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

Mémoire de fin d'études

pour l'obtention du diplôme de Master en Informatique

Option: *Réseaux et Systèmes Distribués*

Thème

Cryptage Chaotique Basé Sur l'Attracteur Clifford

Réalisé par :

- **Mr Medjahdi NASREDDINE**

Présenté le 02 Juillet 2017 devant le jury composé de:

- *Mr Benamar ABDELKRIME* *(Président)*
- *Mr Mana MOHAMED* *(Encadreur)*
- *Mr Benaissa MOHAMED* *(Examinateur)*

Année universitaire : 2016-2017

Remerciement

Avant de commencer ; Je remercie le dieu le tout puissant pour son aide et pour la volonté qui ma donnée pour finir mon travail.

permettez-moi de remercier mes parents pour leur amour, ma femme et pour son soutient, et l'encadreur Mr MANA MOHAMED d'avoir dirigé cette mémoire ainsi que pour leurs efforts, leurs conseils et leurs encouragements.

Je remercie les membres du jury Mr Benamar.A et Mr Benaissa.M pours nous avoir honorés en acceptant de juger ce travail.

Je remercie aussi tous ceux qui ont contribué de prés ou de loin pours terminer ce travail.

Merci a tous.

N.medjahdi

Dédicace

Je dédie ce travail à

Toute ma famille mon pére ma mère ma femme et mon trés chére fils Mohamed FIRAS et Nour el YAKINE .

Mes frères et ma sœur et ces enfants Wael , Aya , Tesnim , Israe ,Anes,Chiheb.

Mes collégues de travail et surtout Ahmed et El Hadi

Mes amis et toute la famille MEDJAHDI .

Nasreddine.M

Introduction générale

Aujourd'hui, la protection et la sécurité d'information est devenue d'une importance primordiale dans les déférents domaines.En effet, l'espionnage touche une très grande gamme d'informations telles que les images, les mots de passe, la vidéo, les codes de cartes bancaires, les messages électroniques… etc. Ces attaches peuvent toucher des particuliers ou individus comme ils peuvent toucher des organisations et des états sur déférentes secteurs (militaires, médicales, industrielles).

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

L'histoire de la cryptographie est déjà longue. Nous rapportons son utilisation en Egypte plus de 1000 ans. Les méthodes utilisées étaient restées souvent très primitives. D'autre part, sa mise en œuvre était limitée aux besoins de l'armée et de la diplomatie. Ainsi, les méthodes de cryptographie et de cryptanalyse ont connu un développement très important au cours de la seconde guerre mondiale et ont eu une profonde influence.

Le but de notre travail consiste à développer un système cryptographique en se basant sur les systèmes chaotiques.

Ce mémoire s'organise autour de trois chapitres, le premier chapitre est consacré à la présentation de la cryptographie symétrique et asymétrique.Le deuxième chapitre aborde les systèmes chaotiques et présente une comparaison entre les déférents Attracteurs chaotiques. Le dernier chapitre présente notre méthode de chiffrement basée sur l'attracteur de Clifford.

CHAPITRE I

Introduction à la cryptographie

I. Introduction

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

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

La cryptographie peut être utilise pour atteindre la flexibilité, la conformité et l'intimité des données qui est une exigence dans les systèmes d'aujourd'hui.

Dans ce chapitre on présente les notions de base relié à la cryptographie telle que le chiffrement et ces déférents types.

II. Terminologies

- **Texte en clair :** est le message à protéger.
- **Texte chiffré :** est le résultat du chiffrement du texte en clair.
- **Chiffrement :** est la méthode ou l'algorithme utilisé pour transformer un texte enclair en texte chiffré.
- **Déchiffrement :** est la méthode ou l'algorithme utilisé pour transformer un texte chiffré en texte en clair.
- **Clé :** est le secret partagé utilisé pour chiffrer le texte en clair en texte chiffré et pour déchiffrer le texte chiffré en texte en clair. On peut parfaitement concevoir un algorithme qui n'utilise pas de clé, dans ce cas c'est l'algorithme lui-même qui constitue la clé, et son principe ne doit donc en aucun cas être dévoilé.
- **Cryptographie :** cette branche regroupe l'ensemble des méthodes qui permettent de chiffrer et de déchiffrer un texte en clair afin de le rendre incompréhensible pour qui conque n'est pas en possession de la clé à utiliser pour le déchiffrer.
- **Cryptanalyse :** c'est l'art de révéler les textes en clair qui ont fait l'objet d'un chiffrement sans connaître la clé utilisée pour chiffrer le texte en clair.
- **Cryptologie :** il s'agit de la science qui étudie les communications secrètes. Elle est composée de deux domaines d'étude complémentaires, la cryptographie et la cryptanalyse.

- **Décrypter :** c'est l'action de retrouver le texte en clair correspondant à un texte chiffré sans posséder la clé qui a servi au chiffrement. Ce mot ne devrait donc être employé que dans le contexte de la cryptanalyse.
- **Crypter :** en relisant la définition du mot décrypter, on peut se rendre compte que le mot crypter n'a pas de sens et que son usage devrait être oublié. Le mot cryptage n'a pas plus de sens non plus.
- **Coder, décoder :** c'est une méthode ou un algorithme permettant de modifier la mise en forme d'un message sans introduire d'élément secret. Le Morse est donc un code puisqu'il transforme des lettres en trait et points sans notion de secret. L'ASCII est lui aussi un code puisqu'il permet de transformer une lettre en valeur binaire.**[1]**

III. Objectifs de la cryptographie

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

III.1 Confidentialité : la confidentialité ou masquage des données, le contenu des données va être sauvé de toutes les personnes, machines et systèmes à l'exception de ceux qui ont le droit d'accès.

III.2 Authentification : permet à l'émetteur de signer son message, ainsi, le récepteur n'aura pas de doute sur l'identité du premier.

III.3 Intégrité : les données vont être protégées du changement (suppression, ajout, mise à jour) de la personne non autorisé.

III.4 Non-répudiation : est la garantie qu'aucun des deux individus ayant effectué une transaction ne pourra nier avoir reçu ou envoyé les messages.

IV. Les déférents algorithmes de cryptage et décryptage :

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

IV.1 Méthodes de cryptage Classiques :

IV.1.1 Cryptage par substitution : Les substitutions consistent à remplacer des symboles ou des groupes de symboles par d'autres symboles ou groupes de symboles dans le but de créer de la confusion.

On distingue deux méthodes de substitution, la substitution mono-alphabétique et la substitution poly-alphabétique.

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

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

Tableau I-1 substitution mono-alphabétique

- **Exemple :**

Texte claire« la cryptographie »

Texte Crypté« iweqbgndtqwgkcy »

- **Substitution poly-alphabétique :**le principe consiste à remplacer chaque lettre du message en clair par une nouvelle lettre prisedans plusieurs alphabets aléatoires associés. Par exemple, on pourra utiliser n substitutionsmono-alphabétiques ; celle qui est utilisée dépend de la position du caractère à chiffrer dans le texteen clair. On choisit une clé qui sert d'entrée dans la grille poly alphabétique incluant autant desymboles qu'il y a de lettres différentes à chiffrer. Chaque caractère de la clé désigne une lettreparticulière dans la grille de codage. Pour coder un caractère, on doit lire le caractère correspondantdu texte en clair en utilisant la grille poly alphabétique et le mot clé associé dans l'ordre séquentiel (on répète la clé si la longueur de celle-ci est inférieure à celle du texte de

départ). L'exemple leplus célèbre est l'algorithme de VIGENERE et de BEAUFORT. L'illustration la plus simple quicorresponde à ce principe est l'utilisation d'une fonction à base de ou exclusif (XOR).

IV.1.2 Cryptage par transposition : Les transpositions consistent à mélanger les symboles ou les groupes de symboles d'un message clair suivant des règles prédéfinies pour créer de la diffusion. Ces règles sont déterminées par la clé de chiffrement. Une suite de transpositions forme une permutation.

IV.1.3 Cryptage par produit : C'est la combinaison de chiffrement par substitution etchiffrement par transposition. La plupart des algorithmes à clés symétriques utilisent le chiffrement par produit. On dit qu'un « round » est complété lorsque les deux transformations ont été faites une fois (substitution et transposition). Ces successions des rondes portent également le nom de réseaux S-P de Shannon.

IV.2 Méthodes de cryptage Modernes :

On distingue deux méthodes majeures de cryptage modernes :

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

IV.2.1 Cryptage symétrique

Ce type de cryptage se base sur l'utilisation d'une clé pour crypter et décrypter les messages. La sécurité de cette solution repose sur le fait que la clé est connue uniquement par l'émetteur et le récepteur du message.

L'exemple historique de l'utilisation du cryptage symétrique est le fameux téléphone rouge qui reliait le Kremlin à la Maison Blanche. La clé privée était alors transmise dans une valise diplomatique. Pour une meilleure sécurité, elle était détruite et réinitialisée après chaque conversation.

Le cryptage symétrique fonctionne selon deux procédés différents :

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

- ✓ **Avantages du cryptage symétrique :**

-La rapidité d'exécution (une seule clé utilisée)

-La simplicité d'implémentation (gestion d'une seule clé).

- Permet de concevoir différents mécanismes cryptographiques (fonctions de hachage, etc...)
- Clés relativement courtes.

✓ **Inconvénients du cryptage symétrique :**

- La complexité de fonctionnement : une obligation d'avoir le nombre de clés privées égal au nombre de destinataires.
- La sécurisation de la chaîne de transmission de la clé.
- Impossibilité de garantir la propriété de non-répudiation dans les schémas de signature électronique**.[3]**

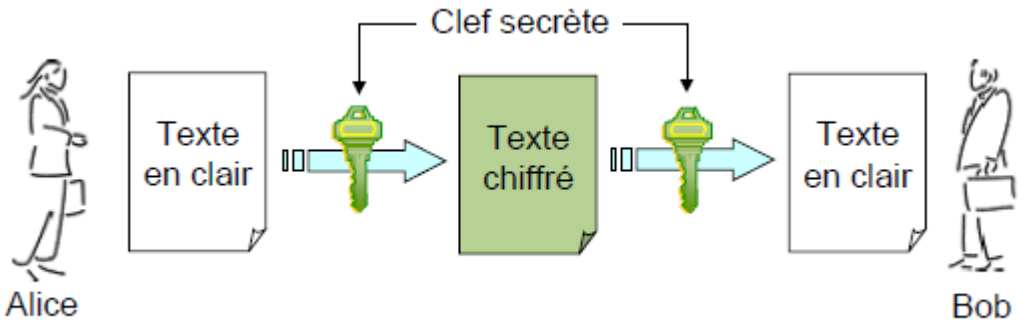


Figure I.1.Principe de cryptage symétrique

IV.2.2 Cryptage asymétrique

Ce cryptage, contrairement au symétrique, se base sur l'utilisation de deux clés, l'une publique(Pour crypter, elle est accessible publiquement) et l'autre privée (pour décrypter le message, elle estgardée secrète). Ce type de cryptage élimine la problématique de la transmission de la clé. Ce mode de cryptage est également nommé le cryptage à clé publique. Il est essentiel Que l'on ne puisse pas déduire la clé privée de la clé publique.

