Université Abou Bekr Belkaid
Tlemcen Algérie
جامعة أبي بكر بلقايد
تلمسان الجزائر

République Algérienne Démocratique et Populaire
Université Abou Bakr Belkaid– Tlemcen
Faculté des Sciences
Département d'Informatique

Mémoire de fin d'études

Pour l'obtention du diplôme de Master en Informatique

Option : *Réseau et Système et Distribué (R.S.D)*

Thème

Cryptage chaotique des images et de texte

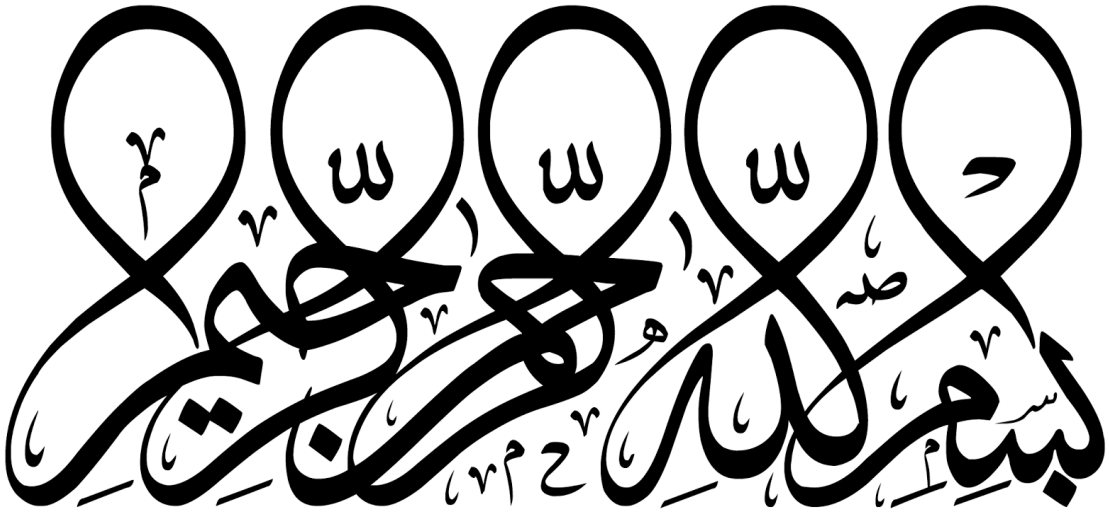
Réalisé par :

- **MANA Boumedyen**

Présenté le 06 Juillet 2019 devant le jury composé de :

- *BENAMMAR Abdelkrim* *(Président)*
- *MANA Mohammed* *(Encadreur)*
- *BENAISSA Mohammed* *(Examinateur)*

Année universitaire : 2018-2019


بسم الله الرحمن الرحيم

Remerciements

Avant tout on tient notre remerciement à notre dieu tout puissant de nous avoir donné la foi, la force et le courage.

Je remercie mon encadreur Dr Mana Mohammed, de sa disponibilité, sa générosité professionnelle et ses précieux conseils.

Je remercie les membres du jury Dr Benammar Abdelkrim et Dr Benaissa Mohammed qui m'ont honoré de leur présence et d'avoir accepté de juger mon travail.

Merci à tous.

Dédicace

Je dédie ce travail à la mémoire de mon père,

Que dieu lui bénisse de l'apaise

A ma chère mère, mes chères enfants Kassem et Razane, à ma femme,

A mes chers frères,

A toute ma famille, tous mes amis

Table des Matières

Liste des figures

Liste des Figures

Liste des tableaux

Liste des tableaux

Introduction générale

Introduction générale

Depuis le début des civilisations, le besoin de dissimuler préoccupe l'humanité. La confidentialité apparaissait notamment nécessaire lors des luttes pour l'accès au pouvoir. Puis elle a été énormément développée pour les besoins militaires et diplomatiques. Aujourd'hui, de plus en plus d'applications dites civiles nécessitent la sécurité des données transitant entre deux interlocuteurs via un vecteur d'information comme les réseaux de télécommunications actuels et futurs. Ainsi les banques l'utilisent 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.

La cryptographie traditionnelle est l'étude des méthodes permettant de transmettre des 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, qui, à partir d'un texte en clair, donne 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 cryptographie est parmi les méthodes les plus efficaces pour établir la confidentialité et l'intégrité de ce type d'information.

Mais ces techniques de cryptographie standard ne conviennent pas aux cas particuliers de la transmission d’images fixes et vidéo en espace libre et sur les lignes de transmission ; surtout pour le cas de certains domaines d’applications du type temps réel comme l’émission des programmes télévision par satellite et la télémédecine où le temps est un facteur capital.

La cryptographie basé chaos semble pallier aux inconvénients cités plus haut de la cryptographie standard et apporter une sécurité maximale.

Un système chaotique est un système dynamique non linéaire déterministe et imprévisible à cause de son extrême sensibilité aux conditions initiales. Un signal chaotique est donc déterministe, mais sa forme d’onde est quasi identique à celui d’un bruit blanc que ce soit dans le domaine temporel ou le domaine fréquentiel. Les signaux

chaotiques issus de récurrences discrètes 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'identiques en émission réception.

Les séquences chaotiques numérisées peuvent alors être utilisées comme clés secrètes dans un cryptosystème basé chaos. La sécurité obtenue est maximale, car la connaissance d'un cryptogramme "message chiffré connu" ne donne aucune indication sur le message clair correspondant.

Le travail réalisé dans ce mémoire s'inscrit dans ce contexte particulier. Son objectif est de proposer un crypto-système (algorithme de chiffrement et de déchiffrement) basé sur les systèmes chaotiques pour chiffrer et déchiffrer les images et les messages échangés entre interlocuteurs.

Nous avons structuré notre mémoire en trois chapitres. Le premier chapitre donnera une brève présentation sur les techniques de cryptographie et ses classifications, particulièrement revue sur la cryptographie symétrique. Dans le deuxième chapitre met le point sur les notions de base des systèmes chaotiques.

Dans le dernier chapitre nous avons implémenté deux algorithmes de chiffrement / déchiffrement le premier basé sur la méthode de baptisa et le deuxième c'est notre schéma basé sur la carte logistique chaotique et le générateur congruentiel linéaire.

Chapitre 1

Cryptographie moderne

Introduction :

Ce chapitre, introduit les notions nécessaires à la compréhension de sécurité de l'information et la cryptographie, Nous commençons par définir la sécurité de l'information et donnons-les éléments de base la concernant. La sécurité de l'information est un domaine très vaste qui regroupe tous les aspects de la sauvegarde ou la protection de l'information ou des données, donc pour garantir la sécurité de l'information c'est la cryptographie qui s'en charge. Ce domaine, qui était il y a encore quelques années, réservé aux militaires et aux grandes entreprises, concerne aujourd'hui tous ceux qui souhaitent transmettre des données protégées, qu'ils soient professionnels ou particuliers. Pour cela, il existe de nombreuses méthodes de cryptographie.

1- La sécurité de l'information :

La cryptologie peut se définir comme étant l'étude des communications dans un environnement non sécurisé. Elle a pour but d'assurer certains services de sécurité de l'information tels que : la confidentialité, l'intégrité et l'authentification.

La cryptologie, appelée aussi science du secret regroupe la cryptographie et la cryptanalyse. [**1**].

1.1- La confidentialité

La confidentialité spécifie que seules les personnes autorisées à accéder à une certaine information ont la possibilité de l'atteindre. Ce service de sécurité concerne tant les données stockées que les données envoyées au travers d'un réseau. Pour l'assurer, nous utiliserons les contrôles d'accès et le chiffrement. La violation de la confidentialité peut se voir, par exemple, quand une information confidentielle est devenue publique, grâce aux logs du système ou aux changements de comportement d'une certaine personne envers l'organisation.

1.2- L'intégrité

L'intégrité spécifie que l'information ne peut être modifiée que par les personnes autorisées. Tout comme pour la confidentialité, ce service concerne tant les informations stockées que les données envoyées au travers d'un réseau. Sa protection est souvent la même que celle qui est garantie par la confidentialité. En effet, en contrôlant l'accès à une donnée, nous assurons aussi son intégrité. La détection d'une violation de cette dernière

est, par exemple, la comparaison entre l'information et ses copies. Une réponse à cela est la réparation de cette donnée. [**2**]

1.3- L'authentification

L'authentification est un mécanisme permettant d'identifier des personnes ou des entités et de certifier leur identité.

1.4- La non répudiation

La non-répudiation signifie la possibilité de vérifier que l'envoyeur et le destinataire sont bien les parties qui disent avoir respectivement envoyé ou reçu le message. Autrement dit, la non-répudiation de l'origine prouve que les données ont été envoyées, et la non-répudiation de l'arrivée prouve qu'elles ont été reçues [**3**].

2- La terminologie de la cryptologie :

2.1- La cryptologie Cela signifie la "science du secret". La cryptologie se partage entre la cryptographie et la cryptanalyse.

2.2- La cryptographie Discipline incluant les principes, les moyens et les méthodes de transformation des données, dans le but de masquer leur contenu, d'empêcher leur modification ou leur utilisation illégale [1].

2.3- La cryptanalyse Analyse des textes chiffrés pour retrouver des informations dissimulées, Analyse des procédés de chiffrement afin d'en découvrir les failles de sécurité.

2.4- Texte en clair Texte en clair c'est les données ou les informations lisibles avant le chiffrement.

2.5- Le chiffrement Procédé grâce auquel on peut rendre la compréhension d'un document impossible à toute personne qui n'a pas la clef d'encodage.

2.6- Clef Dans un système de chiffrement, elle correspond à un nombre, un mot, une phrase, etc. qui permet, grâce à l'algorithme de chiffrement, de chiffrer ou de déchiffrer un message.[3]

2.7- Texte chiffré **(Cryptogramme)** Données ou message inintelligible résultant du chiffrement.

2.8- Le déchiffrement Est un moyen qui permet à retrouver le message original (Texte en clair) à partir du message chiffré en utilisant la clé de déchiffrement.

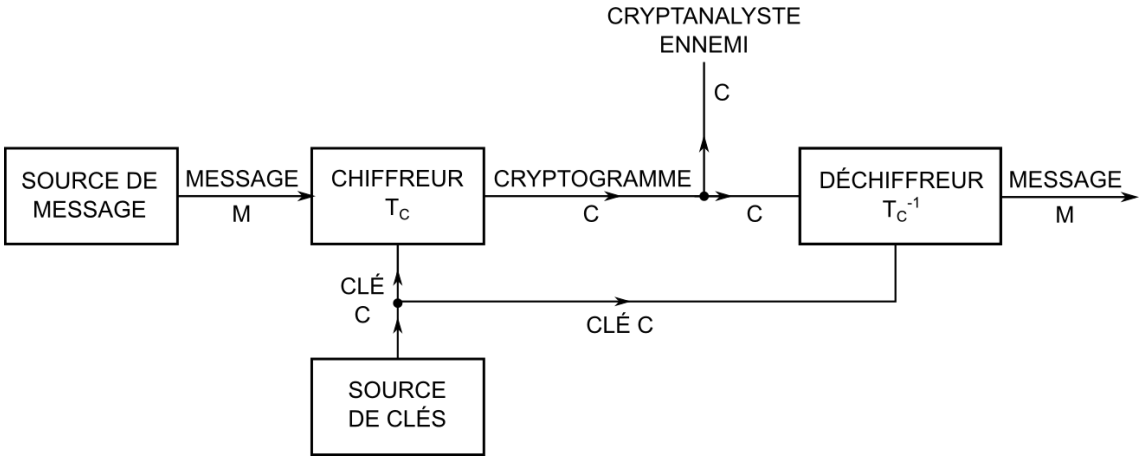


Figure I. 1 système cryptologie (schéma original de C. Shannon)

3- CLASSIFICATION DES SYSTEMES CRYPTOGRAPHIQUES :

Les crypto-systèmes peuvent être classés conformément aux différentes caractéristiques. Ainsi, selon les types des clefs utilisées, nous citons les catégories suivantes des crypto-systèmes : systèmes symétriques, systèmes asymétriques et systèmes hybrides. Une autre catégorie des crypto-systèmes est basée sur les techniques de chiffrement : chiffrement par bloc ou chiffrement par flot.

3.1- La cryptographie symétrique (clé secrète) :

3.1.1- Principe général :

Le chiffrement symétrique appelé aussi système à clé secrète ou privé. La clé de déchiffrement peut être calculée à partir de la clé de chiffrement et vice versa. En générale la même clé est utilisée pour le chiffrement et le déchiffrement, d'où l'obligation que celle-ci reste confidentielle, sous peine de rendre le système inefficient.

Ce type de chiffrement repose sur le partage d'une même clé secrète *k* entre les interlocuteurs. Cette clé sert à chiffrer et déchiffrer les messages échangés.

L'émetteur transmet cette clé k au récepteur à travers un canal de communication d'une façon confidentiel (généralement un canal de communication privé), à ce qu'aucun opposant ne puisse l'intercepter.

3.1.2- Caractéristiques :

- Les clés sont identiques : KE = KD = K,
- La clé doit rester secrète,
- Les algorithmes les plus répandus sont le DES, AES, ...
- Au niveau de la génération des clés, elle est choisie aléatoirement dans l'espace des clés,
- Ces algorithmes sont basés sur des opérations de transposition et de substitution des bits du texte clair en fonction de la clé,
- La taille des clés est souvent de l'ordre de 128 bits. Le DES en utilise 56, mais l'AES peut aller jusque 256,
- L'avantage principal de ce mode de chiffrement est sa rapidité,
- Le principal désavantage réside dans la distribution des clés : pour une meilleure sécurité, on pratiquera à l'échange de manière manuelle. Malheureusement, pour de grands systèmes, le nombre de clés peut devenir conséquent. C'est pourquoi on utilisera souvent des échanges sécurisés pour transmettre les clés.

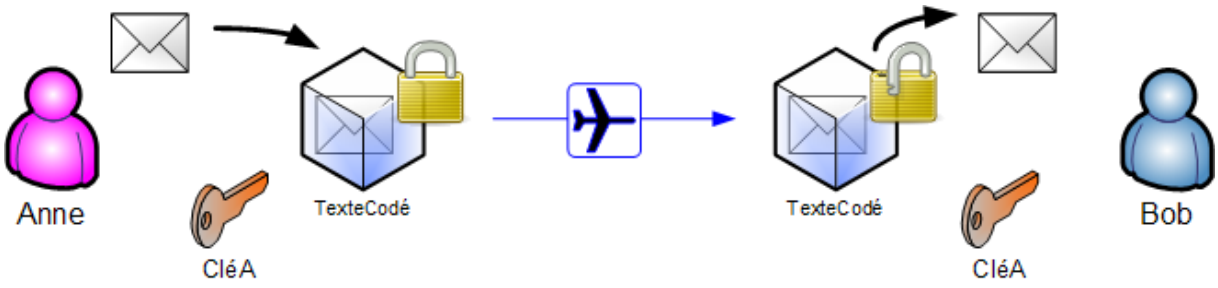


Figure I. 2_chiffrements à clé privée

3.1.3- Les classes de la cryptographie symétrique :

Les schémas de chiffrement symétriques peuvent être classés en deux catégories, le chiffrement par flots et le chiffrement par bloc :

3.1.3.1- Chiffrement à flot :

Dans un crypto-système à flot, le cryptage des messages se fait caractère par caractère ou bit à bit, au moyen de substitutions de type César générées aléatoirement : la taille de la clef est donc égale à la taille du message. L'exemple le plus illustratif de ce principe est le chiffre de Vernam (*inventé par un ingénieur AT&T Gilbert Vernam en 1918*). Cet

algorithme est aussi appelé « One Time Pad » (masque jetable), c'est à dire que la clef n'est utilisée qu'une seule fois.

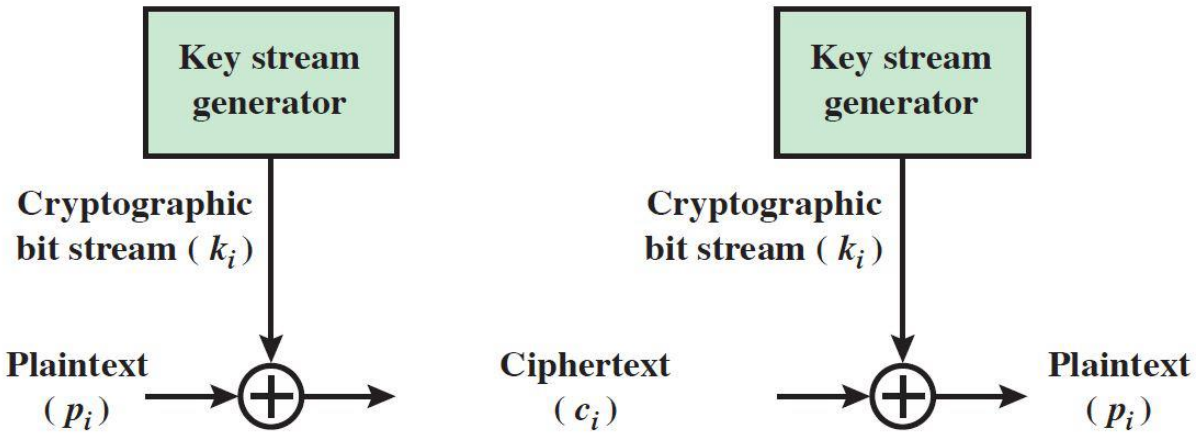


Figure I. 3le Chiffrement symétrique à flot.

