REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

Université Mohamed Seddik Benyahia Jijel

Faculté des Sciences et de la Technologie

Département d'Electronique

Projet de fin d'études pour l'obtention du diplôme de Master en Télécommunications

Option

Systèmes des télécommunications

Thème

Conception et Réalisation d'un Crypto-Système pour la Sécurisation des Données Médicales

Présenté par :

Mr. Mohammed KADDOURI

Encadré par :

Dr. Samira DIB

Dr. Morad GRIMES

Année universitaire : 2020-2021

Remerciements

*Au terme de ce travail, je voudrais d'abord remercier **Allah** de m'avoir donné la santé et la volonté dans la réalisation de ce projet.*

*Je tiens à remercier particulièrement et chaleureusement mon encadreur, **Mme DIB Samira**, Docteur à l'université de Jijel, pour son encadrement, sa patience, ses conseils très judicieux, ses encouragements et sa disponibilité tout au long de mon projet.*

*Je remercie également mon second encadreur **Mr GRIMES Morad**, Docteur à l'université de Jijel, pour ses précieux conseils et son judicieux choix de ce thème qui m'a apporté de nouvelles connaissances dans ce large domaine.*

Mes remerciements vont aussi à Mr Boubakir Chaabane, Docteur à l'université de Jijel, pour ses conseils surtout dans la réalisation de la partie pratique.

J'exprime toute ma gratitude aux membres du jury pour avoir accepté de juger mon travail, ainsi que tous les enseignants du département d'électronique.

Dédicaces

Je voudrais dédier le présent travail tout spécialement

À mes très chers parents

Ma mère, qui a œuvré pour ma réussite, de par son amour, son soutien, tous les sacrifices consentis et ses précieux conseils, pour toute son assistance et sa présence dans ma vie…

Reçois, à travers ce travail aussi modeste soit-il, l'expression de mes sentiments et de mon éternelle gratitude.

Mon père, qui pourra être fier et trouvera ici le résultat de longues années de sacrifices pour m'avoir aidé à avancer dans la vie.

Puisse Dieu faire en sorte que ce travail porte son fruit…

Merci pour les valeurs nobles, l'éducation et le soutien permanent venus de toi.

A toute la famille Kaddouri et Bousri qui n'ont cessé d'être pour moi des exemples de persévérance, de courage et de générosité.

A tous ceux qui m'aiment.

A tous ceux que j'aime.

Enfin, à toute personne ayant participé de loin ou de près à la réalisation de ce travail

Table des matières

Chapitre 1

Introduction à la Cryptographie

Chapitre 2

Généralités sur les systèmes chaotiques

Chapitre 3

Cryptage chaotique - Application à la transmission des images médicales

Chapitre 4

Implémentation du crypto système sur cartes Arduino UNO

Liste des Figures

CHAPITRE 1

CHAPITRE 2

CHAPITRE 3

CHAPITRE 4

Liste des tableaux

Abréviations

ARDS	Acute Respiratory Distress Syndrome
ASK	Amplitude Shift Keying
AVR	Automatic voltage regulator
BRIE	Bit Recirculation Image Encryption
CKBA	Chaotic Key-Based Algorithm
CNNSE	Chaotic Neural Network for Signal Encryption
DSEA	Domino Signal Encryption Algorithm
ECC	Elliptic Curve Cryptography
HCIE	Hierarchic Chaotic Image Encryption
LCD	Liquid Crystal Display
MERS	Middle East respiratory syndrome
MSE	Mean Square Error
NPCR	Number of Pixels Change Rate
PRNG	Générateur de Nombres Pseudo-Aléatoires
PSNR	Peak Signal to Noise Ratio
RSA	Nommé par les initiales de ses trois inventeurs (Rivest, Shamir et Adleman).
SRAS	Syndrome Respiratoire Aigu Sévère
SSIM	Structural SIMilarity
US	Ultrasound
1D	Unidimensionnelle
2D	Bidimensionnelle
3D	Tridimensionnel

Introduction générale

Depuis l'Antiquité, l'être humain n'a cessé de chercher différents moyens pour envoyer un message à son correspondant pour pouvoir communiquer d'une manière sécurisée. Tous ses efforts ont abouti à des méthodes de communication et à leur développement dans le but d'obtenir une confidentialité totale dans les communications.

La révolution numérique a permis de simplifier le traitement et la transmission des informations multimédia, notamment des données médicales telles que des photos médicales de nombreux patients ainsi que nom, prénom, date de naissance, diagnostic, numéro de sécurité sociale, etc. Informations hautement sensibles, dont l'utilisation frauduleuse peut être exploitée à des fins d'usurpation d'identité et de fraude à l'assurance. Parallèlement, il a également développé des moyens très sophistiqués de fraude et d'espionnage. Dans ces circonstances, il devenait nécessaire de crypter ces données avant de les envoyer.

Une science est ainsi née « La cryptologie », étymologiquement la science du caché ou par extension la science du secret, qui est quasiment la base de tous les mécanismes, outils et concepts de la sécurité des différentes communications. Elle est subdivisée en deux domaines distincts et complémentaires, la cryptographie qui est la branche qui s'intéresse aux méthodes de protection de messages ou documents ; et la cryptanalyse qui consiste en l'étude des procédés et méthodes cryptographiques dans le but de trouver des faiblesses et en particulier de pouvoir déchiffrer des messages chiffrés sans posséder la clé de chiffrement.

Les techniques de cryptographie classique sont basées sur la théorie des nombres et en particulier sur la décomposition d'un entier en éléments simples. La majorité de ces protocoles ont déjà été cassés et d'autres présentent une charge calculatoire très grande qui limitent leur utilisation. Pour ces raisons, plusieurs chercheurs essayent de mettre en œuvre d'autres crypto-systèmes. Durant ces dernières décennies, les systèmes non linéaires chaotiques ont été appliqués à la cryptographie afin d'augmenter le degré de sécurité. L'étude de ces systèmes est liée à la théorie du chaos qui a connu une grande évolution à partir des années 1960 grâce aux travaux du météorologiste Edward Lorenz. Grâce aux propriétés intrinsèques des systèmes chaotiques telle que leur sensibilité aux conditions initiales, les systèmes chaotiques sont de bons candidats pour la cryptographie.

D'autre part, la cryptographie à courbe elliptique (ECC) a aussi suscité l'intérêt de nombreux chercheurs ces dernières années. ECC possède certains avantages notamment : efficacité de calcul, faible capacité de stockage et bande passante étroite par rapport à d'autres crypto systèmes à clé publique.

Dans le but de contribuer à la sécurité des données médicales, nous avons présenté ce modeste travail qui s'articule autour de quatre chapitres :

Le premier chapitre a pour objectif de résumer les différentes classes et techniques de cryptographie classique, moderne et autre en cours de développement comme la cryptographie sur courbes elliptiques et la cryptographie quantique. Il est clôturé par quelques notions de cryptanalyse.

Le deuxième chapitre aborde des généralités sur les systèmes chaotiques, leurs caractéristiques ainsi que leur relation avec la cryptographie.

Le troisième chapitre est consacré à l'implémentation sur des images médicales des deux algorithmes CKBA et ECC. Le premier basé sur le chaos et le second sur les courbes elliptiques. L'interprétation des résultats est faite moyennant des critères d'évaluation statistique et différentielle.

Dans le quatrième et dernier chapitre, le crypto-système expérimental construit autour de deux cartes Arduino UNO est exposé. Les résultats des tests obtenus dans le cas d'une transmission sécurisée de texte sont présentés avec des photos réelles du processeur.

Enfin, une conclusion générale est donnée avec quelques perspectives ouvertes pouvant être envisagées comme suite à notre projet.

Chapitre 1

Introduction à la Cryptographie

1. Introduction
2. Histoire de la cryptographie
3. Définitions
4. Cryptographie
5. Classes de cryptographie
6. Cryptographie sur Courbes Elliptiques
7. Notions de cryptanalyse
8. Applications de la cryptographie
9. Conclusion

1. Introduction

La cryptographie est par définition l'art de cacher l'information. Elle désigne l'ensemble des techniques qui permettent de chiffrer les messages. Son objectif principal est de permettre à deux personnes Alice et Bob de communiquer à travers un canal peu sûr de telle sorte qu'un opposant Eve ne puisse pas comprendre ce qui est échangé.

La cryptographie a toujours eu une grande importance dans l'histoire. Actuellement les réseaux informatiques exigent son utilisation pour assurer la confidentialité des données transmises notamment dans la téléphonie mobile, le paiement bancaire, les pièces d'identité, la télésanté, etc.
Ce chapitre est alors une introduction à la cryptographie. Il aborde, après un historique, différentes généralités sur la cryptographie. Il introduit aussi les deux principaux schémas cryptographiques (symétrique et asymétrique). Enfin, un aperçu des différentes attaques (cryptanalyses) cryptographiques sera donné.

2. Histoire de la cryptographie

Anciennement considérée comme un art, la cryptographie est désormais reconnue comme une science à part entière.

Les premières utilisations connues de la cryptographie remontent à l'Antiquité, où la plus ancienne trace de message chiffré a été retrouvée sur une table en argile sur les bords du Tigre en Irak. Au fil des années, les motivations militaires ont conduit les Hommes à développer de nouvelles méthodes de chiffrement plus robustes afin d'éviter que les tactiques ou plans de bataille ne tombent dans les mains de l'ennemi. Les Spartiates ont ainsi inventé le premier dispositif militaire connu : *la scytale*, ou *bâton de Plutarque*. La scytale en elle-même est un bâton de bois, dont le diamètre est connu uniquement de l'émetteur et du destinataire du message.

Il a fallu attendre l'époque de *Jule César,* vers 50 avant J-C, pour voir apparaitre de véritables systèmes cryptographiques. Le plus célèbre d'entre eux est *le chiffre de César,* qui consistait simplement à décaler les lettres d'un message de trois positions vers la droite dans l'alphabet latin. Plus tard, *Blaise de Vigenère* (1586) introduit un nouveau chiffrement dans lequel on ne se contente pas d'un seul décalage comme pour César mais de plusieurs.

En 1883, *Auguste Kirckhoffs* énonce un principe fondateur de la cryptographie moderne :

« *Les mécanismes de chiffrement et de déchiffrement doivent pouvoir être rendus publics, la confidentialité des messages doit être garantie uniquement par le secret d'une clé* ».
Le bond technologique suivant survient au XXème siècle lors des deux guerres mondiales. Les besoins militaires des différentes armées de protéger leurs communications ont permis de voir l'apparition de machines spécialement conçues pour le chiffrement et le déchiffrement, on peut citer par exemple, *Enigma*, *la C-36*, et la *machine de Lorenz*. Dans la deuxième moitié du vingtième siècle, la cryptographie est devenue beaucoup plus mathématique et a été grandement facilitée par l'apparition des premiers ordinateurs. Cette cryptographie moderne est initiée par le travail de *Claude Shannon* en 1948 sur la *théorie mathématique de l'information.*

De nos jours, en plus de l'amélioration des méthodes classiques, de nouvelles techniques de chiffrement sont introduites, telles que : la *cryptographie quantique* qui consiste à chiffrer une clé en utilisant des photons envoyés par fibre optique, et toute tentative d'interception de la clé modifie la polarisation des photons ; et la *cryptographie chaotique* qui se base sur des instabilités de natures inhabituelles des systèmes non linéaires. Ce fut alors la découverte des signaux chaotiques qui ont un comportement déterministe mais qui font penser à des allures pseudo-aléatoires. Le principe de la cryptographie chaotique est alors de noyer le message en clair dans un signal chaotique. Pour le chiffrement et le déchiffrement, on doit alors disposer au niveau de l'émetteur et du récepteur du même signal chaotique pour pouvoir récupérer le message chiffré [1 - 4].

3. Définitions [5]

A cause de l'utilisation de termes empruntés à l'anglais, on rencontre souvent une certaine confusion concernant les différents termes de la cryptographie. Ainsi on va définir la terminologie qui va être utilisée tout au long de ce manuscrit afin d'éviter toute ambigüité :

- **Chiffrer ou Chiffrement :** Il s'agit d'une méthode ou d'un algorithme qui empêche quiconque autre que l'expéditeur et le destinataire de comprendre les données.
- **Déchiffrer ou Déchiffrement :** C'est la fonction qui permet de retrouver la donnée claire à partir de la donnée chiffrée à condition de connaitre la clé de déchiffrement.
- **Décrypter :** retrouver le message clair correspondant à un message chiffré sans posséder la clé de déchiffrement.
- **Texte chiffré :** ou cryptogramme c'est le résultat de l'application d'un chiffrement sur une donnée claire ; (en anglais *Ciphertext*).

- **Texte clair :** C'est une donnée lisible et compréhensible par opposition au texte chiffré ; (en anglais *Plaintext*).
- **Clé :** C'est un ensemble de paramètres d'un algorithme de chiffrement ou de déchiffrement, sur lequel repose le secret. C'est la combinaison d'algorithmes complexes et de clés importantes qui peut garantir une solution sûre et fiable.
- **Crypto-système :** Il est défini comme l'ensemble des clés possibles (espace de clés), des textes clairs et chiffrés possibles associés à un algorithme donné.
- **Cryptographie :** Etymologiquement «écriture secrète», devenue par extension l'étude de cet art (donc aujourd'hui la science visant à chiffrer).
- **Cryptanalyse :** Science analysant les cryptogrammes en vue de les décrypter.
- **Cryptologie :** Mot composé de deux termes d'origine grec, kruptos «caché» et Logos «discours». C'est une combinaison des sciences des mathématiques et informatiques qui étudient les communications secrètes et est composée de deux branches complémentaires à savoir : *la cryptographie* et *la cryptanalyse*.

4. Cryptographie

La cryptographie est la science qui utilise les mathématiques pour le cryptage et le décryptage de données.

Elle permet ainsi de stocker des informations confidentielles ou de les transmettre sur des réseaux non sécurisés (comme l'internet), afin qu'aucune personne autre que le destinataire ne puisse les lire.
Alors que la cryptographie consiste à sécuriser les données, la cryptanalyse est l'étude des informations cryptées, afin d'en découvrir le secret. La cryptanalyse classique implique une combinaison intéressante de raisonnement analytique, d'application d'outils mathématiques, de recherche de modèle, de patience, de détermination et de chance. Les cryptanalystes sont également appelés des pirates.

On attend souvent de la cryptographie d'accomplir plusieurs fonctions pour garantir la sécurité de communication :

- **La confidentialité :** permet de garantir que les données transmises vers un destinataire ne seraient déchiffrées que par celui-ci, et par aucun autre. Ceci nécessite une identification précise du destinataire, et une méthodologie permettant de rendre inutilisable l'information à tout autre qu'à ce destinataire.
- **La disponibilité :** a pour but de s'assurer qu'un système ou une donnée soit accessible et permanente durant le temps d'utilisation prévu.

- **L'authentification** : permet de s'assurer de l'origine d'un message, ainsi que de l'identité du destinataire. Par les mécanismes d'authentification d'un protocole, on doit donc pouvoir garantir l'identité des deux partenaires d'une communication.
- **L'intégrité :** est la méthode permettant de s'assurer que l'information n'a pas été altérée pendant son passage ou son stockage sur le réseau.
- **Le non–reniement :** est la méthode pour s'assurer que l'information ne peut pas être désavouée. Une fois que le procédé de non–reniement est en place, l'expéditeur ne peut pas nier être le créateur des données.

5. Classes de la cryptographie

De nombreux systèmes de cryptographie ont été imaginés depuis plusieurs siècles. On peut les regrouper en trois grandes classes illustrées dans la figure 1.1.

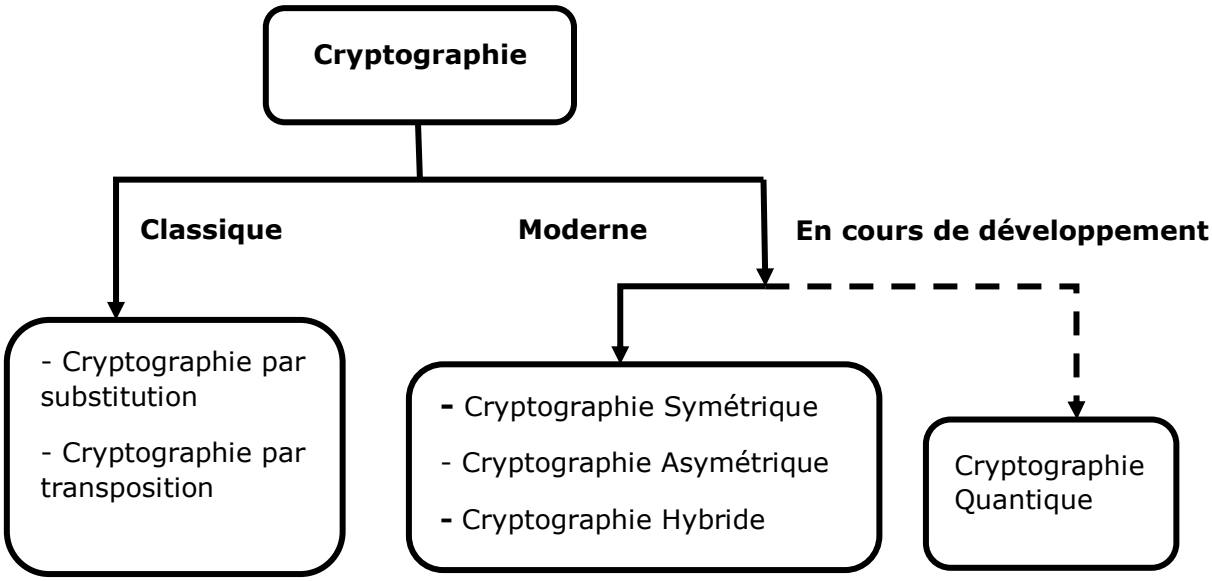

Figure 1.1 : Schéma résumant les différentes classes de la cryptographie.

5.1 Cryptographie classique

La cryptographie classique décrit une période antérieure aux ordinateurs, où les principaux outils utilisés consistaient à remplacer des caractères par d'autres et à les transposer dans des séquences différentes tout en gardant secrètes les procédures de cryptage ou de décryptage. Sans cela, le système est complètement inefficace car n'importe qui peut

déchiffrer le message chiffré. Cette classe de méthodes regroupe deux types de cryptographie :

- **Cryptographie par substitution :** Ce mode de cryptage remplace les lettres d'un message texte par d'autres lettres, chiffres ou autres symboles. En raison de la méthode de substitution, les substitutions mono-alphabétiques et poly-alphabétiques sont distinguées.
- **Cryptographie par transposition :** On distingue la transposition simple par colonne et la transposition complexe par colonne.

5.2 Cryptographie Moderne

Avec l'avancement des ordinateurs, les techniques cryptographiques ont considérablement évolué, mettant en jeu le cryptage manuel. Même ainsi, les processus de substitution et de transposition sont toujours pertinents, mais cette fois en manipulant des séquences de bits car les ordinateurs ne manipulent que des données numériques. Ce qui rend les techniques de cryptage actuelles plus sûres et même incassables avec certaines techniques, ou du moins nécessiteraient des millions d'années à la puissance actuelle les meilleurs supercalculateurs. D'un autre côté, cela signifie que désormais les algorithmes ne sont plus cachés, au contraire, ils sont connus de tout le monde, et leur sécurité est uniquement liée aux clés utilisées. La cryptographie moderne est divisée en deux parties distinctes :

- La *cryptographie à clé secrète*, ou encore appelée *symétrique*.
- La *cryptographie à clé publique*, dite également *asymétrique*.

5.2.1 Cryptographie symétrique (à clé secrète)

L'algorithme de chiffrement dépend de l'utilisation de la même clé par l'émetteur et le destinataire, c'est à dire que la clé de chiffrement et celle de déchiffrement sont identiques. La figure 1.2 illustre le principe du chiffrement à clé secrète.

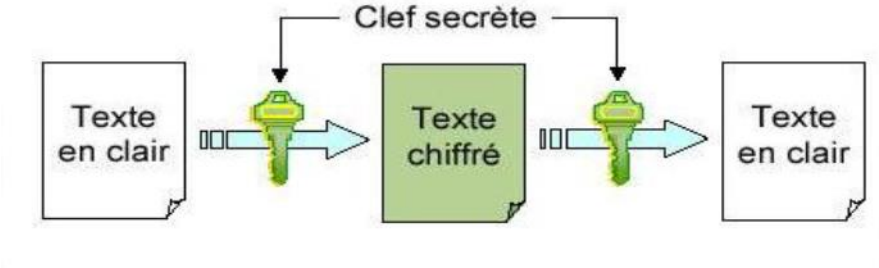

Figure 1.2 : Cryptographie symétrique.

Les avantages de la cryptographie symétrique sont :

- La rapidité d'exécution (jusqu'à 100 fois plus rapide que les solutions asymétriques).
- La simplicité d'implémentation sur hardware (gestion d'une seule clé).
- Clés relativement courtes (64 bits ou 8 caractères qui sont facilement mémorisables).

Les inconvénients de la cryptographie symétrique sont :

- Echange de la clé secrète.
- Gestion difficile des clés (nombreuses clés).
- Dans un réseau de N entités susceptibles de communiquer secrètement, il faut distribuer N*(N-1)/2 clés.

5.2.2 Cryptographie asymétrique

La cryptographie asymétrique est un procédé qui intègre deux clés de chiffrement : une clé publique et une clé privée. Par convention, la clé de chiffrement du message est appelée clé publique (et peut-être communiquée sans aucune restriction), et la clé de déchiffrement est appelée clé privée [6]. Cette dernière ne doit être communiquée sous aucun prétexte. Avec une clé publique, l'expéditeur code dans un algorithme de chiffrement un message qui ne pourra être, au final, décodé ou résolu que par le destinataire détenteur d'une clé privée donnée en entrée d'un algorithme de déchiffrement.

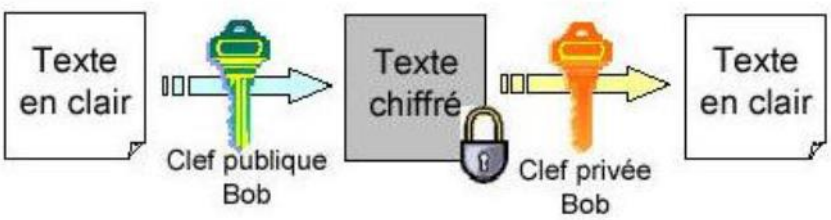

Figure 1.3 : Chiffrement asymétrique

Les avantages de la cryptographie asymétrique sont :

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

Les inconvénients de la cryptographie asymétrique sont :

- Le temps d'exécution : plus long que le cryptage symétrique.
- Le danger des attaques par substitution des clés ; d'où la nécessité de valider les émetteurs des clés.
- Taille des clés plus grande que celle des systèmes symétriques.

Il existe plusieurs systèmes asymétriques, les plus connus sont le RSA et El Gamal.

Le premier algorithme est basé sur la difficulté calculatoire de la factorisation des grands entiers. Il a été décrit, pour la première fois, en 1977 par Ron Rivest, Adi Shamir et Leonard Adleman du MIT. Dans le chiffrement RSA, tant la clé publique que la clé privée peuvent servir à chiffrer un message [7]. Dans ce cas, c'est la clé opposée à celle ayant servi au chiffrement qui est utilisée pour le déchiffrement. C'est notamment grâce à cette caractéristique que RSA est devenu l'algorithme asymétrique le plus répandu. Il offre, en effet, une méthode permettant d'assurer la confidentialité, l'intégrité, l'authenticité et la non-répudiabilité des communications électroniques et du stockage de données.

Le second algorithme de chiffrement à clé publique a été inventé par Tahar El Gamal en 1985. Il est lié au problème du logarithme discret utilisé pour le chiffrement asymétrique [8].

