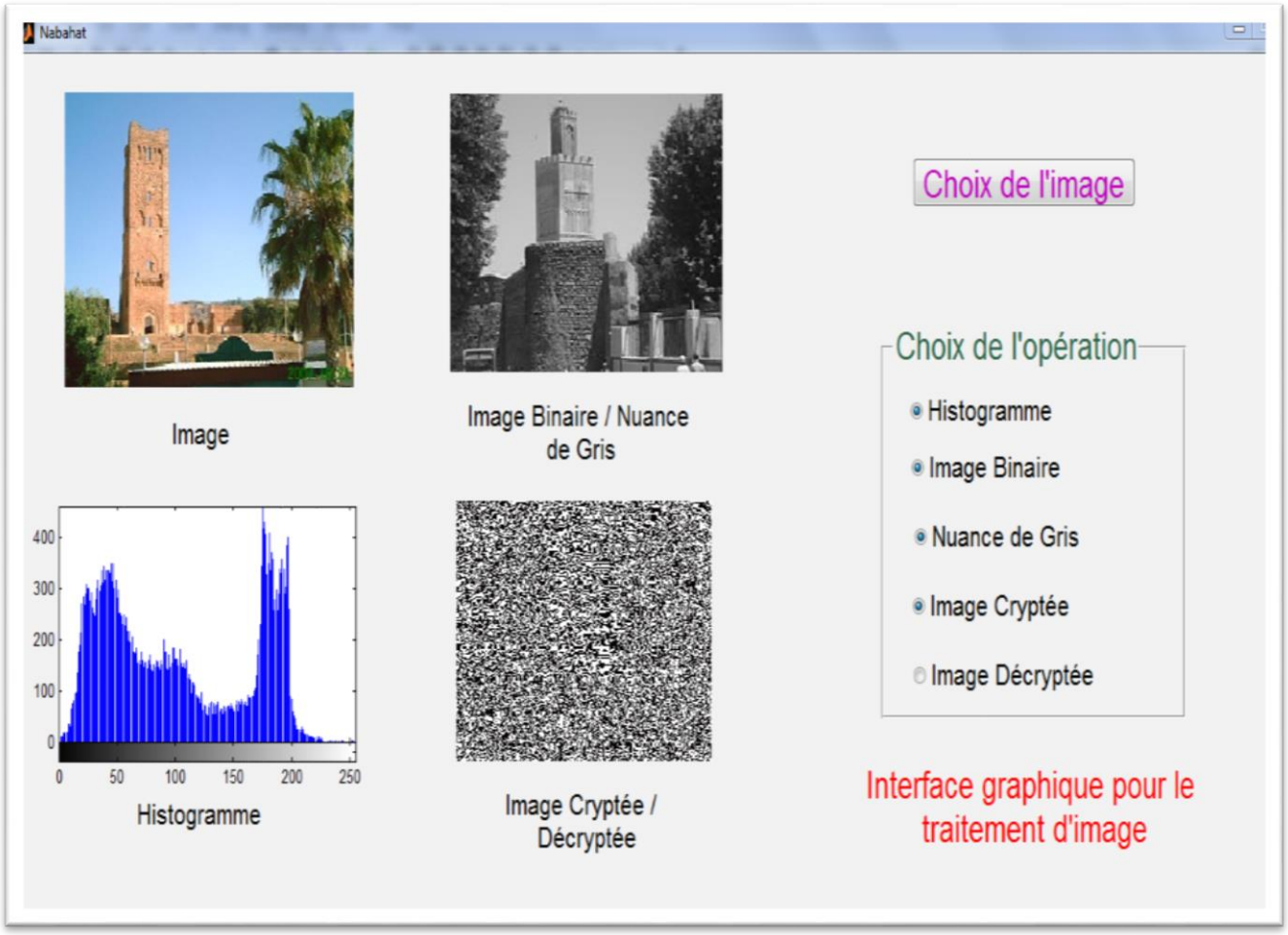


Figure III.5 : Interface Graphique

Le script sous Matlab est le suivant :

```
function varargout = Nabahat(varargin)
% NABAHAT MATLAB code for Nabahat.fig
%      NABAHAT, by itself, creates a new NABAHAT or raises the existing
%      singleton*.
%
%      H = NABAHAT returns the handle to a new NABAHAT or the handle to
%      the existing singleton*.
%
%      NABAHAT('CALLBACK',hObject,eventData,handles,...) calls the local
%      function named CALLBACK in NABAHAT.M with the given input
arguments.
%
%      NABAHAT('Property','Value',...) creates a new NABAHAT or raises the
%      existing singleton*.  Starting from the left, property value pairs
are
%      applied to the GUI before Nabahat_OpeningFcn gets called.  An
%      unrecognized property name or invalid value makes property
application
%      stop.  All inputs are passed to Nabahat_OpeningFcn via varargin.
%
%      *See GUI Options on GUIDE's Tools menu.  Choose "GUI allows only
one
```

```
%      instance to run (singleton)".

%

% See also: GUIDE, GUIDATA, GUIHANDLES



% Edit the above text to modify the response to help Nabahat



% Last Modified by GUIDE v2.5 10-Jun-2015 00:39:44



% Begin initialization code - DO NOT EDIT
global x
gui_Singleton = 1;
gui_State = struct('gui_Name',       mfilename, ...
                   'gui_Singleton',  gui_Singleton, ...
                   'gui_OpeningFcn', @Nabahat_OpeningFcn, ...
                   'gui_OutputFcn',  @Nabahat_OutputFcn, ...
                   'gui_LayoutFcn',  [] , ...
                   'gui_Callback',   []);
if nargin && ischar(varargin{1})
    gui_State.gui_Callback = str2func(varargin{1});
end



if nargout
```

```
    [varargout{1:nargout}] = gui_mainfcn(gui_State, varargin{:});
else
    gui_mainfcn(gui_State, varargin{:});
end
% End initialization code - DO NOT EDIT



% --- Executes just before Nabahat is made visible.
function Nabahat_OpeningFcn(hObject, eventdata, handles, varargin)
% This function has no output args, see OutputFcn.
% hObject    handle to figure
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
% varargin   command line arguments to Nabahat (see VARARGIN)


% Choose default command line output for Nabahat
handles.output = hObject;


% Update handles structure
guidata(hObject, handles);


% UIWAIT makes Nabahat wait for user response (see UIRESUME)
```

```