- Il a été démontré par le mathématicien Claude Elwood Shannon qu'il était impossible de retrouver un message crypté par le principe de Vernam sans connaître la clef. Ce qui ferait en théorie du chiffre de Vernam un crypto-système incassable. Mais dans la pratique, le crypto-système par flots pose des problèmes délicats : canaux sûrs de distribution des clefs, taille des clefs encombrantes car de même taille que le message et surtout caractère aléatoire des générateurs de bits de clefs utilisés. En revanche, un des avantages du système est qu'il est insensible aux phénomènes de propagation d'erreurs : un bit erroné donne une erreur à la réception ou à l'émission, mais est sans incidence sur les bits suivants. [**4**]

Parmi les algorithmes qui utilisent chiffrement à flots c'est : *RC4*, *A5/1*,*E0*,...etc.

Algorithme RC4

RC4 = système de chiffrement à flot dû à Ron Rivest, couramment utilisé dans les protocoles SSL et Wi-Fi.

Principe général

RC4 fonctionne de la façon suivante : la clef RC4 permet d'initialiser un tableau de 256 octets en répétant la clef autant de fois que nécessaire pour remplir le tableau. Par la suite, des opérations très simples sont effectuées : les octets sont déplacés dans le tableau, des additions sont effectuées, etc. Le but est de mélanger autant que possible le tableau. Finalement on obtient une suite de bits pseudo-aléatoires qui peuvent être utilisés pour chiffrer les données via un XOR.

Description détaillée

RC4 est un générateur de bits pseudo-aléatoires dont le résultat est combiné avec le texte en clair via une opération XOR, le déchiffrement se fait de la même manière.

Pour générer le flot de bits, l'algorithme dispose d'un état interne, tenu secret, qui comprend deux parties :

– une permutation S de tous les 256 octets possibles

– deux pointeurs i et j de 8 bits qui servent d'index dans un tableau

La permutation est initialisée grâce à la clé de taille variable, typiquement entre 40 et 256 bits, grâce au key Schedule de RC4.

Utilisation des chiffrements par flot

Les avantages des algorithmes de chiffrements par flot découlent de la petite taille de bloc utilisée, ce qui est d'autant plus vrai dans le cas des chiffrements où le bloc est réduit à un unique bit. Cette faible taille permet une réduction des délais et de la taille de la mémoire-tampon nécessaire pour stocker le message avant l'obtention d'un bloc complet. L'emploi de blocs de petite taille limite aussi la propagation d'erreurs de transmission lors du déchiffrement. Lorsque les ressources sont limitées, souvent parce qu'il faut restreindre la consommation électrique du circuit électrique dédié au chiffrement, ou qu'il est nécessaire de pouvoir chiffrer et déchiffrer très rapidement, on utilise généralement des algorithmes de chiffrement par flot, par exemple sur les systèmes embarqués. [**5**]

3.1.3.2- Chiffrement par bloc :

a- Introduction :

Dans un système par blocs, chaque texte clair est découpé en blocs de même longueur et chiffré bloc par bloc.

La longueur l des clés doit être suffisante pour que l'attaque exhaustive consistant à déchiffrer le chiffré avec toutes les clés possibles jusqu'à l'obtention du clair, soit irréaliste (l ¸ 128).

Le principe général d'un chiffrement itératif par blocs est le suivant : pour chaque bloc, on itère r fois une fonction interne F ; à chacun des r tours, la fonction F est paramétrée par une clef Ki (1 <= i <= r), et la fonction du tour i peut être notée F_{Ki} . Comme on veut que le chiffrement soit inversible (pour pouvoir déchiffrer), il faut que les fonctions F_{Ki} soient bijectives.

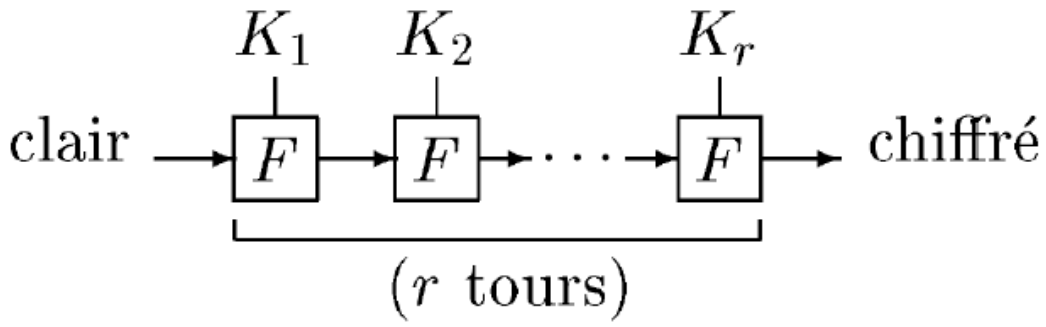


Figure I. 4 chiffrements par bloc.

Donc L'idée générale du chiffrement par blocs est la suivante :

1. Remplacer les caractères par un code binaire

2. Découper cette chaîne en blocs de longueur donnée

3. Chiffrer un bloc en l'"additionnant" bit par bit à une clef.

4. Déplacer certains bits du bloc.

5. Recommencer éventuellement un certain nombre de fois l'opération 3.

6. Passer au bloc suivant et retourner au point 3 jusqu'à ce que tout le message soit chiffré.

On distingue trois catégories de chiffrement par bloc :

– **Chiffrement par substitution** : 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.

– **Chiffrement par transposition** : Les transpositions consistent à mélanger les symboles 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.

– **Chiffrement par produit** : C'est la combinaison des deux. Le chiffrement par substitution ou par transposition ne fournit pas un haut niveau de sécurité, mais en combinant ces deux transformations, on peut obtenir un chiffrement plus robuste. 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).

b- Les structures de Feistel

Cette structure fut décrite en 1973 (par Feistel, employé chez IBM). La plupart des chiffrements de la fin du XXè siècle sont basés sur cette structure. Elle découle des réseaux S-P de Shannon. Il adapte la structure de Shannon afin de la rendre inversible ce qui permet de réutiliser le matériel de chiffrement pour déchiffrer un message. La seule modification s'opère dans la manière dont la clé est utilisée.

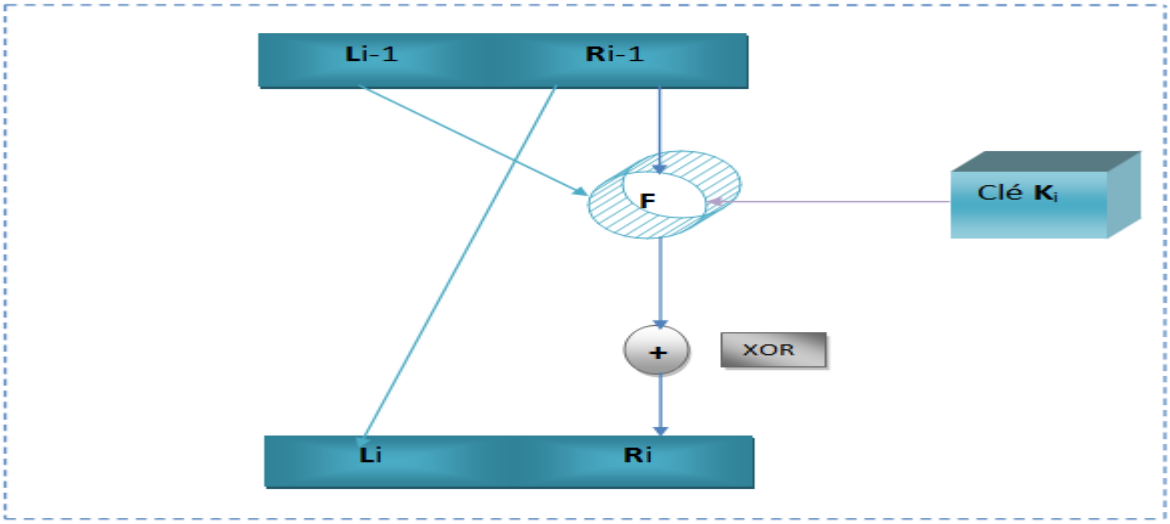


Figure I. 5 Stucture de Feistel.

Dans une construction de Feistel, le bloc d'entrée d'un round est séparé en deux parties. La fonction de chiffrement est appliquée sur la première partie du bloc et l'opération binaire OU-Exclusif ($\oplus$) est appliquée sur la partie sortante de la fonction et la deuxième partie. Ensuite les deux parties sont permutées et le prochain round commence.

L'avantage est que la fonction de chiffrement et la fonction de déchiffrement sont identiques. Ainsi la fonction n'a pas à être inversible, c'est la structure qui l'est.

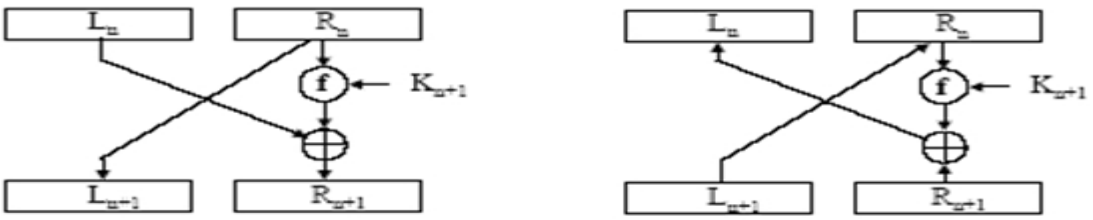


Figure I. 6 La structure est inversible

Parmi les algorithmes de chiffrement par bloc qui utilise la structure de Feistel on a D.E.S, A.E.S.

c- Data Encryptions Standard (D.E.S)

Le *Data Encryptions Standard* (standard de chiffrement de données) a été publié en 1977, et fut ainsi le premier algorithme cryptographique à petite clé secrète (56 bits) à avoir été rendu public. Le DES consiste en un réseau de Feistel de 16 tours : le message à chiffrer est découpé en blocs de 64 bits, chacun d'eux étant séparé en deux sous-blocs de 32 bits.

L'algorithme du DES sera le plus utilisé dans le monde jusqu'en 1998. A cette époque, une association de particuliers fit construire, pour moins de 250 000 $ (somme dérisoire pour un Etat ou une organisation mafieuse), un processeur capable de casser le DES. A l'heure actuelle, trois jours suffisent aux ordinateurs pour le percer, et ce grâce à des attaques exhaustives !

On aura bien tenté d'améliorer le DES, en doublant la taille de sa clé (on parle alors de TDES), mais cette version n'était pas assez rapide. Le NIST (National Institute of Standards and Technologies) lance donc un concours pour créer un successeur au DES, et ce sont les belges Joan Daemen et Vincent Rijmen qui seront retenus.

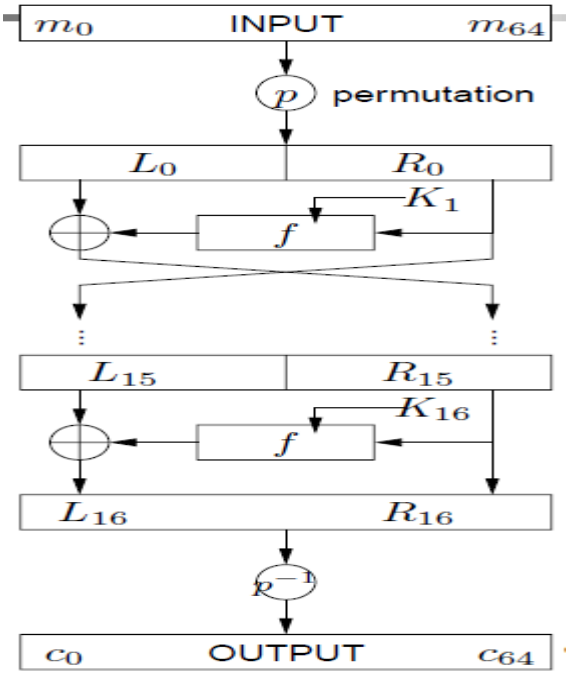


Figure I. 7 Algorithme principal du D.E.S

La fonction F :

$f : \{0, 1\}^{32} \times \{0, 1\}^{48} \longrightarrow \{0, 1\}^{32}$

$R_{i-1} \quad K_i \longrightarrow f(R_{i-1} \quad K_i)$

C'est une fonction qui se compose de :

Une augmentation E de $Ri-1$ pour en faire un bloc de 48 octets, c'est-à-dire que $E(Ri-1)$ est composé de tous les bits de $Ri-1$, 16 d'entre eux apparaissant deux fois.

On calcule $E(Ri-1)$ Ki, et on le découpe en 8 sous-chaînes de 6 bits.

Chacune des sous-chaînes de 6 bits est transformée par une fonction non linéaire fixée en une sous-chaîne de 4 bits. [**6**]

Les sous-chaînes de 4 bits sont réordonnées suivant une permutation fixée.

d- Advanced Encryption Standard (A.E.S)

L'AES a été retenu par le NIST (National Institue of Standard and Technologie) comme un nouveau standard de chiffrement, il est plus puissant et plus sûr que le DES. Il chiffre les blocs de 128bits avec clés varies entre 128, 192 ou 256 bits.

L'AES est un chiffrement itératif effectue plusieurs tours (itérations) d'une même composition de transformation. Le nombre de tours n=10 pour une clé de 128bits et n=14 pour une clé de 256bits. [**7**]

Structure générale :

→ AddRoundKey Addition initiale de clé

Nr - 1 rondes, chacune constituées de 4 étapes :

SubBytes : substitution non-linéaire via S-Box.

ShiftRows : transposition matricielle par décalage à gauche

MixColumns : produit matriciel sur colonne

AddRoundKey Addition avec les octets des sous-clés

FinalRound : ronde finale (sans MixColumns)

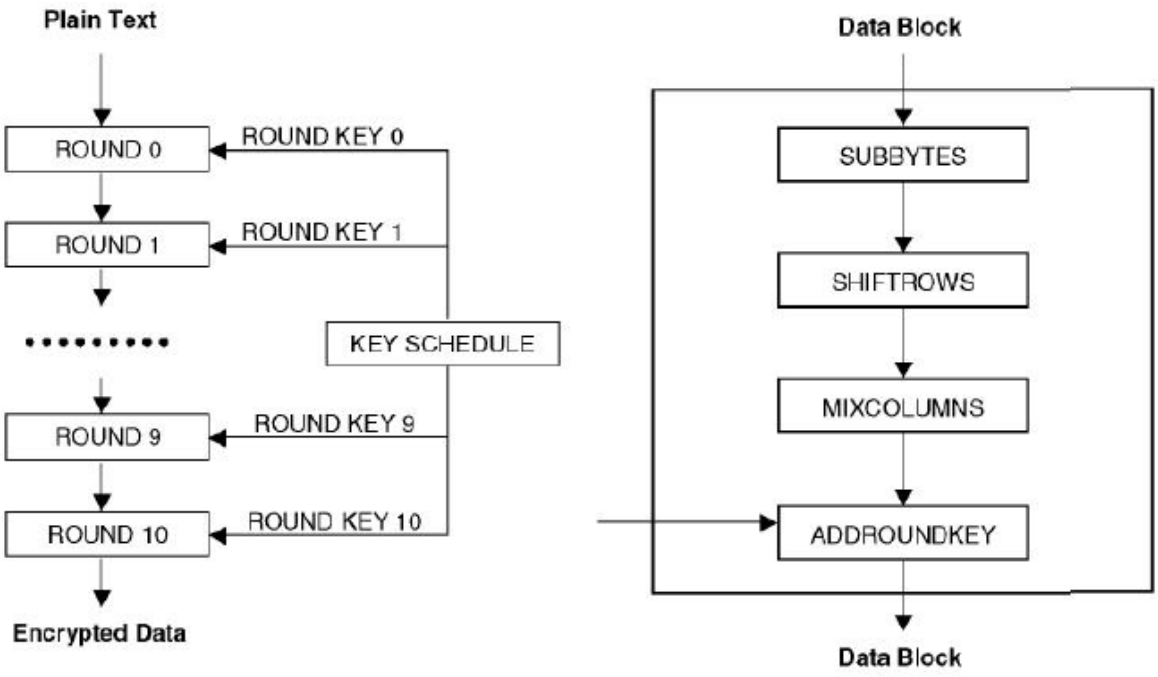


Figure I. 8 Algorithme A.E.S

4.2- La cryptographie asymétrique (clé publique) :

4.2.1 Principe

Le **chiffrement à clé publique, ou chiffrement asymétrique**, a été proposé par Diffie et Hellman, 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, Cette clé peut être conservée sur une carte à puce ou sur un token USB.