5.3 Cryptographie quantique

Elle est aussi appelée cryptographie à clé inviolable et permet de garantir un secret absolu sur des communications chiffrées. Fondée sur une idée originale de S. Wiesner, refusée en 1969 par une revue scientifique, la cryptographie quantique abrégée par BB84 s'est développée à partir de la publication de C.H. Bennett et G. Brassard, en 1984 [9].

Plusieurs versions du protocole BB84 ont vu le jour. Dans la plus simple, on polarise les photons avec des valeurs binaires '0' et '1' dont l'état de polarisation est orthogonal pour coder des données suivant deux bases :

- Base horizontale/verticale : les valeurs '0' et '1' correspondent aux photons ayant respectivement des polarisations de 0° et 90°.
- Base diagonale/anti-diagonale les valeurs '0' et '1' correspondent aux photons ayant respectivement des polarisations de 45° et 135°.

En considérant deux points communiquant 'Alice' et 'Bob', le protocole de cryptographie quantique suivra 6 étapes :

Étape 1 *:* Alice sélectionne aléatoirement une des bases citées ci-dessus et encode une suite de photons et l'envoie à Bob via un canal quantique.

Étape 2 *:* Bob reçoit les photons et mesure leurs polarisations en choisissant aléatoirement une base d'analyse.

Étape 3 : Alice communique à Bob, via un canal publique, ses choix de bases pour qu'il mesure la polarisation de chacun des photons.

Étape 4 *:* Bob compare ses choix avec ceux d'Alice et lui communique par la suite, via le canal publique, les positions des bits correspondants au cas où le choix de bases est similaire ; les bits sont rejetés dans le cas contraire.

Étape 5 : Bob envoie aléatoirement à Alice, via le canal publique, un sous ensemble de données résultantes de l'étape 4, pour qu'elle procède à une analyse d'erreurs en effectuant une comparaison avec sa propre séquence. Cette étape détermine s'ils ont été espionnés.

Étape 6 : Si le taux d'erreurs 'QBER' est supérieur à 11%, Alice et Bob rejettent les données échangées et recommencent le protocole à l'étape 1. Sinon (QBER<11%) Alice déduit qu'il n'y a pas eu d'espionnage, Alice et Bob conservent les bits restants de l'étape 5 pour former la clé secrète qui n'est connue que par eux.

6. Cryptographie sur Courbes Elliptiques

La cryptographie sur courbes elliptiques (ou Elliptic Curve Cryptography, ECC, en Anglais) a été proposée indépendamment par Koblitz [10] et Miller [11] dans les années 80. Elle comprend un ensemble de techniques qui permettent de sécuriser des données en consommant moins de ressources. L'avantage le plus important de l'ECC par rapport aux autres algorithmes de cryptographie asymétrique, par exemple RSA, est que l'on peut avoir un bon niveau de sécurité en utilisant une clé beaucoup plus courte [12]. Pour expliquer le fonctionnement de l'ECC, on présente la définition d'une courbe elliptique et les concepts mathématiques fondamentaux qui la caractérisent, ainsi que les opérations les plus importantes sur lesquelles sont basées les courbes elliptiques.

6.1 Courbe elliptique

Une courbe elliptique est un cas particulier d'une courbe algébrique munie d'une loi de groupe, telle que les coordonnées de la somme s'expriment en fonction de celles des points de départ suivant l'équation de *Weierstrass* :

$$E : y^2 + a_1xy + a_3y = x_3 + a_2x_2 + a_4 + a_6 \quad (1.1)$$

- Les coefficients a_1, a_2, a_3, a_4, a_6 représentent un ensemble d'éléments formés de deux opérations : l'addition et la multiplication. On suppose que la courbe est définie dans un corps et les paramètres $a_1, a_2, a_3, a_4, a_5, a_6 \in K$
- Une courbe elliptique E est définie sur K à laquelle on a rajouté un point à l'infini (l'élément zéro de l'addition) :

$$E = \{(x,y)\epsilon\bar{k}^2 | y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6| \cup \{O\} \quad (1.2)$$

La condition $\Delta = -16(4a^3 + 27b^2) \neq 0$ s'assure que la courbe elliptique est « lisse », c.àd. qu'elle ne possède ni point double, ni point de rebroussement (il n'y aucun point auquel la courbe possède deux ou plusieurs tangentes distinctes).

- **Forme réduite de l'équation de Weierstrass**

Pour son usage en cryptographie, on considère k un nombre fini et a_1, a_2 et a_3 doivent être égaux à 0. Comme les cryptographes ont l'habitude de renommer $a_4 = a$ et $a_6 = b$ on obtient la forme réduite de l'équation Weierstrass :

$$y^2 = x^3 + ax + b \quad (1.3)$$

Cette équation est utilisée pour former un groupe où *a* et *b* sont deux éléments réels de K vérifiant la condition : $4a^3 + 27b^2 \neq 0$. Dans ce cas, la courbe est lisse (elle possède une tangente en tout point de sa courbe représentative) [13].

- **Champ de points sur une courbe elliptique**

Soit *E* une courbe elliptique sur Z_p. Les variables de l'équation cubique obtenue peuvent prendre l'ensemble des entiers $E_P(a,b)$: $\{0,1,\ldots,p-1\}$ vérifiant l'équation :

$$y^2 \equiv x^3 + ax + b mod(p) \quad (1.4)$$

6.2 Opérations sur les courbes elliptiques

On va définir les formules qui permettent de calculer les coordonnées du point R résultant d'une addition ou multiplication ou soustraction de deux points P et Q.

- **Addition de points**

Soient E une courbe elliptique définie sur un corps K, et deux points P, Q ∈ E(K), L la droite reliant P à Q (la tangente à E si P = Q) et R le troisième point d'intersection de L avec E. Soit L' la droite verticale passant par R. On définit $P+Q \in$ E(K) comme étant le deuxième point d'intersection de L' avec E. Muni de cette loi de composition, $\left(E(K),+\right)$ est un groupe abélien dont l'élément neutre est le point à l'infini (O).

- **Algorithme d'addition de deux points dans E_p (a,b)** [14]

Soient deux points sur la courbe elliptique *E*, avec $P_1 = (x_1, y_1)\ et\ P_2(x_2, y_2) \neq 0$

On a : $P_1 + P_2 = P_3 = (x_3, y_3)$

- Si $x_1 \neq x_2$, alors

$$\begin{cases} x_3 = \left(m^2 - (x_1 + x_2)\right) mod(p) \\ y_3 = (m(x_1 - x_2) - y_{1)} mod(p) \end{cases} \text{où : } m = \frac{y_2 - y_1}{x_2 - x_2} = \frac{c}{d} = \left(c.inv(d)\right) mod(p) \qquad (1.5)$$

- Si $x_1 = x_2$ et $y_1 \neq y_2$, alors : $P_3 = 0$
- Si $P_1 = P_2$ et $y_1 \neq 0$,alors :

$$\begin{cases} x_3 = \left(m^2 - (x_1 + x_2)\right) mod(p) \\ y_3 = (m(x_1 - x_2) - y_{1)} mod(p) \end{cases} o\text{ù : } m = \frac{3x_1^2 + a}{2y_1} = \frac{c}{d} = \left(c.inv(d)\right) mod(p) \qquad (1.6)$$

- Si $P_1 = P_2$ et $y_1 = 0$, alors : $P_3 = 0$

- **Soustraction de deux points**

Soient E une courbe elliptique définie sur un corps K, et deux points P, Q de E(K). Donc pour soustraire Q de P, on fait la négation de Q puis l'addition. La négation se fait comme suit [15]:

On considère $Q = (x_q, y_q)$, et on veut calculer $R = -Q = (x_r y_r)$.

On choisit deux points $S = (x_s, y_s)$ et $T = (x_t, y_t)$ symétriques par rapport à la droite

$$y = moy = \frac{y_s + y_t}{2} \rightarrow \begin{cases} y_r = y_q + 2(moy - y_q) \\ x_r = x_q \end{cases} \quad (1.7)$$

Enfin, $P + (-Q)$ est calculé en utilisant l'algorithme d'addition décrit précédemment.

- **Doublement successif** [16]

On considère un point sur une courbe elliptique, P et n un nombre entier positif, alors nP peut être calculé par :

$$nP = \begin{cases} P + P + \cdots P & n > 0 \\ -P - P - \cdots - P & n < 0 \end{cases} \quad (1.8)$$

Quand l'entier n est très grand, il est pratique d'utiliser le doublement consécutif.

7. Notions de cryptanalyse

La cryptanalyse est un terme créé en 1920 par le cryptographe américain William Friedman. Il est extrait des mots grecs kruptos et analusis, "parse, disband". La cryptanalyse ou l'attaque regroupe tous les moyens pour déchiffrer un texte chiffré sans connaitre la clé [1]. Le rôle du cryptanalyste n'a pas changé suivant les évolutions de la cryptographie, mais les moyens mis à sa disposition sont plus performants. En outre, les schémas auxquels il s'attaque sont complètement différents des simples algorithmes de substitutions utilisés dans la première ère de la cryptographie [2]. La recherche sur les faiblesses des systèmes cryptographiques est généralement effectuée par des intrus qui mettent en œuvre diverses méthodes pour trouver des informations secrètes, telles que des clés, des messages clairs à partir d'informations (mots de passe, algorithmes) qui sont considérées comme publiques [4]. Le but est de casser la protection développée par la cryptographie. Les cryptanalystes sont les "ennemis" des cryptographes, puisque leur but est de "casser" un algorithme de cryptographie afin d'en permettre le décodage par une tierce personne. Tenter de cryptanalyser le système s'appelle une attaque, et cela peut conduire à des résultats différents.

Du point de vue de l'attaquant, on distingue cinq scénarios d'attaque différents suivant l'information que cet attaquant soit capable de récupérer. Dans tous les cas, le but du cryptanalyste est de retrouver la clé utilisée pour le chiffrement des messages qu'il aurait intercepté [17-19]. Par attaque, on entend une tentative de cryptanalyse d'un schéma donné qui utilise de l'information dans l'un des cas suivants :

- **Chiffré seul *(ciphertext only)* :** L'attaquant possède uniquement un ou plusieurs messages chiffrés, mais ne détient aucune information sur les messages en clair correspondants. En pratique, ce scénario est le plus courant.
- **Clair connu *(known Plaintext)* :** Dans ce cas, le cryptanalyste a non seulement accès aux messages chiffrés, mais également aux messages en clair correspondants. On parle de paires clairs/chiffrés.
- **Clair choisi *(chosen Plaintext)* :** En donnant plus de puissance à l'attaquant, on lui permet de chiffrer les messages qu'il souhaite avec une clé qui lui est inconnue, et son but est d'en déterminer la valeur. Bien que ce scénario avantage grandement l'attaquant, on le retrouve dans diverses implémentations pratiques telles que dans les cartes à puce. La clé secrète est protégée physiquement, mais on peut demander le chiffrement de messages par la carte et en récupérer les chiffrés.
- **Chiffré choisi *(chosen ciphertext)* :** De la même manière, l'attaquant peut dans ce cas demander le déchiffrement de messages quelconques et obtenir leur déchiffrement par la clé secrète.
- **L'attaque par force brute ou attaque exhaustive *(Brute-force attack)* :** L'attaquant essaye alors toutes les combinaisons de clés possibles jusqu'à obtention du texte clair. Cette attaque est la plus coûteuse en termes de calculs et en mémoire à cause de l'attaque exhaustive. La réussite de cette attaque est contrainte au nombre de possibilités pour la clé recherchée. Plus il y aura de possibilités, plus la probabilité de trouver la bonne clé de déchiffrement est faible et l'attaque est coûteuse.

La création des techniques modernes de chiffrement a fait ressortir de nouvelles méthodes de cryptanalyse. On peut regrouper les diverses techniques de cryptanalyse en deux grandes familles.

- **Cryptanalyse différentielle**

Elle a été proposée par Eli Biham et Adi Shamir en 1991. Elle permet de trouver la clé en utilisant une quantité de textes clairs. L'idée est alors de fournir comme entrée des textes clairs avec de légères différences (un bit par exemple), on analyse ensuite statistiquement le comportement des sorties selon les entrées pour retrouver la clé. En regardant comment les différences en entrée affectent les sorties, on peut établir des règles statistiques.

- **Cryptanalyse linéaire**

Elle a été inventée par le japonais Mitsuru Matsui et consiste à faire une approximation linéaire de la structure interne de la méthode de chiffrement. L'idée est alors de trouver des approximations linéaires entre les bits de sortie, les bits d'entrée et les bits de la clé. Elle remonte à 1993 et s'avère être l'attaque la plus efficace sur le DES.

8. Applications de la cryptographie

L'application la plus évidente de la cryptographie est la protection de la confidentialité d'une information, qu'elle soit stockée localement sur une machine, ou transmise sur un réseau. Le besoin de la confidentialité n'est pas l'apanage des militaires ou de certains gros industriels. Tous les individus, toutes les organisations ont, à des degrés divers, un tel besoin :

- Confidentialité des transactions bancaires,
- Protection de secrets industriels ou commerciaux,
- Protection des sessions de télétravail,
- Protection du secret médical,
- Protection des systèmes informatiques contre les intrusions,
- Protection de la confidentialité des communications dans le cadre d'une association, d'un parti politique, d'un syndicat…
- Protection de la vie privée,
- …

9. Conclusion

Ce chapitre est une introduction générale à la cryptographie, dans lequel nous avons évoqué après un bref historique des généralités sur la cryptographie, la terminologie utilisée dans ce domaine, les différents objectifs de sécurité envisagés en cryptographie ainsi que les différentes techniques de chiffrement.

Ensuite, nous avons défini les deux grandes classes cryptographiques classiques qui sont : la cryptographie symétrique et la cryptographie asymétrique. En outre, on a abordé la notion de cryptographie sur courbes elliptiques ainsi que des notions de cryptanalyse. Quelques applications sont citées avant de terminer par une conclusion résumant le contenu du chapitre.
Le chapitre qui suit est consacré aux principes des systèmes chaotiques et l'introduction du chaos dans la cryptographie.

Chapitre 2

Généralités sur les Systèmes Chaotiques

1. Introduction
2. Définitions
3. Carte logistique
4. Caractéristiques des systèmes chaotiques
5. Le chaos et la cryptographie
6. Conclusion

1. Introduction

La théorie du chaos est une discipline à part entière basée sur la théorie des systèmes dynamiques qui résulte, en partie, des travaux du mathématicien Henri Poincaré (1854-1912) à la fin du XIX^{ième} siècle. Cette théorie est utilisée pour prévoir l'évolution des populations avec la transformation de Myrberg (encore appelée transformation logistique). Une autre application importante de la théorie du chaos se trouve dans les prédictions en météorologie avec les travaux de Lorentz en 1963. Il existe beaucoup d'autres domaines dans lesquels le chaos est utilisé, à savoir : l'étude du système solaire, l'écoulement des fluides, les rythmes biologiques, …. Dans le domaine de l'électronique et plus particulièrement des télécommunications, les signaux chaotiques peuvent être employés pour le codage, le chiffrement, etc.

L'avantage d'employer des méthodes basées sur la théorie du chaos réside dans le haut niveau de sécurité qu'offre ce type de systèmes ainsi que la rapidité de calcul due à leur structure dynamique. Ainsi ils sont très compétitifs en raison du fait, qu'ils soient peu coûteux à mettre en œuvre et à implémenter.

1.1 Bref historique du chaos

A l'ère d'Isaac Newton (1642-1727), le déterminisme dominait la science et les scientifiques croyaient pouvoir prédire et prévoir le futur d'une manière exacte à condition de connaitre les conditions initiales et les paramètres. Cette théorie a été confirmée par Newton et Laplace qui affirmait la notion du déterminisme en disant qu'il pouvait prédire le futur de l'univers en connaissant juste son état présent. Cependant, cette théorie a été contredite par Poincaré (1913) en avançant qu'il ne pouvait connaitre l'évolution et prédire le problème des trois corps de la mécanique céleste (exemple : lune, terre et soleil) et ceci malgré leur nature déterministe [20].

L'étude de la stabilité en comparant les trajectoires suivies par un des corps à partir de deux positions initiales très proches, où on a conclu que les trajectoires étaient presque identiques à court terme, mais à long terme il y'avait une nette différence, donc on ne peut jamais prédire complètement l'évolution d'un système chaotique. Cette signification a été avancée en 1908 par pierre Duhem [21].

La première visualisation du phénomène du chaos déterministe a été observée par coïncidence par Edward Lorenz en 1961, à la suite d'une série de calculs qui avaient pour but de prévoir des phénomènes météorologiques. Ce dernier se servait de son ordinateur

(royal McBean lgp-300) pour calculer ses prévisions. En obtenant les résultats finaux, il voulait les refaire une deuxième fois pour s'assurer. Pour gagner du temps, il n'a pris en compte que trois chiffres après la virgule au lieu de six en croyant qu'il aurait une petite variation dans les résultats, mais il a été stupéfait par ces derniers qui étaient totalement différents des premiers.
A partir de là, on a découvert le comportement chaotique d'un système non linéaire, une métaphore a contribué à l'essor de la théorie de Lorenz : « le simple battement d'aile du papillon au Brésil pourrait déclencher une tornade au Texas » [22].

2. Définitions

2.1 Système dynamique

Le concept du système dynamique possède ses origines dans la mécanique newtonienne. C'est un modèle mathématique qui décrit l'évolution des phénomènes soit mécanique, physique, etc. par rapport au temps. Il est caractérisé par un plan de phase et un système d'état. Il peut être décrit par un ensemble d'équations qui peuvent prendre des formes diverses (équations différentielles ordinaires, équations aux dérivées partielles, etc.) [23]. La détermination de l'état futur exige de réitérer la relation plusieurs fois. Une fois que le système puisse être résolu, donner un premier point permet de déterminer tous ses points futurs : cette collection est connue sous le nom de trajectoire.

2.2 Système non linéaire

Un système est dit non linéaire s'il ne respecte pas le principe de superposition et si la relation entre les grandeurs d'entrée et de sortie est une équation différentielle avec des coefficients généralement non constants.
Il est à noter que la plupart des systèmes physiques sont des systèmes non linéaires.

2.3 Système déterministe

Un système est dit déterministe, si pour exactement les mêmes paramètres, les mêmes conditions initiales et les mêmes conditions aux limites, il donne les mêmes résultats uniques.

2.4 Espace des phases

Les trajectoires dynamiques d'un système se situent dans un espace mathématique appelé espace des phases. Cet espace, bien qu'abstrait, contient sous forme géométrique une

information concrète. Les variables qui sont à la base de la construction de cet espace sont des grandeurs réelles et à chaque point correspond une situation physique bien déterminée. Le choix de ces variables n'est pas arbitraire, l'espace doit contenir toute l'information sur la dynamique du système étudié [24].

2.5 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 [24].

2.6 Exposant de Lyapunov

Dans l'analyse d'un système dynamique, l'exposant de Lyapunov est un coefficient qui mesure le taux de convergence ou de divergence de deux trajectoires voisines au départ dans l'espace des phases. Souvent représenté par le symbole lambda, λ, il permet d'approximer la durée du comportement prévisible d'un système dynamique et le moment où il basculera dans un comportement chaotique. Le nombre des exposants de Lyapunov est égal à la dimension du système [25].

2.7 Système chaotique

Un système chaotique est un système déterministe et imprévisible mais c'est aussi et surtout un système non linéaire. Le lien qui relie ces deux notions paradoxales, déterminisme et imprévisibilité, est la propriété de sensibilité aux conditions initiales. En effet, deux conditions initiales infiniment proches peuvent conduire à des états futurs très différents du système.
En première définition, un système dynamique est dit chaotique si les solutions du système se trouvent dans un ensemble borné B de l'espace des phases et présentent plusieurs caractéristiques fondamentales, à savoir :

- Une transformée de Fourier ou un spectre de puissance analogue à celui d'un bruit blanc. Cette propriété indique l'aspect non périodique de la trajectoire chaotique.
- Des trajectoires très proches l'une de l'autre divergent de façon exponentielle. Cela se traduit par l'extrême sensibilité aux conditions initiales.

3. La carte logistique

La carte logistique trouve son origine dans les travaux du mathématicien belge Pierre-Francois Verhulst dans la première moitié du XVIIIe siècle. Verhulst publiait en 1845 et 1847 deux articles sur la façon dont la croissance démographique pourrait être modélisée mathématiquement. Il a appelé ce modèle la courbe logistique [26-29].

La carte logistique, version en temps discret de celle du modèle logistique de Verhulst, est chaotique sous certaines conditions. Son équation est donnée par :

$$x_{n+1} = f(x_n) = r x_n (1 - x_n) \quad avec \begin{cases} 0 \leq r \leq 4 \\ 0 \leq x_n \leq 1 \end{cases} \tag{2.1}$$

Où *r* représente le paramètre du système et x_n la variable dynamique.

Suivant la valeur de r et la valeur initiale x_0 de la suite $\{x_n\}$, celle-ci présente des comportements très différents.

Dans le cas de la figure 2.1, en prenant $r = 2.8$ et $x_0 = 0.04$, la suite $\{x_n\}$ converge rapidement vers une valeur fixe figure 2.1 (a). La figure 2.1 (b) illustre dans le plan (x_n, x_{n+1}) la construction géométrique de la suite.

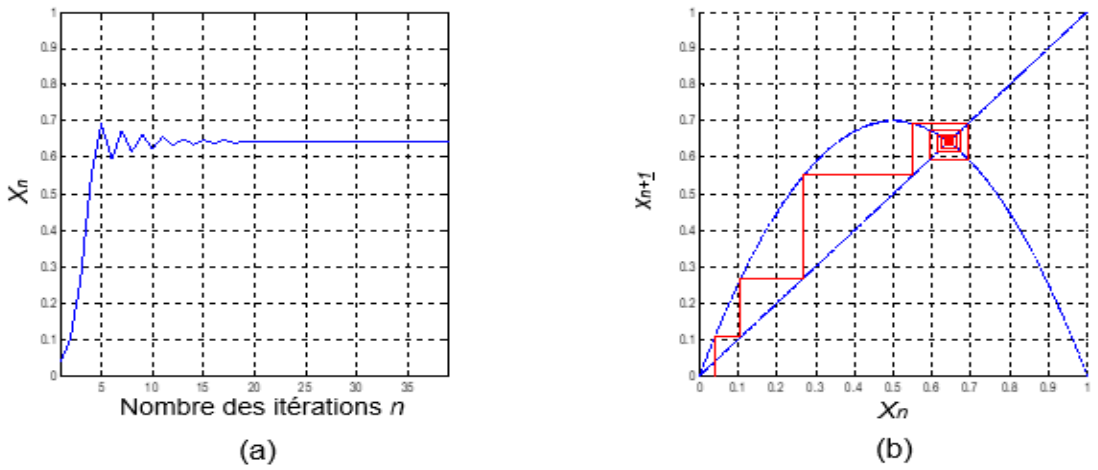

Figure 2.1 : Evolution de la suite $\{x_n\}$ pour r = 2.8 et x_0 = 0.04

La figure 2.2 illustre l'évolution de la suite $\{x_n\}$ lorsque $r = 3.2$. En gardant la même valeur initiale que dans le cas précédent, la suite converge vers une solution périodique composée de deux points. On dit que la trajectoire converge vers un cycle d'ordre 2.