% uiwait(handles.figure1);




% --- Outputs from this function are returned to the command line.
function varargout = Nabahat_OutputFcn(hObject, eventdata, handles)
% varargout  cell array for returning output args (see VARARGOUT);
% hObject    handle to figure
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)


% Get default command line output from handles structure
varargout{1} = handles.output;




% --- Executes on button press in hist.
function hist_Callback(hObject, eventdata, handles)
global x
axes(handles.axes3);
x=imread('mech.jpg');
c=rgb2gray(x);
imhist(c);
```

```
% --- Executes on button press in binary.
function binary_Callback(hObject, eventdata, handles)
global x
axes(handles.axes2);
x=imread('mech.jpg');
b=im2bw(x);
imshow(b);


% --- Executes on button press in nuancedegris.
function nuancedegris_Callback(hObject, eventdata, handles)
global x
axes(handles.axes2);
x=imread('mech.jpg');
c=rgb2gray(x);
imshow(c);


% --- Executes on button press in cryptage.
function cryptage_Callback(hObject, eventdata, handles)


global x
axes(handles.axes4);
```

```
x=imread('mans.jpg');

%[ind,map]=rgb2ind(x,128);

%imshow(ind);

c=rgb2gray(x);

d = double(c);

imshow(d/255);

c = mod(d,2);

imshow(c);



% --- Executes on button press in decryptage.

function decryptage_Callback(hObject, eventdata, handles)

global x

axes(handles.axes4);

x=imread('mech.jpg');



imshow(x);




% --- Executes on button press in pushbutton2.

function pushbutton2_Callback(hObject, eventdata, handles)

global x

axes(handles.axes1);
```

```
[nom,chemin]=uigetfile('*.jpg');

x=imread(nom);



imshow(x);
```

Conclusion :

Ce chapitre s'est intéressé au chiffrement d'images numériques à partir de séquences chaotiques obtenues par discrétisation d’une récurrence logistique.

Conclusion Générale

Conclusion Générale

La cryptographie basée sur la théorie du chaos s'est rapidement développée au cours de ces dernières années. Aujourd'hui, la plupart des recherches se concentrent sur l'utilisation du chaos dans des cryptosystèmes en vue d'apporter une amélioration (temps de chiffrement, sécurité) par rapport aux méthodes standards de la cryptographie (DES, AES), ceci grâce aux caractéristiques des signaux chaotiques telles que: bonnes propriétés cryptographiques, reproductibilité à l'identique (caractère déterministe des systèmes chaotiques) et l'hyper sensibilité à la clé secrète.