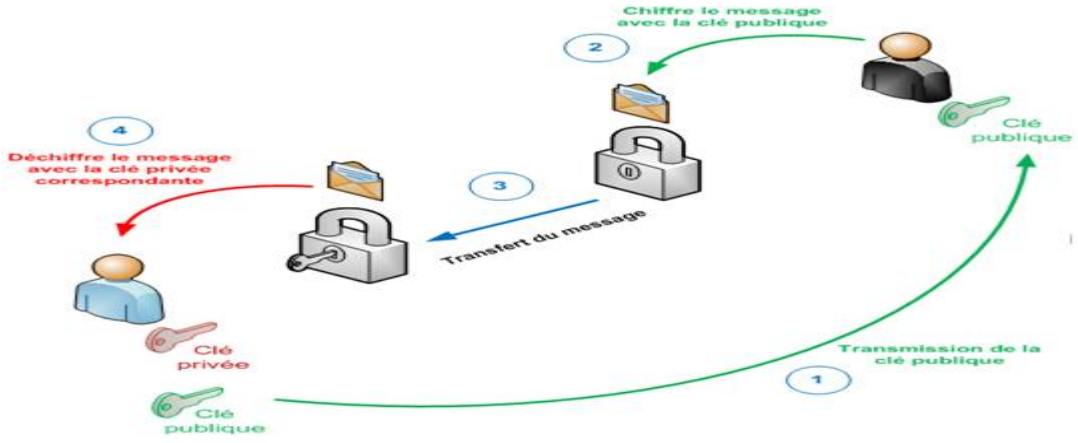


Figure I. 9 Chiffrement à clé publique.

Parmi les algorithmes qui utilise le chiffrement asymétrique on a le RSA :

4.2.2 Algorithme RSA (*R*ivest *S*hamir *A*dleman)

Cet algorithme est inventé par **R**ivest, **S**hamir et **A**dleman en 1978. C'est l'algorithme à clé publique le plus commode qui existe. Il est basé sur le calcul exponentiel.

Sa sécurité repose sur la factorisation unidirectionnelle suivante, le calcul du produit de deux nombres premiers est aisé. La factorisation d'un nombre en ses deux facteurs premiers est très complexe. [**8**]

RSA est aujourd'hui utilisé dans une large variété de produits (téléphones, réseaux internet, …), de logiciels de différentes marques (Microsoft, Sun, …) et enfin dans les télécommunications.

Le protocole RSA

● Génération des clés

– Générer deux grands nombres premiers p et q

– Soit n = pq – Soit m = (p-1)(q-1)

– Choisir un nombre e premier avec m (choix fréquent : e = 3)

– Trouver d tel que de mod m = 1

● Clés obtenues

– Clé publique : (e,n)

– Clé privée : (d,n)

● Cryptage et décryptage

– Cryptage : y = xe mod n

– Décryptage : x = yd mod n

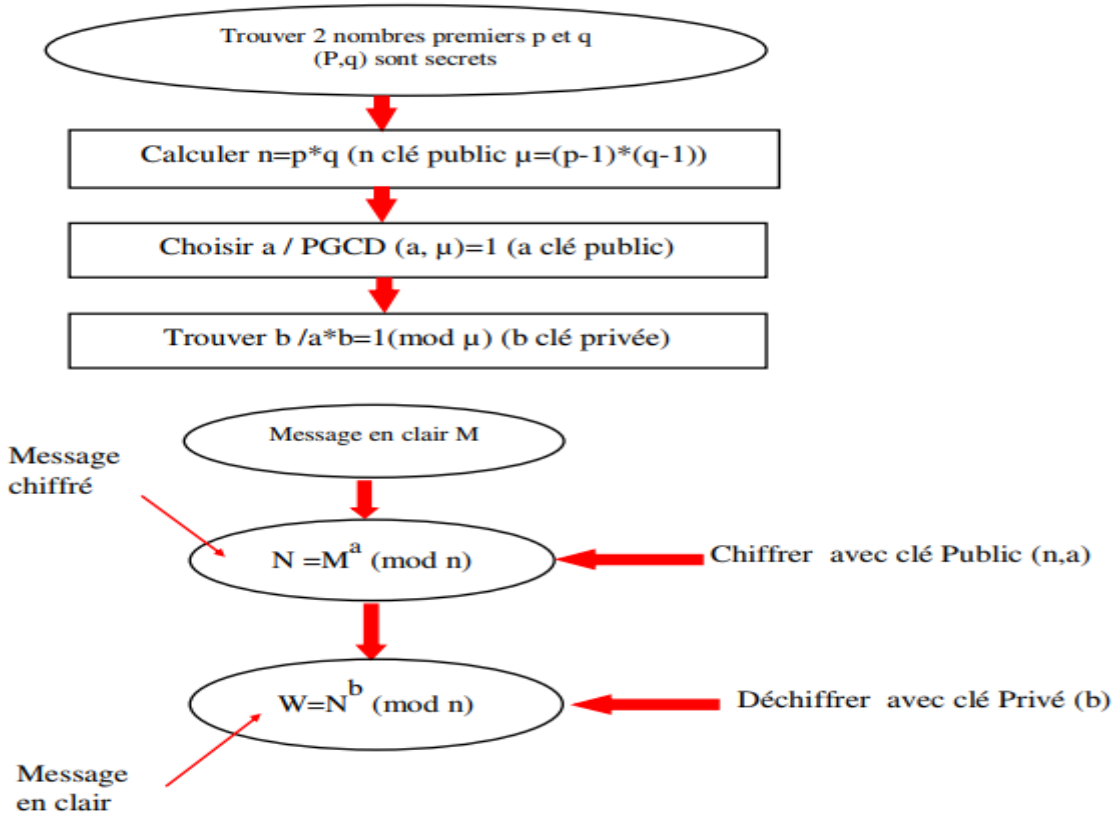


Figure I. 10 Principe de R.S.A

4-3- Cryptographie hybride

La cryptographie hybride utilise des algorithmes à clé publique et des algorithmes à clé privée, d'où l'adjectif hybride. Ce faisant, il combine les avantages des deux systèmes et pallie à certains inconvénients. En effet, un chiffrement hybride est rapide mais ne présente pas de faiblesse au niveau de la clé comme un chiffrement à clé publique. En effet, un algorithme symétrique oblige à conserver la clé sur le disque dur ou sur une clé USB, ce qui implique un risque qu'un pirate s'infiltre dans la mémoire de l'ordinateur ou du support USB pour avoir accès à la clé.

La plupart des systèmes hybrides fonctionnent de la manière suivante. Une clé aléatoire (ou pseudo-aléatoire) est générée pour l'algorithme symétrique (par exemple AES). Elle varie généralement entre 128, 256 ou 512 bits selon les algorithmes. Le destinataire génère alors une clé publique et une clé privée. La clé publique sert à chiffrer la clé aléatoire. Etant donné que cette dernière est courte, la chiffrer est rapide, alors que chiffrer le message avec un algorithme asymétrique aurait été bien plus long. Il ne reste plus qu'à envoyer le message chiffré accompagné de la clé chiffrée correspondante. Le

destinataire utilise alors sa clé privée pour déchiffrer la clé aléatoire. Avec cette dernière, il retrouve le message via un déchiffrement symétrique.

Les plus classiques de ces logiciels sont GnuPG (GNU Privacy Guard) et PGP (Pretty Good Privacy). Ces logiciels sont notamment très utilisés pour sécuriser les envois de courriels. PGP joui depuis longtemps d'une grande popularité en raison de son efficacité et de son développeur, Philip Zimmerman.

GnuPG s'est quant à lui fait une réputation en sa qualité d'algorithme stable et libre, inclus dans les systèmes d'exploitation libres (par exemple Linux). Il a également été intégré dans Mozilla Firefox, Thunderbird et bien d'autres logiciels libres. [**9]**

4-4 Cryptographie quantique :

4-4-1 définition :

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.

4-4-2 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. Dans la section suivante, nous ne présenterons que le plus célèbre des protocoles (BB84), les autres protocoles pouvant être consultés dans la référence [**10**].

4.4.3 Protocole BB84

C'est le tout premier protocole de distribution quantique des clés. Le but du protocole BB84 proposé en 1984 par Charles Bennett et Gilles Brassard est de permettre à deux utilisateurs, Alice et Bob, d'échanger une clef aléatoire et secrète pouvant être utilisée ensuite pour crypter un message selon le code de Vernam. Le protocole nécessite que les deux utilisateurs aient accès à un canal quantique et à un canal classique. Voici les étapes du protocole :

1. Alice génère et envoie à Bob par le canal quantique une suite de photons polarisés dont la polarisation est choisie aléatoirement parmi les éléments des bases rectilinéaires et circulaires.

2. Bob reçoit les photons et pour chacun décide de mesurer la polarisation selon la base rectilinéaire ou circulaire.

3. Bob annonce à Alice par le canal classique la base choisie pour mesurer la polarisation de chacun des photons.

4. Alice et Bob comparent leurs résultats en communiquant par le canal classique et rejettent tous les cas où Bob n'a pas fait le bon choix pour la base.

5. Alice et Bob déterminent s'ils ont été espionnés, par exemple en comparant publiquement quelques données d'un sous-ensemble choisi aléatoirement parmi l'ensemble de leurs données restantes après l'étape 4.

6. Si le test montre de manière évidente qu'il y a eu espionnage (taux d'erreurs dépassant un seul), alors Alice et Bob rejettent les données échangées et recommencent à l'étape 1. Autrement Alice et Bob conservent les données restantes de l'étape 5 et interprètent alors, par exemple, la polarisation horizontale et circulaire-droite comme un bit de valeur 0 et la polarisation verticale et circulaire-gauche comme un bit de valeur 1. Ces bits forment la clé sécrète connue d'Alice et Bob seulement. Il est à noter qu'à aucun moment Alice et Bob n'ont échangé les informations sur le contenu des messages. Ils n'ont échangé que sur les bases. [10]

4.5 Chiffrement basé sur le chaos

Dans certain cas, la cryptanalyse peut se baser sur la répétabilité du signal transmis car les algorithmes de cryptage produisent des suites de nombres pseudo aléatoires. Il est alors possible de reconstruire la clé à partir du signal crypté. Pour éviter ce type de faille, il faut donc que la clé ait une dimension suffisamment complexe pour que même à long terme, on ne puisse pas remonter au code. Le principe serait alors de se servir, en guise de clé, d'un bruit aléatoire évoluant dans le temps dont on connaît les caractéristiques. Les signaux chaotiques offrent cette possibilité. Les systèmes chaotiques sont en fait des systèmes déterministes pseudo-aléatoires dont les propriétés remarquables sont de nos jours exploitées à des fins de sécurisation des données. Deux approches sont utilisées : la première exploite les propriétés pseudo-aléatoires des orbites générées par itération des systèmes chaotiques discrets pour chiffrer des données.

La seconde approche est simple et directe. Elle consiste à mélanger l'information avec une séquence chaotique issue d'un émetteur, décrit généralement par une représentation d'état avec le vecteur d'état. Seule la sortie de l'émetteur est transmise au récepteur. Le récepteur a pour rôle d'extraire l'information originale du signal reçu. La récupération de l'information est généralement basée sur la synchronisation des états de l'émetteur et des états du récepteur [10].

4.5- Fonction d'Hachage

Une fonction de hachage H est une application facilement calculable qui transforme une chaîne binaire de taille quelconque « t » en une chaîne binaire de taille fixe « n » ; appelé empreinte de hachage (résumé, ou condensé)

Les algorithmes de hachage les plus utilisés actuellement sont :

- MD5 (Message Digest)
- SHA-1 (Secure Hash Algorithm 1)
- SHA-2 (Secure Hash Algorithm 2)
- RIPEMD-160 (Ripe Message Digest)

En expédiant un message accompagné de son haché, il est possible de garantir l'intégrité d'un message, c'est-à-dire que le destinataire peut vérifier que le message n'a pas été altéré durant la communication. Lors de la réception du message, il suffit au destinataire de calculer le haché du message reçu et de le comparer avec le haché accompagnant le document. Si le message (ou le haché) a été falsifié durant la communication, les deux empreintes ne correspondront pas.[11]

4-6 Certificat électronique

Les certificats électroniques sont utilisés principalement pour assurer l'authentification. Le certificat est en quelque sorte une carte d'identité numérique. Pour en obtenir un, il faut s'adresser à une autorité de certification (Certificate Authority, ou CA).

« Un certificat est un document numérique qui contient toutes les coordonnées d'un interlocuteur utiles pour communiquer avec d'autre, ainsi que sa clé publique ». [12]

4-7 Signature électronique :

Une signature électronique doit garantir deux propriétés : elle doit identifier le signataire du document, et garantir que le document n'a pas été altéré depuis l'apposition de la signature. Pour cela, les caractéristiques suivantes doivent être respectées :

- Une signature est authentique. L'identité du signataire doit pouvoir être retrouvée de manière certaine.
- Une signature ne peut être falsifiée (imitée), quelqu'un d'autre ne peut se faire passer pour un autre.

- Une signature n’est pas réutilisable. Elle fait partie du document. Elle n’est pas déplaçable sur d’autre document.
- Un document signé est inaltérable. Le document signé ne peut plus être modifié.
- Une signature ne peut pas être reniée.
- Dans les signatures on utilise généralement les crypto-systèmes à clé publique et les fonctions d’hachage à sens unique.

En pratique ce n’est pas le document à transmettre qui est directement signé, mais son empreinte.

C’est la clé privée d’Alice qui est utilisé pour générer la signature d’un document (à partir de son empreinte). On garantit ainsi que seul Alice a pu signer le document ; et on vérifie la validité de la signature grâce à la clé publique d’Alice qui tout le monde peut la connaître.[7]

CONCLUSION :

Dans le présent chapitre nous avons présenté quelques définitions et notions sur la cryptographie moderne, qui est sans doute la technique la plus utilisée dans le cadre des réseaux filaires et des réseaux sans fil traditionnels disposant d’une capacite de calcul et de mémoire conséquente. Les solutions de cryptographie sont réputées comme des solutions sûres qui répondent à l’ensemble des problèmes liés à la sécurité des données.

Chapitre II

Introduction aux systèmes chaotiques

Introduction

Les différentes possibilités d'utiliser les signaux chaotiques en cryptographie s'articulent aujourd'hui autour de deux directions principales de travail : l'utilisation de chaos pour crypter les messages à transmettre et l'utilisation de chaos pour l'échange d'un secret commun servant de clé de communication entre interlocuteurs autorisés. Ces deux directions sont indépendantes et compatibles entre elles : elles peuvent donc être réunies au sein d'un même système final.

Plusieurs propriétés des systèmes chaotiques ont leurs contreparties correspondantes dans des systèmes de cryptage traditionnel, comme :

• Sensibilité aux conditions initiales • Dynamique déterministe et aspect pseudo aléatoire • Complexité de structure et complexité d'algorithme • Ergodicité.

1- Théorie du chaos :

Il n'existe pas de définition rigoureuse du chaos mais par chaos, il faut admettre la notion de "phénomène imprévisible et erratique". Cependant, depuis une vingtaine d'années, on attribue le terme chaos à des "comportements erratiques qui sont liés à des systèmes simples pouvant être régis par un petit nombre de variables entre lesquelles les relations décrivant leur évolution peuvent être écrites. Ces systèmes sont donc déterministes bien qu'imprévisibles. La théorie du chaos, déjà entrevue par Jacques Hadamard et Henri Poincaré au début du XXe siècle, a été définie à partir des années 1960 par de nombreux scientifiques.

On appelle chaotiques des phénomènes complexes, dépendant de plusieurs paramètres et caractérisés par une extrême sensibilité aux conditions initiales : par exemple, les volutes décrites par la fumée d'une cigarette, ou la trajectoire d'un ballon qui se dégonfle. Ces courbes ne sont pas déterminées, modélisées par des systèmes d'équations linéaires ni par les lois de la mécanique classique ; pourtant, elles ne sont pas nécessairement aléatoires, relevant du seul calcul des probabilités : elles sont liées au chaos dit déterministe.

L'imprédictibilité est présente dans de tels systèmes, qui n'en sont pas moins munis d'un ordre sous-jacent. Les signaux chaotiques peuvent être obtenus à partir de circuits non linéaires où interviennent des paramètres.

Géométriquement, ces phénomènes dynamiques sont représentés dans un espace dont la dimension, qui peut être supérieure à celle de l'espace à trois dimensions, dépend du nombre de paramètres choisis pour les décrire. À chaque instant, l'état du phénomène est représenté par un point dans cet espace appelé espace des phases. L'évolution du système est décrite par la trajectoire de ce point. Pour les phénomènes les plus simples, ce point est attiré vers un point d'équilibre ou une courbe limite, près desquels il repasse périodiquement. Les mathématiciens appellent ces courbes limites des attracteurs étranges. [13]

1.1- Système Dynamique Non Linéaire

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

Mathématiquement, un système dynamique est décrit par un problème où seules sont données les valeurs de départ des variables d'état. Il peut avoir une composante de temps "discrète" ou "continue".