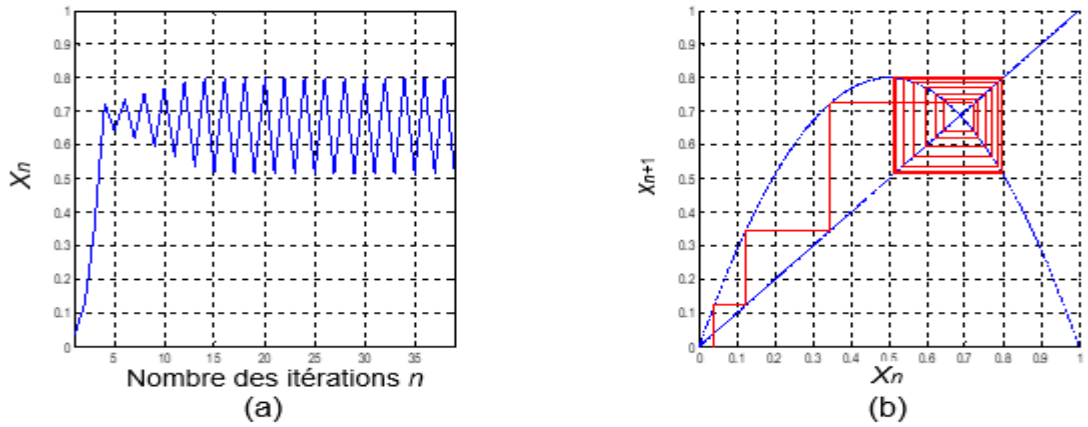

Figure 2.2 : Evolution de la suite $\{x_n\}$ pour r = 3.2 et x_n = 0.04

Remarque :

En modifiant la condition initiale x_0, la suite converge toujours vers le cycle d'ordre 2, par contre la vitesse de convergence est différente.

Il a été montré que pour une valeur critique r_c=3.56996, la suite $\{x_n\}$ ne présente plus une structure ordonnée : cette suite s'apparente à un cycle d'ordre infini. De plus à chaque valeur de x_0 correspond une suite différente. Pour les valeurs de $r < r_c$, quelle que soit la valeur de $x_0 \in]0;1[$, la suite converge vers une structure finie. Pour $r > r_c$, le système devient chaotique.

La figure 2.3 montre l'évolution de la suite dans le cas où r est égal à 4 qui est supérieur à r_c. Contrairement aux exemples précédents, la suite ne converge ni vers un point fixe ni vers une solution périodique : le système que décrit la transformation logistique se trouve dans un régime chaotique.

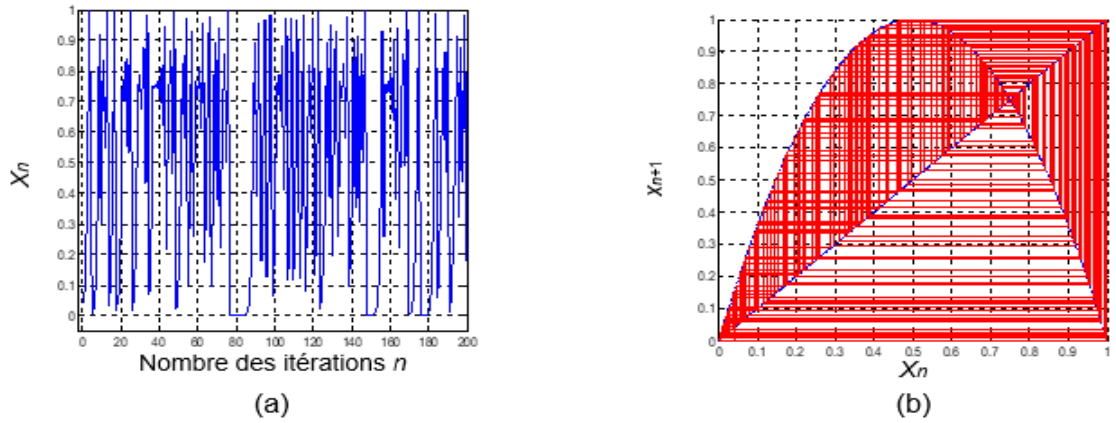

Figure 2.3 : Evolution de la suite $\{x_n\}$ pour r =4 et x_0 =0.04

4. Caractéristiques des systèmes chaotiques

On reconnaît un système chaotique par l'analyse de ses caractéristiques. Dans ce qui suit, on va définir plus précisément les propriétés des systèmes chaotiques dans le cadre particulier d'une fonction d'un segment de R dans lui-même, et on se limitera à une fonction $f : [0;1] \to [0;1]$. Ces définitions seront illustrées par l'exemple du système dynamique dont la carte logistique est donnée par la formule (2.1).

4.1 Sensibilité aux conditions initiales

Pour des conditions initiales très proches, les courbes se superposent, et petit à petit, elles se dissocient pour donner des valeurs complètement différentes. Malgré son caractère déterministe, il est impossible de prédire l'évolution de la trajectoire [25].

Prenons comme valeur de référence x=0.1, pour l'équation logistique et introduisons une erreur de 0.00001 soit $x = 0.10001$. On peut observer sur la figure 2.4 que l'erreur introduite modifie l'évolution des résultats trouvés. Lors des premières itérations, l'erreur est faible, proche de 0, mais que l'erreur initiale introduite génère des résultats erronés.

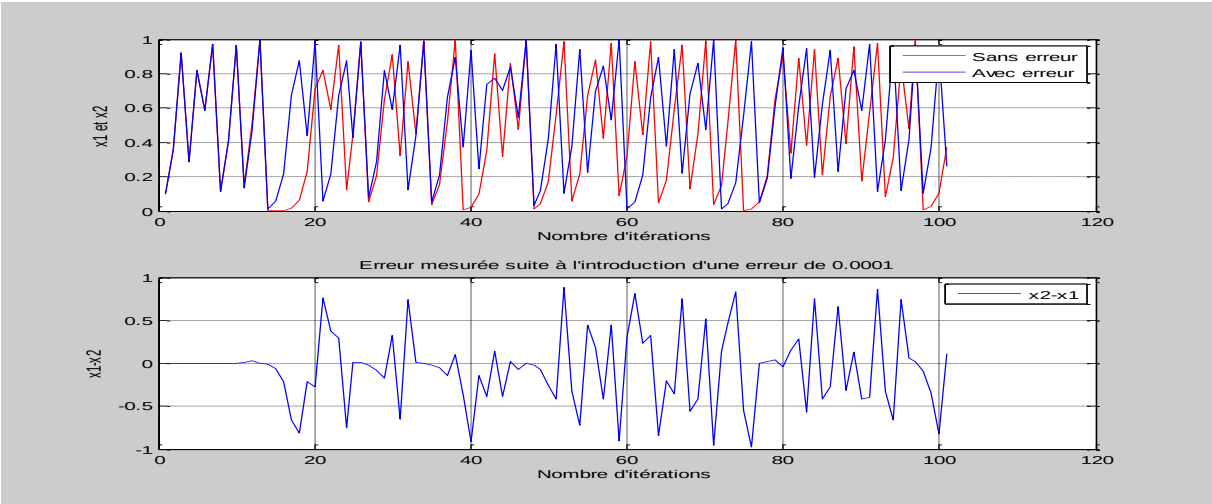

Figure 2.4 : Erreur mesurée suite à l'introduction d'une erreur de 0.0001

4.2 Aspect aléatoire

Une des caractéristiques des systèmes chaotiques est l'aspect aléatoire de son évolution temporel : il est non périodique [25].

La figure 2.5 illustre le caractère de l'évolution de l'un des composants du système de Lorenz par rapport au temps.

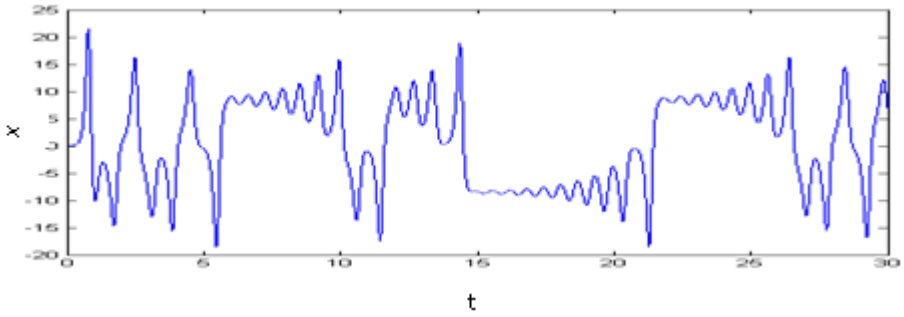

Figure 2.5 : Aspect aléatoire du système de Lorenz.

4.3 Spectre de puissance

Pour un signal chaotique, le spectre de puissance possède une large bande riche en fréquences (figure 2.6), ce qui donne un intérêt à utiliser les systèmes chaotique dans la transmission de données.

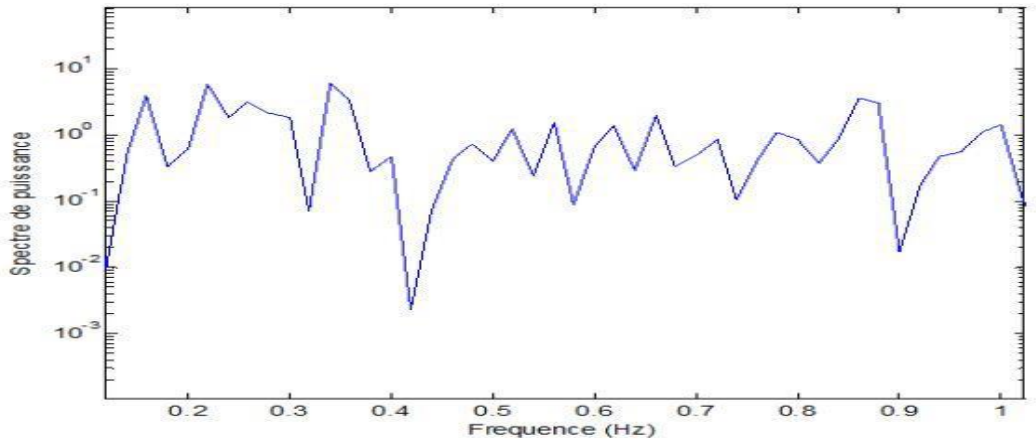

Figure 2.6 : Spectre de puissance du modèle de Lorenz [25]

4.4 Exposants de Lyapunov [30]

Dans les études sur le concept des exposants de Lyapunov, on s'attachait à déterminer si une solution pour un système dynamique pouvait être stable ou non pour tous les temps d'observation. La méthode habituelle pour étudier la stabilité, par exemple la stabilité linéaire, ne convenait pas par le fait de l'existence d'une sensibilité aux conditions initiales.

Les exposants de Lyapunov mesurent le taux de divergence des orbites voisines et Lyapunov a démontré qu'il y avait en fait autant d'exposants que de dimensions dans l'espace de phase du système étudié. Par ailleurs, parmi les exposants retenus pour un système donné, on a l'habitude de prendre généralement l'exposant le plus élevé. Lyapunov a découvert ensuite que cette erreur tendait vers une limite dont la formule est la suivante :

$$\delta(x_0) = \lim_{x\to\infty} \frac{1}{n}\sum_{k=1}^{n} ln|f'(x_{k-1})| \qquad (2.2)$$

Pour le cas de l'équation logistique $x_{n+1} = rx_n(1 - x_n)$, la formule devient :

$$\delta(x_0) = \frac{1}{n}\sum_{k=1}^{n} ln|r - 2rx_n| \qquad (2.3)$$

Pour qu'un système ait une dynamique chaotique, trois conditions sont nécessaires :

- Au moins un exposant de Lyapunov positif qui fait diverger la trajectoire ;
- Au moins un exposant de Lyapunov négatif qui fait replier la trajectoire ;
- La somme des exposants doit être négative pour un système dissipatif (système qui évolue dans un environnement avec lequel il échange de l'énergie).

Un système discret chaotique possède au moins un exposant de Lyapunov négatif.

A partir de la figure 2.7, on remarque que si λ est négatif ou égal à zéro, on est en présence d'un phénomène stable ou périodique. On peut voir que l'exposant de Lyapunov, devient positif pour des valeurs approximativement supérieures à 3.56, ce qui est un fort indicateur du chaos.

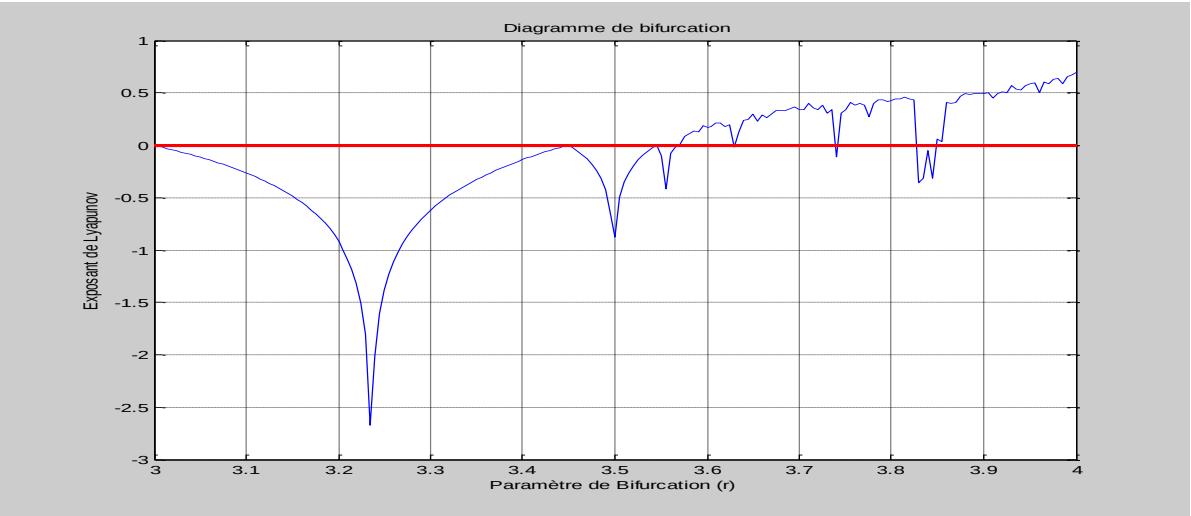

Figure 2.7 : Les exposants de Lyapunov pour la carte logistique

4.5 Diagramme de bifurcation

La figure 2.8 représente le diagramme de bifurcation de la carte logistique créée en faisant varier le paramètre r de 2.5 à 4.

Comme on peut le constater, il y a différentes régions qui dépendent de la valeur de r. C'est d'un intérêt particulier lorsque r = 3 car là commence le doublement de période qui conduit à la dynamique chaotique lorsque r=3.5699 jusqu'à r= 4.

Si l'on fait les différents calculs pour voir l'évolution de la fonction paramétrée de r, on remarque qu'il existe un « trajet » qui mène d'un état - l'ordre - à un autre état - le chaos - Ce trajet, dont les expériences montre qu'il est universel, a été mis en évidence par Mitchell Feigenbaum. Ce dernier a ainsi montré que ce trajet signifie en fait qu'il existe des variations qualitatives abruptes.

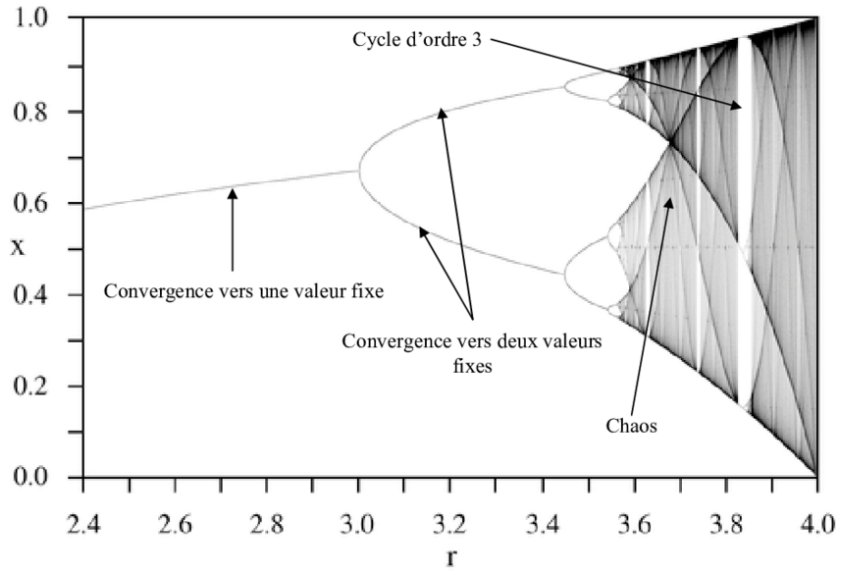

Figure 2.8 : Diagramme de Feigenbaum [24]

Le diagramme de Feigenbaum est devenu, au fil du temps, une des images-types du chaos. La structure qui apparaît directement au regard est celle d'une arborescence. Ainsi, on peut voir que d'une branche principale on passe à deux branches qui elles-mêmes se subdivisent en deux autres branches.

Il est à montrer qu'à chaque division correspond en fait un doublement de la période de régime de la fonction.

5. Le chaos et la cryptographie

A cause de ses propriétés, le chaos présente plusieurs applications dans la cryptographie, car il est difficile de faire des prévisions à long terme sur les systèmes chaotiques.

D'abord, ces systèmes présentent des moyens complètement déterministes qui permettent toujours d'obtenir le même ensemble de valeurs si on a exactement la même fonction (par exemple la carte logistique) et la même valeur initiale. Comparant à l'utilisation des générateurs conventionnels de nombres aléatoires, où la corde des nombres aléatoires ne peut pas être régénérée, le chaos permet de répéter la même corde des nombres si nous employons la même fonction et la même valeur initiale.

Aussi, puisque les fonctions chaotiques sont sensibles aux conditions initiales, n'importe quelle légère différence en valeur initiale utilisée signifierait que le texte chiffré produit en utilisant le chaos sera rigoureusement différent. Ceci signifie que le système sera "plus résistant" contre des attaques fortes car le nombre de clefs possibles, qui dépend du matériel utilisé, est élevé.

6. Conclusion

L'objectif de ce chapitre est de donner quelques généralités sur les systèmes chaotiques. Après un bref historique sur l'évolution de la théorie du chaos, on a défini quelques notions utiles pour la résolution des systèmes chaotiques. Les propriétés des systèmes chaotiques sont présentées avec un peu plus de détail. En particulier les exposants de Lyapunov qui permettent de déterminer si un système est en régime chaotique ou non ainsi que la bifurcation qui permet de visualiser les changements qualitatifs du comportement d'un système chaotique.

Les propriétés que possède le chaos offre la possibilité d'utiliser des systèmes chaotiques dans le domaine de la cryptographie. Le haut niveau de sécurité qu'offre ce type de systèmes ainsi que la rapidité de calcul due à leur structure dynamique permet d'envisager l'utilisation du chaos pour réaliser la fonction de chiffrement et de déchiffrement des documents de grande taille telles que les images. Le chapitre suivant sera consacré à l'étude de cette possibilité.

Chapitre 3

Cryptage Chaotique

Application à la Transmission des Images Médicales

1. Introduction
2. Revue de la littérature
3. Classes et type des systèmes de chiffrement
4. Cryptage chaotique des images
5. Schémas du chiffrement des images
6. Algorithme CKBA
7. Algorithme ECC
8. Description des images utilisées
9. Critères d'évaluation
10. Performances et analyse de sécurité du crypto système
11. Conclusion

1. Introduction

Depuis 1980, l'idée d'utiliser les systèmes chaotiques numériques pour concevoir de nouveaux crypto-systèmes a attiré de plus en plus l'attention de plusieurs chercheurs. En effet, plusieurs caractéristiques fondamentales du chaos, telles que l'ergodicité, la capacité de mélange et la sensibilité aux conditions initiales, peuvent être reliées avec les propriétés de "confusion" et "diffusion" dans la cryptographie classique. Donc c'est une idée naturelle d'utiliser le chaos pour concevoir de nouveaux crypto-systèmes.

Actuellement, il existe deux façons pour utiliser le chaos dans la cryptographie :

- Dans les crypto-systèmes de communications analogiques, qui sont basés principalement sur les techniques de la synchronisation du chaos.
- Dans les crypto-systèmes numériques (Digital Chaotic Ciphers), où on utilise des circuits numériques ou des ordinateurs pour les concevoir.

Dans ce chapitre, on s'intéresse au cryptage chaotique numérique des images [24].

2. Revue de la littérature [31-34]

Avec l'énorme développement de la technologie informatique, l'utilisation d'images numériques comme stockage d'informations ont tendance à augmenter. Parfois, l'image numérique doit être masquée car elle pourrait infliger des préjudices au propriétaire si quelqu'un connaissait ou pouvait manipuler ces images. Ainsi, la cryptographie d'images numériques apparaît comme l'une des méthodes permettant de surmonter ce problème.

En 1975 fut proposé le principe de la cryptographie à clé publique. Ce n'est qu'en 1977 que fut présenté le premier protocole effectif : RSA et le deuxième en 1985 : l'algorithme El Gamel. Principalement basé sur le problème de la factorisation des grands entiers, RSA est encore aujourd'hui la primitive la plus utilisée en cryptographie. Cependant les nombreux progrès effectués dans le domaine de la factorisation font que la taille des clés RSA augmente plus rapidement que ne le requiert l'augmentation de la puissance des ordinateurs. C'est l'une des raisons pour lesquelles la cryptographie basée sur le chaos a connu un grand intérêt depuis son développement durant cette dernière décennie. Elle a non seulement répondu aux exigences de la sécurité mais a aussi démontré une grande résistance à la cryptanalyse.

Les cartes chaotiques ont été utilisées par plusieurs groupes de chercheurs. En particulier, Ekhlas et al. ont proposé une approche de cryptage de contenu textuel basée sur le

chiffrement par bloc et cartes chaotiques. Bien que leur méthode utilise un grand espace de clé, ils ont démontré une faible sécurité. Un ensemble de règles de chiffrement de texte symétrique basé totalement sur le chaos a été proposé par Murillo et al. Leur schéma combinait une clé mystère de longueur 128 bits, cartes logistiques optimisées avec des séquences pseudo-aléatoires, des caractéristiques de texte brut et des permutations à diffusion sphérique. La méthode a démontré une vitesse de cryptage rapide. Volos et al. ont conçu un processus de cryptage de contenu textuel qui est réalisé avec un générateur de bits pseudo-aléatoire chaotique. Le principal avantage de la méthode est sa réalisation simple en utilisant la fonction XOR dans les séquences de bits.

D'autre part, le cryptage d'images chaotique a été étudié de manière approfondie dans la littérature. Par exemple, Wang et al. ont proposé une technique de cryptage d'image utilisant la fonction de hachage et de décalage cyclique. Résistance aux attaques courantes était l'avantage caractéristique de la méthode proposée. Wu et al. ont présenté une photo technique de cryptage entièrement basée sur des cartes chaotiques bidimensionnelles (2D) générées par la combinaison des cartes Henon et Sine. Amina et al. ont proposé une nouvelle approche de chiffrement chaotique spécialisée pour les images médicales. Leur technique comprenait deux étapes : la diffusion des pixels et la confusion chaotique.

Un autre schéma a été développé par Lou et al. pour protéger le contenu des images lors de leur transfert sur Internet. Leur approche a utilisé une carte Hénon-Sine 2D (HSM 2D) pour la diffusion et la permutation des pixels. Bien que leur méthode ait démontré une faible entropie, elle était hautement compressible. Alwadi et al. ont proposé un système rapide et hybride qui combine des cartes chaotiques. Cependant, leur méthode s'est révélée peu robuste contre certaines attaques. Yousfi et al. ont développé un cadre de chiffrement qui utilise une banque de cartes chaotiques, à partir desquelles un critère basé sur la corrélation est utilisé pour sélectionner le candidat carte pour le cryptage.

Parmi les nombreux articles proposés avec l'idée du chaos pour le chiffrement, on cite l'algorithme basé sur des clés chaotiques (CKBA) pour le cryptage d'images présenté par Jui-Cheng Yen et JiunIn Guo [34] qui sera détaillé dans les sections suivantes.

3. Classes et types des systèmes de chiffrement [35]

Depuis 1990, de nombreux systèmes chaotiques numériques ont été proposés et analysés. Il existe en général trois types de systèmes de chiffrement :

3.1 Systèmes de chiffrement chaotiques continus (bit à bit)

3.1.1 Chiffres chaotiques continus basés sur PRNG

Les systèmes chaotiques peuvent produire des orbites pseudo-aléatoires imprévisibles. Grand nombre de chercheurs ont considéré les algorithmes, et les performances d'estimation de PRNG (Générateur de Nombres Pseudo-Aléatoires) basés sur le chaos dont le XOR est l'opération de base. Ces systèmes chaotiques utilisent en général: la fonction logistique et sa version généralisée [36], 2-D attracteur de Hénon [37], fonction de Chebyshev [38], des piecewises linéaires et non linéaires [35], et des systèmes chaotiques p-adique [39].