Pour bien comprendre le principe, on peut l'illustrer avec l'échange d'une lettre entre un émetteur etun destinataire**.**

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

✓ **Avantages du cryptage asymétrique :**

- l'élimination de la problématique de la transmission de clé
- la possibilité d'utiliser la signature électronique
- l'impossibilité de décrypter le message dans le cas de son interception par une personne non autorisé.

-Une paire de clés (publique/secrète) peut être utilisée plus longtemps qu'une clé Symétrie.

✓ **Inconvénients du cryptage asymétrique :**

- Un temps d'exécution plus lent que le cryptage symétrique
- le danger des attaques par substitution des clés (d'où la nécessité de valider les émetteurs des clés)

-Taille des clés, plus grand que celle des systèmes symétriques. **[3]**

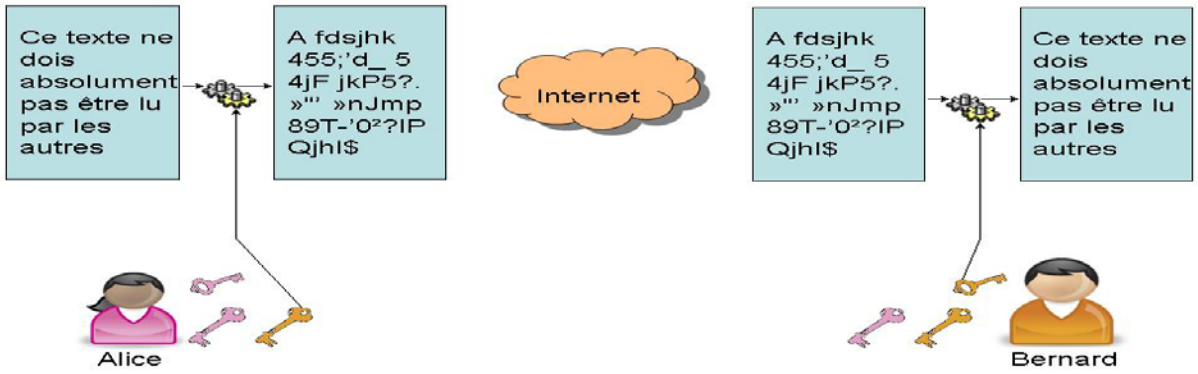


Figure I.2.Principe de cryptage Asymétrique

IV.2.3 Exemples d'algorithmes de cryptage symétriques et asymétriques

IV.2.3.1 Cryptage DES (Data Encryptions Standard) :

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

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

La clé est codée sur 64 bits et formée de 16 blocs de 4 bits, généralement notés k1 à k16 Etant donné que « seuls » 56 bits servent effectivement à chiffrer, il peut exister 256 (soit 7.2*1016) clés différentes **[2].**

IV.2.3.2 CryptageAES (Advanced Encryption Standard)

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

Finalement, un XOR entre la matrice et une autre matrice permet d'obtenir une matrice intermédiaire. Ces différentes opérations sont répétées plusieurs fois et définissent un « tour ». Pour une clé de 128, 192 ou 256, AES nécessite respectivement 10, 12 ou 14 tours**[2].**

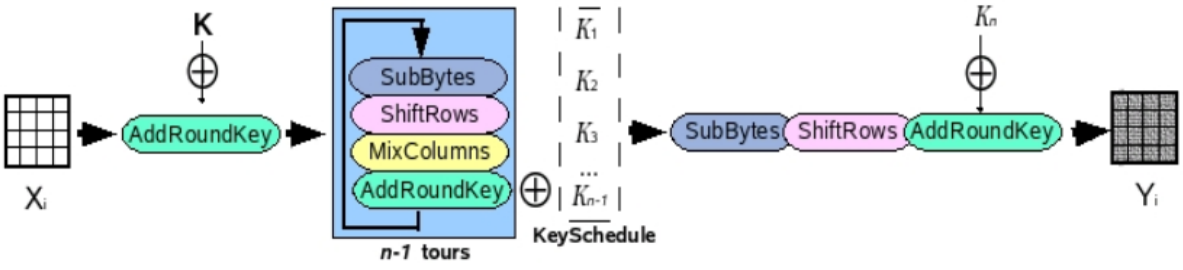


Figure I.3 Le schéma général d'AES.

IV.2.3.3 Méthode de cryptage RSA

La méthode RSA est asymétrique, cette méthode utilise une paire de clés (des nombres entiers) composé d'une clé publique pour chiffrer et d'une clé privée pour déchiffrer des données confidentielles. Les deux clés sont créées par une personne, souvent nommée par convention Alice, qui souhaite que lui soient envoyées des données confidentielles. Alice rend la clé publique accessible. Cette clé est utilisée par ses correspondants (Bob, etc.) pour chiffrer les données qui lui sont envoyées. La clé privée est quant à elle réservée à Alice, et lui permet de déchiffrer ces données. La clé privée peut aussi être utilisée par Alice pour signer une donnée qu'elle envoie, la clé publique permet à n'importe lequel de ses correspondants de vérifier la signature.

Une condition indispensable est qu'il soit « calculatoire ment impossible » de déchiffrer à l'aide de la seule clé publique, en particulier de reconstituer la clé privée à partir de la clé publique, c'est-à-dire que les moyens de calcul disponibles et les méthodes connues au moment de l'échange (et le temps que le secret doit être conservé) ne le permettent pas.

Le chiffrement RSA est souvent utilisé pour communiquer une clé de chiffrement symétrique, qui permet alors de poursuivre l'échange de façon confidentielle : Bob envoie à Alice une clé de chiffrement symétrique qui peut ensuite être utilisée par Alice et Bob pour échanger des données **[2].**

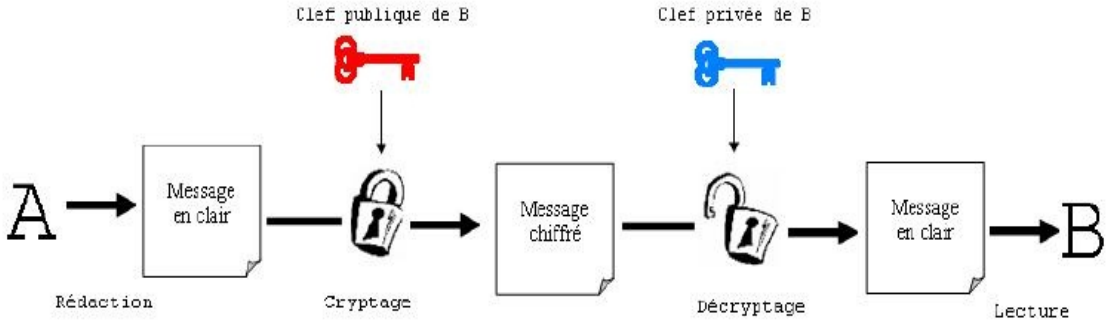


Figure I.4 Principe général de chiffrement RSA.

IV.2.3.4 Cryptage par flot

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

Quand la clef dynamique est générée indépendamment du texte clair et du texte chiffré, l'algorithme de chiffrement par flot est dit synchrone. Avec un chiffrement par flot, l'émetteur et le récepteur doivent se synchroniser en utilisant la même clef et en l'utilisant à la même position. Les chiffrements par flot synchrone sont utilisés principalement dans des environnements où les erreurs sont fréquentes car ils ont l'avantage de ne pas propager les erreurs. Concernant les attaques actives comme l'insertion, la suppression et la copie de digits du texte chiffré par un adversaire actif, celles-ci produisent immédiatement une perte de synchronisation. Le processus de cryptage d'un chiffrement par flot synchrone est décrit (**Figure I.4)** où $f()$ est la fonction qui détermine l'état suivant, $g()$ est la fonction génératrice de la clef dynamique et $h()$ la fonction de sortie de cryptage :

$$\begin{cases} s_{i+1} = f(k, s_i) \\ z_i = g(k, s_i) \\ c_i = h(z_i, m_i) \end{cases} \quad \textbf{(1)}$$

où *K* est la clef, s_i, m_i, $c_i$et $z_i$sont respectivement le i^e état, le texte clair, le texte chiffré et la clef dynamique. Le processus de décryptage est illustré figure (**Figure I.5)**.

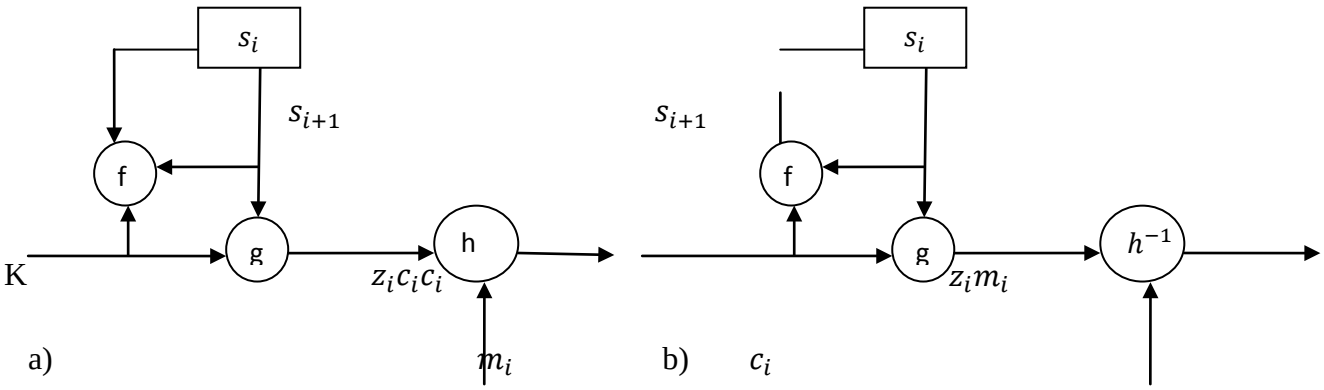


Figure I.5 Cryptage par flot synchrone. a) Cryptage. b) Décryptage.