Dans ce travail, nous avons présenté une chaine de transmission sécurisée par chaos Afin de mener à bien une telle étude, le travail présenté a été regroupé en trois parties :

La première est consacrée à une présentation générale sur les différents cryptosystèmes, et a permis de montrer les limites de la cryptographie classique, de la cryptographie quantique et de présenter la cryptographie chaotique comme une alternative intéressante pour le chiffrement en temps réel de grosses quantités de données (images numériques).

La deuxième partie quant à elle, constitue le coeur de ce travail. elle aborde les origines de la théorie du chaos, comment on l'obtient ; puis, elle présente les récurrences logistiques ainsi que les récurrences skew tent qui sont par ailleurs très importants pour caractériser le chaos. Pour finir par une présentation des modèles de chiffrement par chaos.

La dernière partie est consacrée à la présentation de notre simulation de la chaîne de transmission sous simulink ainsi que la réalisation de notre interface graphique qui est un résumé de notre travail, dans cette interface on présente les différentes opérations qu'on peut appliquées à une image dans le but de la traiter ou de chiffrer et déchiffrer cette image tout en donnant un histogramme Les simulations numériques ont été menées afin de prouver le niveau de sécurité élevé et l'effectivité de la méthode de chiffrage proposée.

Le modèle de chiffrement réalisé nous a permis d'étudier les algorithmes de chiffrement traditionnels aussi bien à clé publique ou asymétrique comme le modèle RSA ou à clé privée

ou symétrique tel que le modèle AES... avant d'aboutir à la cryptographie par chaos numérique à l'aide des récurrences logistiques ou skew tent .

Les perspectives qui se dégagent de ce travail :

- Essayer d'améliorer la longueur des clés pour un meilleur résultat de chiffrement.
- Voir comment transmettre les clés de chiffrement au récepteur et voir la synchronisation de l'émetteur et du récepteur afin d'éviter la construction du générateur de chaos côté récepteur.
- Améliorer la construction de la chaîne de transmission sous Simulink pour obtenir de meilleurs résultats.

RÉSUMÉ :

Le travail porte sur la transmission sécurisée utilisant un cryptosystème numérique par chaos. Le mémoire s'ouvre par des généralités sur les cryptosystèmes traditionnels et conduit à la nécessité d'adapter la réflexion sur d'autres méthodes de cryptage afin de protéger plus efficacement les flots de données sans cesse croissants.

Les séquences chaotiques sont générées à partir du système chaotique et constituent la clé de chiffrement. Le choix du générateur de chaos qui délivre les séquences chaotiques est réalisée à partir de récurrences logistiques et de récurrences Skew tent

L'analyse de sécurité et les simulations numériques prouvent le niveau de sécurité élevé et l'effectivité de la méthode.

Mots clés : Transmissions sécurisées, cryptographie par chaos, chiffrement de l'image…

Abstract :

The work focuses on the secure transmission by using a digital chaos cryptosystem . The thesis begins with generalities on traditional cryptosystems and leads to the need to adapt thinking about other encryption methods to more effectively protect data flows constantly growing .
Chaotic sequences are generated from the chaotic system and provide the encryption key. The choice of the chaos generator which delivers the chaotic sequences is performed using logistic recurrences and recurrences skew tent
Analysis of safety and numerical simulations show the high level of safety and effectiveness of the method.

Keywords: Secure Transmissions, chaos cryptography, encryption image ...

الملخص:

يركز العمل على نقل آمن باستخدام نظام تشفير الفوضى الرقمية . أطروحة تبدأ مع العموميات على نظم الترميز التقليدية و يؤدي إلى الحاجة إلى التكيف مع التفكير في أساليب التشفير أخرى لحماية بيانات تدفقات المتزايدة باستمرار على نحو أكثر فعالية .
يتم إنشاء تسلسل الفوضى من النظام الفوضوي وتوفير مفتاح التشفير . يتم تنفيذ خيار مولد الفوضى التي توفر تسلسل الفوضى باستخدام تكرار اللوجستية و تكرار خيمة الانحراف
تحليل السلامة و المحاكاة العددية إظهار مستوى عال من الأمان والفعالية في الأسلوب.

كلمات البحث: الإرسال الآمنة والفوضى الترميز، صورة التشفير ...