3.1.2 Chiffrement par approche des systèmes chaotiques inverses

Feldmann et ses collaborateurs ont proposé le modèle général pour concevoir des systèmes de communications chaotiques sécurisés qu'ils ont appelés systèmes chaotiques inverses. Ce modèle peut être utilisé dans les deux cas analogique et numérique [35].

3.2 Systèmes de chiffrement chaotique par blocs

Les systèmes de chiffrement chaotique par blocs manipulent des blocs de texte en clair et de texte chiffré, où en général, ils sont basés sur des systèmes chaotiques inverses (Backwards) et des systèmes par itérations de la fonction chaotique (Forwards) [35].

3.3 Autres systèmes chaotiques

Récemment, des idées nouvelles ont été proposées, par exemple l'introduction des automates cellulaires [40], la recherche du texte en clair dans les séquences pseudo-aléatoires (Searching-Based Chaotic Ciphers), les chiffres chaotiques à clef publique (Chaotic Public-Key Ciphers), et des méthodes chaotiques pour le cryptage des images qui fera l'objet de la prochaine section.

4. Le cryptage chaotique des images

Le développement énorme des télécommunications et d'internet rend la sécurité d'image numérique de plus en plus importante ; qui est nécessaire dans plusieurs applications, TV, systèmes médicaux, images militaires, images médical, …etc.

Les techniques de cryptage classiques telles que le DES, RSA,… ne sont pas généralement convenables pour le chiffrement des images en temps réel, et ce à cause de leur faible vitesse.
L'idée d'utiliser le chaos dans le chiffrement des images a été introduite et discutée par Fridrich, Scharinger (1998) ; Kocarev & Jakimovski (2001) ; Masuda & Aihara, Li (2002) ; Mao et Chen (2003).

5. Schémas du chiffrement des images [41]

Fondamentalement, il y a deux façons pour utiliser le chaos, dans le domaine du chiffrement des images :

- Utiliser le chaos comme une source pour produire des bits pseudo-aléatoires avec les propriétés statistiques désirées au chiffrement.
- Utiliser des fonctions chaotiques en 1-D, 2-D ou 3-D pour faire les permutations et les substitutions secrètes nécessaires à l'image cryptée.

On s'intéresse ici aux algorithmes chaotiques 1-D, proposés par Yen et Guo [34], qui sont la base de tous les autres algorithmes qui utilisent la fonction logistique $f(x) = rx(1-x)$, où la condition initiale $x(0)$ et le paramètre de control r jouent le rôle de la clef secrète. Ils sont basés sur l'idée de base suivante :

- Exécuter la fonction logistique pour produire des séquences binaires pseudo-aléatoires $\{b(i)\}$, à partir de la représentation n bits de chaque état chaotique.
$$x(k) = b(nk+0)b(nk+1)\dots b(nk+n-1)$$

- Utiliser ces séquences binaires chaotiques $\{b(i)\}$, pour contrôler les permutations, et les substitutions pseudo-aléatoires de chaque pixel de l'image.

On distingue les algorithmes suivants :

- **BRIE** (Bit Recirculation Image Encryption)
- **CKBA** (Chaotic Key-Based Algorithm)
- **HCIE** (Hierarchic Chaotic Image Encryption)
- **CNNSE** (Chaotic Neural Network for Signal Encryption)
- **DSEA** (Domino Signal Encryption Algorithm)

6. CKBA (Chaotic Key-Based Algorithm) [34, 35]

La transmission de données d'images fixes doit satisfaire à deux objectifs, à savoir, la réduction limitée du volume des données pour la facturation des réseaux publics de communication et la sécurité maximale des informations transmises. Afin de satisfaire les deux objectifs, un algorithme chaotique à base de clés (CKBA) a été proposé.

Supposant que l'image en clair ait une dimension de *M*×*N.*

Processus de chiffrement :

1. *Les clefs secrètes* :
   Sélectionner deux clefs *key*1 et key2 (8 bits), et la condition initiale $x(0)$ d'un système chaotique unidimensionnel, comme une clef secrète du système de chiffrement.
   Le critère de base pour choisir les clefs doit satisfaire :
   $$\sum_{i=0}^{7}(a_i \oplus d_i) = 4 \quad O\grave{u} \quad Key1 = \sum_{i=0}^{7} a_i \times 2^i \quad et \quad key2 = \sum_{i=0}^{7} b_i \times 2^i \qquad (3.1)$$

2. *Initialisation* :
   Générer les séquences chaotiques $\{x(i)\}_{i=0}^{MN/8-1}$.
   À partir de la représentation binaire de 16 bits de $x(i)$, générer une séquence pseudo-aléatoire binaire (PRBS) $\{b(i)\}_{i=0}^{2MN-1}$.
   $$x(i) = 0, b(16i+0)b(16i+1)\ldots b(16i+15) \qquad (3.2)$$

3. *Chiffrement* :
   Une fois les $\{b(i)\}$ sont générés, le chiffrement peut commencer. Pour le pixel en clair $(x,y)(0 \le x \le M-1, 0 \le y \le N-1$, le pixel chiffré correspondant $f'(x,y)$ est déterminé par la règle suivante :
   $$f'(x,y) = \begin{cases} f(x,y) & XOR & Key1, b'(x,y) = 3 \\ f(x,y) & XNOR & Key1, b'(x,y) = 2 \\ f(x,y) & XOR & Key2, b'(x,y) = 1 \\ f(x,y) & XNOR & Key2, b'(x,y) = 0 \end{cases} \qquad (3.3)$$
   Où $b'(x,y) = 2 \times b(l) + b(l+1)$ et $l = x \times N + y$.

Processus de déchiffrement :

La procédure de déchiffrement est juste comme celle de chiffrement.

- **Exemple de chiffrement d'un texte :**

Processus de chiffrement

Étape 1 : Alice écrit le texte à crypter : « **cryptosystem for securing medical data »**

Étape 2 : Les codes ASCII correspondants aux caractères du texte sont :

{99, 114, 121, 116, 111, 115, 121, 115, 116, 101, 109, 32, 102, 111, 114, 32, 115, 101, 99, 117, 114, 105, 110, 103, 32, 109, 101, 100, 105, 99, 97, 108, 32, 100, 97, 116, 97}

Étape 3 : Génération de la fonction logistique : $X_{(n+1)} = rX_{(n)}(1-X_{(n)})$

{0.66, 0.89, 0.39, 0.95, 0.20, 0.63, 0.93, 0.26, 0.76, 0.7, 0.80, 0.63, 0.93, 0.25, 0.75, 0.76, 0.74, 0.77, 0.70, 0.84, 0.54, 0.99, 0.02, 0.09, 0.32, 0.87 ,0.45, 0.99, 0.04, 0.14, 0.49, 1.00, 0.00, 0.01, 0.02, 0.09, 0.32, 0.87, 0.44, 0.99, 0.06, 0.21, 0.67, 0.88, 0.42, 0.98, 0.10, 0.35, 0.91, 0.33, 0.88, 0.43, 0.98, 0.09, 0.31, 0.8, 0.48, 1.00, 0.01, 0.02, 0.09, 0.33, 0.88, 0.41, 0.97, 0.13, 0.44, 0.99, 0.06, 0.22, 0.68, 0.87, 0.45, 0.99, 0.04, 0.14, 0.49, 1.00, 0.00 ,0.00, 0.01, 0.05, 0.18, 0.59, 0.97}

Étape 4 : Conversion binaire de x (i) sur 16 bits :

{1100101000100011101010100001111011100100010001110110001011011110111001011110100110010010010011010000110100010111011100101001001000001110101000111000001110011010}

Étape 5 : Calcul de b'

b' = { 1, 3, 2, 0, 1, 2, 1, 2, 0, 0, 0, 1, 2, 1, 2, 0, 0, 1, 2, 0, 1, 2, 0, 0, 1, 2, 0, 0, 1, 3, 0, 1, 2, 0, 0, 1, 3, 3, 2, 1, 0, 0, 1, 3, 3, 2, 1, 2, 1, 2, 3, 3, 2, 1, 2, 1, 2, 1, 2, 0, 1, 2, 1, 2, 1, 2, 0, 0, 0, 1, 2, 1, 2, 0, 0, 0, 1, 3, 3, 3, 0, 0, 0, 1}

Étape 6 : Calcul de f' (le Message chiffré) avec : key1 = 23, key2= 84

f' = {138, 101, 45, 220, 157, 59, 154, … 200, 205, 157, 118}

Étape 9 : Alice envoie à Bob le message chiffré f'

Processus de déchiffrement

Bob reçoit le message chiffré et suit les mêmes étapes qu'Alice a suivies pour déchiffrer le message. Il retrouve le même vecteur b' et donc le message est récupéré.

7. Algorithme ECC [42]

Afin d'analyser les performances de l'algorithme CKBA, basé sur un système chaotique, on a proposé de faire une comparaison avec l'algorithme ECC, basé sur les courbes elliptiques. Ce dernier a été abordé d'une manière détaillée dans la référence [42].

Dans cet algorithme, Alice et Bob s'accordent sur plusieurs paramètres publiquement :

- Une courbe elliptique dont les paramètres sont : *A, B* et *p* :

$$E : y^2 = x^3 + Ax + B \ \ mod(p) \tag{3.4}$$

- Un générateur de clés publiques qui représente un point de la courbe, $G \in E$
- Deux clés privées ka et kb pour calculer les deux clés publiques (* représente un doublement consécutif de points). :

$$Wa = ka * G \quad \text{et} \quad Wb = kb * G$$

Secrètement, Alice forme la clé commune K= (k1, k2), en utilisant sa clé privée ka et la clé publique de Bob Wb : $k = ka * Wa = (k_1, k_2) mod(p)$

Processus de chiffrement :

1. Alice écrit le message à envoyer ; puis le convertit en code ASCII correspondant.
2. Elle partitionne les valeurs obtenues sur des groupes de dimension prédéfinie.
3. Elle convertit les valeurs de chaque groupe en grandes valeurs entières, en utilisant la fonction *sum*.
4. Le nombre de groupes est-il impair ?
   Si Oui : Ajouter 32 à la fin pour pouvoir former des paires M= (m_1, m_2) qui représentent des points sur la courbe elliptique (32 représente un espace donc cette étape ne va pas modifier l'information).

   Sinon : À partir des paires obtenues, on calcule : C= (C_1, C_2) tel que :

$$C_1 = m_2 * k_1 + m_1 mod(p) \ \ et \ \ C_2 = m_2 + m_2 * k_2 + m_1 mod(p) \tag{3.5}$$

5. Sélectionner 1<ρ<p-1 et calculer ρ*G et ρ*Wb en utilisant le doublement successif de points.

6. Calculer C+ρ*Wb en utilisant l'algorithme d'addition de points.
7. Alice envoie {ρ*G & C+ρ*Wb}.

Processus de déchiffrement :

1. Bob reçoit {ρ*G & C+ρ*Wb} séparément.
2. Bob multiplie sa clé privée Kb par le point ρ*G et le soustrait de C+ ρ*Wb pour obtenir C= (C_1, C_2) : {C+ ρ*Wb}-Kb*ρ*G. (pour la soustraction, on multiplie Kb*ρ*G par (-1) et on applique une addition de deux points.
3. Une fois C obtenu, Bob utilise la clé commune K= (k1, k2) pour récupérer M= (m1, m2) tel que : $m_2=C_2-k_2C_1$ mod(p) et $m_1=C_1-k_1m_2$ mod(p).
4. Récupérer les valeurs ASCII en utilisant la fonction fixe.
5. Convertir les valeurs ASCII en caractères.
6. Bob récupère le texte clair.

8. Description des images utilisées

Les images médicales que nous avons implémentées sont :

8.1 Image de Scanner ou CT

L'image de la Figure 3.1 est récupérée d'une base de données ouverte d'images de radiographie pulmonaire et de tomodensitométrie de patients positifs ou suspectés de COVID-19 ou d'autres pneumonies virales et bactériennes (MERS, SRAS et ARDS). Les données sont collectées auprès de sources publiques ainsi que par collecte indirecte auprès des hôpitaux et des médecins.

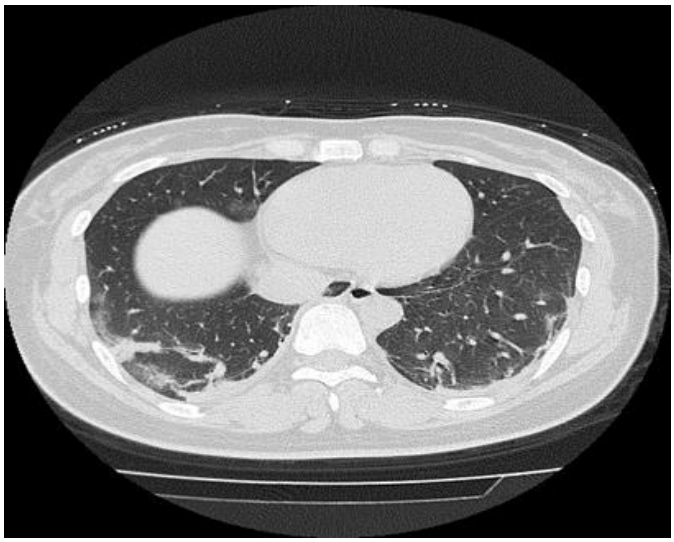

Figure 3.1 : Image médicale Scanner de taille 512*512 pixels [43].

8.2 Image par ultrasons ou US

L'image de la Figure 3.2 est téléchargée du site ultrasoundcases qui possède une bibliothèque d'échographie gratuite comptant plus de 7000 cas, proposée par SonoSkills et FUJIFILM Healthcare Europe [44].

L'image choisie décrit l'aspect des calculs biliaires : Lithiase biliaire avec calculs biliaires mobiles dans la vésicule biliaire.

Figure 3.2 *:* Image médicale US, de taille 300*225 Pixels [44].

9. Critères d'évaluation

Pour analyser la robustesse du crypto système de transmission étudié, la simple inspection visuelle s'avère être insuffisante pour juger le chiffrement d'une image. L'analyse menée dans ce qui suit a alors pour but d'évaluer le degré de chiffrement des images.

9.1 Analyse statistique

9.1.1 Histogramme

L'histogramme d'une image montre la manière de distribution des pixels dans cette image en traçant le nombre de pixels correspondant à chaque intensité de couleur [25].

Les images générées par un bon algorithme de cryptage doivent avoir des histogrammes uniformes (toutes les couleurs ont la même probabilité de se produire), de manière à améliorer leur résistance à l'analyse statistique c.à.d. que l'histogramme de l'image cryptée doit être très différent de celui de l'image originale. Ainsi, l'attaquant ne peut pas extraire l'information à partir de l'histogramme de l'image cryptée.

9.1.2 Corrélation entre l'image originale et l'image chiffrée

En plus de l'analyse d'histogrammes qui est juste un test visuel, nous allons également analyser la corrélation entre les diverses paires des images originale, chiffrée et déchiffrée. Les coefficients de corrélation sont calculés comme suit [45]:

$$CC = \frac{\frac{1}{(H.W)}\sum_i^H \Sigma_j^W \left(o_{i,j}-\bar{O}\right)\left(C_{i,j}-\bar{C}\right)}{\left[\left(\frac{1}{(H.W)}\sum_i^H \Sigma_j^W \left(o_{i,j}-\bar{O}\right)^2\right)\left(\frac{1}{(H.W)}\sum_i^H \Sigma_j^W \left(C_{i,j}-\bar{C}\right)^2\right)\right]^{1/2}} \quad (3.6)$$

$$\text{Avec}: \bar{0} = \frac{1}{(H.W)}\sum_i^H \sum_j^W \left(o_{i,j}\right) \quad \text{et} \quad \bar{C} = \frac{1}{(H.W)}\sum_i^H \sum_j^W \left(C_{i,j}\right)$$

9.2 Analyse différentielle

Par cette analyse, on met en évidence la sensibilité des images chiffrée et déchiffrée par rapport à l'image originale. PSNR et SSIM sont des mesures que nous allons utiliser pour quantifier la différence entre deux images.

9.2.1 **PSNR** [42]

PSNR est l'acronyme de Peak Signal to Noise Ratio ou rapport signal à bruit de crête. Il représente une mesure de distorsion et est largement utilisé dans le traitement du signal pour mesurer la qualité d'un signal en calculant le rapport entre le signal d'origine et le bruit. Il se mesure en décibels (dB) :

$$PSNR = 10 \times log_{10} \frac{(2^R - 1)^2}{MSE} \tag{3.7}$$

Où R représente le nombre de bits désignés pour un pixel ; et MSE est l'erreur quadratique moyenne.

Si MSE est égale à zéro, cela signifie que l'image d'origine et celle après traitement sont identiques et la valeur du PSNR sera infinie. Plus ce rapport est grand, meilleure est la qualité de l'image.

Un PSNR élevé, indique que l'image modifiée est très proche de l'originale. Une valeur de plus de 20 dB est acceptable (varie dans différents cas selon le type de problème). Cependant, le PSNR fonctionne pour la comparaison d'intensité et ne fournit aucune information structurelle. Par conséquent, on peut également appliquer d'autres méthodes telles que le SSIM.

9.2.2 **SSIM** [42]

Aucune de ces mesures objectives citées n'est particulièrement efficace pour prédire la réponse visuelle humaine à la qualité d'image. Parfois, les PSNR varient énormément entre deux images presque impossibles à distinguer ; de même, on peut avoir deux images avec le même PSNR où il y a une différence de qualité très évidente. La mesure de l'indice de similarité structurelle (SSIM) et certaines de ses variantes sont généralement considérées comme meilleures de ce point de vue, mais pas encore des modèles parfaits pour la perception humaine.

Le SSIM est une mesure de la similitude entre deux images. Ses valeurs sont comprises entre 0 et 1. Le 1 signifie que l'image de reconstruction correspond parfaitement à l'image d'origine ; alors que le 0 indique la différence totale.

Généralement, on retient les valeurs : 0.97, 0.98 et 0.99 pour de bonnes techniques de reconstruction de qualité.

$$SSIM(x,y) = \frac{(2\mu_x\mu_y+c_1)(2\sigma_{xy}+c_2)}{(\mu_x^2+\mu_y^2+c_1)(\sigma_x^2+\sigma_y^2+c_2)} \quad (3.8)$$

Où μ_x *et* μ_y: Moyenne de *x et y* respectivement.

σ_x *et* σ_y: Ecart type de *x* et *y*, respectivement.

σ_{xy} : Covariance de *x* et *y*.

$c_1 = (k_1 L)^2$; $c_2 = (k_2 L)^2$.

$k_1 = 0.01$; $k_2 = 0.03$.

$L = 2^R - 1$; R représente le nombre de bits par pixel

10. Performances et analyse de la sécurité du crypto système

10.1 Implémentation sur l'image Scanner

Les figures 3.3 – 3.4 représentent le chiffrement/déchiffrement de l'image CT décrite précédemment avec les deux algorithmes ECC et CKBA. Les valeurs du PSNR, SSIM et coefficient de corrélation sont données dans le Tableau 3.1.

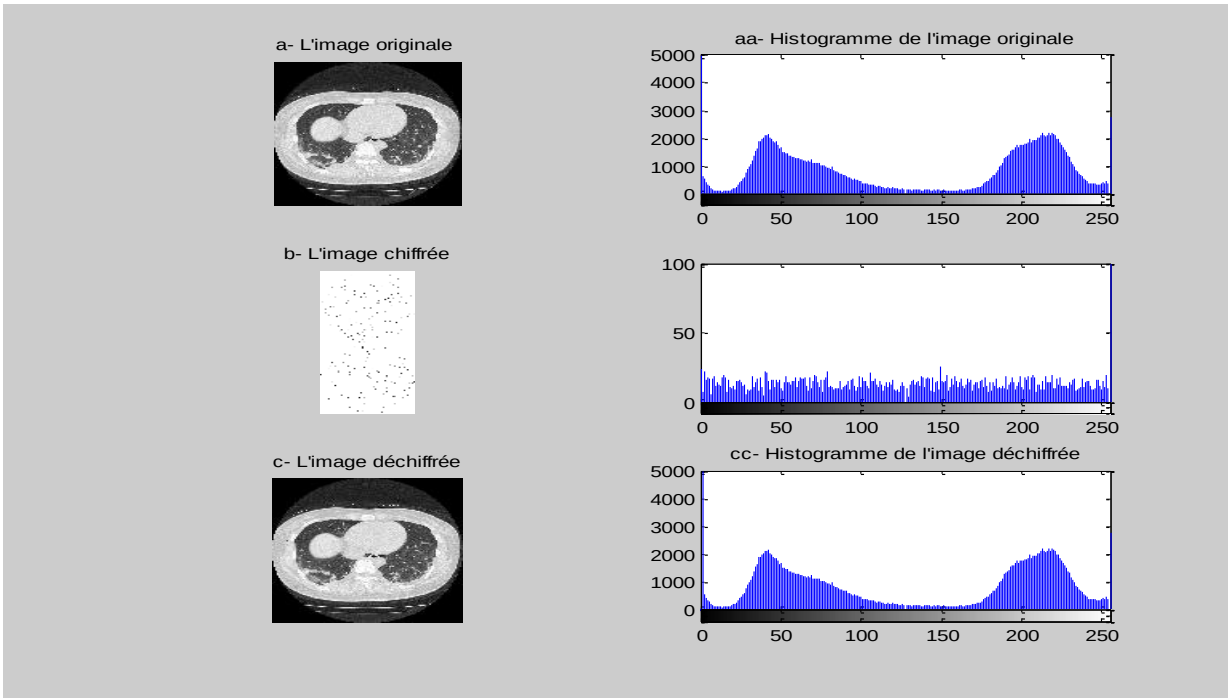

Figure 3.3 : Images originale, chiffrée et déchiffrée avec leurs histogrammes respectifs : *Algorithme ECC.*

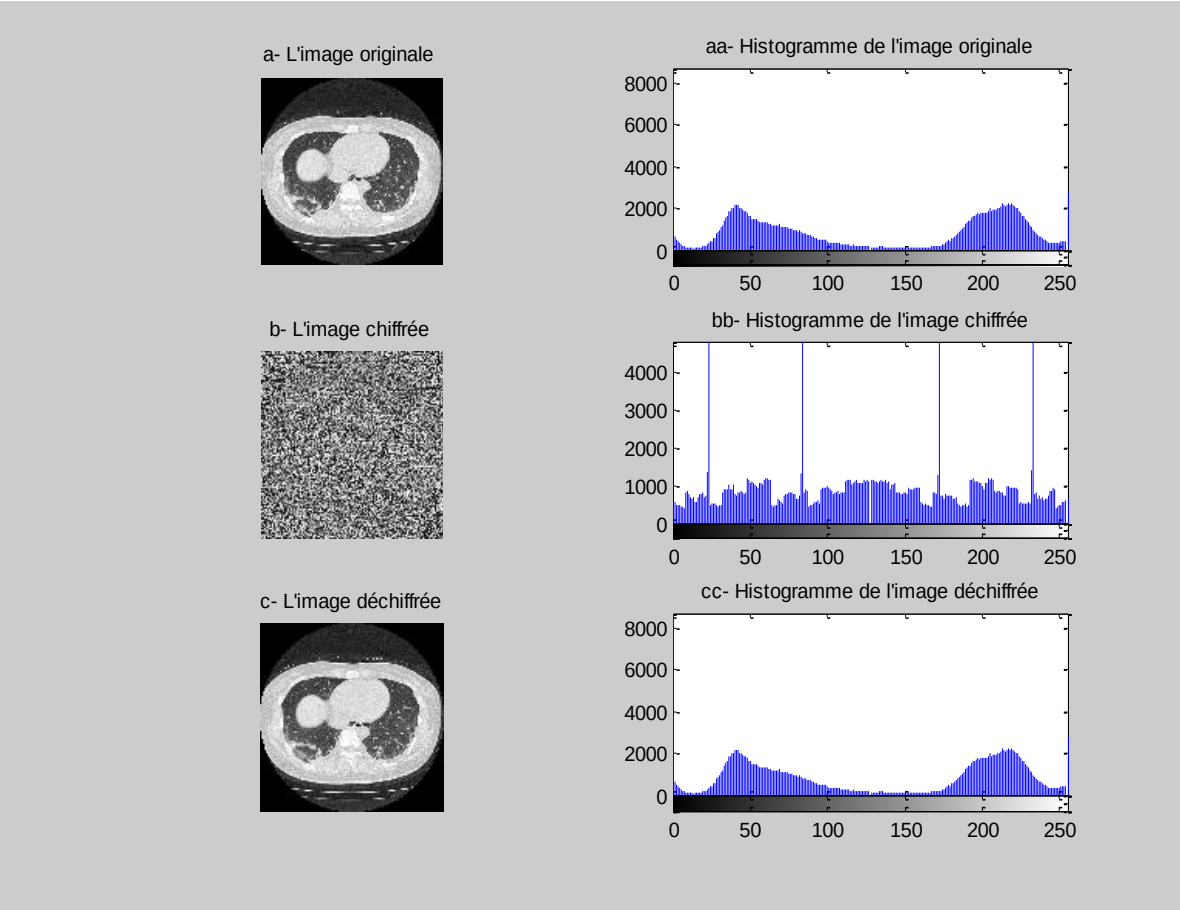

Figure 3.4: Images originale, chiffrée et déchiffrée avec leurs histogrammes respectifs : *Algorithme CKBA*.