Quand la clef dynamique est générée à partir de la clef et d'un certain nombre de digits précédemment cryptés, l'algorithme de chiffrement par flot est dit asynchrone, appelé aussi chiffrement par flot auto-synchronisant. La propagation des erreurs est limitée à la taille de la mémoire. Si des digits du texte chiffré sont effacés ou insérés en plus, le récepteur est capable avec la mémoire de se resynchroniser avec l'émetteur. Concernant les attaques actives, si un adversaire actif modifie une part des digits du texte chiffré, le récepteur est capable de la détecter. Le processus de cryptage d'un chiffrement par flot asynchrone est décrit (**Figure I.6)**, où $g()$ est la fonction génératrice de la clef dynamique et $h()$ la fonction de sortie de cryptage

$$\begin{cases} z_i = g(k, c_{i-t}, c_{i-t+1,\ldots\ldots,} c_{i-2}, c_{i-1}) \\ c_i = h(z_i, m_i) \end{cases} \textbf{(2)}$$

où K est la clef, mi, ci et z_i sont respectivement le i^e texte clair, le texte chiffré et la clef dynamique. Nous pouvons remarquer équations (**2**) que la clef dynamique dépend des t digits précédents du texte chiffré. Afin d'être robuste à de nombreuses attaques statistiques, la fonction génératrice de la clef dynamique $g()$ doit produire une séquence d'une large période avec de bonnes propriétés statistiques qui peuvent être appelées séquences binaires pseudo aléatoires. Le processus de décryptage est illustré figure (**Figure I.5)[2].**

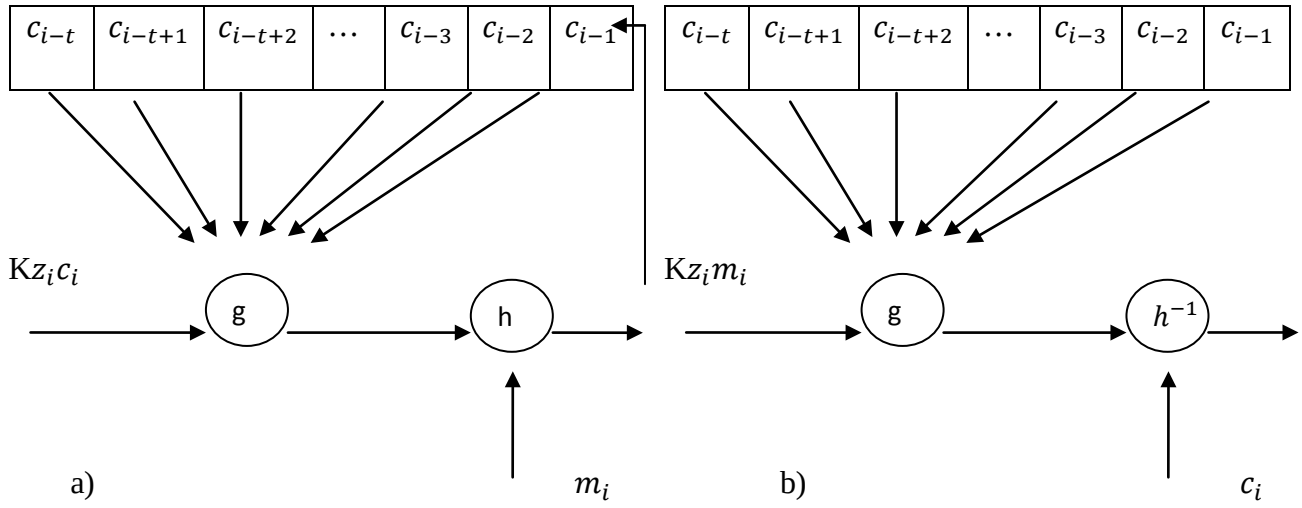


Figure I.6 Chiffrement par flot asynchrone a) Cryptage. b) Décryptage.

IV.2.3.5 Fonction de hachage

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

Une fonction de hachage doit être à sens unique, c'est à dire qu'il doit être impossible étant donné une empreinte de retrouver le message original, et sans collisions, ça veut dire l'impossibilité de trouver deux messages distincts ayant la même valeur decondensé. La moindre modification du message entraîne la modification de l'empreinte.

MD5 (Message Digest 5 - Rivest1991-RFC 1321) et SHA sont deux exemples de fonctions de hachage.

IV.2.3.6 Scellement (MAC) :

Est un mécanisme qui consiste à calculer (ou sceller) une empreinte à partir d'un message et d'une clé privée pour:

- Authentifier l'origine des données
- Vérifier l'intégrité des données

Le scellement d'une empreinte génère :

- un **sceau**ou**code d'authentification de message** *(MAC)*

Le scellement est calculé en appliquant une fonction de hachage à un message et une clé privée tel qu'illustré dans la figure suivante :

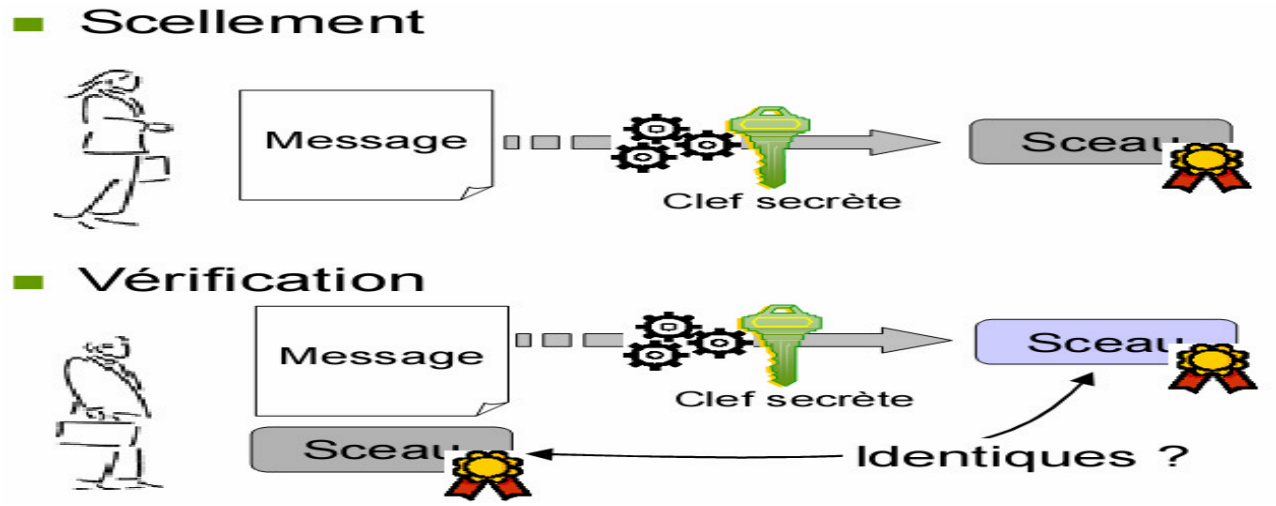


Figure I.7 Scellement

IV.2.3.7 Signature numérique

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

- d'authentifier l'auteur d'un document électronique
- de garantir son intégrité
- de se protéger contre la contrefaçon (seul l'expéditeur doit être capable degénérer la signature) -> non-répudiation.

La signature électronique est basée sur l'utilisation conjointe d'une fonction de hachage et de la cryptographie asymétrique. **[4]**

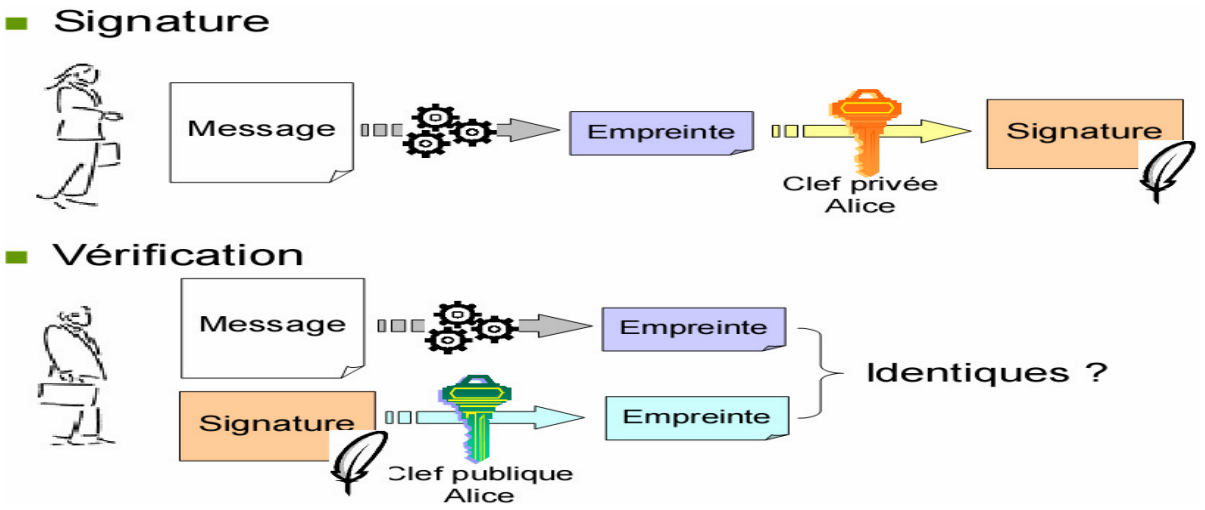


Figure I.8 Signature numérique

IV.2.3.8 Certificat électronique

Un certificat numérique est un bloc de données contenant, dans unformat spécifié, les parties suivantes :

- la clé publique d'une paire de clés asymétriques,
- des informations identifiant le porteur de cette paire de clés (qui peutêtre une personne ou un équipement), telles que son nom, son adresse IP, son adresse de messagerie électronique, son URL, son titre, son numéro de téléphone, etc...
- l'identité de l'entité ou de la personne qui a délivré ce certificat(autorité de certification), Ex. Verisign,
- La signature numérique des données générée par lapersonne ou l'entité prenant en charge la création ou l'authentificationde ce certificat et servant d'autorité de certification.

Usuellement, on distingue deux familles de certificats numériques :

- les certificats de signature, utilisés pour signer des e-mails ou s'authentifier sur un site web.
- les certificats de chiffrement : les gens qui vous envoient des e-mailsutilisent la partie publique de votre certificat pour chiffrer le contenuque vous serez seul à pouvoir déchiffrer.

Il existe deux façons distinctes de créer des certificats électroniques :

- le mode décentralisé (le plus courant) qui consiste à faire créer, parl'utilisateur (ou, plus exactement par son logiciel ou carte à puce) la biclef cryptographique et de remettre la partie publique à l'AC qui va yadjoindre les informations de l'utilisateur et signer l'ensemble(information + clé publique)

- le mode centralisé qui consiste en la création de la biclef par l'AC, quigénère le certificat et le remet avec la clé privée à son utilisateur.