Une classe importante de phénomènes naturels peut être décrite par un ensemble de *p* équations différentielles ordinaires du premier ordre du type :

$$\frac{d}{dt} X_i(t) = F_i(X_j(t), \Lambda)$$

$$X \in IR^p,\ p \geq 1 \text{ et } i, j = 1,..,p$$

P représente la dimension du système. La fonction F dépend des variables du système et du vecteur de paramètres qui conditionne le comportement du système. Si F ne dépend pas explicitement du temps, mais seulement de X, le système est dit autonome. Mais on peut également rendre compte de l'évolution d'un système dynamique au moyen d'une application à temps discret :

$Xn+1 = T(Xn, \Lambda)$, $Xn \in IR^p$ ($p > 1$), *n* est un entier naturel, X0 est la condition initiale et L le vecteur de paramètres de la récurrence. Le débat entre modèle discret et modèle continu n'est pas aussi anodin qu'on pourrait le croire. Dans le cas continu (équations différentielles), il faut un minimum de 3 équations autonomes pour faire apparaître un comportement chaotique. Par contre, un modèle discret peut générer du chaos à partir d'une seule équation. Dans la suite de cette communication nous ne considérerons que les systèmes à temps discrets.[13]

1.2 Sensibilité aux Conditions initiales

La sensibilité aux conditions initiales **(S.C.I)** est une caractéristique fondamentale des systèmes dynamiques. Il faut entendre ici qu'un système réagira de façon totalement différente selon la condition initiale. Ceci a notamment comme conséquence le fait qu'un système chaotique, même si toutes ses composantes sont déterminées, est totalement imprévisible car sensible à d'infimes perturbations initiales.

Attracteurs étranges et chaos ont permis de mieux comprendre des phénomènes comme l'apparition de la turbulence en hydrodynamique, les perturbations orbitales dans le système solaire, et la météorologie, qui permet de bien illustrer la dépendance sensitive des conditions initiales, comme l'a fait Edward Lorenz dans sa célèbre remarque que «le battement des ailes d'un papillon aura pour effet après quelque temps de changer complètement l'état de l'atmosphère terrestre».[14]

1.3- Attracteur :

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 considérer. 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.[7]

1.4- Espace des phases

Les trajectoires dynamiques des systèmes chaotiques sont fréquemment situées dans un espace appelé espace de phase. Les régions de l'espace sans l'existence permanente

des dynamiques chaotiques seront inutiles puisque les points dans ces zones tendent vers l'infini et ne contribuent pas à la continuité du processus chaotique. Les variables qui construisent cet espace doivent contenir toute information sur la dynamique du système. On forme alors des équations chaotiques fonctionnant avec ces coordonnées dans l'espace et chaque itération de ces équations signifie l'incrémentation au temps suivant.[14]

2- Génération du chaos

Il existe plusieurs systèmes chaotiques qui sont utilisés pour générer les signaux chaotiques. Dans ce paragraphe, nous présenterons deux classes : les systèmes chaotiques continus et les systèmes chaotiques à temps discret.[14]

2-1 Systèmes chaotiques continus

2-1-1- Attracteur de Lorenz

Cet exemple a été publié en 1963 dans un journal météorologique. L'attracteur de Lorenz est généré par le système d'équations suivant :

$$\begin{cases} \dot{x} = -\sigma x + \sigma y \\ \dot{y} = \rho x - y - xz \\ \dot{z} = -\beta z + xy \end{cases}$$

Les paramètres σ, β et ρ sont des réels strictement positifs.

Le chaos est obtenu pour les valeurs suivantes : $\sigma > \beta+1$; $\rho > 0$ et $\rho > \frac{\sigma(\sigma+\beta+3)}{\sigma-\beta-1}$

La figure II.1 illustre l'attracteur de Lorenz en 3 dimensions x(t), y(t) et z(t) tel que σ = 10, β = 8/3 et ρ = 28.

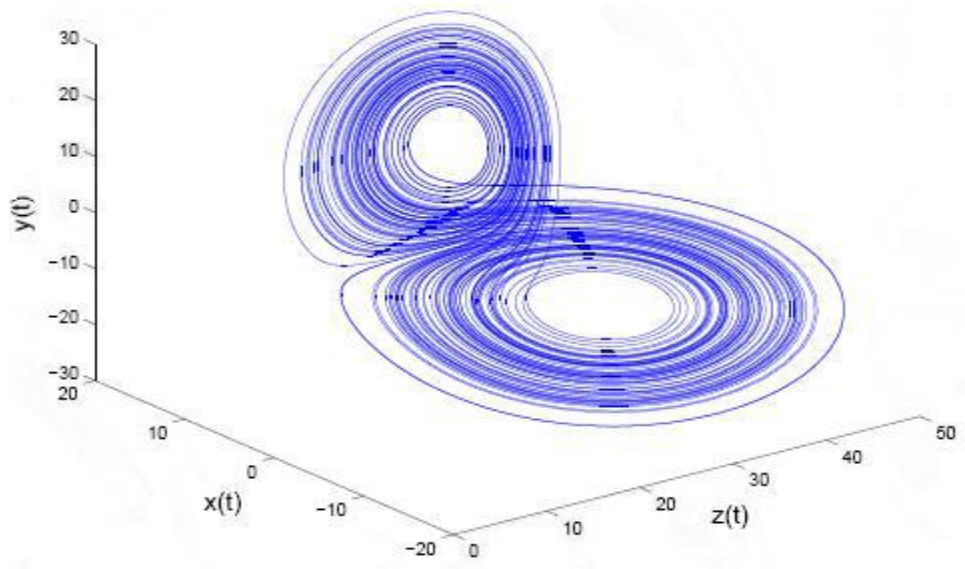


Figure II. 1 : **Attracteur de Lorenz.**

2-1-2- Attracteur de Rössler

Proposé par l'Allemand Otto Rössler, le système de 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.

$$\begin{cases} X' = -(Y + Z) \\ Y' = X + aY \\ Z' = b + Z(X - c) \end{cases}$$

Les dérivées des premiers membres sont des dérivées partielles par rapport au temps.

a, *b* et *c* sont des constantes réelles. Sauf précisions contraires, on prendra désormais : $a = 0.398$, $b = 2$ et $c = 4$. On est alors en présence d'un système chaotique.

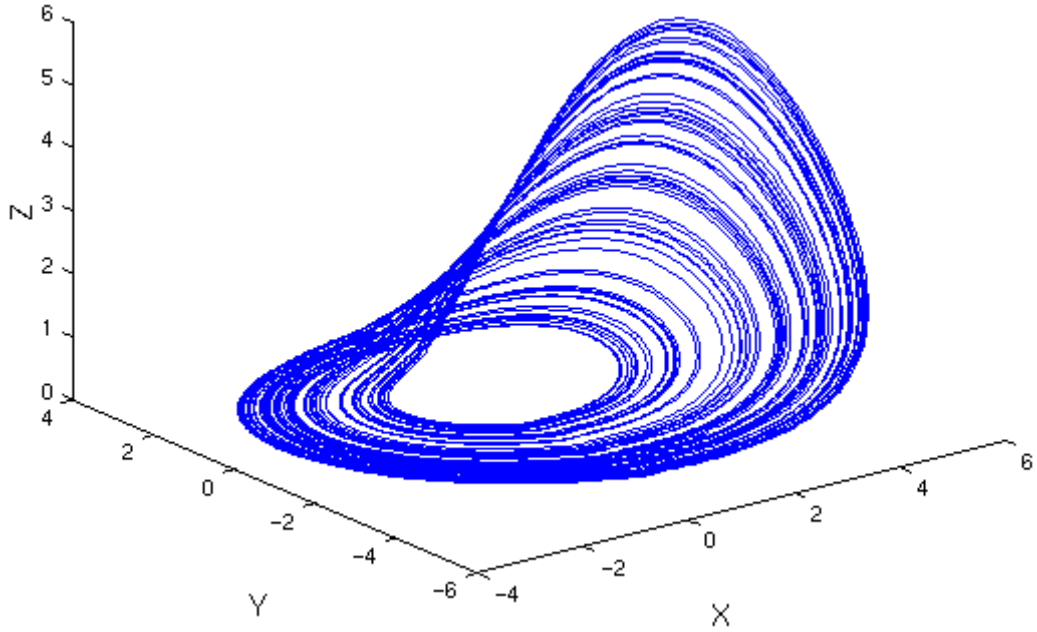


Figure II. 2: **Attracteur de Rössler.**

2-1-3- Système de Chen

Il est donné par le système d'équations suivant :

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

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

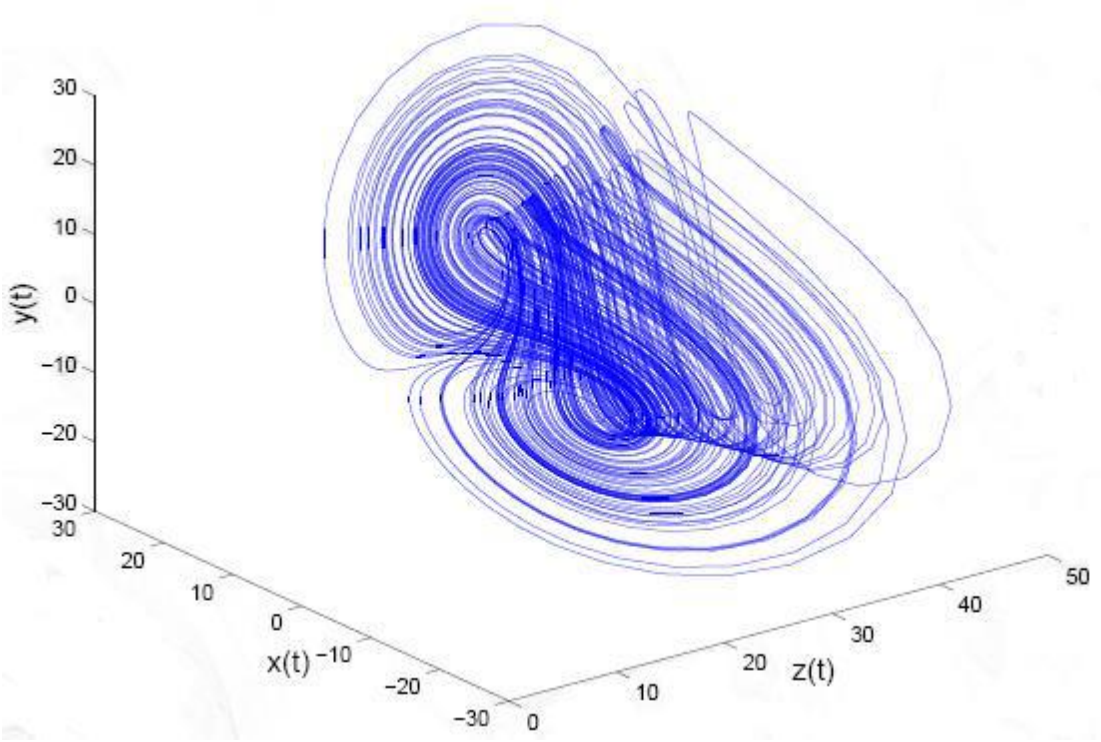


Figure II. 3 Attracteur de Chen.

2-1-4- Système de Chua

Il est donné par le système d'équations suivant :

$$\begin{cases} \dot{x} = p(-x + y - f(x)) \\ \quad = p(-x + y - (m_o x + \dfrac{(m_1 - m_o)(|x+1| - |x-1|)}{2}) \\ \dot{y} = x - y + z \\ \dot{z} = -qy \end{cases}$$

$f(x)$ est la caractéristique non linéaire de la diode du circuit de Chua, avec *m0* et *m1* des constantes négatives. On prend $p = 10$, $m0 = -0.7$, $m1 = -1.3$ et $q = 15$. La figure II.4 représente l'attracteur de Chua.

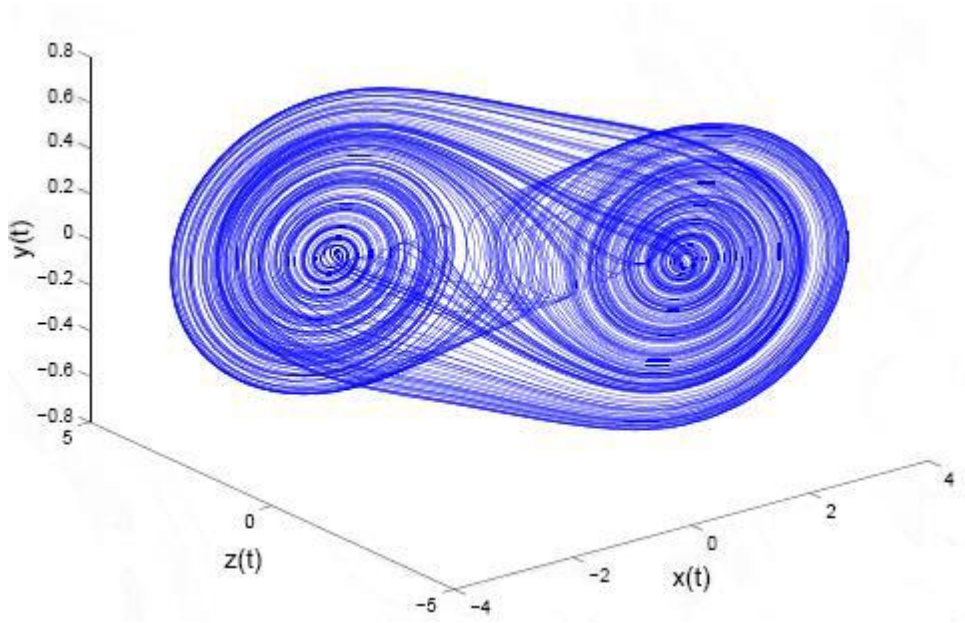


Figure II. 4Attracteur de Chua.

2-2- Suites chaotiques à temps discret

2-2-1 Suite logistique (Logistic Map)

Cette fonction est donnée par l'équation suivante :

$$Xn + 1 = r\,Xn(1 - Xn)$$

Xn est compris entre 0 et 1 et r est un nombre positif compris entre 1 et 4. Le comportement est chaotique à partir de r égal à 3.6.
La figure II.5 illustre le diagramme de bifurcation (Xn en fonction de r).

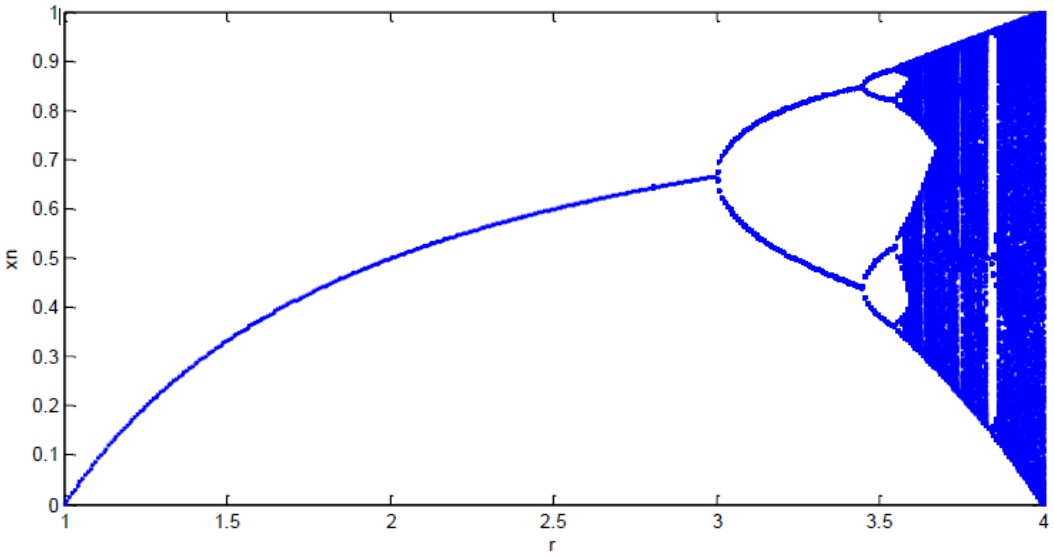


Figure II. 5 Diagramme de bifurcation.