Tableau 3.1 : Mesures des performances des différents algorithmes pour l'image CT.

Critère	CKBA	ECC
PNSR (Originale et chiffrée) en dB	6.91	3.64
PNSR (Originale et déchiffrée) en dB	**∞**	**47.25**
SSIM (Originale et chiffrée)	0.03	0.09
SSIM (Originale et déchiffrée)	**1.00**	0.98
Corrélation (Originale et chiffrée)	0.0202	-0.0028
Corrélation (Originale et déchiffrée)	**1.00**	0.9999

Interprétation :

D'après les histogrammes représentés dans les figures 3.3 – 3.4, on constate visuellement que l'image originale est différente de l'image chiffrée mais similaire à celle déchiffrée.

Les valeurs du PSNR montrent que l'image originale est différente de l'image chiffrée cependant elle est parfaitement reconstruite avec les deux algorithmes. Les valeurs du

SSIM confirment que l'image chiffrée est dégradée et l'image reconstruite est de très bonne qualité avec l'algorithme CKBA (égale à 1) ; cependant elle est largement acceptable avec ECC. On peut conclure que les algorithmes de chiffrement utilisés font en sorte que la dépendance des propriétés statistiques des images chiffrées et originales soit quasi aléatoire.

Il est clair que les coefficients de corrélation de l'image originale et l'image chiffrée dans les deux algorithmes sont très petits. Par conséquent, il n'y a pas de corrélation entre l'image originale et l'image chiffrée qui prend alors les caractéristiques d'une image aléatoire. Par contre la corrélation est forte entre l'image originale et déchiffrée.

10.2 Implémentation sur l'image US

Les figures 3.5 – 3.6 représentent le chiffrement/déchiffrement de l'image CT décrite précédemment avec les deux algorithmes ECC et CKBA. Les valeurs du PSNR, SSIM et coefficient de corrélation sont données dans le Tableau 3.2.

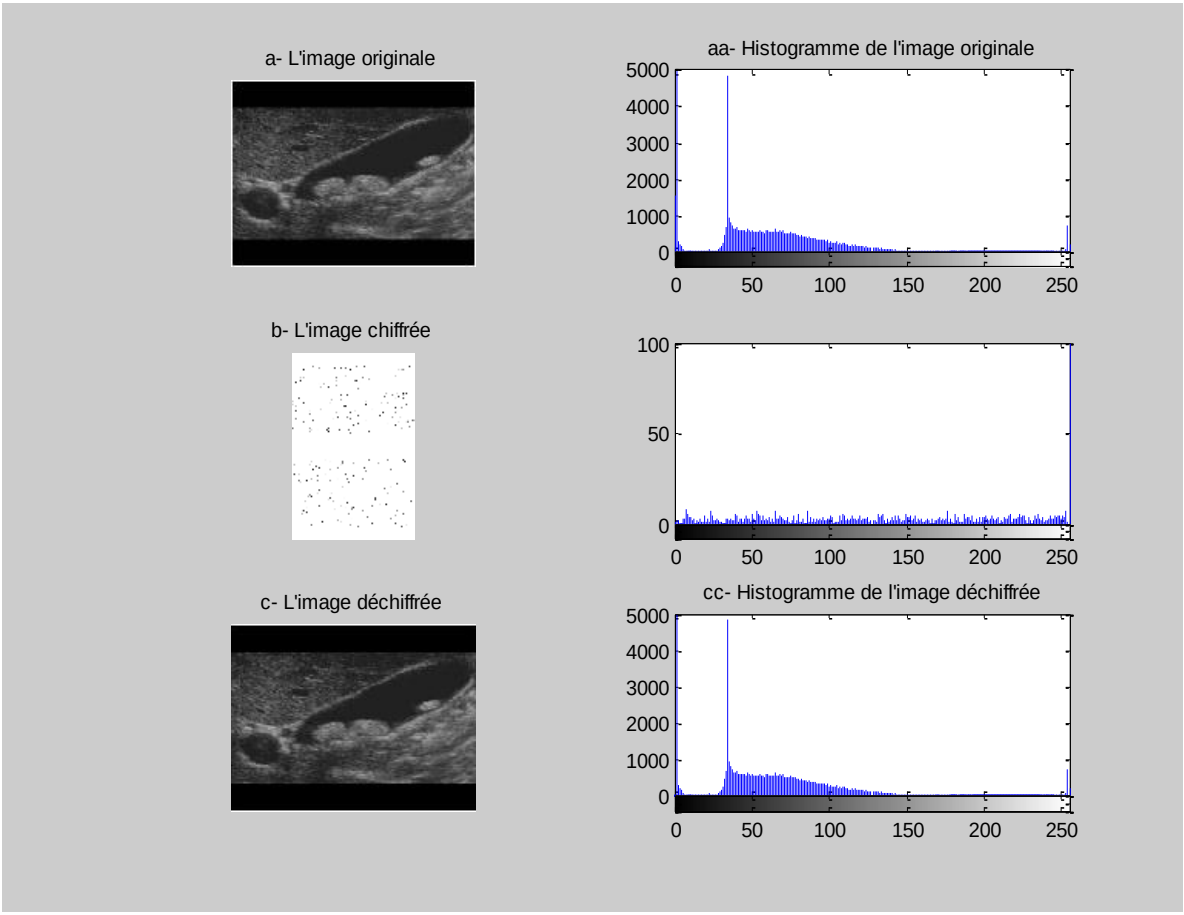

Figure 3.5 : Images originale, chiffrée et déchiffrée avec leurs histogrammes respectifs : *Algorithme ECC*.

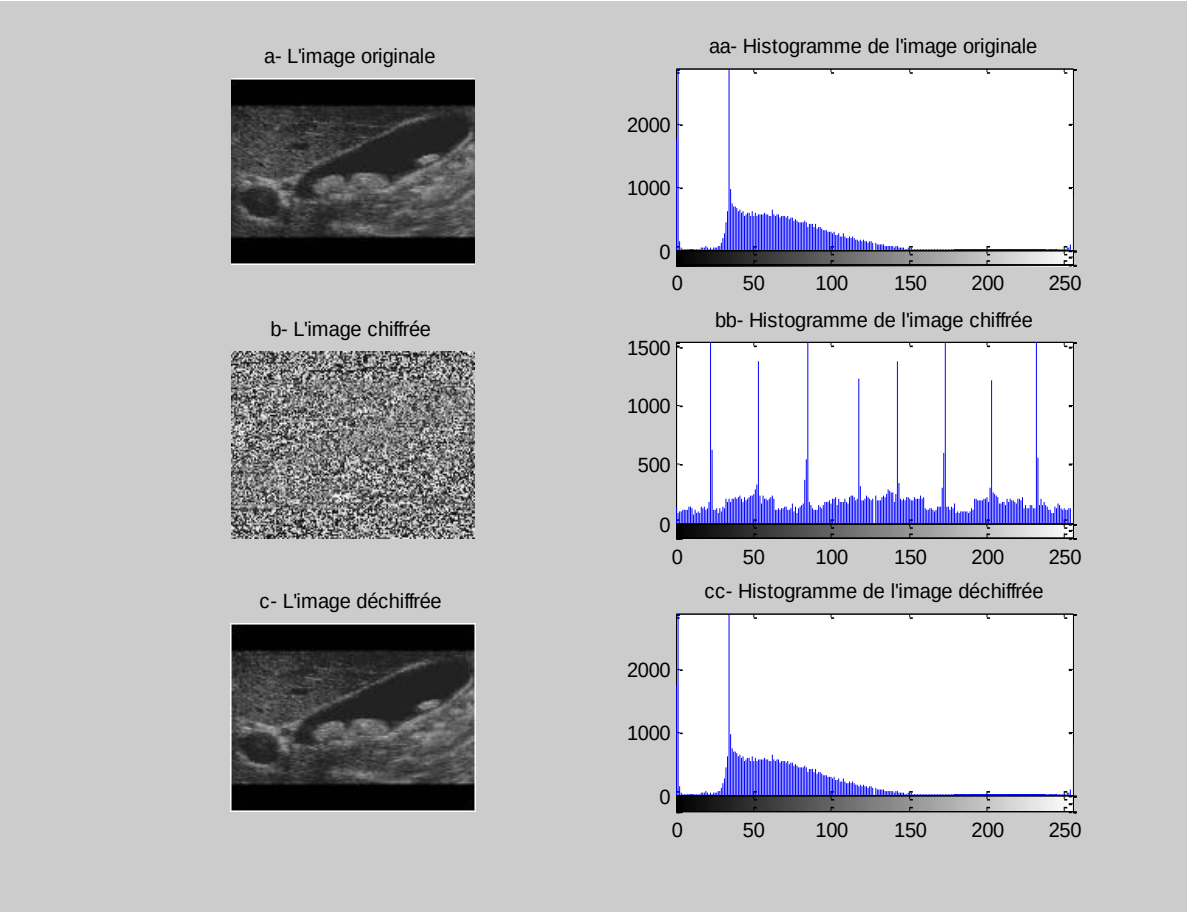

Figure 3.6 : Images originale, chiffrée et déchiffrée avec leurs histogrammes respectifs : *Algorithme CKBA*.

Tableau 3.2 : Mesures des performances des différents algorithmes pour l'image US.

Critère	CKBA	ECC
PNSR (Originale et chiffrée) en dB	**7.03**	1.77
PNSR (Originale et déchiffrée) en dB	∞	51.86
SSIM (Originale et chiffrée)	0.01	0.07
SSIM (Originale et déchiffrée)	**1.00**	**1.00**
Corrélation (Originale et chiffrée)	0.0230	-0.0025
Corrélation (Originale et déchiffrée)	**1.00**	0.9999

Interprétation :

Il ressort des figures 3.5 – 3.6 que les histogrammes des images chiffrées sont uniformément distribués (ECC) et aléatoires (CKBA) par rapport aux histogrammes des images d'origine. La dépendance des histogrammes des images chiffrées et celles d'origine

est quasi aléatoire. Ceci rend la cryptanalyse de plus en plus difficile car les images chiffrées ne fournissent aucun élément reposant sur l'exploitation de l'histogramme et permettant de concevoir une attaque statistique sur les procédés de chiffrement étudiés. Cependant, cette dépendance est relativement la même pour les histogrammes des images déchiffrées et originales.

D'après le tableau 3.2, la valeur du PSNR (Originale et chiffrée) est très faible et s'approche du zéro pour ECC. Ce qui montre que l'image chiffrée est nettement dégradée. Alors que l'image chiffrée est parfaitement reconstruite avec les deux algorithmes utilisés (PSNR tend vers l'infini).

Les valeurs du SSIM confirment que, pour les deux algorithmes, l'image chiffrée est dégradée $(SSIM \approx 0)$ (pas de similitude entre les deux images) et l'image déchiffrée est de très bonne qualité$(SSIM = 1)$.
Il est clair que les coefficients de corrélation des images originale et chiffrée dans les deux algorithmes ECC et CKBA sont très petits. Par conséquent, il n'y a pas de corrélation entre ces images.

10.3 Temps d'exécution

Le temps d'exécution est l'un des paramètres importants qu'on doit prendre en considération pour tester les performances de l'opération de chiffrement/déchiffrement en temps réel. Le temps d'exécution a été calculé pour les deux images avec différentes tailles.

Tableau 3.3 : Temps d'exécution de chaque algorithme pour chaque image**.**

Image	Taille (Pixels)	Temps d'exécution (s)	
		CKBA	ECC
US	300x225	1.516531	16.8643
CT	512x512	3.263263	51.9003

10.4 Sensibilité au changement des conditions initiales

La sensibilité au changement des conditions initiales est une caractéristique essentielle pour un bon crypto système qui contribue à la sécurité de ce dernier contre les attaques exhaustives. Pour évaluer les performances du système dans ce sens, on effectue le test suivant :

Une image est chiffrée et déchiffrée avec des conditions initiales différentes.

D'après la Figure 3.7, on constate que l'image n'a pas été déchiffrée correctement déchiffrée par l'algorithme CKBA.
On peut conclure que le système chaotique utilisé est très sensible à tout changement dans la condition initiale.

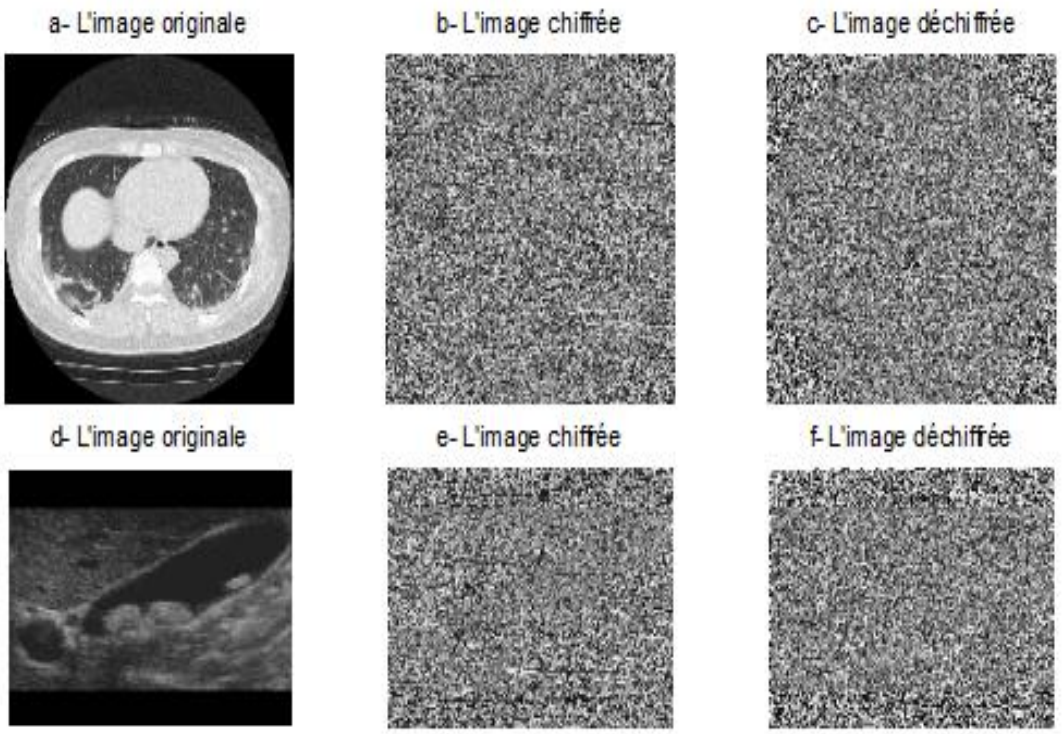

Figure 3.7 : Images originales, chiffrées et déchiffrées avec une condition initiale égale à :

x(0) = 0.78963145698 au niveau de l'émetteur ;

x(0) =0.78963145699 au niveau du récepteur

11. Conclusion

Dans ce chapitre, nous avons chiffré/déchiffré les images US et Scanner avec les deux algorithmes : CKBA et ECC. Les critères de validation sur lesquels nous nous sommes basés sont : Histogramme, PSNR, SSIM, Corrélation et le temps d'exécution.

Les résultats obtenus montrent que l'algorithme CKBA présente les meilleures performances en chiffrement vue la distribution uniforme ou aléatoire de l'histogramme de l'image

chiffrée. On parle ici de dépendance des propriétés statistiques de l'image chiffrée et originale. Dans ce cas la probabilité qu'un cryptanalyste puisse exploiter l'histogramme de l'image chiffrée pour tirer une information utile est quasi nulle.

D'après le temps d'exécution, l'algorithme CKBA offre le meilleur compris entre la qualité et la rapidité de chiffrement/déchiffrement.

Cependant, des tests de cryptanalyse sont nécessaires pour confirmer la supériorité d'un algorithme sur un autre. Analyse suggérée pour un travail futur.

Chapitre 4

Implémentation du Crypto-Système sur Cartes Arduino UNO

1. Introduction
2. Description de la partie matérielle
3. Description de la partie logicielle
4. Présentation de l'application pratique réalisée
5. Conclusion

1. Introduction

Dans ce chapitre, on envisage une implémentation du crypto-système chaotique, étudié dans le chapitre précédent, sur deux cartes Arduino UNO. Sur ces dernières seront implémentés les blocs émetteur et récepteur respectivement. Une description détaillée de la carte utilisée sera présentée. On termine par la présentation de l'application pratique réalisée, l'interprétation et la comparaison des résultats pratiques obtenus avec les résultats théoriques du chapitre précédent.

2. Description de la partie matérielle

2.1 La carte Arduino

2.1.1 Présentation de la carte

Le projet Arduino a été créé, en hiver 2005, par une équipe de développeurs, composée de Massimo Banzi, David Cuartielles, Tom, Igoe, Gianluca Martino, David Mellis et Nicholas Zambetti. Le "système Arduino" a été créé dans le but de permettre aux débutants, amateurs ou professionnels de créer des systèmes électroniques plus ou moins complexes de manière aisée.

Le nom Arduino trouve son origine dans le nom du bar dans lequel l'équipe avait l'habitude de se retrouver. Arduino est aussi le nom d'un roi italien, personnage historique de la ville «Arduino d'Ivrée».
Le système Arduino donne la possibilité d'allier les performances de la programmation à celles de l'électronique. L'avantage majeur de l'électronique programmée c'est qu'elle simplifie grandement les schémas électroniques et par conséquent, le coût de la réalisation, mais aussi la charge de travail à la conception d'une carte électronique.
Arduino est une plate-forme de prototypage d'objets interactifs à usage créatif constituée d'une carte électronique et d'un environnement de programmation. Sans tout connaître ni tout comprendre de l'électronique, cet environnement matériel et logiciel permet à l'utilisateur de formuler ses projets par l'expérimentation directe avec l'aide de nombreuses ressources disponibles en ligne.
Arduino est utilisé dans de nombreuses applications comme l'électrotechnique industrielle et embarquée, la modélisation, la domotique mais aussi dans des domaines différents comme l'art contemporain et le pilotage d'un robot, la commande des moteurs et la conception des jeux de lumières.

2.1.2 Différents composants de la carte Arduino UNO [46,47]

Les cartes Arduino sont généralement équipées d'une puce ATmega 328. Celles qui sont plus évoluées sont dotées d'une puce ATmega 2560 qui a plus de mémoire et d'E/S. La méthode de programmation est pratiquement la même, les différences peuvent apparaitre pour les fonctions les plus complexes.

Le modèle UNO de Arduino est une carte dont le cœur est un microcontrôleur de référence ATMega 328 cadencé à 16 MHz. Elle possède 32 Ko de mémoire flash destinée à recevoir le programme, 2 Ko SRAM (mémoire vive) et 1 Ko d'EEPROM (mémoire morte pour les données). Elle offre 14 broches d'entrée/sortie numériques dont 6 peuvent générer des PWM.
Elle permet aussi de mesurer des grandeurs analogiques grâce à ses 6 entrées analogiques.
Cette carte Arduino peut aussi s'alimenter et communiquer avec un ordinateur grâce à son port USB. Une autre alimentation est possible grâce à son connecteur power jack. Ci-dessous est représentée une synoptique de la carte avec l'indication de ses différents composants.

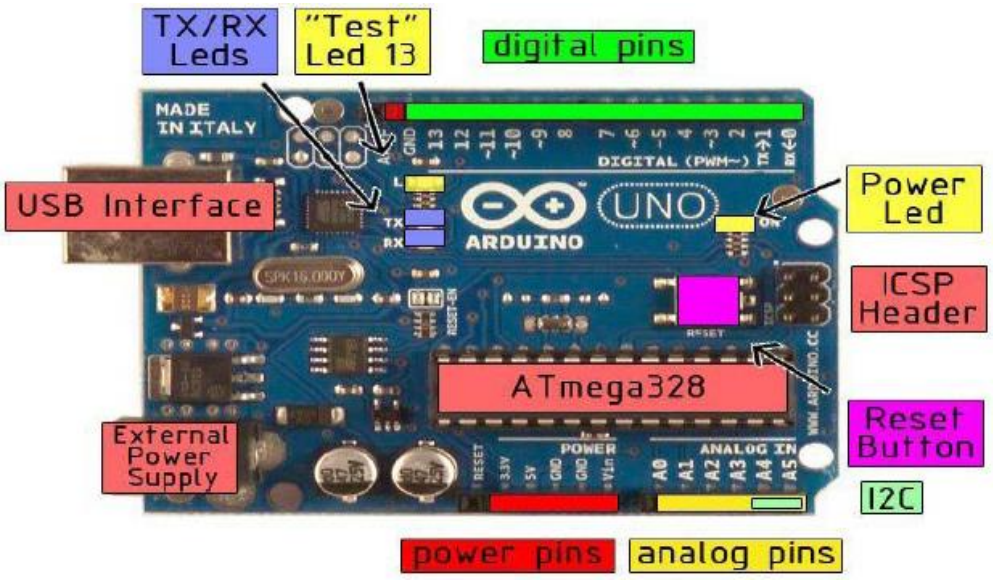

Figure 4.1: Synoptique illustrant les différents composants de la carte Arduino UNO

On représente aussi le microcontrôleur ATMega 328, un Atmel de la famille AVR.