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

- la norme X.509 en version 1, 2, et 3, sur lequel se fondentcertaines infrastructures à clés publiques.
- OpenPGP, format standard (normalisé dans le RFC 2440) delogiciels comme GnuPG.**[4]**

Conclusion

Dans ce chapitre, nous avons présenté des généralités sur la cryptographie. En premier lieu, nous avons commencé par donner quelques terminologies. Puis nous avons cité les différents algorithmes de cryptage classiques et modernes. Enfin, nous avons abordé la notion de signature numérique et certificat électronique.

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

CHAPITRE II

INTRODUCTION AUX SYSTEMES CHAOTIQUES

I. Introduction

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

La définition qu'on peut donner au chaos est que c'est un phénomène qui peut apparaître dans les systèmes dynamiques déterministes non linéaires. Il présente un aspect fondamental d'instabilité appelé sensibilité aux conditions initiales, ce qui le rend imprédictible en pratique à long terme. Une autre caractéristique du système chaotique est son évolution qui semble aléatoire

II. Systèmes Dynamiques chaotiques

Le chaos tel que le scientifique le comprend ne signifie pas l'absence d'ordre, il se rattache plutôt à une notion d'imprévisibilité, d'impossibilité de prévoir une évolution à long terme du fait que l'état final dépend de manière si sensible de l'état initial. On appelle donc un système dynamique chaotique, un système qui dépend de plusieurs paramètres et qui est caractérisé par une extrême sensibilité aux conditions initiales. Il n'est pas déterminé ou modélisé par des systèmes d'équations linéaires ni par les lois de la mécanique classique..**[5] [6]**

a) La non-linéarité

Un système chaotique est un système dynamique non linéaire. Un système linéaire ne peut pasêtre chaotique.

La notion de système dynamique est relative à tous les systèmes dont l'évolution dépend dutemps. En général, pour prévoir des phénomènes réels générés par ces systèmes, la démarche consiste à construire un modèle mathématique qui établit une relation entre un ensemble de causes et un ensemble d'effets. Si cette relation est une opération de proportionnalité, le phénomène est linéaire. Dans le cas d'un phénomène non linéaire, l'effet n'est pas proportionnel à la cause..**[5] [6]**

b) Le déterminisme

Un système chaotique a des règles fondamentales déterministes et non probabilistes. Il est généralement régi par des équations différentielles non linéaires qui sont connues, donc par des lois rigoureuses et parfaitement déterministes..**[5] [6]**

c) Sensibilité aux conditions initiales

Quelques systèmes physiques se comportent de manière chaotique. Parmi ces systèmes, on peut citer l'atmosphère, un robinet qui goutte, un pendule excité dans un champ magnétique... Ces quelques systèmes se démarquent par leurs dimensions et l'origine de leurs mouvements. Ainsi, on remarque que le chaos peut surgir dans divers systèmes et est, de ce fait, assez répandu. Quelques caractéristiques permettent de comprendre qualitativement les points marquants de ces systèmes..**[5] [6]**

Tout d'abord, ils sont extrêmement sensibles aux perturbations. On peut illustrer ce fait par l'effet papillon. Popularisé par le météorologue Edward Lorenz, cet effet papillon consiste en l'image suivante. On peut considérer que le simple battement d'aile d'un papillon en Australie peut entraîner une tempête sur côte américaine. Ceci signifie qu'une perturbation en apparence mineure à l'échelle de l'atmosphère peut avoir de grandes répercutions.

Plus précisément, il faudrait comprendre que si on considérait deux planètes Terre, placées presque dans les mêmes conditions, ne différant que par la présence d'un papillon, on constaterait que les deux planètes initialement dans des conditions très proches finiraient par se comporter de manières très différentes; l'une connaîtrait des tempêtes là où l'autre présenterait un soleil au beau fixe...

Il faut néanmoins garder à l'esprit qu'il s'agit d'une image qui n'est pas tout à fait exacte car l'atmosphère n'est pas un système chaotique "parfait". Le battement d'aile d'un papillon n'aurait en réalité pas une influence si grande car il existe des phénomènes limitant. Notons d'ailleurs que ces effets limitants sont plus importants qu'on ne l'avait pensé au début. Quoiqu'il en soit, l'image permet de comprendre le phénomène de sensibilité aux perturbations, plus souvent appelé "sensibilité aux conditions initiales".

Illustrons ce phénomène par une simulation numérique. On affecte à un système chaotique deux conditions initiales très proches, c'est-à-dire ne différant que très peu ("d'un papillon"...). Dans un premier temps, les deux systèmes évoluent de la même manière mais, très vite, leur comportement devient différent pour n'avoir plus grande chose à voir.

II.1 La différence entre le chaos et l'aléatoire

La différence entre le chaos et l'aléatoire nous a paru le point le plus important de la compréhension du chaos. En effet, on a toujours tendance à considérer qu'un phénomène tire son imprédictibilité du nombre trop important de paramètres en jeu dans sa description. Ce qui nous pousse à en donner une approche probabiliste qui peut être parfaitement satisfaisante, garde par définition une certaine marge d'aléatoire.

En ce qui concerne le chaos, il n'en est rien, les systèmes chaotiques se comportent, en effet, d'une manière qui peut sembler aléatoire. Mais ce comportement est en fait décrit de manière déterministe par des équations non linéaires parfaitement déterministes, c'est-à-dire en particulier avec des outils mathématiques permettant une approche précise et certaine.**[7]**

II.2 Présentation des attracteurs

Lorsqu'on étudie le comportement des systèmes chaotiques, on ne peut se contenter de l'évolution d'une seule variable au cours du temps car son évolution est trop complexe pour cela. Ainsi, on considère ce qu'on appelle des attracteurs, qui sont définis dans cechapitre pour ceux qui suivent le parcours "formel" ou le parcours complet.

Sans la définition exacte, on peut retenir que les attracteurs rendent compte de l'évolution du système. Ils forment généralement des formes bien définies.

II.2.1 Attracteur de Hénon

a) Présentation et définition

Le système de Hénon est un modèle proposé en 1976 par le mathématicien Michel Hénon. Ce modèle vise à rendre compte de certaines propriétés d'une section de Poincaré (définie plus loin) de l'attracteur de Lorenz. Il s'agit d'un système qui introduit des itérations dans le plan. Ces itérations sont définies par les relations suivantes. **[8]**

$$\begin{cases} X_{n+1} = a - X_n^2 + bY_n \\ Y_{n+1} = X_n \end{cases} \quad (3)$$

On prendra pour conditions initiales :

$(X_0, Y_0) = (1, 0)$, $a = 1.4$ et $b = 0.3$. Ces valeurs furent proposées par Michel Hénon et permettent d'observer un comportement chaotique.

b) Attracteur de Hénon

Alors, en très peu d'itérations, on considère que les points calculés sont sur l'attracteur. On obtient alors l'attracteur de Hénon.

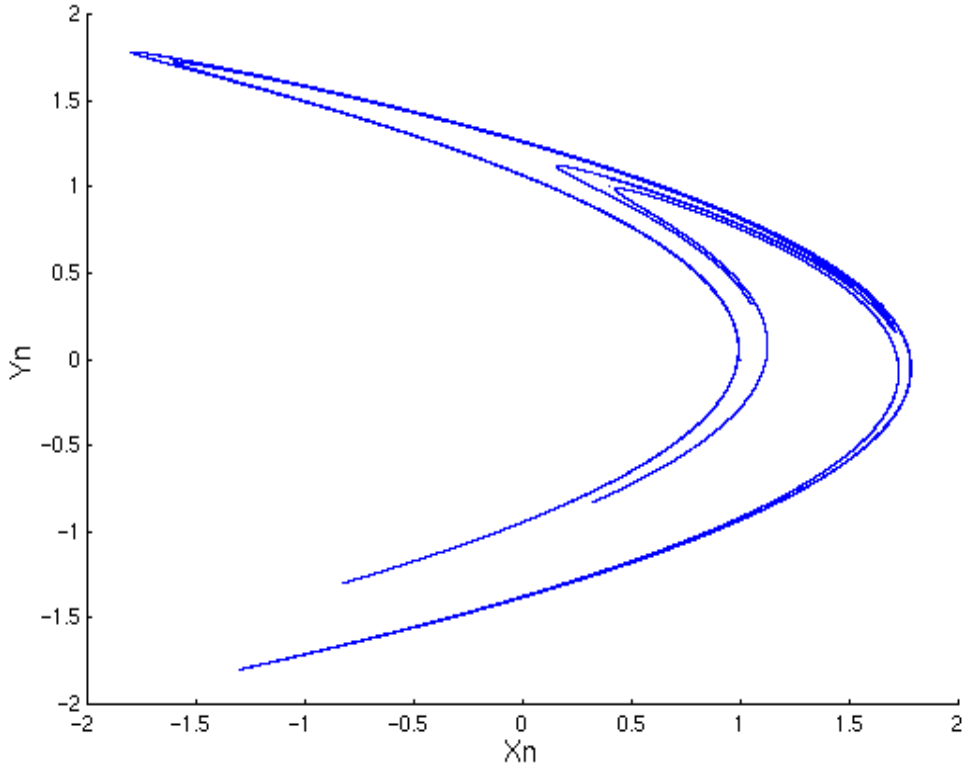
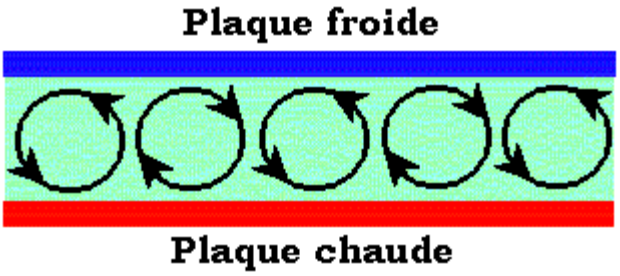


Figure II.1: Attracteur de Hénon, contenu dans le plan.

II.2.2 Attracteur de Lorenz

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

Les équations correspondent aux équations de la convection de Rayleigh-Bénard. Dans cette expérience, on considère un fluide entre deux plaques portées à deux températures légèrement différentes. Les deux plaques sont horizontales et la plaque la plus chaude est située en bas. On observe des tourbillons.**[6]**



FigureII.2: Convection de Rayleigh-Bénard - des tourbillons convectifs apparaissent entre deux plaques parallèles portées à deux températures différentes et disposées horizontalement de façon à ce que la plaque la plus chaude soit située en bas.