2-2-2 La récurrence de Hénon

Ce système est un modèle proposé en 1976 par le mathématicien Michel Hénon. L'intérêt de ce modèle est l'étude de certaines propriétés d'une section de Poincaré de l'attracteur de Lorenz par l'introduction d'itérations dans le plan. Le modèle mathématique de ce système est donné par :

$$\begin{cases} x_{k+1} = a - x_k^2 + b.y_k \\ y_{k+1} = x_k \end{cases}$$

Les valeurs des paramètres proposées par Michel Hénon pour observer le phénomène chaotique sont : a =1.4 *et* b= 0.3, Pour simuler l'attracteur de Hénon on a pris pour conditions initiales ($x0$=0, $y0$=0). Ainsi la figure II.6 représente l'attracteur de Hénon.[15]

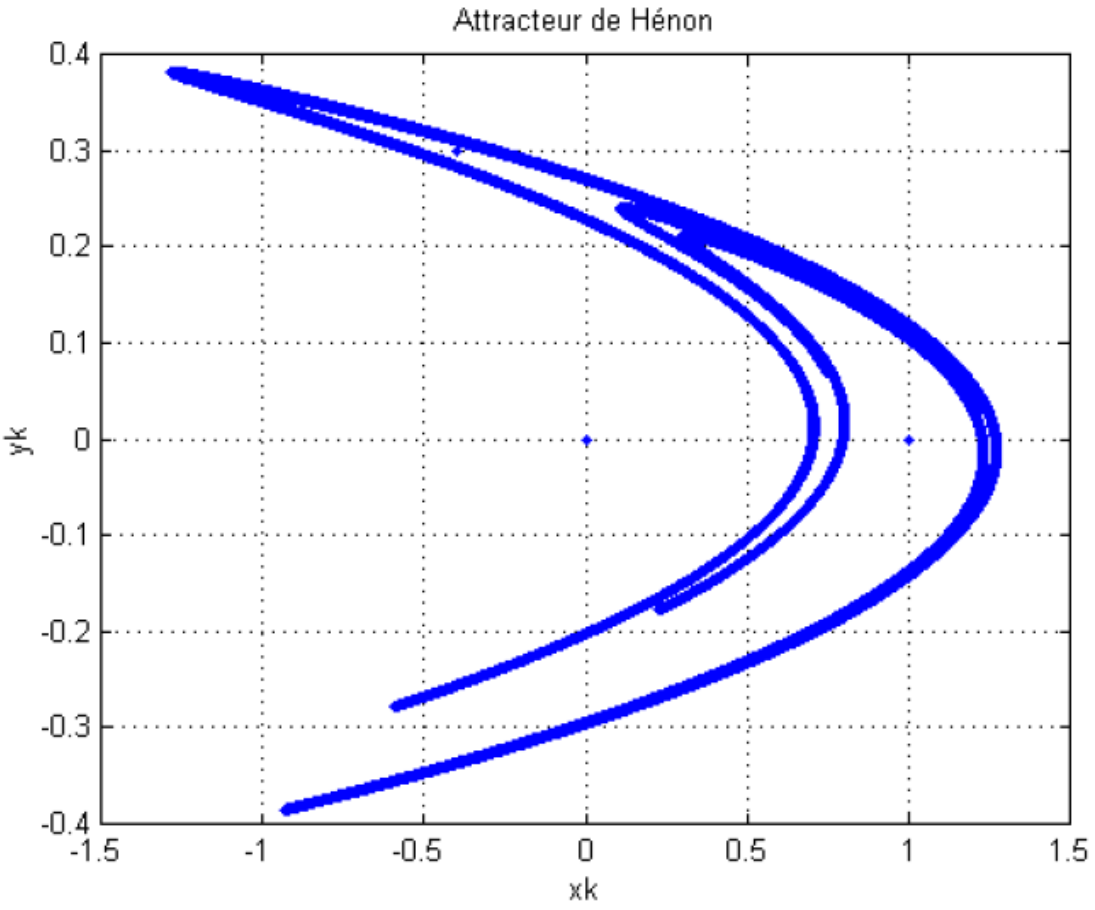


Figure II. 6: Attracteur chaotique de Hénon

3- Relation entre le chaos et les crypto-systèmes :

Tout d'abord, nous notons qu'il y a une forte ressemblance entre les systèmes chaotiques et les crypto-systèmes symétriques à chiffrement par bloc. En ce qui concerne les caractéristiques particulières des systèmes chaotiques, notons qu'un système chaotique est constitué de quelques fonctions de base *f* qui sont itérées sur un ensemble *X*. Le fonctionnement d'un tel système consiste à remplir les conditions suivante : 1) soit un mélangeur, ceci signifie que l'ensemble *X* devrait être aléatoirement mélangé par la répétition de l'action de *f*, 2) soit sensible à l'état initial de telle sorte qu'une légère modification dans les états initiaux engendra des états complètement différents, 3) soit sensible aux certains paramètres de contrôle et un léger changement dans ces paramètres causera un changement dans les propriétés de la carte chaotique.

En comparant entres les particularités d'un crypto-système et les caractéristiques d'un système chaotique, il est évident que le chiffrage et le chaos montrent des similarités remarquables, si nous considérons que les données nettes correspondent à un état initial, la clef correspond à l'ensemble des paramètres, et la fonction de chiffrage correspond à la fonction de base *f*.

Cependant, il y a une différence importante entre ces deux concepts. En fait, le crypto-système travaille sur des ensembles finis (discrets), alors que le système chaotique est conçu pour travailler sur des ensembles infinis (continus). C'est probablement la raison principale pour laquelle la relation entre le chaos et le chiffrage a été restée inaperçue. [16]

4- Technique de cryptage

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

3-1- Principe du cryptage par chaos

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.

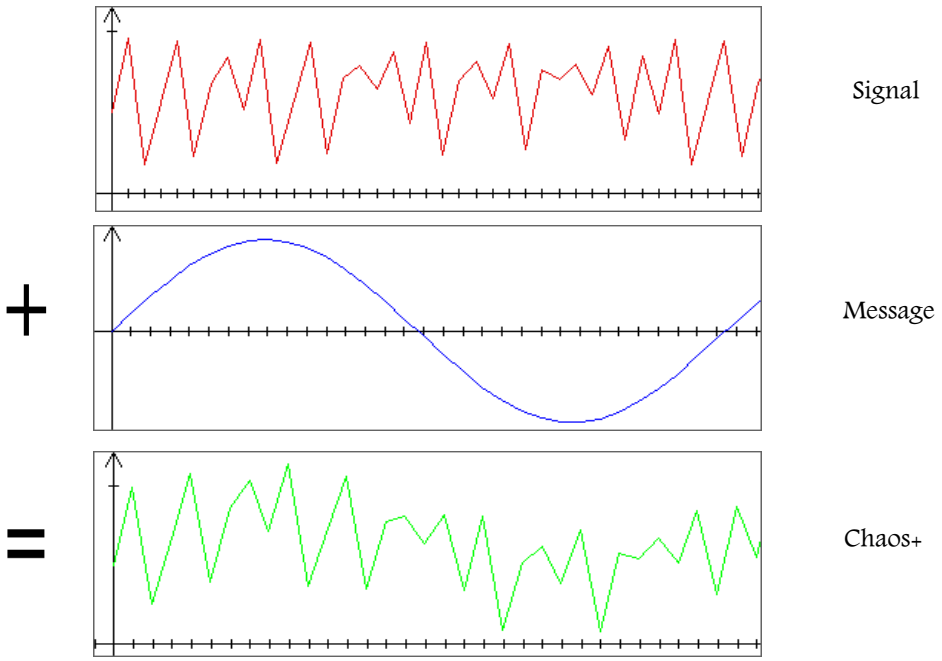


Figure II. 7 Message noyé dans un signal chaotique

3-2- Système de cryptage par chaos :

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 1 présente les différents éléments d'un système de cryptage symétrique basé sur le chaos.

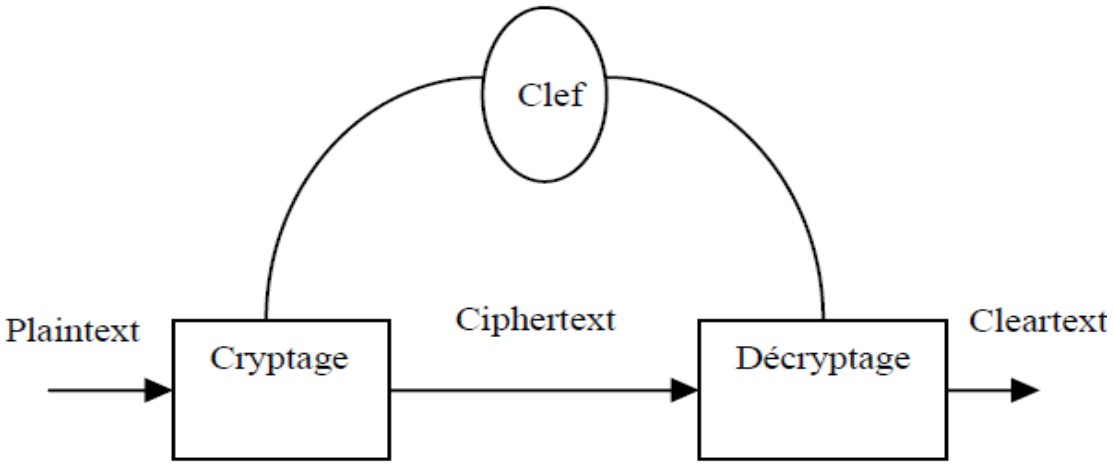


Figure II. 8 Système de cryptage symétrique

L'idée fondamentale exige que l'émetteur produise 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). [17]

5- 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. Le tableau suivant illustre parfaitement cette correspondance.[26]

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 II. 1: Correspondance entre la théorie du 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.

Tableau II. 2 Comparaison entre le chaos et la cryptographie

Conclusion

Dans le présent chapitre nous avons présenté quelques définitions et notions sur les systèmes chaotiques et nous avons mis l'accent sur leurs utilisations à des fins de chiffrement de données.

Dans le chapitre suivant nous allons implémenter deux méthodes de cryptage, la première méthode de Baptista pour crypter le texte et les images et la deuxième basée sur charte logistique et le générateur congruentiel linéaire.

Chapitre III

Implémentation

Introduction

Une alternative très prometteuse a été développée durant la dernière décennie, la cryptographie chaotique. Cette dernière a déjà donné la preuve de sa faisabilité et de sa puissance de chiffrage (supérieur à 1 Gbits/s).

Dans ce chapitre, nous allons présenter deux méthodes de cryptage : la première est méthode de cryptage de Baptista qui sera utilisé pour crypter et décrypter le texte et les images et la deuxième méthode basée sur la carte logistique chaotique et le générateur congruentiel linéaire. Nous présentons notre application réalisée et les différents outils nécessaires pour le développement.

1- Etude d'un crypteur/décrypteur de texte et image par la méthode de Baptista

1.1- Présentation de la méthode

La méthode de cryptage de Baptista est basée sur la propriété d'ergodicité de tout système chaotique qui exige qu'une unité simple dans un plaintext puisse être chiffrée dans un nombre infini de manières. C'est la raison pour laquelle cette méthode propose la possibilité de chiffrer un message en employant la carte logistique unidimensionnelle simple définie dans un intervalle E par : $Xn + 1 = b\,Xn\,(1-Xn)$ …. **(1)**

Où $X_n \in [0, 1]$, et le paramètre de contrôle *b* est choisi de façon que l'équation (1) aura un comportement chaotique. Pour un message composé par *S* caractères différents, l'intervalle E sera divisé en *S* sous intervalles de largeur ε, avec :

$\varepsilon = \frac{X\,max - X\,min}{S}$, et l'intervalle $[Xmin, Xmax]$ peut être l'ensemble E ou une partie de l'ensemble E.

Nous associons alors les *S* intervalles avec les *S* caractères différents. L'idée est de chiffrer chaque caractère du message comme nombre entier qui représente le nombre d'itérations effectuées dans l'équation logistique, afin de transférer la trajectoire à partir d'un premier état X_0 jusqu'à atteindre le sous intervalle lié à ce caractère. Si nous référerons à X_0 comme condition initiale chiffrant la première unité dans un plaintext, pour chiffrer la deuxième unité dans ce plaintext, nous utilisons comme état initial $X_0' = F^{C_1}(X_0)$ou F^{C_1}est la $C_1^{ème}$itération de l'équation (1).

Cette règle est alors simplement appliquée aux unités restantes dans le plaintext.

Fonction d'association

Les S associations entre les S intervalles et les S unités d'alphabet, l'état initial X_0 et le paramètre b seront utilisés par le récepteur pour déchiffrer le texte chiffré (récupérer le caractère original) en réitérant l'équation (1) autant de fois comme indiqué par le ciphertext (le nombre d'itérations).

Chaque unité de message chiffré doit satisfaire la condition $N0 \leq Ci \leq Nmax$. A partir de là, il existe beaucoup d'options pour chaque Ci dans $[N0, Nmax]$.

Dans le tableau 1, nous montrons la manière avec laquelle nous associons les unités d'alphabet au $S:$ [même127pdf]

Unité d'alphabet	Numéro d'emplacement	Intervalle correspondant
*	S	[Xmin +(S-1)ε, Xmin +Sε]
@	S-1	[Xmin +(S-2)ε, Xmin+(S-1) ε]
#	s-2	[Xmin +(S-3)ε, Xmin+(S-2)ε]
$	s-3	[Xmin +(S-4)ε, Xmin+(S-3)ε]
. . .	. . .	. . .
B	4	[Xmin +3ε, Xmin +4ε]
A	3	[Xmin +2ε, Xmin +3ε]
/	2	[Xmin +ε, Xmin +2ε]
%	1	[Xmin, Xmin +ε]

Tableau III. 1 Association entre les alphabets et les S intervalles.

1.2- Fonctions de cryptage et de décryptage de texte :

Pour la première application de notre méthode, nous choisissons de crypter et décrypter des fichiers textes (composé par un certain alphabet)

1- Fonction de chiffrement :

- Fixer les paramètres de système de cryptage : X_0=0.4320125, R=3.78

La fonction d'association entre les emplacements et les alphabets la fonction char(a_i) (char donne le code ASCII du caractère a_i)

L'intervalle [Xmin-Xmax], Xmin=0.2, Xmax=0.8 | $\varepsilon = \frac{Xmax-Xmin}{255}$

C : nombre entier pour calculer le nombre d'itérations

A : nombre entier reçoit le Code ASCII des caractères

Tab : Tableau d'entiers ou on stock le nombre d'itérations des cractères a_i

Pour i 1→0 jusqu'à Taille_Texte

faire début

A ← char(a_i)

Tanque (Condition) faire

début

*Xn ← R*X₀ *(1-X₀)*

X₀ ← Xn

C ← C + 1

Fin Tanque

Si $Xmin + A - 1 * \varepsilon < Xn < Xmax + A * \varepsilon$

Condition non vérifiée

Fin Si

Tab(i) ← C

Fin Pour

2-Fonction de déchiffrement :

Le décryptage de texte se fait en utilisant ces nombres d'itérations en commençant d'étirer C1 fois l'équation (1) à partir de l'état $X0$, (C1 est le nombre d'itérations correspondant à le premièr charactère dans le texte) pour arriver à déterminer l'intervalle associé au caractère. De la même façon, nous déterminons le reste des caractères du texte.

1.3- Fonctions de cryptage et de décryptage des images :

- Cryptage :

Pour appliquer la méthode de cryptage sur une image, nous faisons une association entre les niveaux des gris des pixels de l'image et les différents intervalles. Nous prenons chaque comme une matrice de N lignes et M colonnes, qui sera convertie en un vecteur de NxM pixels.

Le cryptage de cette image se fait en utilisant les mêmes clefs secrètes et les mêmes paramètres comme le cas précédent (cryptage de texte).

Après le cryptage, l'image est transmise sous la forme d'une série de NxM entiers tel que chaque entier représente le ciphertext (le nombre d'itérations) correspondant à un parmi les NxM colonnes de vecteurs des pixels (tout en conservant l'ordre).

- Décryptage :

Le décryptage des images se fait en utilisant ces nombres d'itérations en commençant d'étirer C1 fois l'équation (1) à partir de l'état $X0$, (C1 est le nombre d'itérations correspondant à la première colonne du vecteur NxM) pour arriver à déterminer l'intervalle associé au niveau de gris du premier pixel. De la même façon, nous déterminons le reste des pixels.[17]

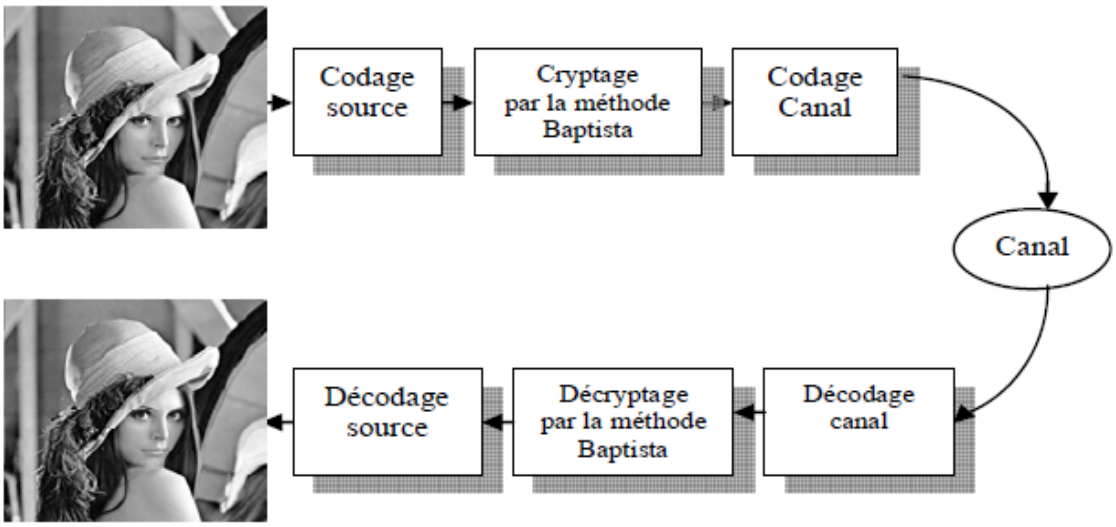


Figure III. 1Chaîne de transmission d'une image cryptée par la méthode de Baptista.

2- Notre schéma de cryptage des images basé de la carte logistique chaotique et le générateur congruentiel linéaire :

Dans le schéma proposé, nous avons utilisé deux algorithmes qui utilisent les formules mathématiques du « Chaotique carte logistique » et le « Générateur Congruentiel Linéaire » pour générer la clés pseudo aléatoire avec même taille d'image, puis faire l'opération XOR élément par élément entre image en clair et la clés pseudo aléatoire généré, afin d'obtenir une image cryptée.