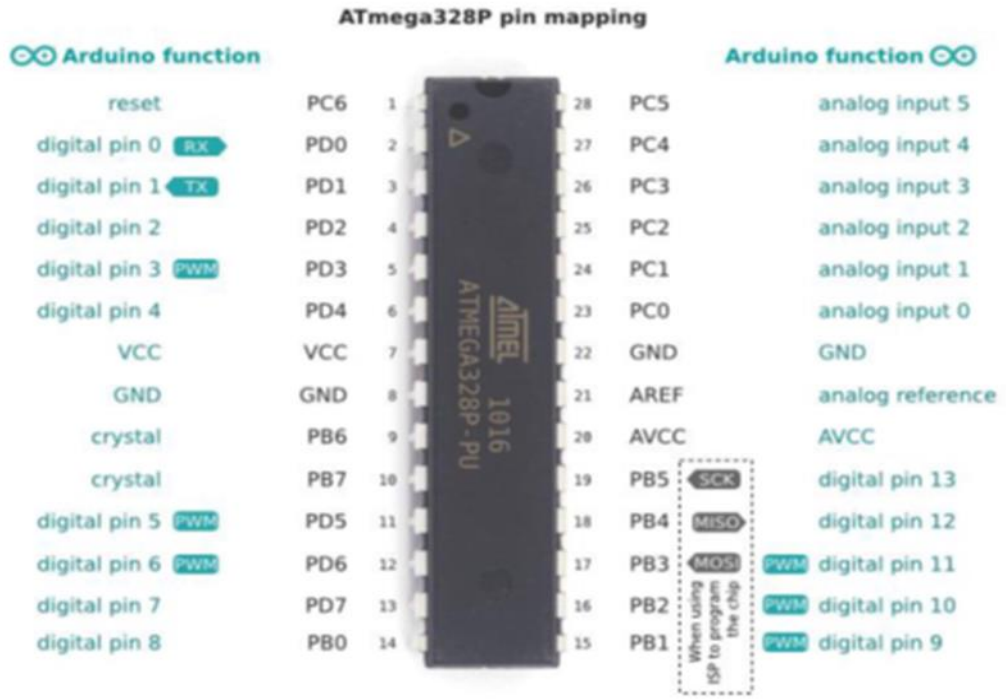

Figure 4.2 : Synoptique du microcontrôleur ATMega 328 d'Arduino UNO.

2.1.3 Caractéristiques de la carte Arduino UNO [47-49]

Un microcontrôleur ATMega328 est en fait constitué des mêmes éléments que sur la carte mère d'un ordinateur. Dans le tableau 4.1 sont donnés les éléments qui constituent une carte Arduino UNO ainsi que leurs caractéristiques.

Tableau 4.1 : les éléments de microcontrôleur ATMega328 [50].

Arduino UNO	
Microcontrôleur	ATMega 328
Tensions de fonctionnement	5 Volts, la plage limite est 6 -20 Volts, recommandée 7-12 Volts.
Broches E/S numériques	14 dont 6 disposent d'une sortie PMW.
Broches d'entrées analogiques	6 qui sont aussi utilisables en broches E/S numériques.
Mémoire programme flash	32 KB dont 0.5 KB sont utilisées pour le boot loader.
Mémoire RAM(Volatile)	2 KB
Mémoire EEPROM (Non volatile)	1 KB
Vitesse d'horloge	16 MHz

2.2 Module RF 433 MHz

Les modules sans fil 433 MHz ne peuvent être utilisés que par paires et seule la communication simplex est possible. Cela signifie que l'émetteur ne peut transmettre que des informations et que le récepteur ne peut que les recevoir. On ne peut donc envoyer des données que du point A vers B et non de B vers A.

Le module peut couvrir un minimum de 3 mètres et avec une antenne appropriée, une peut atteindre jusqu'à 100 mètres en théorie. Mais pratiquement, on peut difficilement obtenir environ 30 mètres dans des conditions de test normales. Ce module est utilisé dans plusieurs applications notamment dans la transmission des données série pour une courte distance, système de sécurité automobile et communication à courte distance.

2.2.1 Emetteur [51]

Le schéma bloc de l'émetteur est donné par la figure 4.3.

Les caractéristiques techniques sont les suivantes :

- Tension de fonctionnement : 3.5 - 12 V.
- Fréquence de travail : 433,92 MHz (une autre fréquence peut être personnalisée).
- Courant de fonctionnement : 20 - 28 mA
- Distance de transmission : 100 m.
- Puissance de sortie (10 mW)
- Taux de transfert : 4 kB/s
- Température de fonctionnement :-10°C à +70°C.
- Taille : 19 x 19 x 8 mm

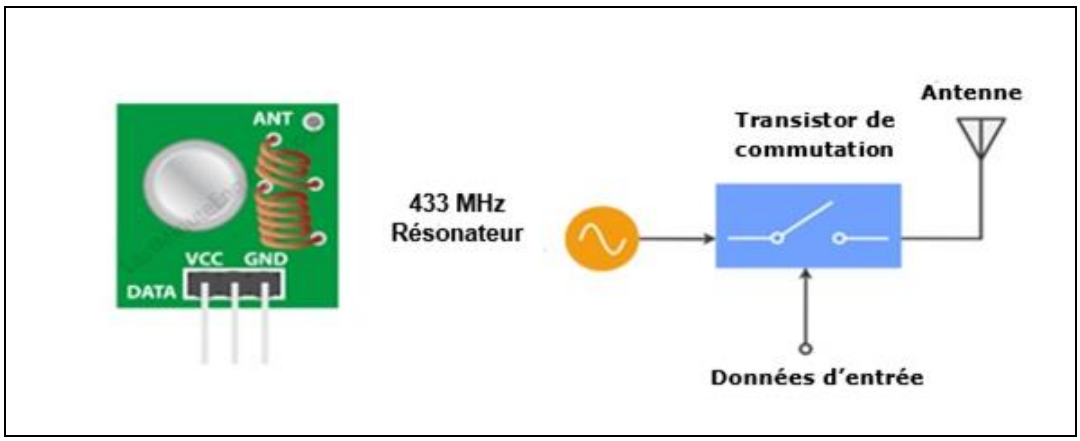

Figure 4.3 : Schéma bloc de l'émetteur [52].

2.2.2 Récepteur [51]

Le schéma bloc du récepteur est donné par la figure 4.4.

Les caractéristiques techniques sont les suivantes :

- 1 ANT antenne
- Tension de fonctionnement : DC 5 V.
- Courant statique : 4 mA.
- Température de fonctionnement :-10°C à + 70° C.
- Sensibilité de réception Rx (dBm) : -105 dB.
- Fréquence de travail : 315, 433,92 MHz (266 - 433 MHz).
- Taille : 30 x 7 mm.

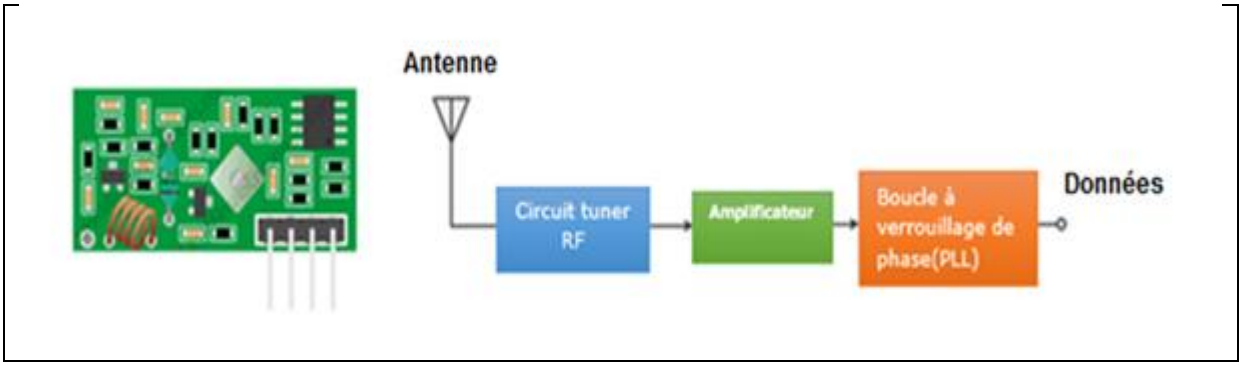

Figure 4.4 : Schéma bloc du récepteur [51].

2.3 Claviers numériques (Keypad (4x4)) [51]

Les claviers numériques sont un excellent moyen permettant aux utilisateurs d'interagir avec leur projet. Un clavier numérique est constitué d'un ensemble de touches ou bien de boutons poussoirs qui sont réunis en une matrice.

Figure 4.5 : Clavier à membrane de matrice 4*4.

Les touches sont alors disposées en 4 lignes et 4 colonnes. Sous chaque touche se trouve un interrupteur à membrane. A l'intérieur du clavier, chaque interrupteur d'une ligne est connecté d'un côté aux autres interrupteurs de la même ligne par un trait conducteur. Chaque interrupteur dans une colonne est connecté de la même manière – un côté de l'interrupteur est connecté aux autres interrupteurs de cette colonne par un trait conducteur. Chaque ligne et chaque colonne est amenée vers une seule broche de sortie, ce qui donne un total de 8 broches sur un clavier 4*4.

Appuyer sur une touche ferme l'interrupteur entre un trait de colonne et un trait de ligne permettant au courant de circuler entre une broche de colonne et une broche de ligne. Le schéma suivant d'un keypad 4*4 montre la connexion des lignes et des colonnes :

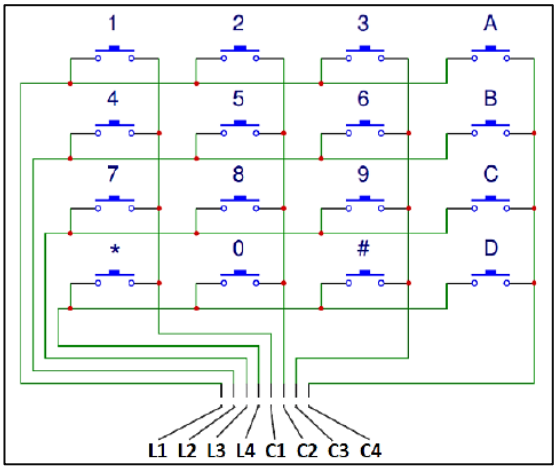

Figure 4.6 : Schéma simplifié d'un keypad 4*4.

2.4 Afficheur LCD [51]

Un afficheur LCD (**L**iquid **C**rystal **D**isplay) ou afficheur à cristaux liquides, est un module électronique compact intelligent et nécessite peu de composants externes pour un bon fonctionnement. Il consomme relativement peu (de 1 à 5 mA).

Les LCD s'utilisent avec beaucoup de facilité. Ils contiennent des cristaux liquides capables de modifier leur orientation en fonction d'une tension appliquée, et de jouer plus ou moins sur l'incidence de la lumière.
Les éléments d'affichage utilisent en général des motifs composés de points (Dot-Matrix) pour représenter à peu près tous les signes (chiffres, lettres ou caractères spéciaux). Dans ce projet, on a utilisé un afficheur LCD 16*02 dont la commande se fait d'une manière parallèle, c'est-à-dire que tous les bits de données sont envoyés en même temps au

contrôleur. Il existe deux modes différents (4 bits et 8bits). Le mode 4 bits étant le plus utilisé parce qu'un nombre moindre de lignes de données doit être relié à l'afficheur, ce qui fait diminuer le coût.

Sur les 8 lignes de données, seules les 4 lignes supérieures (D0 à D4) sont nécessaires. La figure suivante montre le brochage du module LCD 16*02 à 16 broches.

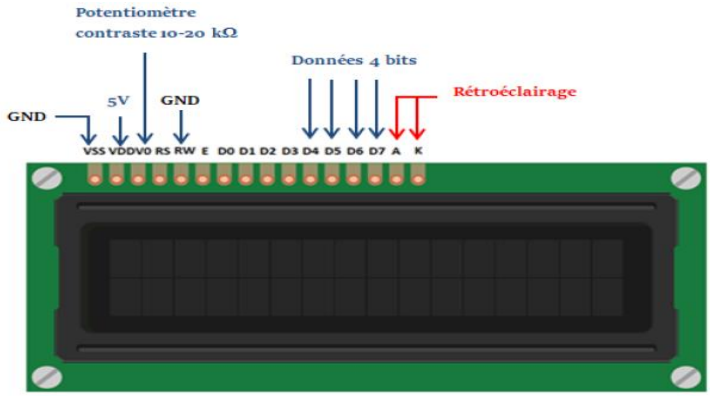

Figure 4.7 : Branchement du module LCD (16*02) à 16 broches.

Remarque : Avec certains types d'afficheurs LCD, on peut brancher le rétroéclairage sur +5V sans résistance série ; avec d'autres, une résistance dimensionnée en conséquence est nécessaire. Avant de connecter les deux broches (A et K) du rétroéclairage, il faut consulter la documentation du constructeur de l'afficheur utilisé.

3. Description de la partie logicielle

3.1 Programmation de l'Arduino [47,48]

En parallèle au matériel, un IDE (Environnement de développement) a été développé afin de permettre la programmation des modules de l'Arduino. Cet IDE est une application Java libre servant d'éditeur de codes (programmes) et de compilateur. Les opérations de compilation et de chargement dans la mémoire du microcontrôleur sont alors ramenées à de simples clics. La communication en Arduino et le PC se fait via le port USB.

L'IDE Arduino est plutôt simple (Figure 4.8) : il offre une interface minimale et épurée pour développer les codes. Il est doté d'un **éditeur** de codes avec coloration syntaxique et d'une **barre d'outils** rapide. On retrouve aussi une **barre de menus** plus classique qui est utilisée pour accéder à différentes fonctionnalités de l'IDE.

Enfin une **console** affichant les résultats de la compilation du code source, des opérations sur la carte, etc.

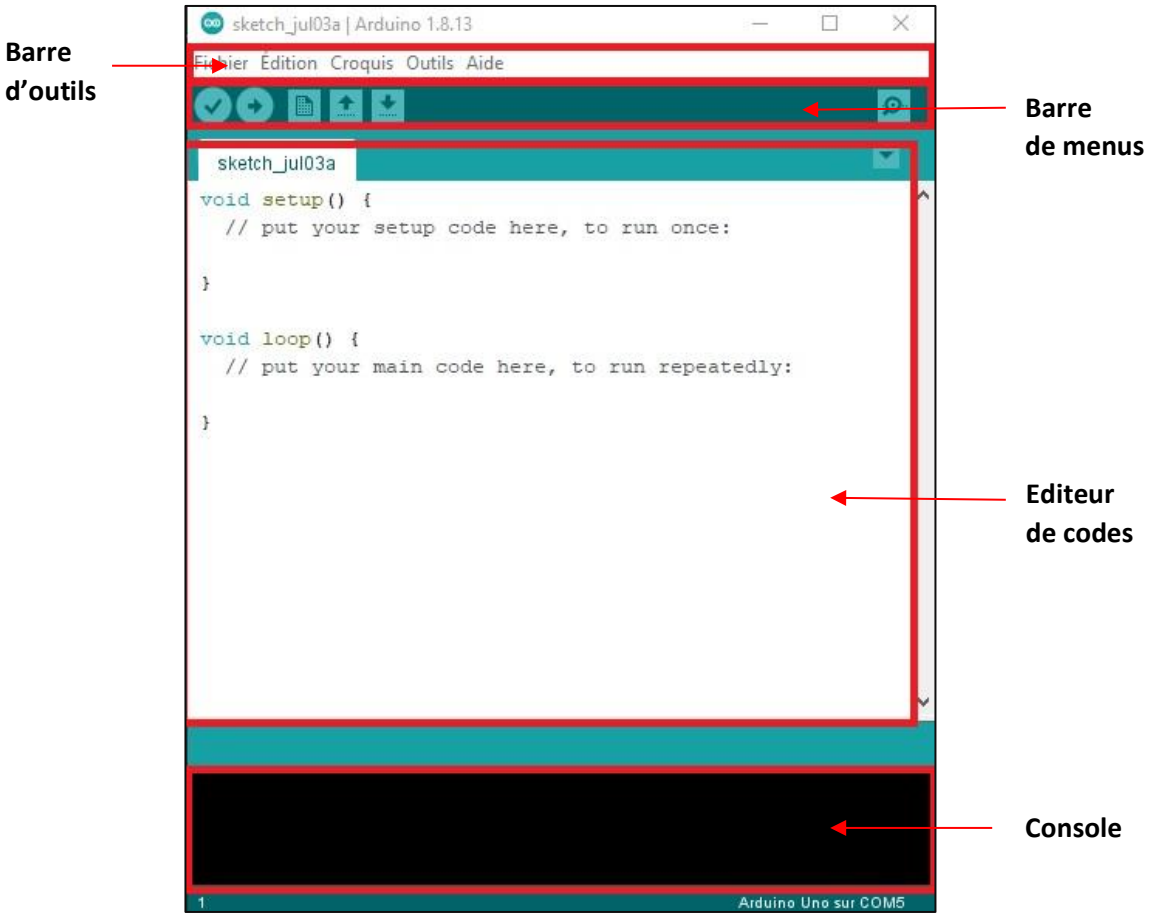

Figure 4.8 : Interface de l'IDE d'Arduino.

- **Communication de l'Arduino**

L'IDE Arduino inclut une fenêtre terminal série (moniteur série) sur l'ordinateur qui permet d'envoyer des textes simples depuis et vers la carte Arduino (Figure 4.9).

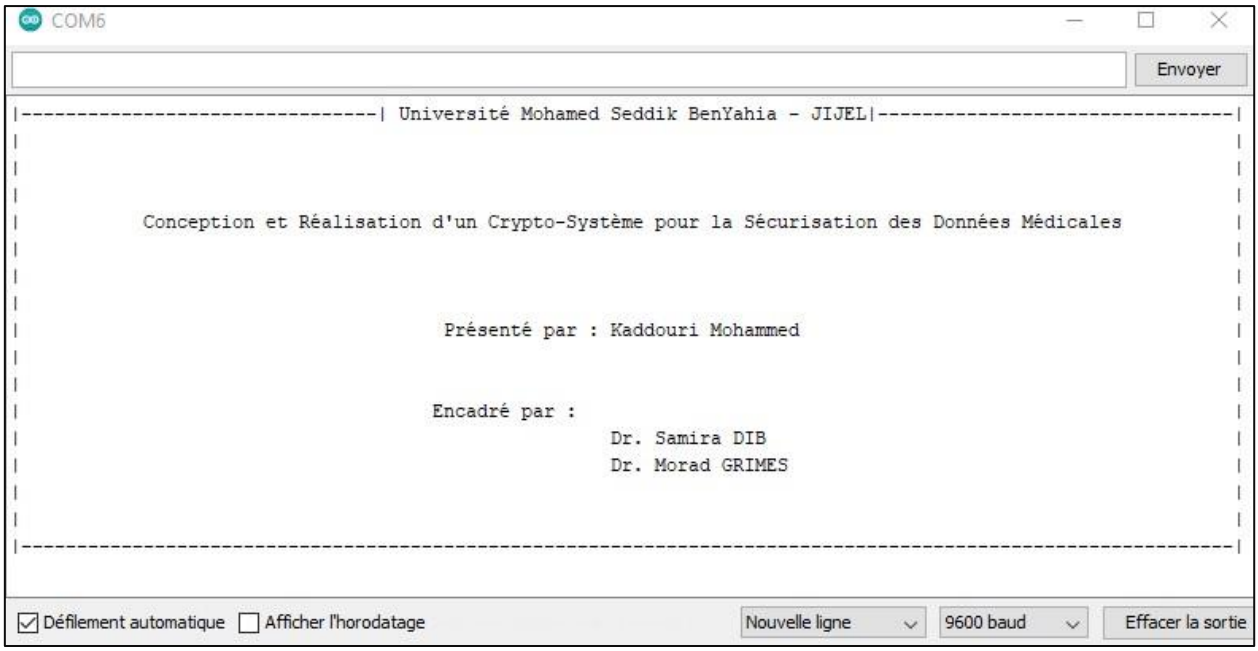

Figure 4.9 : Interface du moniteur série d'Arduino.

4. Présentation de l'application pratique réalisée

Dans ce qui suit, on va expliquer le schéma de cryptage chaotique et ce dans l'objectif de concevoir un système de transmission de données sécurisées composé d'un bloc pour l'émission et d'un autre pour la réception. Les deux systèmes communiquent par une liaison radiofréquence.

4.1 Problématique

Parmi les problèmes qui s'opposent à la mise en œuvre de notre crypto-système sur une carte Arduino UNO, nous avons le problème de la gestion de la mémoire disponible. Comme nous l'avons vu dans la première partie la carte dispose d'une capacité mémoire RAM d'un 1KB et une mémoire Flash de 32 KB assez limitées. Ceci nous a poussés à restreindre notre application pratique à l'implémentation de l'algorithme chaotique appliqué au chiffrement d'un texte en utilisant CKBA.

4.2 Mise en œuvre

4.2.1 Bloc émetteur

Le bloc émetteur est construit autour d'une carte Arduino UNO. Il comprend l'algorithme de chiffrement CKBA. Les résultats du chiffrement sont affichés sur le terminal série de l'IDE Arduino et sur l'afficheur LCD.

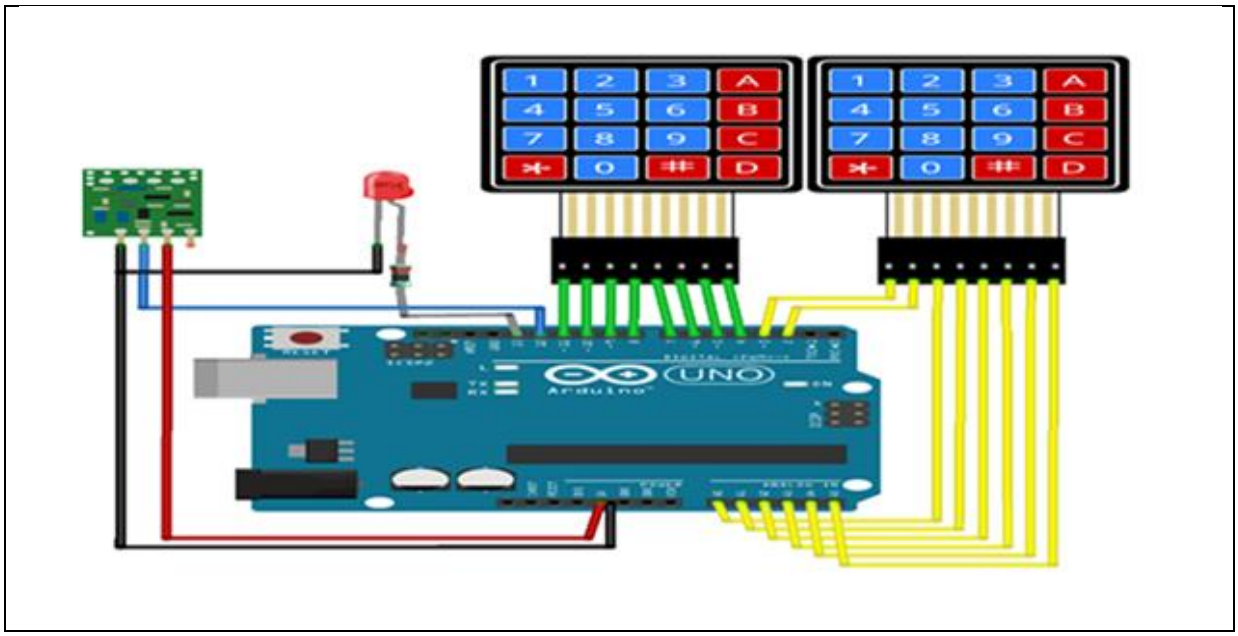

Figure 4.10 : Câblage du bloc émetteur

Figure 4.11: Photo réelle du bloc émetteur

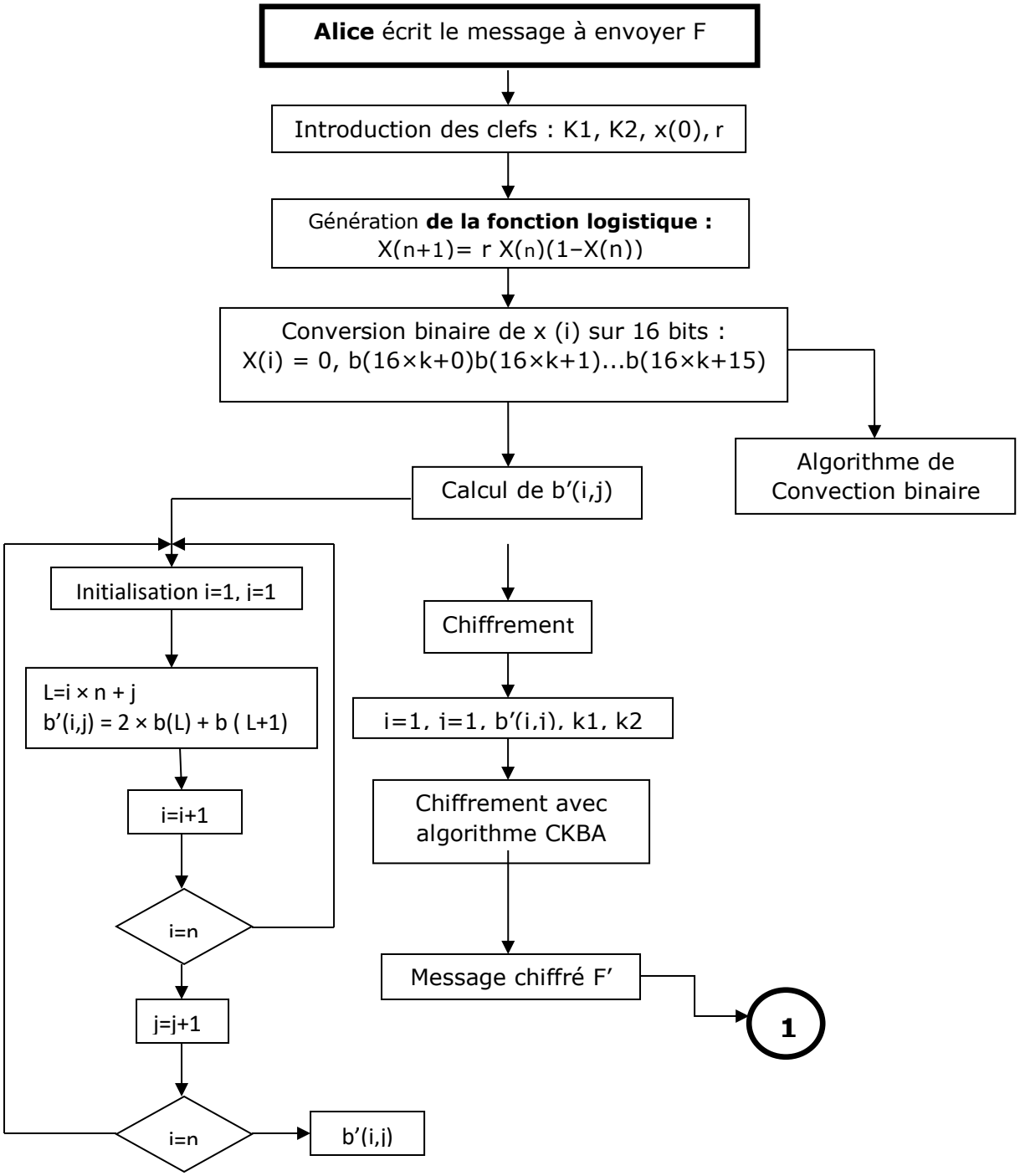

Figure 4.12 : Algorithme CKBA - Chiffrement

4.2.2 Bloc récepteur

Le bloc récepteur est aussi construit autour d'une deuxième carte Arduino. Il comprend l'algorithme de déchiffrement CKBA, Les résultats du déchiffrement des données reçues du bloc émetteur sont affichés sur le terminal série de l'IDE de l'Arduino.