Cette expérience a été réalisée pour quelques fluides présentant des propriétés adaptées (viscosité, coefficient de dilatation, densité moyenne). Elle donne des résultats illustrant très bien le comportement chaotique.

a) Mise en équations

Le comportement du fluide est très bien déterminé par les équations de la mécanique des fluides. Ces dernières aboutissent aux équations suivantes.

Équation de Navier-Stokes:

$$\frac{\partial \vec{v}}{\partial t} + \vec{v} \cdot \vec{\nabla} \vec{v} = (-\vec{\nabla} p + T\vec{z} + \vec{\nabla}^2 \vec{v}) \times \mathrm{Pr}$$

Équation II.1: Équation de Navier-Stokes.

Avec *Pr = (n / D),* nombre de Prandtl, rapport de la viscosité cinématique du fluide sur la diffusivité thermique.

Équation de l'incompressibilité du fluide:

$$\vec{\nabla} \cdot \vec{v} = 0 \qquad (5).$$

Équation II.2: Équation de l'incompressibilité du fluide

Équation de propagation de la chaleur:

$$\frac{\partial T}{\partial t} + \vec{v} \cdot \vec{\nabla} T = Ra\, \vec{v} \cdot \vec{z} + \nabla^2 T \quad (6).$$

Équation II.3: Équation de propagation de la chaleur

***T* :** est la température rapportée à celle du fluide sans la convection.

***Ra* :** est le nombre de Rayleigh. Il dépend des propriétés du fluide, de la distance entre les plaques et de la différence de température entre les plaques.

Les équations précédentes peuvent être réduites. Elles se présentent alors sous la forme d'un système, le système de Lorenz que voici:

$$\begin{cases} \frac{\partial v}{\partial t} = Pr \cdot (T - v) \\ \frac{\partial T}{\partial t} = (Ra - Z) \cdot v - T \\ \frac{\partial Z}{\partial t} = v \cdot T - b \cdot Z \end{cases} \quad (4).$$

Dans toute la suite, on prendra:*Pr = 10, b = 8/3* et *Ra = 28*. Ces valeurs impliquent un comportement chaotique.

n est une composante de vitesseet Z est une variable issue des grandeurs physiques évoquées dans les équations (4), (5) et (Equation II.3). Les dérivées introduites dans les premiers membres sont des dérivées partielles par rapport au temps.

Le propos de cet exposé n'est pas la mécanique des fluides, nous ne rentrerons pas dans les détails des calculs qui permettent d'obtenir ce système (d'autant plus qu'il y a une partie délicate...).

b) Évolution dans le temps

L'évolution dans le temps d'un tel système est chaotique. On peut le "constater" intuitivement grâce à la courbe suivante.

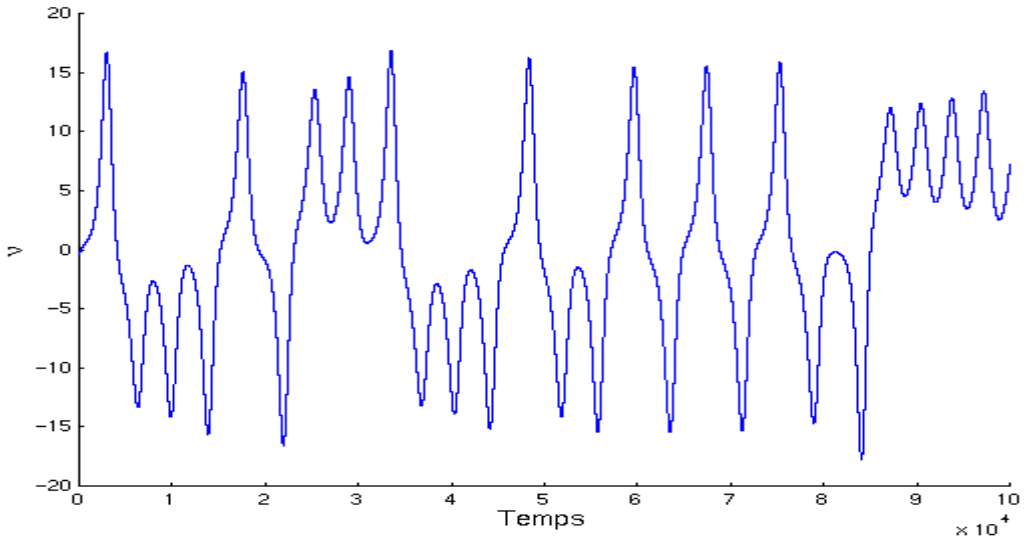


Figure II.3 : Evolution dans le temps de la première coordonnée du système.

c)Attracteur de Lorenz

L'espace des phases est un espace à trois dimensions dans lequel on représente les coordonnées *(n, T, Z)*. On obtient l'attracteur de Lorenz.

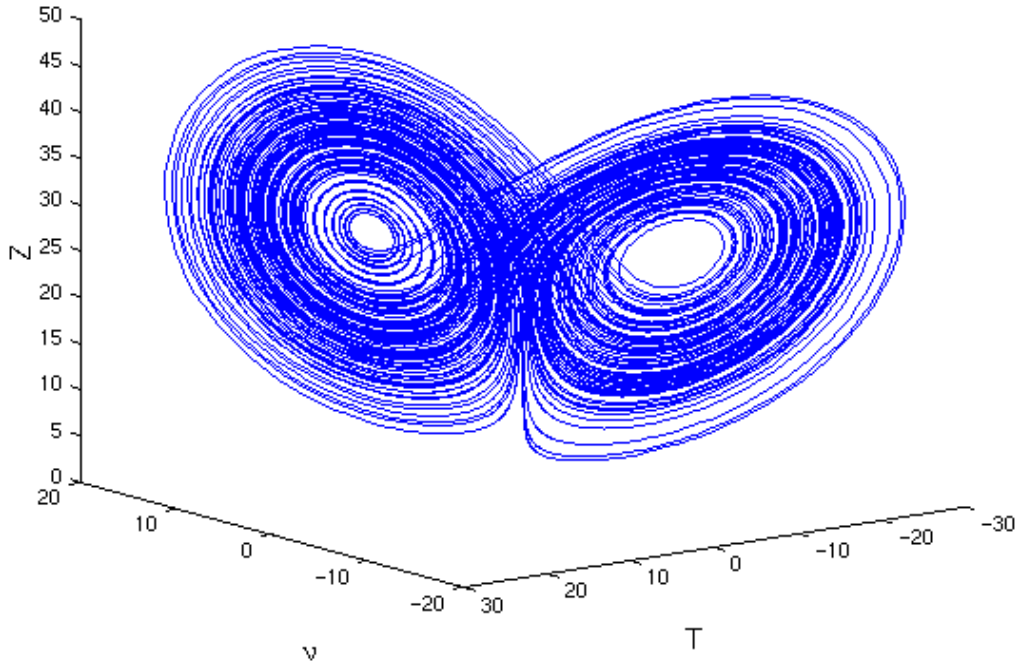


Figure II.4: Attracteur de Lorenz.

II.2.3 Attracteur de Rössler

a) Présentation

Proposé par l'Allemand Otto Rössler, le système de Rössler est lié à l'étude de l'écoulement des fluides; il découle des équations de Navier-Stokes. Les équations de ce système ont été découvertes à la suite de travaux en cinétique chimique.**[9]**

b) Equations

Les équations de ce système sont les suivantes:

$$\begin{cases} X' = -(Y + Z) \\ Y' = X + aY \\ Z' = b + Z(X - c) \end{cases} \quad (8).$$

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

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

c) Evolution dans le temps

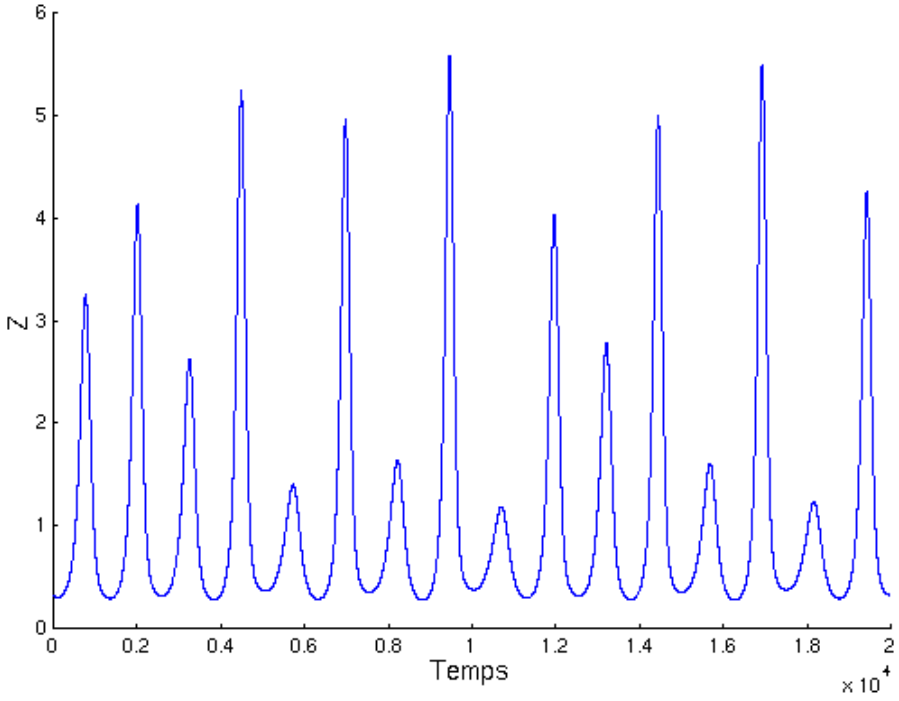


Figure II.5: Évolution dans le temps de la coordonnée Z.

d) Attracteur de Rössler

Tout comme pour les attracteurs précédents, on génère l'espace des phases.