Le but principal de ce chiffrement c'est, masquer les bits d'image en clair avec les bits de la clés pseudo aléatoire généré à travers l'opération OU-exclusif (ou XOR).

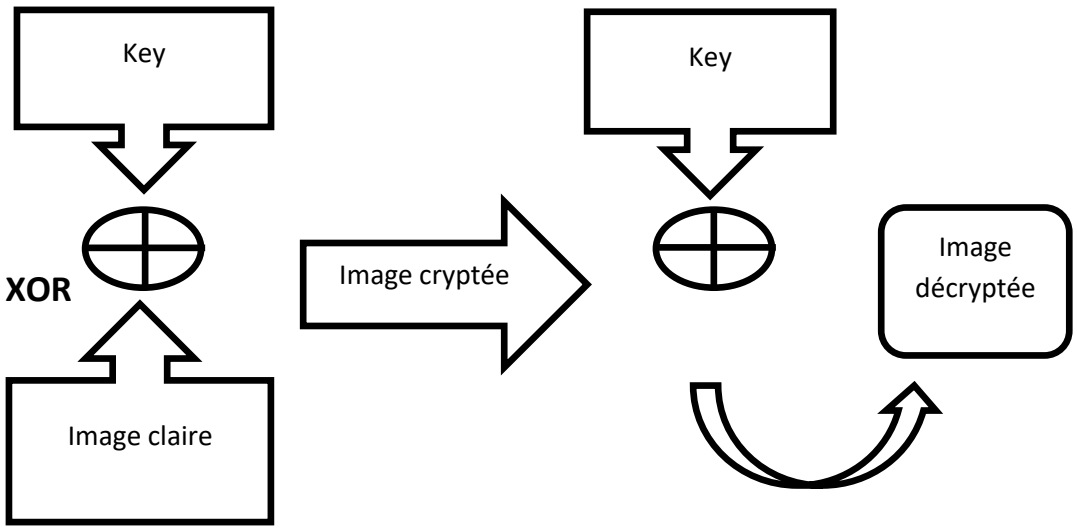


Figure III. 2 : Schéma de chiffrement proposé.

2-1 Générateur de clés pseudo aléatoire :

Dans notre cas, le générateur de clés pseudo aléatoire est réaliser par la combinaison OU exclusif (ou XOR) entre deux générateurs de nombres pseudo aléatoires qui utilisent des formules mathématiques sont les suivants :

1) Le premier générateur pseudo aléatoire appelé le générateur congruentiel linéaire (GCL ou LCG pour Linear congruential generator) :

$$Xn + 1 = (A\,Xn + C)\,Mod\,M \quad \text{..... (a)}$$

Les paramètres initiaux sont : (A, C, X_0), Où M = 255, (A, C, X_0) ∈ $\mathbb{N}$

2) Le deuxième générateur pseudo aléatoire appelé Chaotique carte logistique

$$Xn + 1 = rXn\,(1 - Xn) \text{ ..... (b)}$$

Les paramètres initiaux sont : (R, X), Où $0 < r \leq 4$ et $0 < X \leq 1$

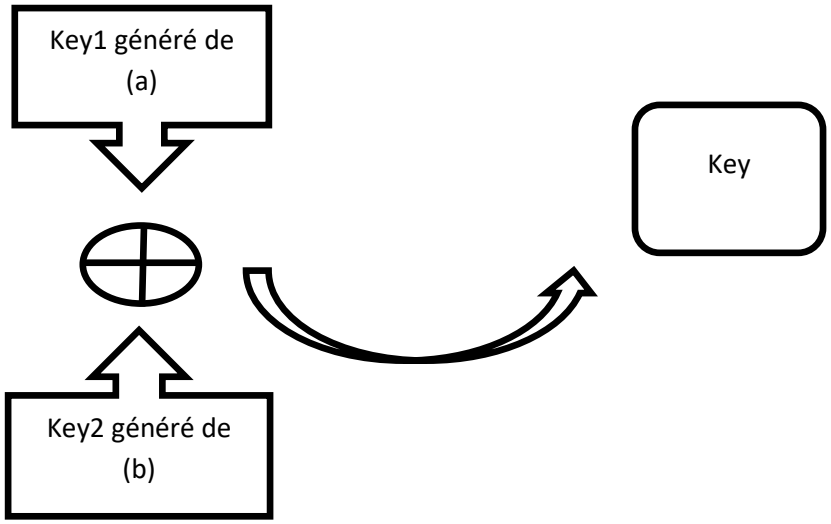


Figure III. 3: Générateur un flux de clés pseudo aléatoire proposé

2.2- Fonction de chiffrement

1) Générer la clés pseudo aléatoire :

- Définissez les valeurs initiales et le paramètre pour le générateur congruentiel linéaire (GCL ou LCG pour Linear congruential generator) (*A, C, X_0*) et la Carte Logistique Chaotique (R, *X*).

- Générer deux flux de nombre pseudo aléatoire à travers les formules mathématiques de LCG (Key1) et de Carte logistique chaotique (Key2), mais à condition que chaque flux généré doive être même taille d'image en clair *N*x*M*.

- Faire la combinaison OU-exclusif (ou XOR) octet par octet entre key1 et key2 généré Pour obtenir un flux de clés pseudo aléatoire (Clé). key = Key1 $\oplus$ Key2

2) Convertir l'image en clair en un tableau d'octets de taille NxM mi

3) Faire la combinaison OU-exclusif (ou XOR) octet par octet entre le tableau d'octets de l'image et la clés key. Pour obtenir un tableau d'octets qui représente l'image chiffrés (image chiffrée Ci) $C(i) = m(i) \oplus$ key(i).

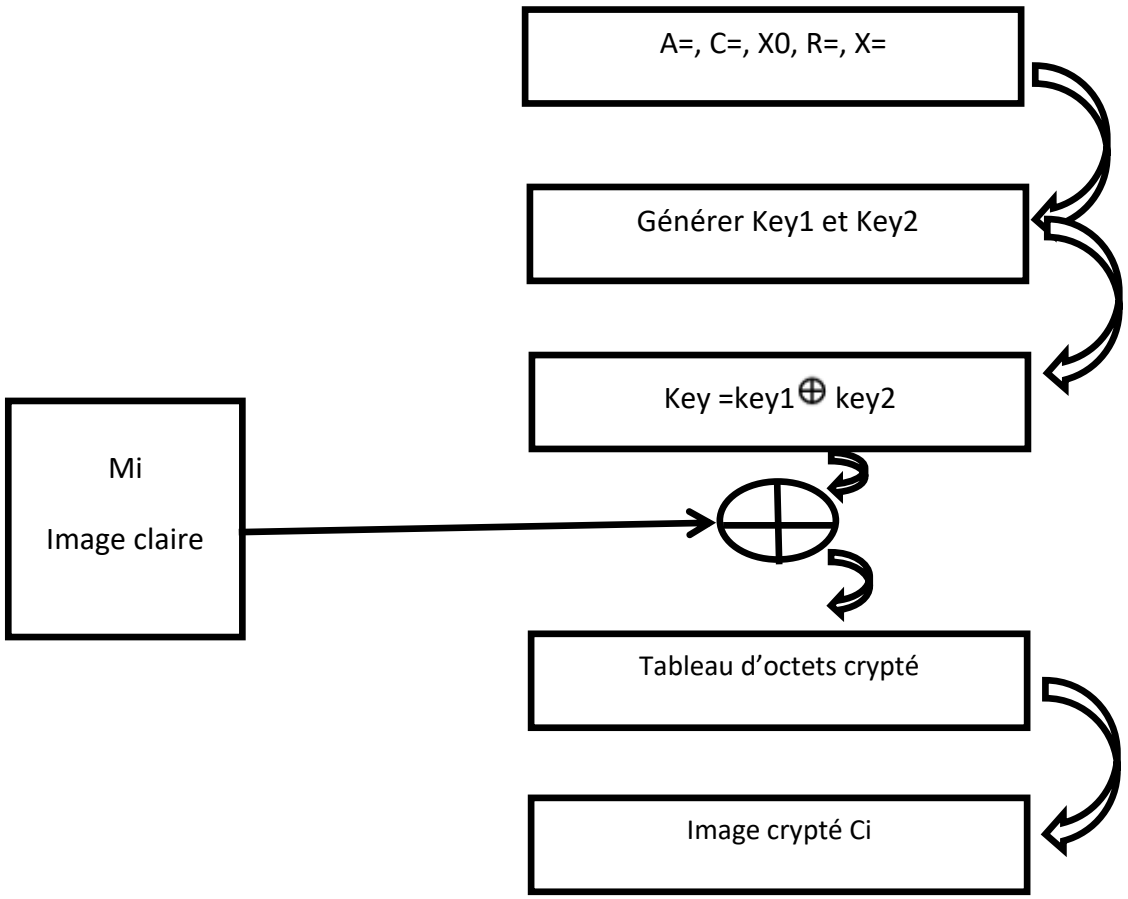


Figure III. 4 : Fonction de chiffrement.

2.3- Fonction de déchiffrement

1) Générer la clés pseudo aléatoire :

- Définissez les valeurs initiales et le paramètre pour le générateur congruentiel linéaire (GCL ou LCG pour Linear congruential generator) (A, C, X_0) et la Carte Logistique Chaotique (R, X).

- Générer deux flux de nombre pseudo aléatoire à travers les formules mathématiques de LCG (Key1) et de Chaotique Carte logistique (Key2), mais à condition que chaque flux généré doive être même taille d'image en clair NxM.

- Faire la combinaison OU-exclusif (ou XOR) octet par octet entre key1 et key2 généré Pour obtenir un flux de clés pseudo aléatoire (Clé). key = Key1 $\oplus$ Key2

2) Convertir l'image cryptée en un tableau d'octets de taille NxM ci

3) Faire la combinaison OU-exclusif (ou XOR) octet par octet entre le tableau d'octets de l'image chiffrée et la clés key. Pour obtenir un tableau d'octets qui représente l'image claire (image claire Mi) M(i) = C(i) $\oplus$ key(i).

3- Résultats expérimentaux

3.1- Environnement de développement

L'application a été créa depuis un PC Asus k55A :

- Mémoire : 6 Go RAM.
- Processeur : Intel ® Core™ i5-3210M CPU @ 2.50 GHZ (4 CPUs).
- Système d'exploitation : Windows 10 64 bits.
- Carte Graphique : Intel® HD Graphique 2Go.

3.2. Langage de programmation

Nous avons choisi le langage ***JAVA*** pour développer notre système. Ce choix de langage est motivé par les raisons suivantes :

 Java est organisée, il contient des classes bien conçu et bien reparties.

 Java est connu et donc plus de chance de trouver des développeurs java, pour concevoir ou amélioré une application.

 Java est portable (donc exécutable sur n'importe quel système, à condition d'avoir installé une JVM).

Nous avons exploité l'environnement de programmation ***Netbeans*** IDE. Et utilisé l'environnement ***SWING*** pour la réalisation de l'interface graphique.

3.3. Les interfaces du logiciel

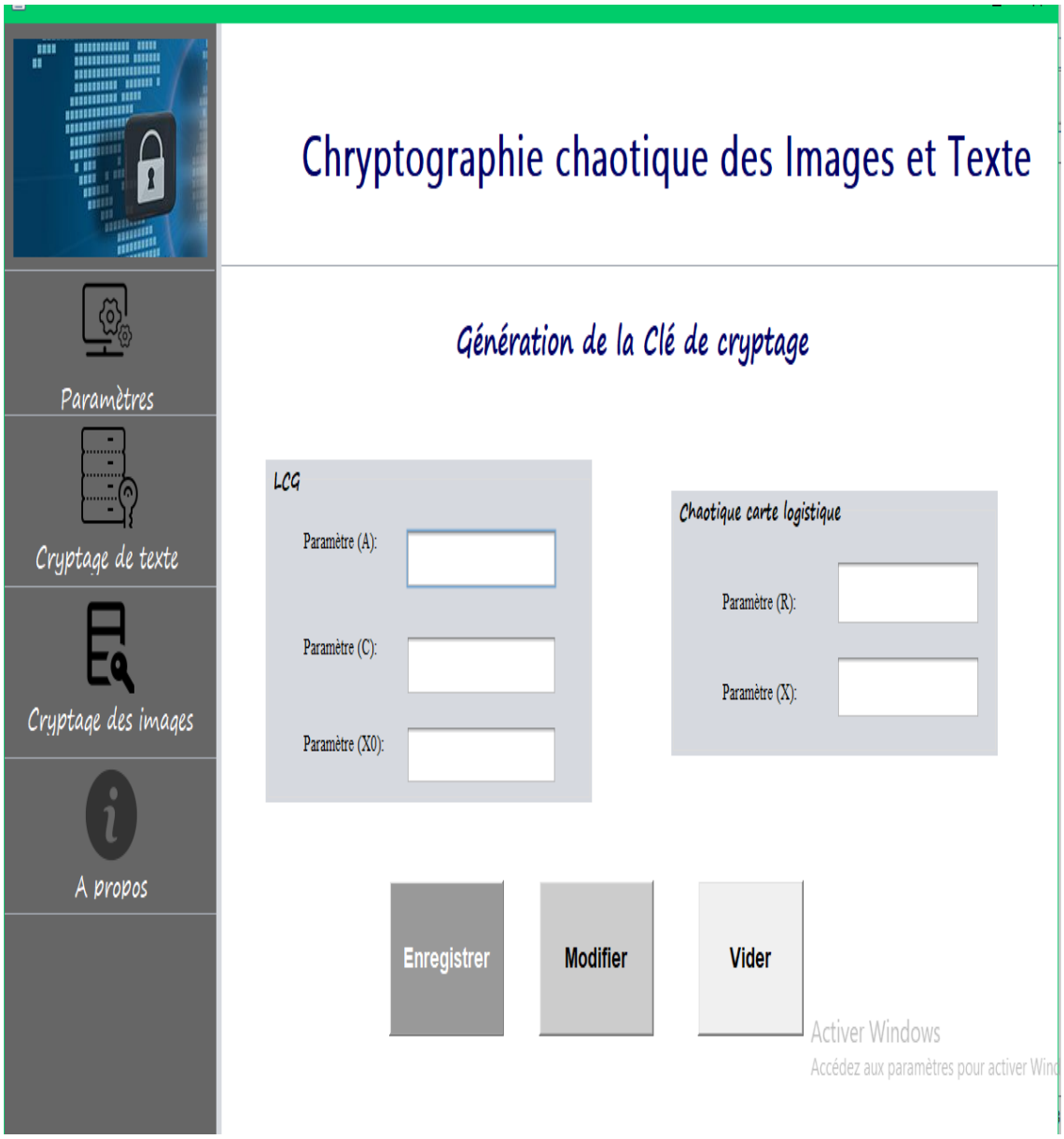


Figure III. 5 : Interface de paramétrage pour générer les clés.

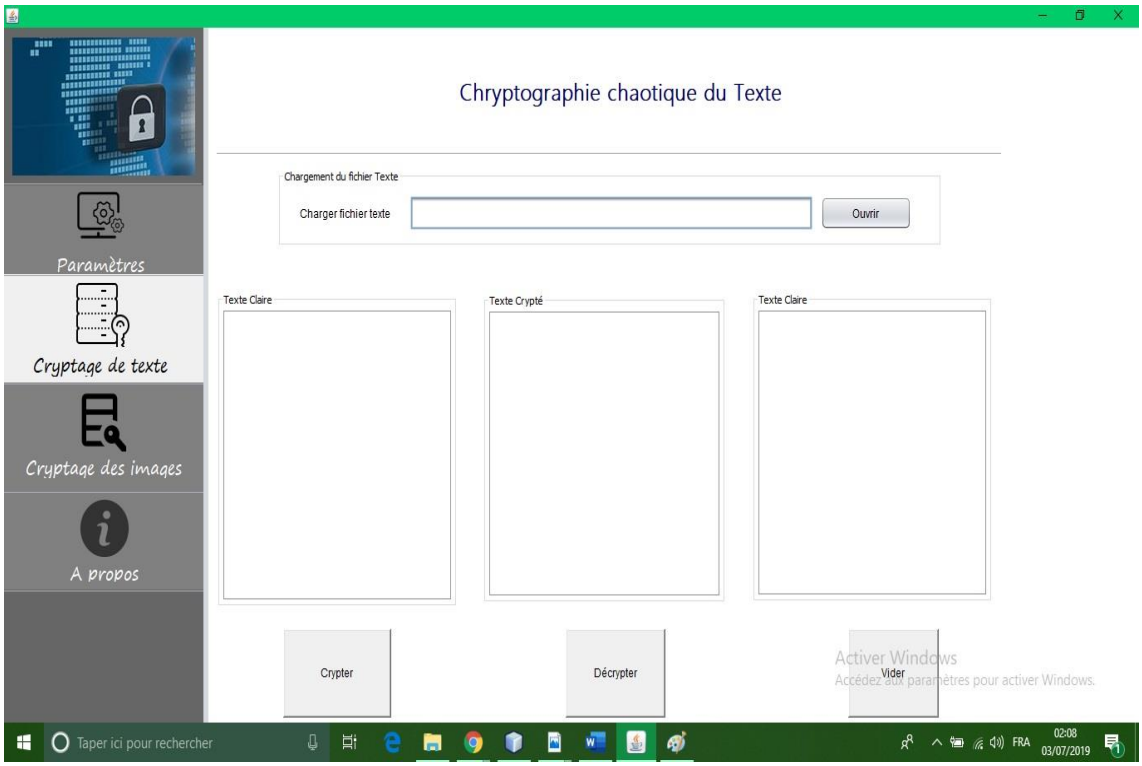


Figure III. 6: interface pour cryptage/décryptage du texte.