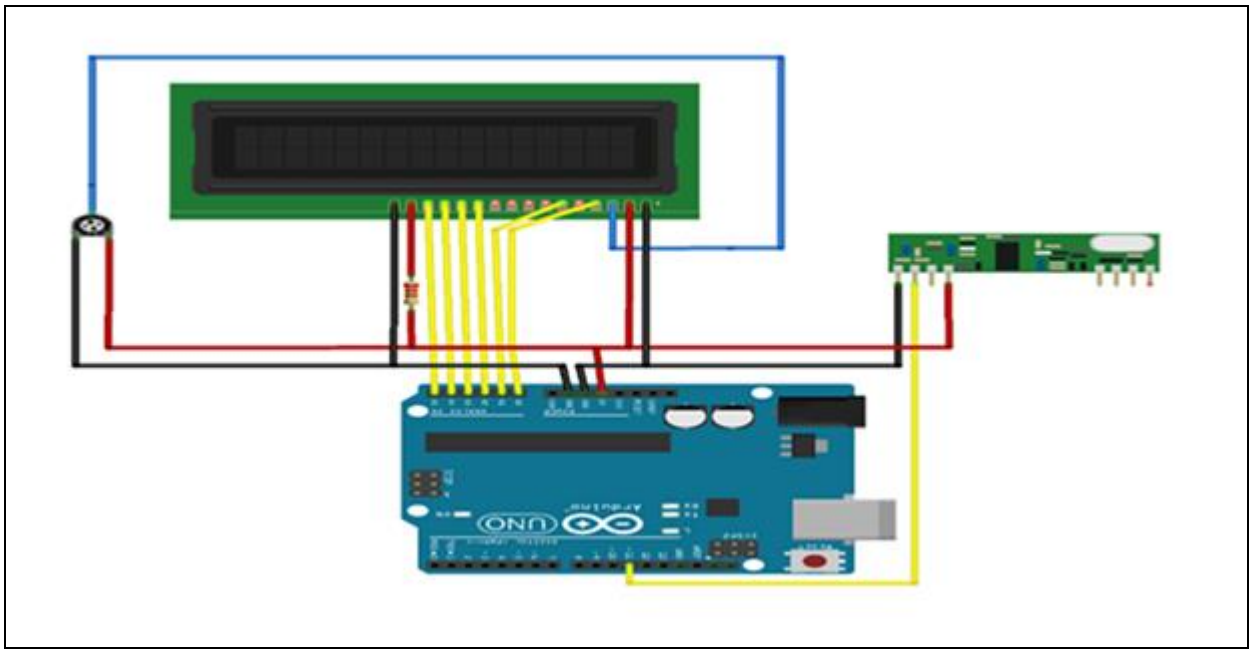

Figure 4.13 : Câblage du bloc récepteur.

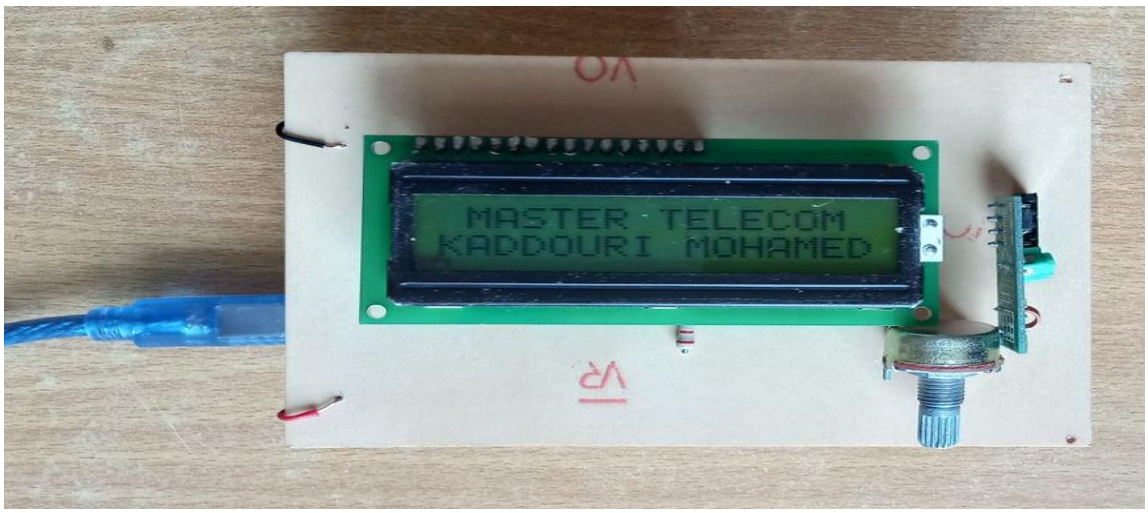

Figure 4.14 : Photo réelle du bloc récepteur.

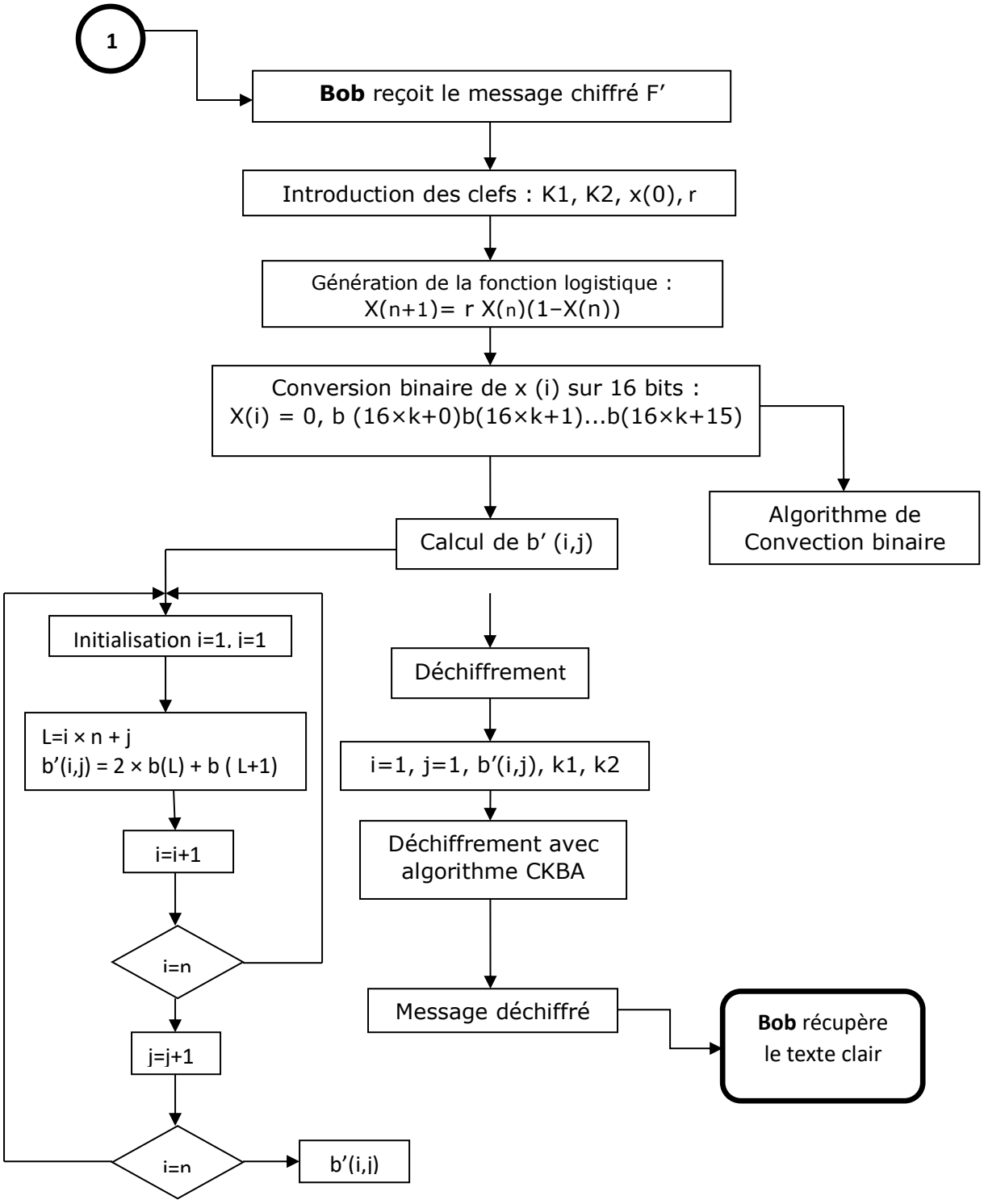

Figure 4.15 : Algorithme CKBA - Déchiffrement

4.2.3 Canal de transmission

On représente ci-dessous une synoptique des deux blocs et le protocole de transmission.

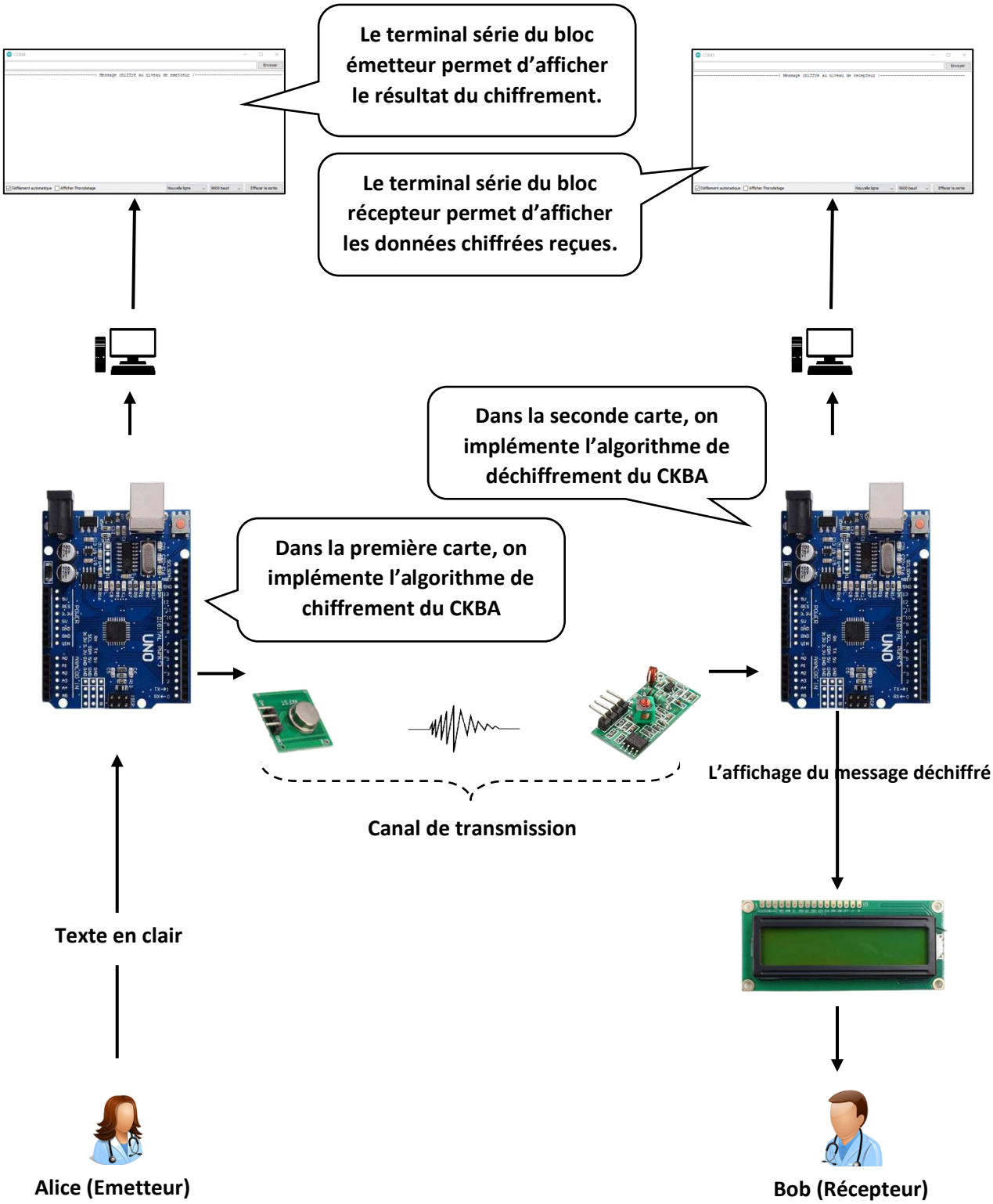

Figure 4.16 : Synoptique des deux blocs et le Protocol de transmission utilisé.

- **Protocole de transmission**

Cette transmission est basée sur la modulation d'amplitude (ASK).

Modulation d'amplitude (ASK : Amplitude Shift Keying) [52]

C'est la technique la plus simple et la plus naturelle pour moduler une porteuse sinusoïdale e(t) = E.cos (w_0t) par un signal numérique.
L'indice de la modulation est en général de 100%, ce qui explique que ce type de modulation s'appelle aussi modulation en tout ou rien. La porteuse est simplement multipliée par le signal numérique x_n.

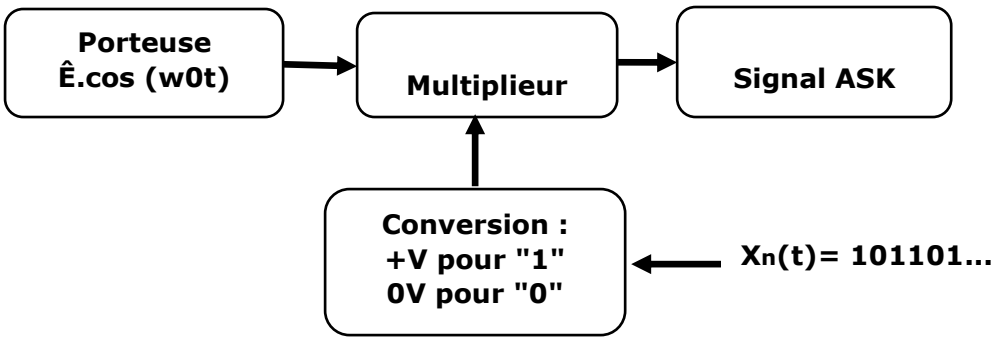

Figure 4.17 : Diagramme de la modulation ASK.

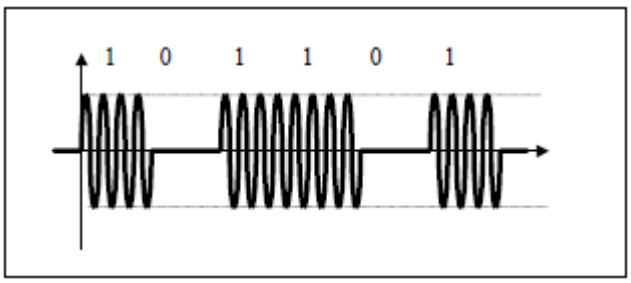

Figure 4.18 : Aspect temporel d'un signal modulé ASK.

En modulation d'amplitude, le spectre du signal modulé est symétrique par rapport à la raie de la porteuse et les deux bandes latérales ont la même forme que le signal BF.

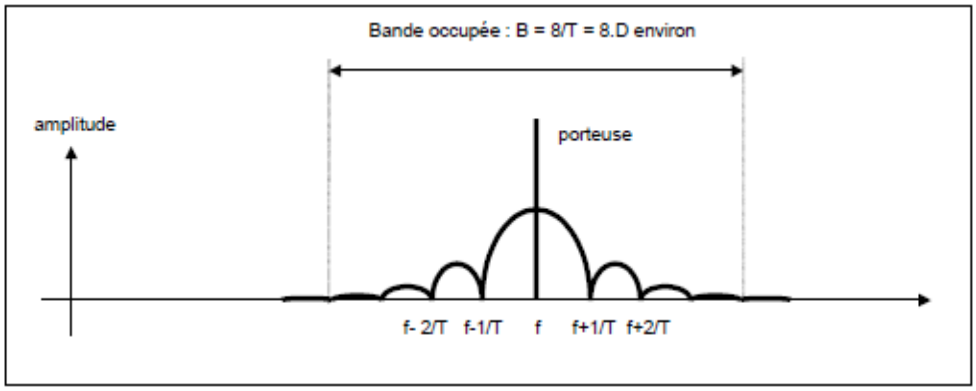

Figure 4.19 : Spectre d'un signal ASK modulé par un signal numérique non filtré [52].

Lorsque le signal numérique n'est pas filtré, le signal modulé ASK occupe, en théorie, une bande infinie ; ce qui est inacceptable dans la pratique. On est donc amené, dans la pratique, à limiter la bande du signal numérique par un filtre passe-bas, simple ou de Nyquist.

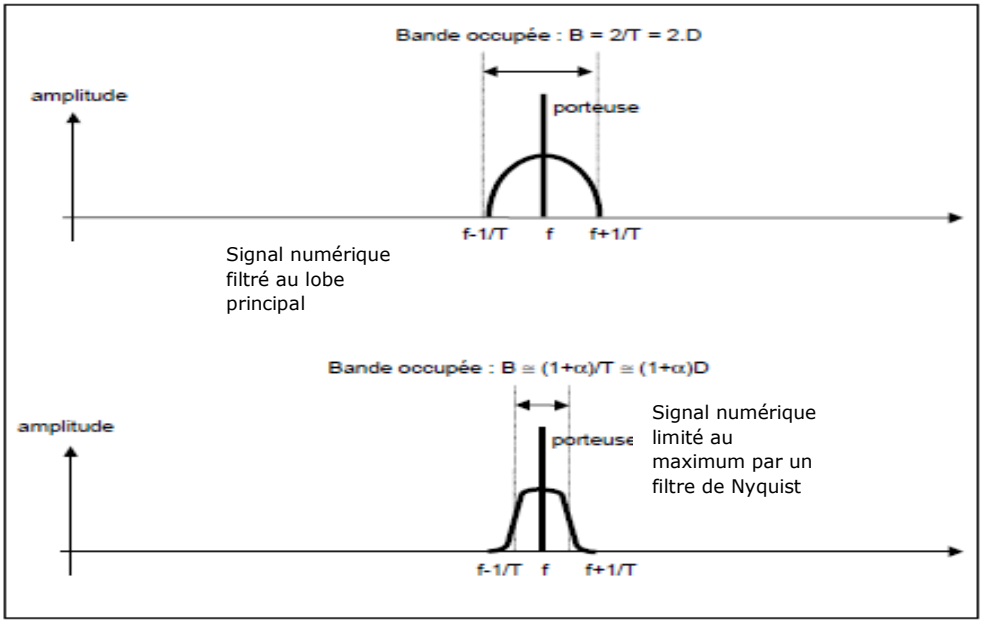

Figure 4.20 : Spectres de signaux modulés ASK [52].

C'est dans le cas du filtrage de Nyquist que l'encombrement spectral est minimal et simplement égal au débit numérique du signal modulant. Dans un système simple, si on veut éviter l'utilisation d'un filtre de Nyquist, il faudra prévoir pour le système une bande passante au moins égale au double numérique.

Dans le cadre de notre projet, on travaille à la fréquence 433.92 MHz. Par conséquent, on peut utiliser des filtres standards à f_i=10.7 MHz de largeur 300 KHz, ce qui nous permettra un débit de 150 Kbits/s.

4.3 Tests

Nous présentons dans cette section quelques tests et résultats pratiques.

Test I : Alice souhaite envoyer à Bob le message suivant :

« SECURITY SYSTEM » en utilisant :

- La fonction logistique : $x(i)= r \times (x (i -1) \times (1 - x (i - 1)))$ avec $r = 4$
- La condition initiale de chiffrement et de déchiffrement : $x(1)= 0.789632145698$
- Les clés de chiffrement et de déchiffrement : $k1 = 23$, $k2 = 84$

Les résultats du chiffrement, au niveau de l'émetteur, sont présentés dans le tableau 4.2 et la figure 4.21 respectivement.

Tableau 4.2 : Résultat de chiffrement du test I.

Message Clair (Plaintext)	**SECURITY SYSTEM**
Message chiffré (Ciphertext)	**68826466699467785568786867829O**

Figure 4.21 : Résultat du chiffrement (test I) affiché dans le moniteur série de l'Arduino.

Le résultat reçu, au niveau du récepteur, est illustré dans la figure 4.22 obtenu sur le terminal série de la carte Arduino et la figure 4.23 représentant le résultat du déchiffrement sur l'afficheur LCD.

Figure 4.22 : Résultat du test I reçu au niveau du récepteur.