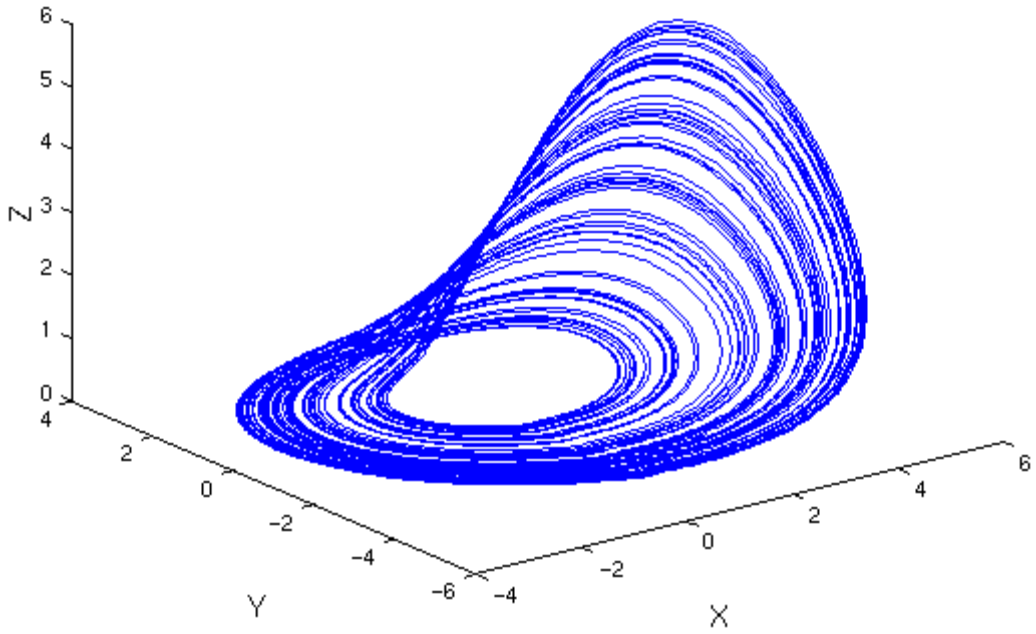


Figure II.6: Attracteur de Rössler.

II.2.4 Pendule de Moon

a) Présentation

Le pendule de Moon est un système physique. Il est constitué d'un pendule (avec une boule métallique à son extrémité) accroché à une potence légèrement flexible. De plus, le pendule est placé entre deux aimants situés à égale distance de la boule lorsque celle-ci et la potence sont au repos.

La potence est ensuite excitée à l'aide d'un mouvement oscillatoire harmonique d'amplitude constante. Stimulé, le pendule se met en mouvement et les forces magnétiques dues aux aimants. Le mouvement est alors chaotique.

b) Équation de Duffing

L'équation de ce système est dite équation de Duffing et s'écrit comme suit.

$$X'' + mX' - \frac{1}{2}(1 - X^2)X = a\cos(at)$$

Équation II.4 : Equation de Duffing

Attention, les variables et constantes de l'équation sont sans dimension: on étudie un modèle mathématique, sans se soucier de l'homogénéité.

X est la position du pendule.

Les dérivées *X'* et *X''* sont respectivement les dérivées partielles par rapport au temps d'ordre un et d'ordre deux.

m est la masse de la boule métallique, *a* est l'amplitude de l'excitation et *w* est la pulsation de cette excitation.

Classiquement, on prend *m = 0.15*, *a = 0.15* (en fait, entre *0.1* et *0.2* environ) et *w=0.81* (en fait, entre *0.8* et *0.82*). On conservera ces valeurs dans la suite.

Il est intéressant de remarquer que ce système n'a qu'un degré de liberté. Un tel système va à l'encontre de l'idée selon laquelle il faut beaucoup de degrés de liberté pour obtenir un système chaotique.

c) Évolution dans le temps

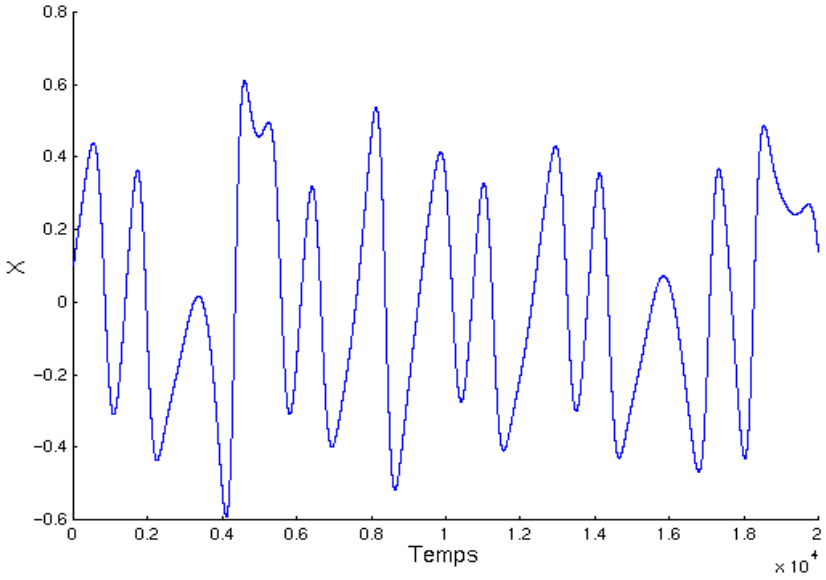


Figure II.7 : Évolution dans le temps de la position X.

d) Attracteur de Moon

Tout comme pour les attracteurs précédents, on génère l'espace des phases.

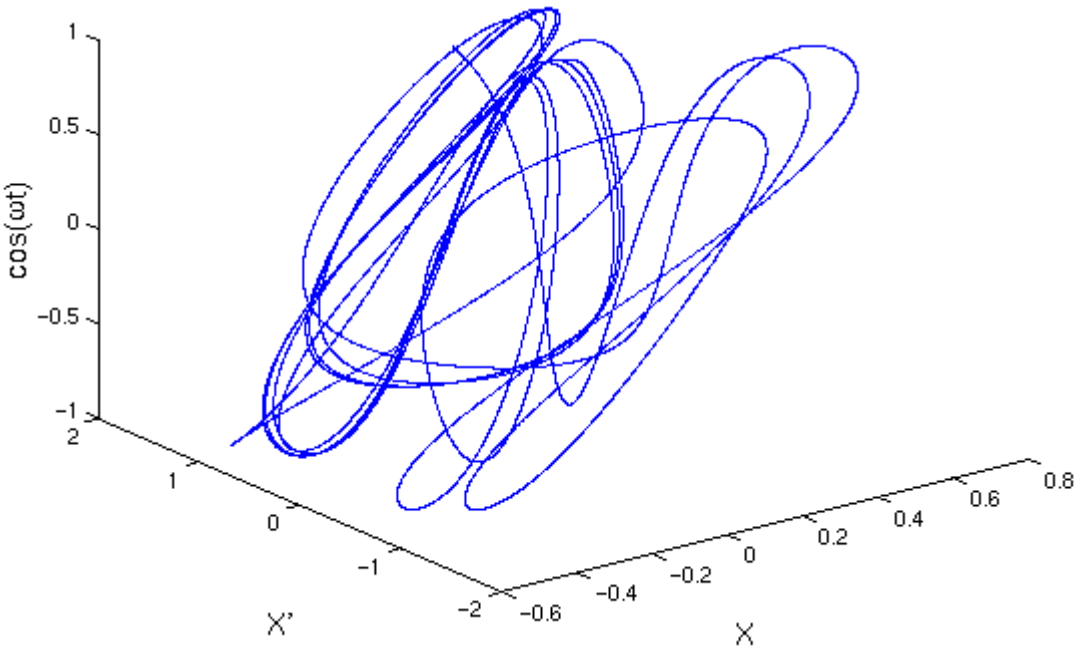


Figure II.8: Partie de l'attracteur de Moon.

L'attracteur de Moon est nettement plus complexe que les autres attracteurs présentés sur le site. On ne représente qu'une partie de cet attracteur car on ne pourrait pas distinguer les trajectoires dans le cas contraire, on verrait une sorte de pelote de laine...

Cet attracteur est plus étendu que les autres attracteurs.

II.2.5 Attracteur de CLIFFORD

Définition :utilisé l'équation suivant :

$x_{n+1} = \sin(a* y_n) + c \cos(a* x_n)$

$y_{n+1} = \sin(b* x_n) + d \cos(b* y_n)$

où a, b, c, d sont les variables qui définissent chaque attracteur **[6].**

Exemples :

a = -1.4, b = 1.6, c = 1.0	a = 1.1, b = -1.0, c = 1.0, d = 1.5	a = 1.6, b = -0.6, c = -1.2, d = 1.6

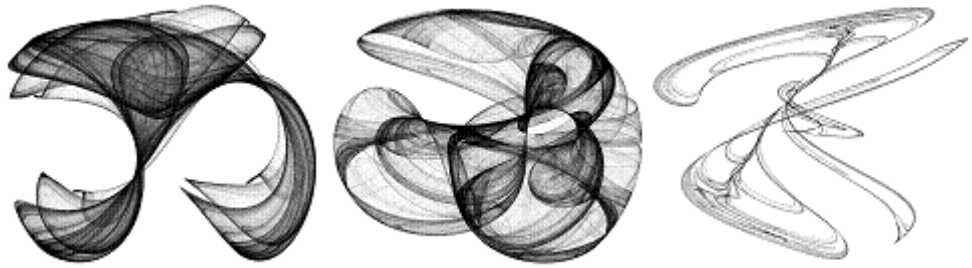


Figure II.2 Attracteur de CLIFFORD

II.3 Communications Sécurisées par chaos

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

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

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

Le diagramme principal de la communication sécurisée par le chaos est montré sur la **Figure II.9** .Le principe est de masquer une information par des signaux chaotiques et de l'envoyer vers le récepteur sur un canal public. L'information cryptée est récupérée au niveau du récepteur.

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

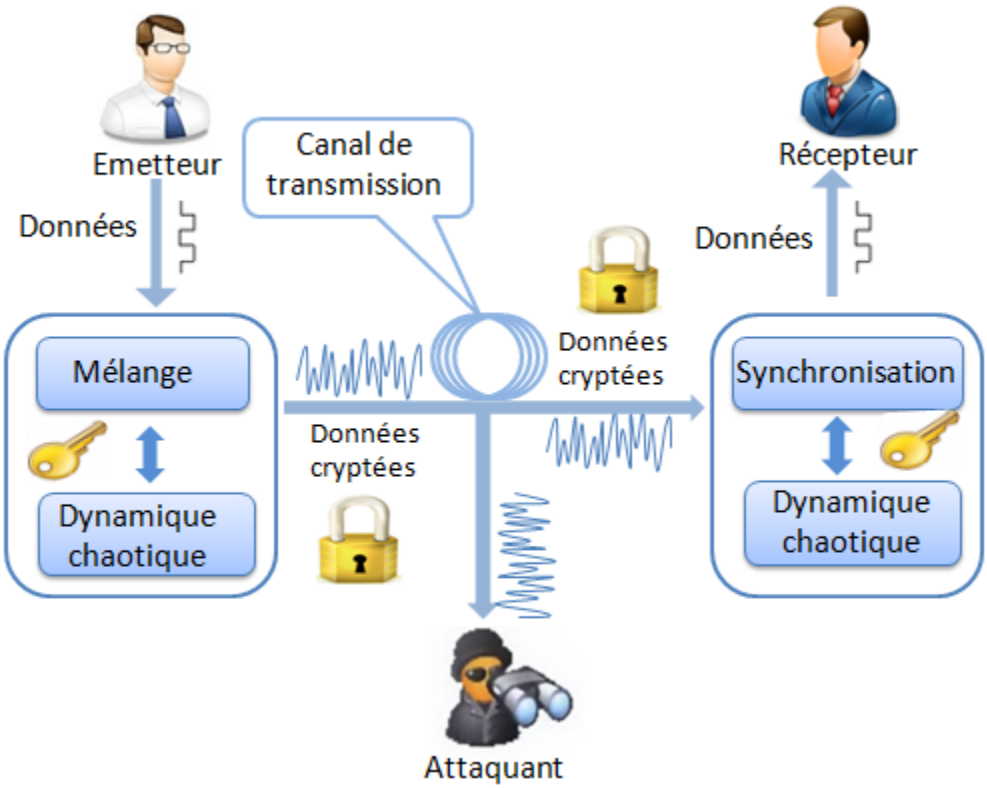


Figure II.9: Principe de Chiffrement par Chaos.