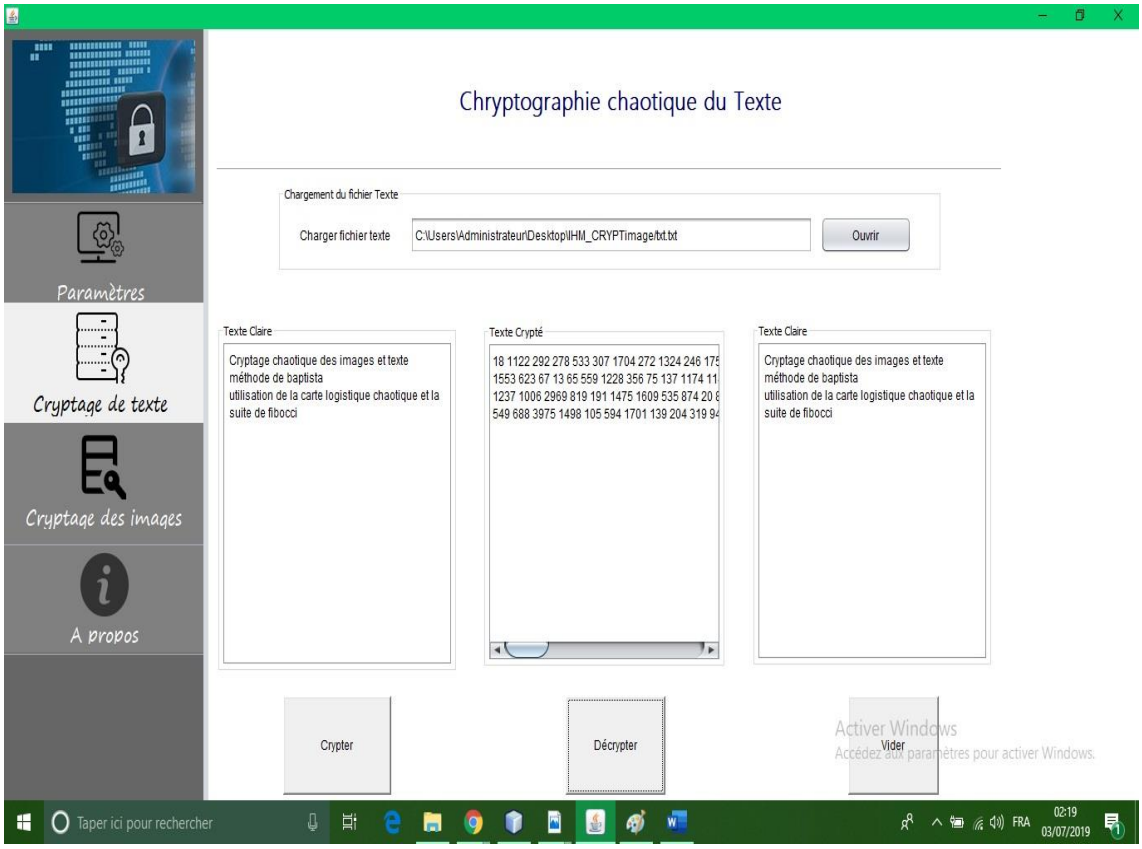


Figure III. 7 : exemple de cryptage/décryptage du texte.

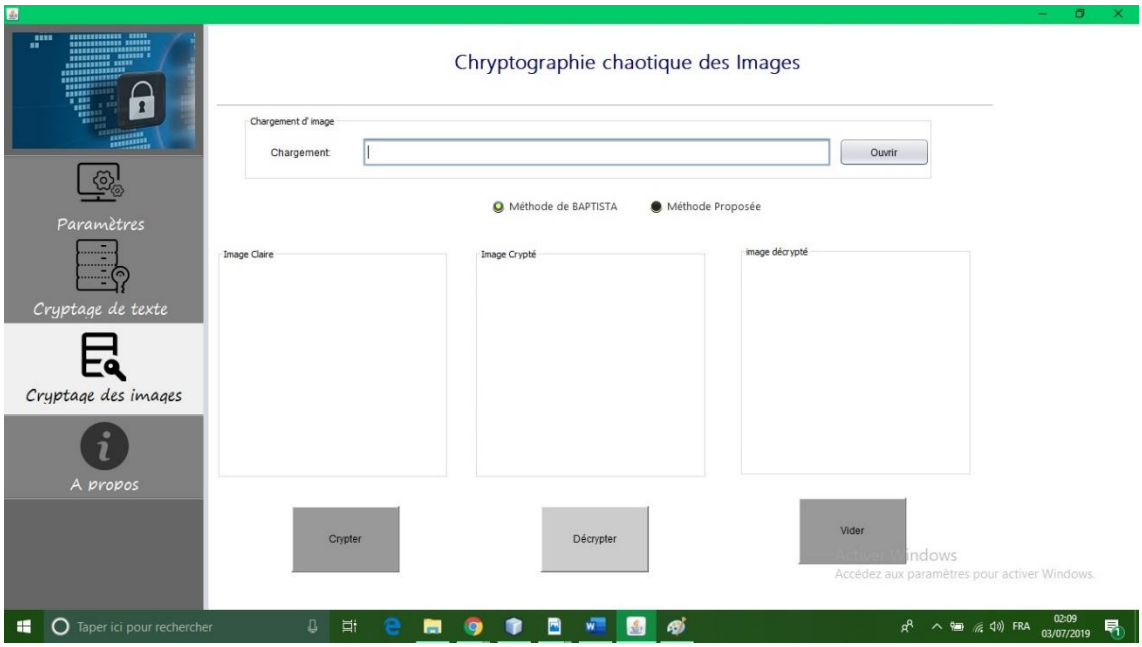


Figure III. 8 : interface pour cryptage/décryptage des images.

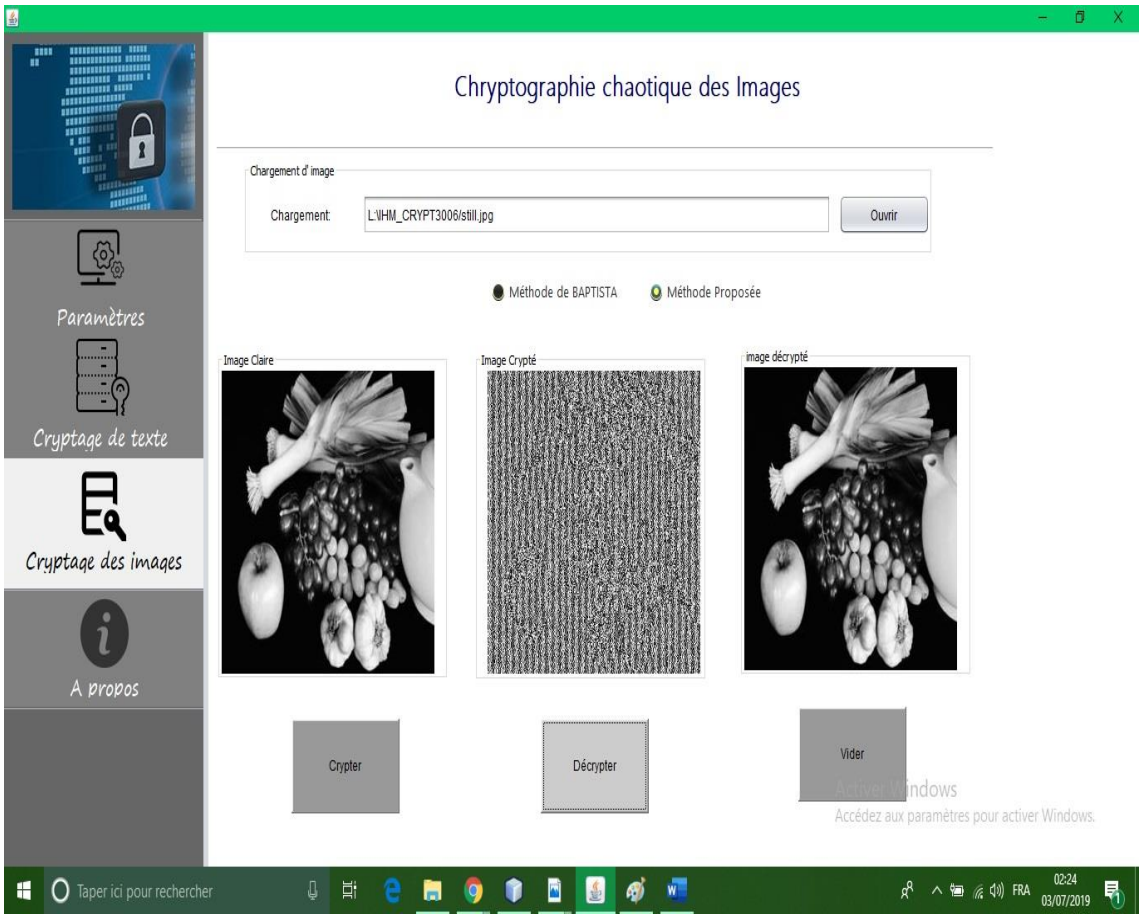


Figure III. 9 : exemple de cryptage/décryptage des images.

3.4- Résultats d'exécution :

- Cryptage du texte : (par la méthode de Baptista)

Soit le texte en clair « Cryptage chaotique des images et de texte ».

Le tableau suivant fait correspondre chaque caractère du message en clair avec la séquence obtenu après itération de l'équation (1). Les séquences obtenues correspondent au message chiffré.

18	1122	292	278	533	307	1704	272	1324	246	175	657	284	472
C	r	y	p	t	a	G	e		c	h	a	o	t
3031	1383	436	7	394	535	757	263	361	757	3276	408	497	1104
i	q	u	e		d	E	s		i	m	a	g	e
2389	226	268	452	17	799	206	954	963	226	113	1191	135	572
s		e	t		d	E		t	e	x	t	e	

Tableau III. 2 cryptages du texte avec r=3.78 et X0=0.4320125

-Décryptage du texte : (par la méthode de Baptista)

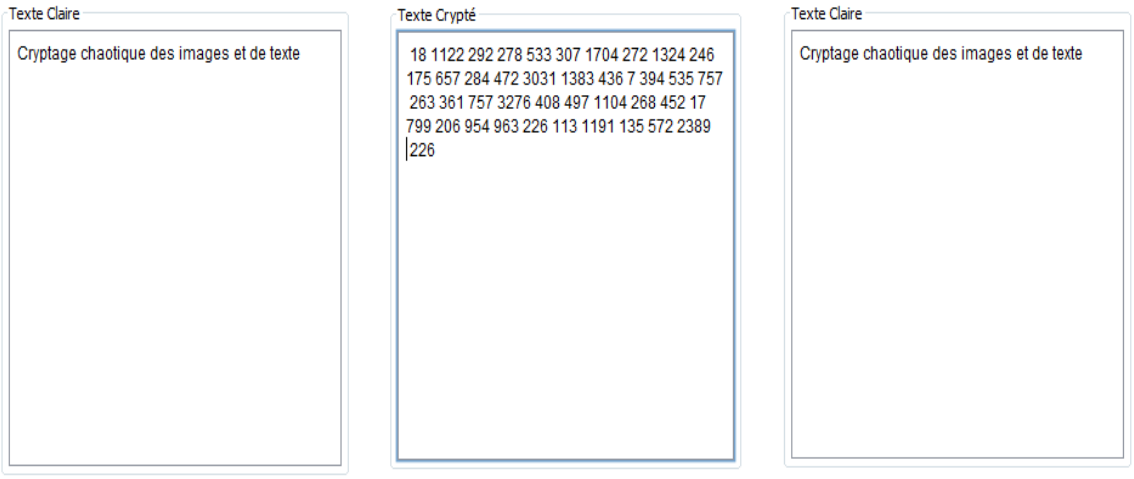


Figure III. 10 décryptage avec r=3.78, X0=0.4320125

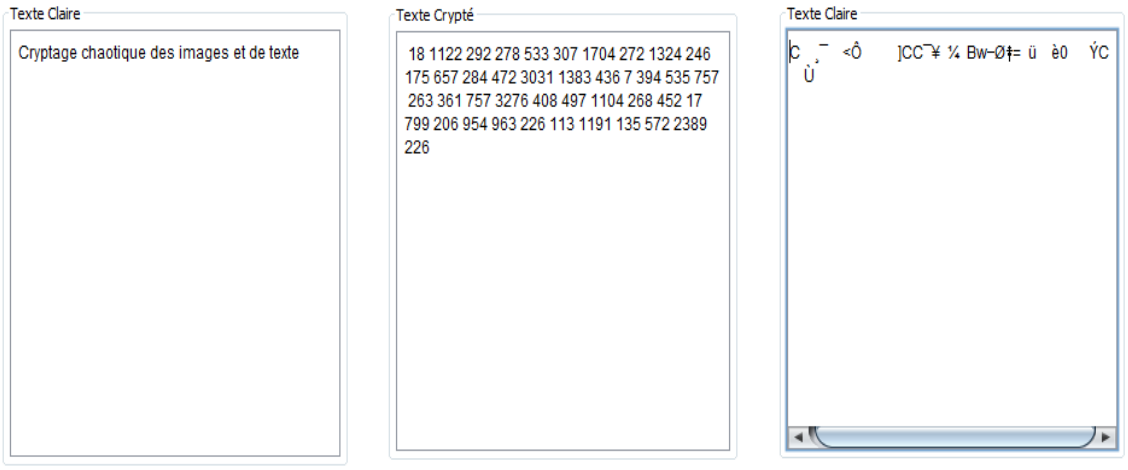


Figure III. 11 décryptage avec r=3.7800000001**, X0=0.4320125**

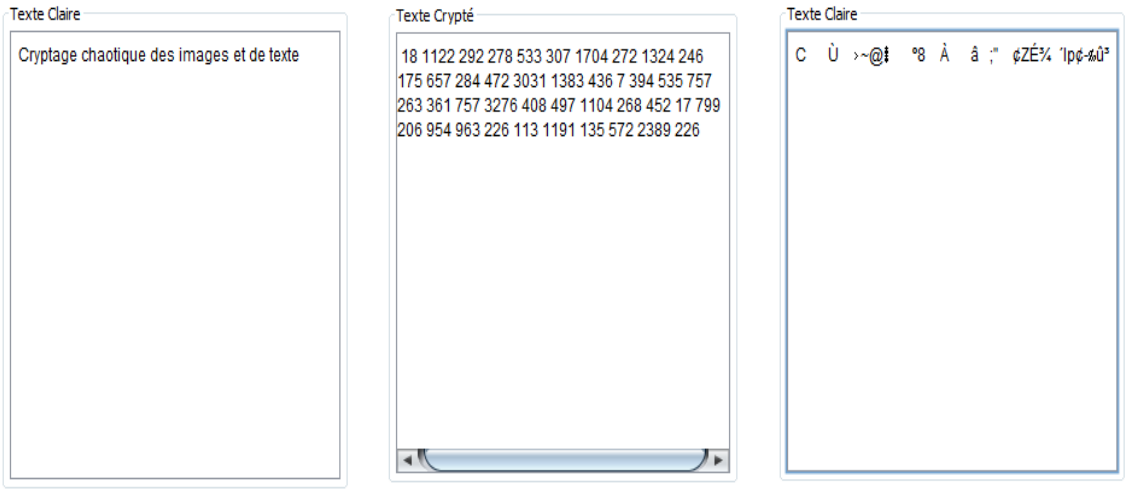
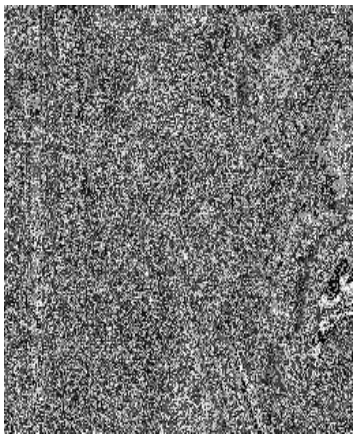
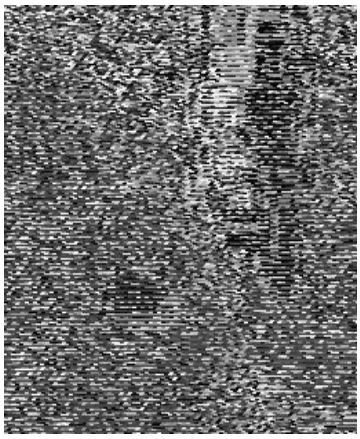
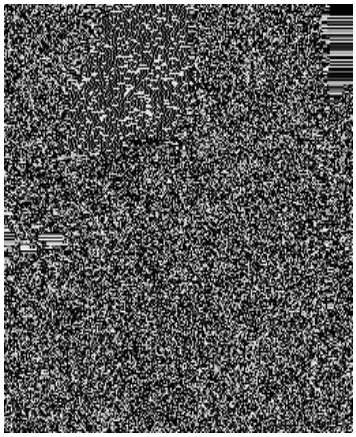


Figure III. 12 décryptage avec r=3.78, X0=0.432012500000001

D'après les tests de décryptage du texte, nous avons observez que la moindre modification dans les conditions initiales conduit à un mauvais déchiffrement.