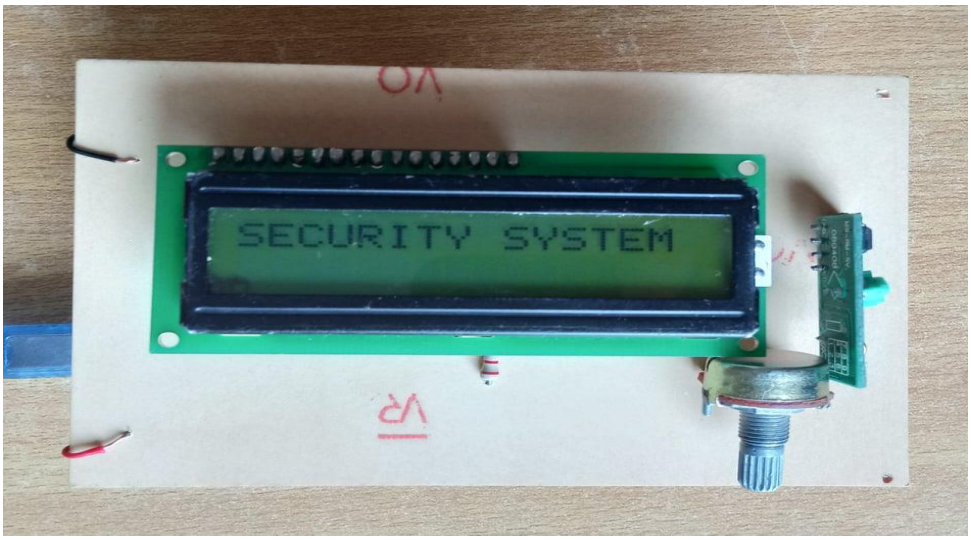

Figure 4.23 : Message du test I déchiffré affiché sur LCD.

Il est clair qu'à partir des résultats du tableau 4.2 et les figures 4.21 - 4.22, le crypto système chiffre et déchiffre de façon parfaite. Ceci est confirmé par la Figure 4.23.

Test II : Alice souhaite envoyer à Bob le message suivant : **« MEDICAL DATA »**.

On a utilisé une condition initiale au récepteur différente que celle à l'émetteur :

- La condition initiale de chiffrement : x(1)= 0.3273
- La condition initiale de déchiffrement : x(1)= 0.3274

Le message chiffré, au niveau de l'émetteur, est donné par le tableau 4.3. Le résultat reçu, au niveau du récepteur, est affiché sur LCD de la figure 4.24.

Tableau 4.3 : Résultat de chiffrement du test II.

Message clair (Plaintext)	**MEDICAL DATA**
Message chiffré (Ciphertext)	**908283948486915583866786**

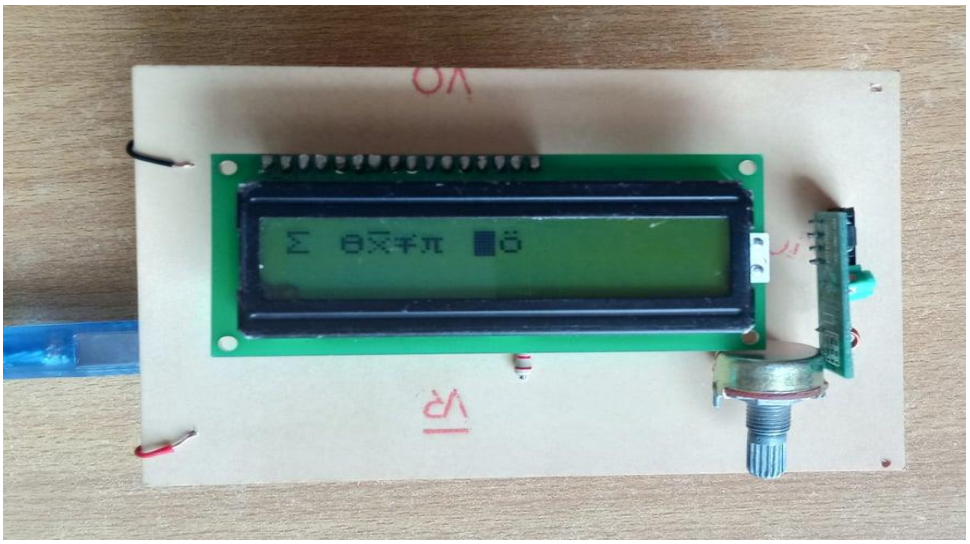

Figure 4.24 : Message du test II déchiffré et affiché sur LCD.

Il est très clair que les résultats obtenus sont assez satisfaisants, et restent dans la gamme des valeurs prévues, c'est-à-dire que notre crypto système est extrêmement sensible au moindre changement de la condition initiale x(1).

Test III : Alice souhaite envoyer à Bob le message suivant : **« @JIJEL 2020/2021»**.

On va utiliser une clé au récepteur différente que celle à l'émetteur :

- Les clés de chiffrement : k1 = 23, k2 = 84
- Les clés de déchiffrement : k1 = 130, k2 = 12

Le message chiffré, au niveau de l'émetteur, est donné par le tableau 4.4. Le résultat reçu, au niveau du récepteur, est affiché sur LCD de la figure 4.25.

Tableau 4.4: Résultat de chiffrement du test III.

Message Clair (Plaintext)	**@JIJEL 2020/2021**
Message chiffré (Ciphertext)	**879394938291553793739563739373 8**

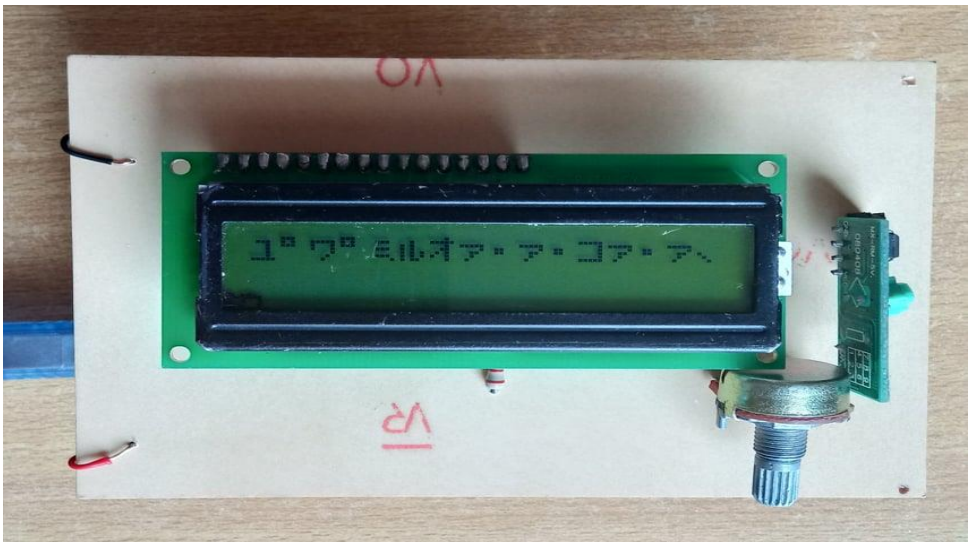

Figure 4.25 : Message du test III déchiffré et affiché sur LCD.

Ce test confirme bien que le crypto système conçu est très sensible à tout changement dans la clé secrète.

5. Conclusion

Ce chapitre a comporté dans une première partie la présentation de la carte Arduino UNO utilisée pour l'implémentation pratique du crypto-système chaotique de transmission de textes. Les ressources en termes de mémoire et de performances très limitées de l'Arduino, se sont avérées problématiques lors de l'implémentation du crypto-système. Cependant, nous avons réussi à implémenter le crypto-système étudié, autour de deux cartes Arduino UNO où la première a fait office d'émetteur et a comporté l'algorithme de chiffrement, et la deuxième de récepteur et a comporté l'algorithme de déchiffrement en utilisant une transmission radiofréquence.

Les résultats pratiques obtenus sur le chiffrement d'un texte démontrent l'implémentation correcte de l'algorithme de chiffrement / déchiffrement dans les deux cartes Arduino UNO, et confirment les résultats de simulation obtenus dans le chapitre 3.

Conclusion générale

Le travail rapporté dans ce mémoire a fait l'objet, dans une première partie, de l'étude des techniques de cryptage, des algorithmes de chiffrement classiques et moderne ainsi que des algorithmes en cours de développement : quantique et courbe elliptique. Ces algorithmes sont nécessaires à la conception du crypto système analysé dans le cadre de ce projet de Master.

Aussi dans une seconde partie, nous avons présenté une vue globale sur le système chaotique, ses caractéristiques et sa relation avec la cryptographie.

Dans la troisième partie, nous avons appliqué l'algorithme de chiffrement chaotique CKBA sur des images médicales. Les résultats obtenus sous MATLAB ont permis d'illustrer le bon fonctionnement et l'efficacité de la méthode proposée. Nous avons exploité plusieurs métriques d'évaluation du degré de chiffrement à savoir : l'analyse statistique et différentielle ainsi que le temps d'exécution. De très bons résultats sont obtenus aux tests de la sensibilité à la condition initiale et à la clé secrète. Une étude comparative est faite entre le CKBA et l'ECC, algorithme basé sur les courbes elliptiques. Cette comparaison vient « s'ajouter » au travail effectué l'année passée sur l'utilisation de courbes elliptiques pour la sécurisation des images médicales. Ce sont là des « pièces » qui font partie d'un projet sur la sécurisation des données médicales.

Dans la quatrième partie, nous avons proposé une réalisation expérimentale du crypto-système chaotique. Cette réalisation est conçue autour de deux cartes Arduino UNO l'une étant l'émetteur et l'autre le récepteur. Les ressources limitées des cartes utilisées en termes de mémoire et de performances nous ont poussées à restreindre notre application pratique à l'implémentation de l'algorithme CKBA, appliqué au chiffrement d'un texte.

Les résultats expérimentaux relevés ont confirmé de la bonne implémentation des algorithmes de chiffrement et de déchiffrement sur les deux cartes Arduino UNO ainsi que la transmission radiofréquence des deux cartes utilisées.

Ce projet nous a permis d'aborder une thématique très attrayante qui est celle de la sécurisation des données et la transmission avec les radiofréquences.

Les différents aspects que nous avons étudiés (cryptographie, traitement d'images, programmation sous MATLAB, réalisations pratiques matérielle et logicielle sous cartes Arduino pilotées par micro-ordinateur) nous ont été bénéfiques aussi bien sur le volet pédagogique en complétant notre formation mais aussi sur le volet de recherche en nous initiant à la lecture d'articles de recherche publiés récemment.

Notre projet est loin d'être complet. En guise de perspectives, nous proposons de :

- Utiliser des cartes plus élaborées comme les cartes Raspberry Pi, FPGA, ou autres cartes plus récentes et plus puissantes afin d'implémenter tous les algorithmes de notre crypto système chaotique de transmission.
- Rendre la cryptanalyse plus difficile en ajoutant de l'aléatoire ou du chaos dans les clés de chiffrement.
- Utiliser le module XBee pour plus d'efficacité notamment l'augmentation de la portée de transmission.
- Utiliser LCD 128×64 ou CLGLCD pour l'affichage des images.
- Envisager de développer et d'implémenter d'autres techniques de chiffrement associant en particulier celles basées sur le chaos et les courbes elliptiques.

Bibliographie

[1] J. Jean, « Cryptanalyse de Primitives Symétriques Basées Sur le Chiffrement AES » Thèse de Doctorat, Université Paris Diderot (Paris 7), 2013.

[2] B. Martin, «Codage, Cryptologie et Applications», Presses Polytechniques et universitaires romandes, 2001.

[3] W. Stalling, «Cryptography and Network Security. Principes and Practice»,5th edition, Prentice Hall, 2010.

[4] R. Halit, M. Habachou «Conception et Réalisation d'un Cryptosystème Hybride». Mémoire de fin d'études d'ingénieur en Electronique, Université MAMMERI Mouloud de Tizi Ouzou, 2008.

[5] R. Dumong, «Cryptographie et sécurité informatique» [en ligne], Cours, Université de Liège, 2009-2010, 213p.

[6] B. Preneel, « Selected areas in cryptography », Staffords Travares, Springer, Canada, Aout 2005, 104p.

[7] JDN [en ligne], (mise à jour le 11/2/2019) Disponible sur :< www.journaldunet. fr/patrimoine/guide-des-financespersonnelles/1209336-cryptographie-asymetrique. >

[8] H. Attaf et H, Cherfa , « Étude sur l'Applicabilité de la Cryptographie Asymétrique aux Réseaux de Capteurs sans Fils » [en ligne], mémoire de Master, Université Abderrahmane Mira- Bejaia, juin 2012, 86p.

[9] F. Grosshans et P, Grancier, « La cryptographie quantique : l'incertitude quantique au service de la confidentialité » [en ligne], optique quantique vol.71, pp.34-39, 2014.

[10] N. Koblitz, «Elliptic curve cryptosystems» [en ligne], Mathematics of computation vol.48, pp : 203–209, 1987.

[11] S. Victor et S. Miller, « Use of elliptic curves in cryptography » [en ligne]. Advances in Cryptology, pp 417–426, 1986.

[12] L. Ronald, S. Adi et L. Adlemen, « A method for obtaining digital signatures and public-key cryptosystems ». [En ligne], Communications of the ACM, vol.21, pp 120–126, 1978.

[13] I. Lotfi, « Cryptographie à base de courbes elliptiques » [en ligne], Thèse de Doctorat, Université de technologie- Nanyang, juin 2017,67p.

[14] J. Wales et L. Sanger, « Encyclopédie » [en ligne].

[15] F. Grosshans et P, Grancier, « La cryptographie quantique : l'incertitude quantique au service de la confidentialité » [en ligne], optique quantique vol.71, pp.34-39, 2014. Disponible sur :< https://www.photoniques.com/articles /photon /abs/ 2014 /03/photon201471p34/Photon201471p34.html. (Consulté en Mai 2021).

[16] S. Ballet et L. Bonecaze, « Cryptographie Avancée Courbes Elliptiques Application à la Cryptographie », [en ligne]. Marseille : École Polytechnique, Cours, 36p.

[17] T. Fuhr, «Conception, Preuve et Analyse de Fonctions de Hachage cryptographiques». Thèse de Doctorat, TELECOM Paris Tech, 2011.

[18] A .Gonsai, N. Kakkad, B. Goswami, N. Shah, « Study and Analusis of Symmmetric Key-Cryptograph DES, Data Encryption Standard », Proceedings of UGC sponsored National Seminar on Scientific Wealth of Physics SWP-2012, Inde, 26 aout 2012.

[19] H. Hamiche, « Inversion à Gauche des Systèmes Dynamiques Hybride Chaotiques, Application à la Transmission Sécurisée de Données », Thèse de Doctorat, Université MAMMERI Mouloud de Tizi Ouzou, 2011.

[20] H. Poincaré, « Science et Méthode », G. ABRAHAM-FROIS(1994), 1909.

[21] J. Integros, «Le problème des trois corps» [en ligne], Paris, 1772.

[22] C. d. R. Philippe Etchecopar, «Quelques éléments sur la théorie du chaos» [en ligne], 2000.

[23] F. P. Yves Benoist, « notes de cours systèmes dynamiques élémentaires » [en ligne], 2003.

[24] A. Mahamdioua et N. Brahimi, «Cryptage chaotique numérique des images» mémoire de Master, Université Mohamed Seddik BenYahia, Jijel, 2005.

[25] S. Allouache, N. Hamma « Conception et réalisation d'un système de transmission sécurisé de données à base de systèmes chaotiques sur cartes Arduino » mémoire de Master, Université Mouloud Mammeri, Tizi-Ouzou, 2015.

[26] J. Kint, D. Constales, et A. Vanderbauwhede, « Pierre-François Verhulst's final triumph » à The Logistic Map and the Route to Chaos, M. Ausloos et M. Dirickx, pp. 13–28, Springer, Heidelberg, Germany, 2006.

[27] H. Pastijn, « The logistic map and the route to chaos » à Chaotic Growth with the Logistic Model of P.-F. Verhulst, M. Ausloos and M. Dirickx, p. 3, Springer, Heidelberg, Germany, 2006.

[28] P. F. Verhulst, « Deuxième mémoire sur la loi d'accroissement de la population » Mémoires de l'Académie Royale des Sciences, des Lettres et des Beaux-Arts de Belgique, vol. 20, pp. 1–32, 1847.

[29] A. Wolf, J. B. Swift, H. L. Swinney, and J. A. Vastano, « Determining Lyapunov exponents from a time series », Physica D. Nonlinear Phenomena, vol. 16, no. 3, pp. 285–317, 1985.

[30] O. Megherbi, « Etude et réalisation d'un système sécurisé à base de système chaotiques », Thèse de Magister, Université Mouloud Mammeri, Tizi-Ouzou, 2013.

[31] G. Zaïbi, « Sécurisation par dynamiques chaotiques des réseaux locaux sans fil au niveau de la couche MAC » [en ligne], Université Toulouse 2 Le Mirail (UT2 Le Mirail), décembre 2012. Disponible sur : < https://tel.archives-ouvertes.fr/tel-00867469. >

[32] I. Yasser, M.A. Mohamed, A.S. Samra, F. Khalifa, « A Chaotic-Based Encryption/Decryption Framework for Secure Multimedia Communications » Article, Egypt, Septembre 2020.

[33] Suryadi MT, Y. Satria, M. Fauzi « Implementation of digital image encryption algorithm using logistic function and DNA encoding » Article, Département of Mathématiques, Universités Indonésie, Indonésie, 2021.

[34] Y. Mao et G. Chen : « Chaos based image encryption » Article, 2004

[35] Li .Shujun: « Analyses and new designs of digital chaotic ciphers » Article, Information and Communication Engineering, 2003.

[36] S.Penaud :« Etudes des potentialités du chaos pour les systèmes de télécommunications ». Thèse pour l'obtention du Doctorat de l'Université de Limoges, France, 2001.

[37] : « A la découverte des attracteurs étranges : L'attracteur de Hénon » information disponible sur :< http://web.ensimag.fr. >

[38] P. Bergamo, P.d'arco, A.de Santis et L.Kocarev : « Security of public key cryptosystems based on chebyshev polynomials » Article, 1 février 2008

[39] Y. Amice « Nombre p-adique » 1975,

[40] R.Cochinos : « Introduction to the theory of cellular automata and one-dimensional traffic simulation » cour, 17 June 2000. Disponible sur :< https://theory.org/complexity/traffic/. >

[41] B. Furht et D. Kirovski : « Multimedia security handbook ». February 2004.

[42] A.K.Amzert, O. Belmerabet, « Sécurisation des images médicales sur courbes elliptique » mémoire de Master, Université Mohamed Seddik BenYahia, Jijel, 2020.

[43] T. Preston-Werner et C. Wanstrath, Github [en ligne]. (2008, mise à jour Aout 2020) Disponible sur :< https://github.com/ieee8023/covid-chestxray-dataset /tree/master/images.com >

[44] Image trouve sur le site web :< https://www.ultrasoundcases.info. > (consulté en juillet 2021).

[45] H. Hamiche, « Inversion à Gauche des Systèmes Dynamiques Hybride Chaotiques, Application à la Transmission Sécurisée de Données », Thèse de Doctorat, université Mouloud Mammeri, Tizi Ouzou, 2011.

[46] J. Lechalupé, « Cours d'initiation à Arduino ». Université Paul Sabatier, France, Mai 2014.

[47] Cours trouvé à la page web http :< //www.mon-club-elec.fr/pmwiki_reference_arduino/pmwiki.php?n=Main.MaterielUno > (consulté en juillet 2021).

[48] M.A. Zerzri « Arduino et Simulink/Matlab un outil innovant à cout réduit pour le prototypage » Article publié par EDP Sciences disponible sur le site : < http://www.j3ea.org. > (consulté en juillet 2021).

[49] M. Mc Roberts, « Begining Arduino », seconde édition, Apress, 2013.

[50] Khalid Lafkih, « Arduino en pratique Avec 10 leçons d'apprentissage », cours trouver à la page web :< https://www.facebook.com/ProSysExplore.> (consulté en juillet 2021).

[51] « How 433MHz RF Tx-Rx Modules Work & Interface with Arduino » cours trouver à la page web :< https://lastminuteengineers.com/433mhz-rf-wireless-arduino-tutorial/ > (consulté en juillet 2021).

[52] Jean-Philippe Muller, « les modulations numérique dans les systèmes de communication », Décembre 2000.

Résumé

Actuellement, les images numériques sont utilisées comme moyen fréquent de transfert de messages. De nombreuses applications réelles exigent un cryptage des images fiable, rapide et sécurisé ; à savoir : bases de données d'images de l'armée, vidéoconférences, images médicales et leurs résultats d'analyse automatisée, etc. Au cours de la dernière décennie, un bon nombre d'algorithmes de chiffrement sont proposés sur la base de divers principes. Parmi ces algorithmes, ceux basés sur le chaos et d'autres sur les courbes elliptiques sont bien connus pour leur sécurité, complexité, vitesse, ... L'objectif principal de ce mémoire est de contribuer à la protection des données médicales. Dans une première partie, nous avons appliqué les algorithmes ECC et CKBA sur des images médicales d'échographie et de scanner. Les résultats obtenus montrent l'efficacité des algorithmes étudiés. Dans une seconde partie, nous avons réalisé expérimentalement un crypto-système chaotique basé sur l'algorithme CKBA et conçu autour de deux cartes Arduino UNO avec une transmission RF. Les ressources limitées en termes de mémoire et de performances nous ont poussées à restreindre l'application pratique à l'implémentation de l'algorithme CKBA, appliqué au chiffrement d'un texte. Les résultats expérimentaux relevés ont confirmé de la bonne implémentation des algorithmes de chiffrement et de déchiffrement sur Arduino ainsi que la transmission RF.

ملخص

حديثا، تُستخدم الصور الرقمية كوسيلة متكررة لنقل الرسائل. تتطلب العديد من تطبيقات العالم الحقيقي تشفيرًا موثوقًا وسريعًا وآمنًا للصور؛ مثلا: قواعد بيانات صور الجيش، ومؤتمرات الفيديو، والصور الطبية ونتائج التحليل الآلي الخاصة بها، إلخ. على مدى العقد الماضي، تم اقتراح عدد من خوارزميات التشفير بناءً على مبادئ مختلفة. من بين هذه الخوارزميات، تلك القائمة على الفوضى وغيرها على المنحنيات الإهليلجية معروفة جيدًا بأمانها وتعقيدها وسرعتها...، الهدف الرئيسي من هذه الرسالة هو المساهمة في حماية البيانات الطبية. في الجزء الأول، طبقنا خوارزميات ECC و CKBA على صور الموجات فوق الصوتية والماسح الضوئي الطبي. النتائج التي تحصلنا عليها تظهر كفاءة الخوارزميات المدروسة. في الجزء الثاني، أنشأنا تجريبياً نظام تشفير فوضوي يعتمد على خوارزمية CKBAومصمم حول لوحين من Arduino UNO مع إرسال RF. دفعتنا الذاكرة المحدودة وموارد الأداء إلى تقييد التطبيق العملي لتنفيذ خوارزمية CKBAالمطبقة على تشفير النص. أكدت النتائج التجريبية المرصودة التنفيذ الجيد لخوارزميات التشفير وفك التشفير على Arduino وكذلك إرسال RF.

Abstract

Nowadays, digital images are used as a frequent means of transferring messages. Many real-world applications require reliable, fast, and secure image encryption; namely: army image databases, videoconferences, medical images and their automated analysis results, etc. During the last decade, a large number of encryption algorithms have been proposed based on various principles. Among these algorithms, those based on chaos and others on elliptical curves are well known for their security, complexity, speed, ... The main objective of this thesis is to contribute to the protection of medical data. In the first part, we applied the ECC and CKBA algorithms on medical ultrasound and scanner images. The results obtained show the efficiency of the studied algorithms. In a second part, we experimentally realized a chaotic crypto-system based on the CKBA algorithm and designed around two Arduino UNO boards with RF transmission. Limited memory and performance resources prompted us to restrict the practical application to the implementation of the CKBA algorithm, applied to text encryption. The observed experimental results confirmed the good implementation of the encryption and decryption algorithms on Arduino as well as the RF transmission.