Le chiffrement d'un message par le chaos s'effectue donc en superposant à l'information initiale un signal chaotique. On envoie par la suite le message noyé dans le chaos à un récepteur qui lui connaît les caractéristiques du générateur de chaos. Il ne reste alors plus au destinataire qu'à soustraire le chaos de son message pour retrouver l'information..**[10][11]**

II.4 Comparaison entre chaos et cryptographie

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

systèmes chaotiques présentent des correspondances similaires ou presque, avec des systèmes cryptographiques traditionnels. Le tableau suivant illustre parfaitement cette correspondance.

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

Tableau II.1 : Correspondance entre la théorie du chaos et la cryptographie.

Conclusion

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

Dans le chapitre suivant, nous allons implémenter la méthode de CLifford pour chiffrer et déchiffrer des messages textes et images.

CHAPITRE III

Cryptage chaotique basé sur l’attracteur de Clifford

I. Introduction

Dans ce chapitre, nous allons tout d’abord présenter la méthode de cryptage chaotique des messages textes et images en se basant sur l’attracteur de Clifford. Ensuite, nous allons présenter notre application qu’on a développé sous Java pour crypter et décrypter des messages textes et images.

II. Approche proposée pour le cryptage d’image

Une image est définie comme une suite de pixels (des points lumineux). Chaque pixel possède une couleur : celle-ci est définie par un nombre entier, converti par la suite en binaire. Le principe de cryptage est simple, il s'agit d' "additionner" deux images, une image-clé et l'image qu'on veut crypter, grâce à l'opérateur XOR.**[7]**

Les éléments de l’image clé sont générés par l’attracteur de Clifford. Ce dernier est aussi initialisé par une graine chiffrée, en combinant par un XOR les codes ASCII d’une chaine de caractère « mot de passe » avec une autre chaine de caractère « Clef ». Comme le montre la suivante :

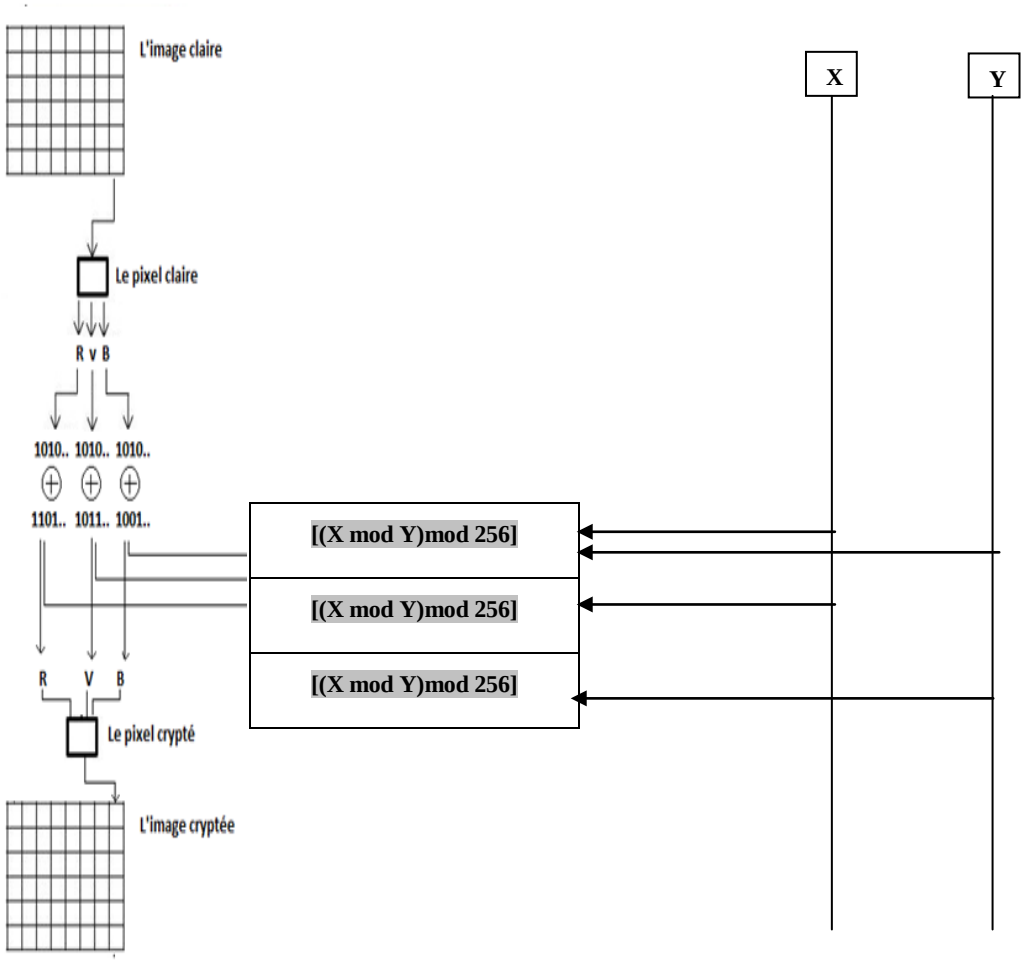


Figure III.1 shéma descriptif de la méthode proposée

Définition de l'attracteur de Clifford

L'attracteur de Clifford est défini par l'équation suivante :

$x_{n+1} = sin(a * y_n) + c\ cos(a * x_n)$

$y_{n+1} = sin(b * x_n) + d\ cos(b * y_n)$

où a, b, c, d sont les variables qui définissent l'attracteur.

Si on programme les formules ci-dessus en EXEL avec les valeurssuivantes :

a = -1.4, b= 1.6, c = 1.0, d = 0.7

on aura le graphe de la figure suivante :

E3 =SIN(-1,4*F2)+1*COS(-1,4*E2)

	A	B	C	D	E	F	G	H
1	-1,4	1,6	1	0,7	x	y		
2					0	0		
3					1	0,7		44
4					-0,66053023	1,30455132		132,021088
5					-0,3654776	-1,21648956		109,477602
6					1,86319126	-0,8087758		51,1361496
7					0,0441621	0,35106355		44,1621005
8					0,52615019	0,66304556		14,1501914
9					-0,0598308	1,08754749		3,71668812
10					-0,00234325	-0,21351377		2,34324574
11					1,2944822	0,65579956		126,682638
12					-1,03359964	1,22613987		192,540228
13					-0,8659489	-1,2633575		97,9489025
14					1,3313207	-1,28772374		220,126782
15					0,68432853	0,51845047		165,878063
16					-0,08864878	1,36155473		248,905951
17					0,04802323	-0,54104443		237,021194
18					1,68482048	0,53045204		93,4643741
19					-1,38514041	0,89391116		146,681919

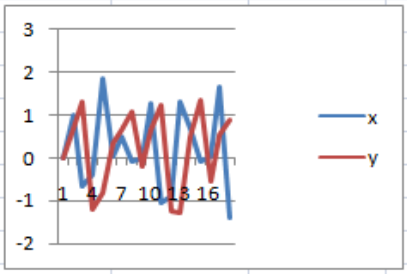


Tableau III.1: *valeurs X,Yet (X mod Y) mod 256 : de l'attracteur Clifford*

Nous allons utiliser l'attracteur de Clifford pour crypter nos données. Le principe du chiffrement continu sera utilisé, les valeurs de X et Y(tableau 1) seront converti pixel clair en pixel crypté en utilisant [*(X mod Y) mod 256]* pour être combiné avec les n-bits de données pour image et [97<ABS(X mod Y)<122] pour texte ou chiffre avec la fonction Xor.

Le codage d'un Pixel pratiquement se fait sur 32 bits, dont 24 bits sont utilisés pour coder la couleur :

- 8 bits sont consacrés à la teinte primaire **Rouge**.
- 8 bits sont consacrés à la teinte primaire **Vert**.
- 8 bits sont consacrés à la teinte primaire **Bleu**.

D'où la combinaison XOR se fait entre chaque 8bits des codes colorimétriques RVB qui composent le pixel et une suite binaire secrète générée par le générateur des nombres aléatoires expliqué précédemment, comme le montre l'exemple détaillé, suivant : (**Figure III.2**)

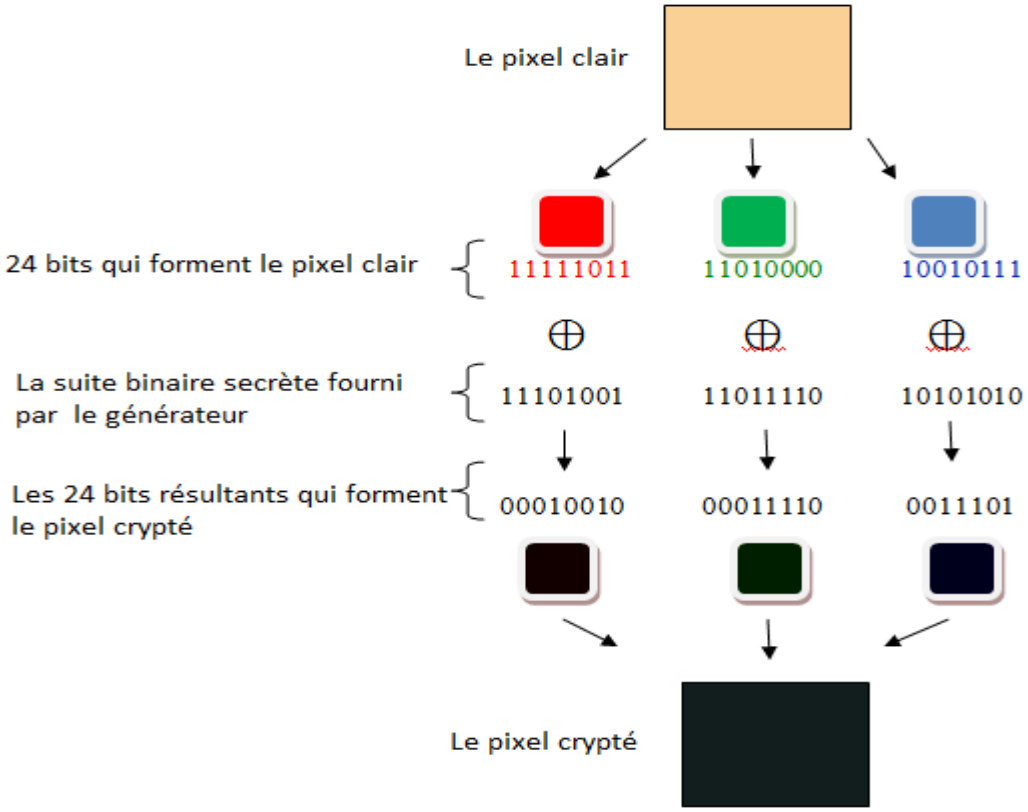


Figure III.2 Exemple de cryptage d'un pixel.