-Cryptage des images : (par la méthode de Baptista)

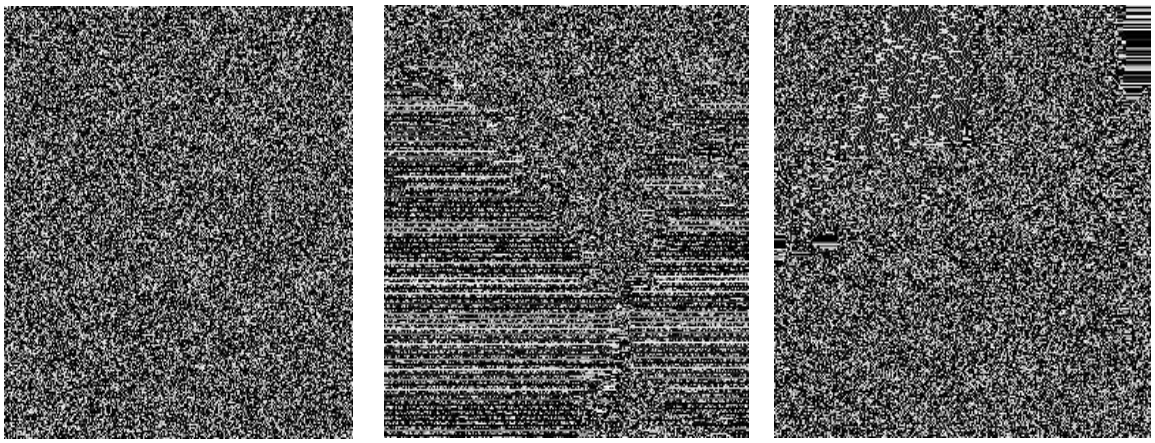


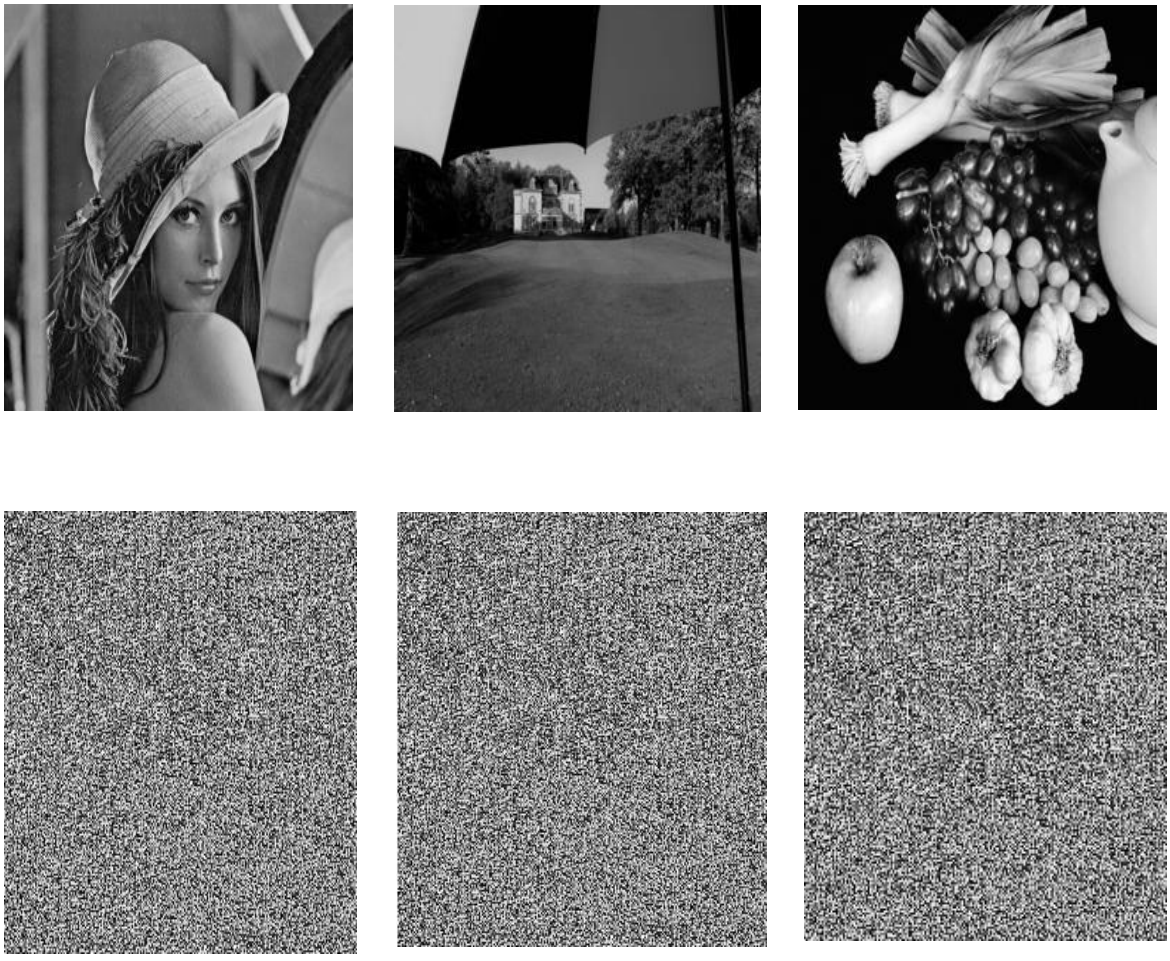
-Décryptage : avec les mèmes conditions initiales X0=0.4320125 et r=3.78



-Décryptage : avec d’autres conditions initiales X0=0.4320203 et r=3.8



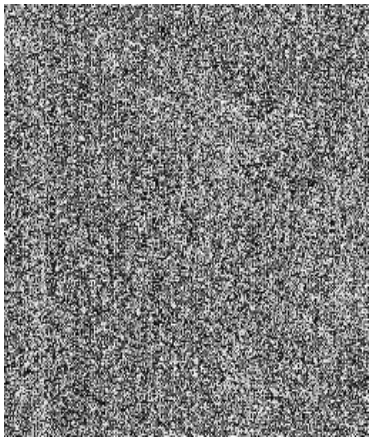
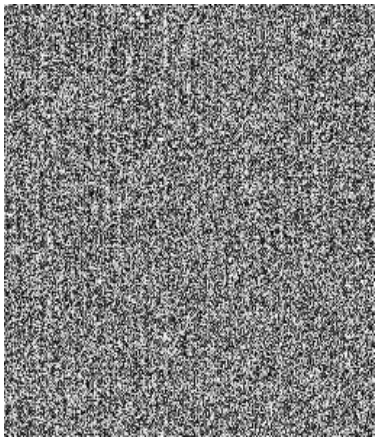
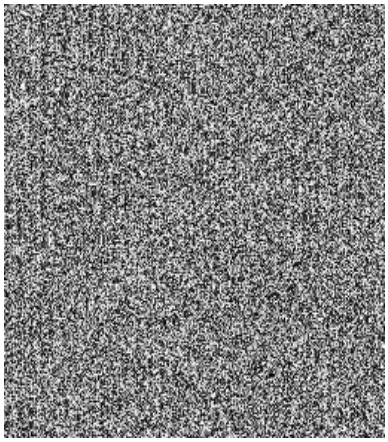
-Cryptage des images : (par notre méthode)



-Décryptage : avec les mèmes conditions initiales A=25, C=16, Xn_0=125, X0=0.4320125 et r=3.78



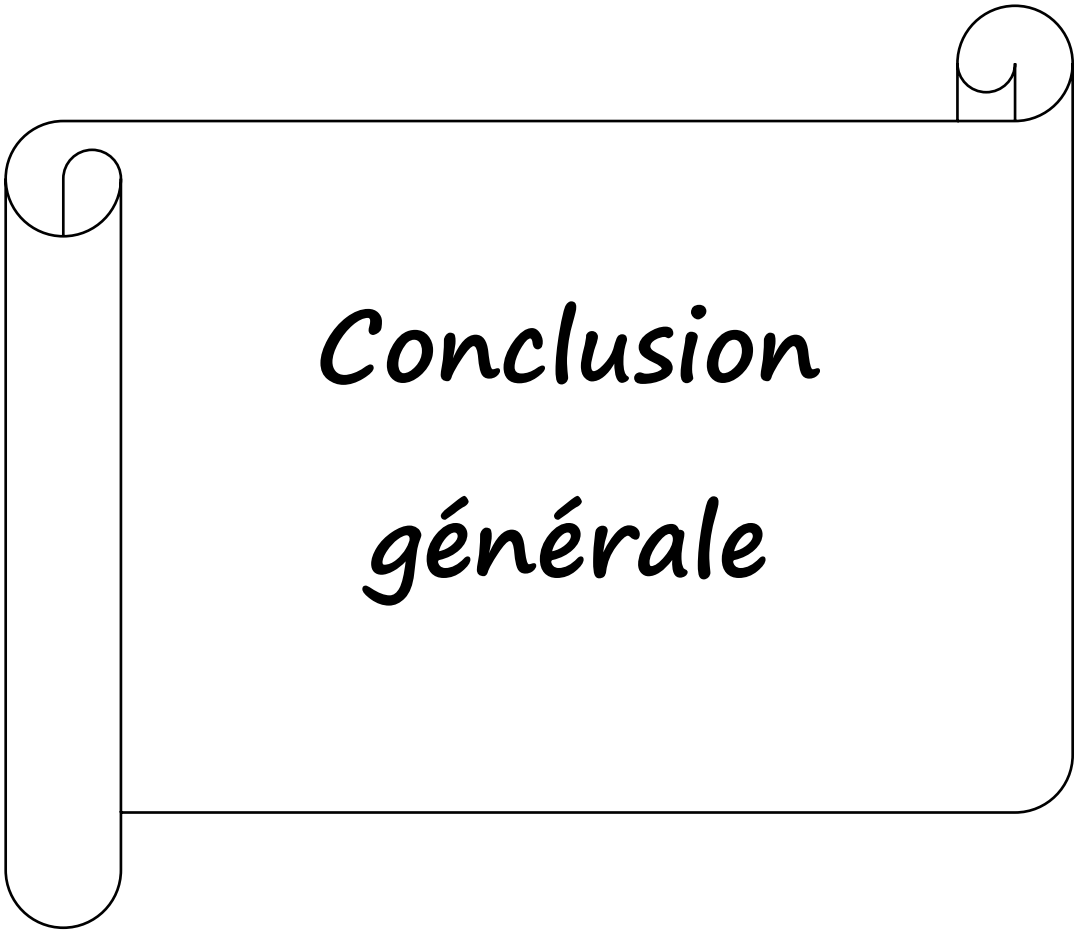
-Décryptage : avec d'autres conditions initiales A=20, K=20, Xn0=145, X0=0.4320123 et r=3.78

D'après les tests de décryptage des images avec les deux méthodes, nous avons observez que la moindre modification dans les conditions initiales conduit à un mauvais déchiffrement.

Conclusion :

Dans ce chapitre, nous avons en premier lieu implémenté la méthode de Baptista pour chiffrer et déchiffrer des messages textes et images, nous avons aussi implémenté notre méthode basée sur la carte logistique chaotique et le générateur congruentiel linéaire.


Conclusion
générale

Conclusion générale :

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.

Au cours de ce projet, nous avons effectué des recherches sur plusieurs axes de la cryptographie chaotique. Nous avons étudié ses origines avec la découverte de la synchronisation et son apogée avec les techniques de « sécurisation » les plus célèbres comme le masquage ou la méthode de Baptista.

Nous avons travaillé sur deux méthodes différentes pour le cryptage et décryptage du texte et d'image dans le cas des équations discrètes non linéaires, la première méthode est basé sur l'approche de Baptista et dans la deuxième méthode nous avons proposé un nouveau schéma de cryptage et décryptage des images aux niveau de gris basé sur les propriétés des systèmes chaotique, nous avons utilisé la carte logistique chaotique et le générateur cogruentiel linéaire les résultats de chiffrement sont satisfaisants.

Comme perspective à ce travail, nous allons améliorer notre approche sur tous les formats des images médicales en général et les images couleur entre eux en particulier.

Bibliographies

Bibliographie

[1] Hassan Noura, Conception et simulation des générateurs, crypto-systèmes et fonctions de hachage basés chaos performants, thèse de doctorat, université de Nantes, 2012.

[2] Liran Lerman, Cryptanalyse par analyse de consommation une approche basée sur l'apprentissage automatique, mémoire de master, université de UNIVERSITÉ LIBRE DE BRUXELLES,2010

[3] Amieur Akram, Conception et implémentation d'un système hybride pour la sécurité de données : application aux images numériques, mémoire de master, université de Msila,2017

[4] Renaud Dumont, Cryptographie et Sécurité informatique INFO0045-2, Notes de cours, Université de Liège.

[5] Stéphane Jacob, Protection cryptographique des bases de données : conception et cryptanalyse, Université Pierre et Marie Curie - Paris VI, 2012.

[6] Niels Ferguson, Bruce Schneir, « Cryptographie en pratique », Edition Vuibert informatique 2004. ISBN : 2-7117-4820-0. Livre

[7] Florent Guilleux, « Sécurité informatique, cryptographie, certificats et signature électronique (DESS NTSI) », 2004.

[8] Renauld Dumont, « Cryptographie et sécurité informatique », Cours Université de Liège 2009/2010.

[9] http://cryptologie-moderne-tpe.e-monsite.com/pages/theorie-et-algorithme/cryptographie-hybride.html visité le 04-04-2019

[10] Nkapkop Jean de dieu. Mémoire de master en cryptage chaotique des images basé sur le modèle du perceptron, université de Ngaoundéré, 2012.

[11] Benhaoua Mohamed Kamel, Approche cryptographique basée sur les algorithmes génétiques pour la sécurité des réseaux ad hoc, mémoire de Magister, université d'Oran,2013.

[12] Sébastien VARRETTE, « Fonctions de Hachage et signature numérique », Cours Universitaire,2008.

[13] A. Ali-pacha, N. Hadj-Said, A M'hamed ,A . belghoraf, chaos crypto-système basé sur l'attracteur de Clifford, SETIT 2009 5th International Conférence: Sciences of Electronic, Technologies of Information and Télécommunications March 22-26, 2009 – TUNISIA.

[14] Ghada Zaibi. Sécurisation par dynamiques chaotiques des réseaux locaux sans fil au niveau de la couche mac. Université de Toulouse, 2012.

[15] Kihal Ahmed Ridha, systèmes chaotiques pour la transmission sécurisée de données, mémoire de magister, université de M'sila ,2013.

[16] Z. Amrani, S Chitroub et A. Boukhari, Cryptage d'Images par Chiffrement de Vigenère Basé sur le Mixage des Cartes Chaotiques, 4th International Conference on Computer Integrated Manufacturing CIP'2007.

[17] Nada REBHI, Mohamed Amine BEN FARAH, Abdennaceur KACHOURI & Mounir SAMET, Analyse De Sécurité d'une Nouvelle Méthode De Cryptage Chaotique, SETIT 2007 4th International Conference: Sciences of Electronic, Technologies of Information and Telecommunications March 25-29, 2007 – TUNISIA

Résumé

Avec la progression rapide de l'utilisation d'images numérique dans de nombreuses applications, Il est important de protéger les données d'image confidentielles contre les accès non autorisés et cela est garantie grâce au cryptographie chaotique.

Dans ce mémoire, nous étudions la possibilité d'utiliser le chaos, partant de ses différentes propriétés et de son comportement spécifique, pour le cryptage / décryptage chaotique des images et de texte. Nous étudions deux méthodes la première basée sur la méthode de Baptista et la deuxième en utilisant la carte logistique et le générateur congruentiel linéaire.

Mots clés : images, cryptographie, chaos, cryptage/ décryptage chaotique.

Abstract

With the rapid growth of digital image usage in many applications, it is important to protect confidential image data from unauthorized access and this is ensured by cryptography.

In this thesis, we study the possibility of using chaos, starting from its different properties and its specific behavior, for the chaotic encryption / decryption of images and text. We study two methods, the first based on the Baptista method and the second using the logistic map and the linear congruential generator.

Keywords: images, cryptography, chaos, chaotic encryption / decryption.

الخلاصة

مع التقدم السريع في استخدام الصور الرقمية في العديد من التطبيقات والكثير من المجالات، بات من الضرورة حماية هذه الصور السرية من الوصول إلى أي شخص كان، وهذا ما تضمنه عملية التشفير.

في هذه الرسالة ، قمنا بدراسة إمكانية استخدام الفوضى ، بدءًا من خصائصها المختلفة وسلوكها المحدد ، للتشفير و فك تشفير الصور والنصوص. في هذا الصدد قمنا بتنفيذ طريقتين: الأولى تعتمد على طريقة بابتيستا(Baptista) والثانية باستخدام الخريطة اللوجستية والمولد التطابقي الخطي.

الكلمات المفتاحية: الصور ، التشفير ، الفوضى ، التشفير / فك التشفير الفوضوي.