Caractéristiques de l'attracteur de Clifford

La première caractéristique des algorithmes de chiffrement quise basent sur l'attracteur de Clifford et le très haut niveau de sécurité et de performances.Lasécurité s'expriment en nombrede clés (a, b, c, d, X, Y) utilisées pour crypté et décrypté. La deuxième caractéristique est la rapidité de chiffrement d'importants volumes de données. Certaines implémentations sous forme matérielle atteignent des débits de quelques gigabits par seconde alors que les implémentations logicielles atteignent des débits de centaines de mégabits par seconde.

III. Développement de notre application de cryptage chaotique

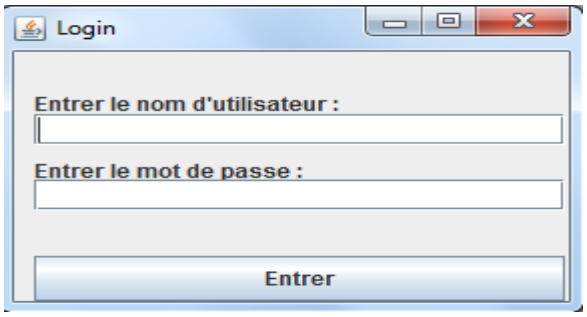
V.1 Langage de développement :

Nous avons utilisé Eclipse Hélios et Netbeans 8.2 pour l'implémentation de notre application

Notre application offre aux utilisateurs deuxInterfaces principales :

- ✓ Interface Login : contient Nom utilisateur et mot de passe (admin_admin).**Figure III.3**

Figure III.3 :L'interface Login



- ✓ Interface générale :contient tous les opérations de cryptage et décryptage (**Figure III.4**)

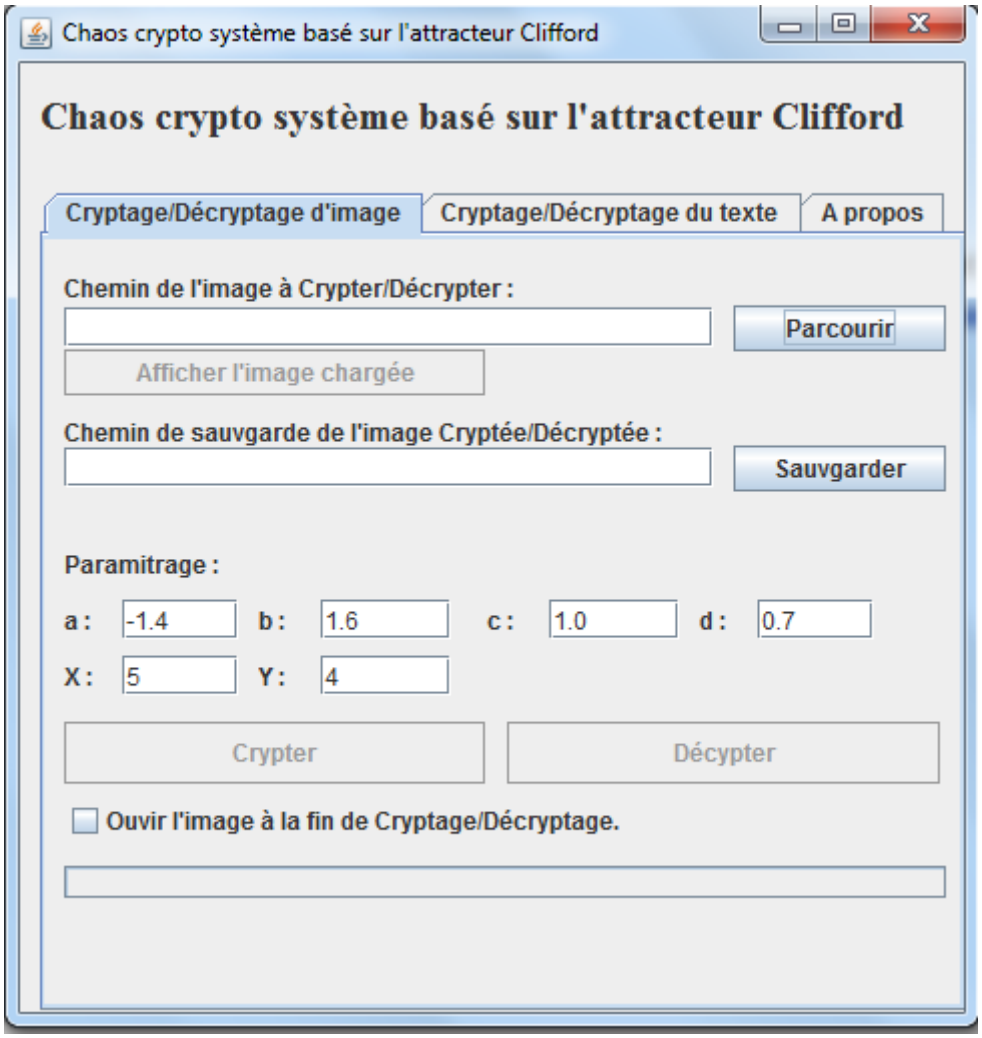


Figure III.4L'interface générale.

Cette interface contient des fenêtres :

- cryptage /décryptage image
- cryptage /décryptage texte

Opération crypté :cette fonctionnalité permet aux utilisateurs le cryptage d'images de différents formats BITMAP, JPEG, PNG, TIFF…

Opération Décrypté :Cette deuxième fonctionnalité permet aux utilisateurs le décryptage d'imagesqui sont déjà cryptées avec notre application

V.2 Résultat d'exécution

V.2.1Cryptage/Décryptage image :

Les figures suivantes montrent le résultat d'exécution de notre application

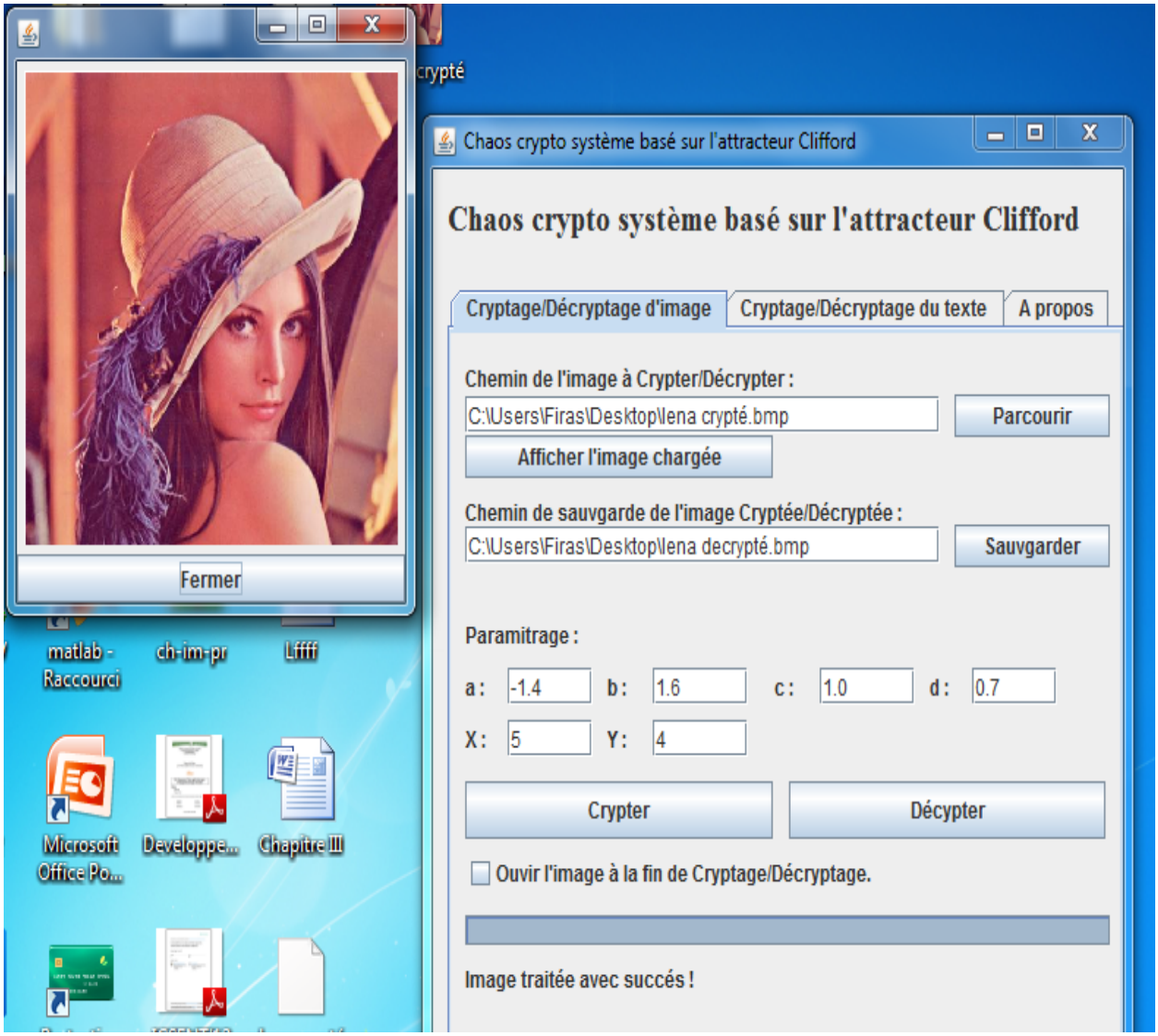


Figure III.5 Chargement d'image

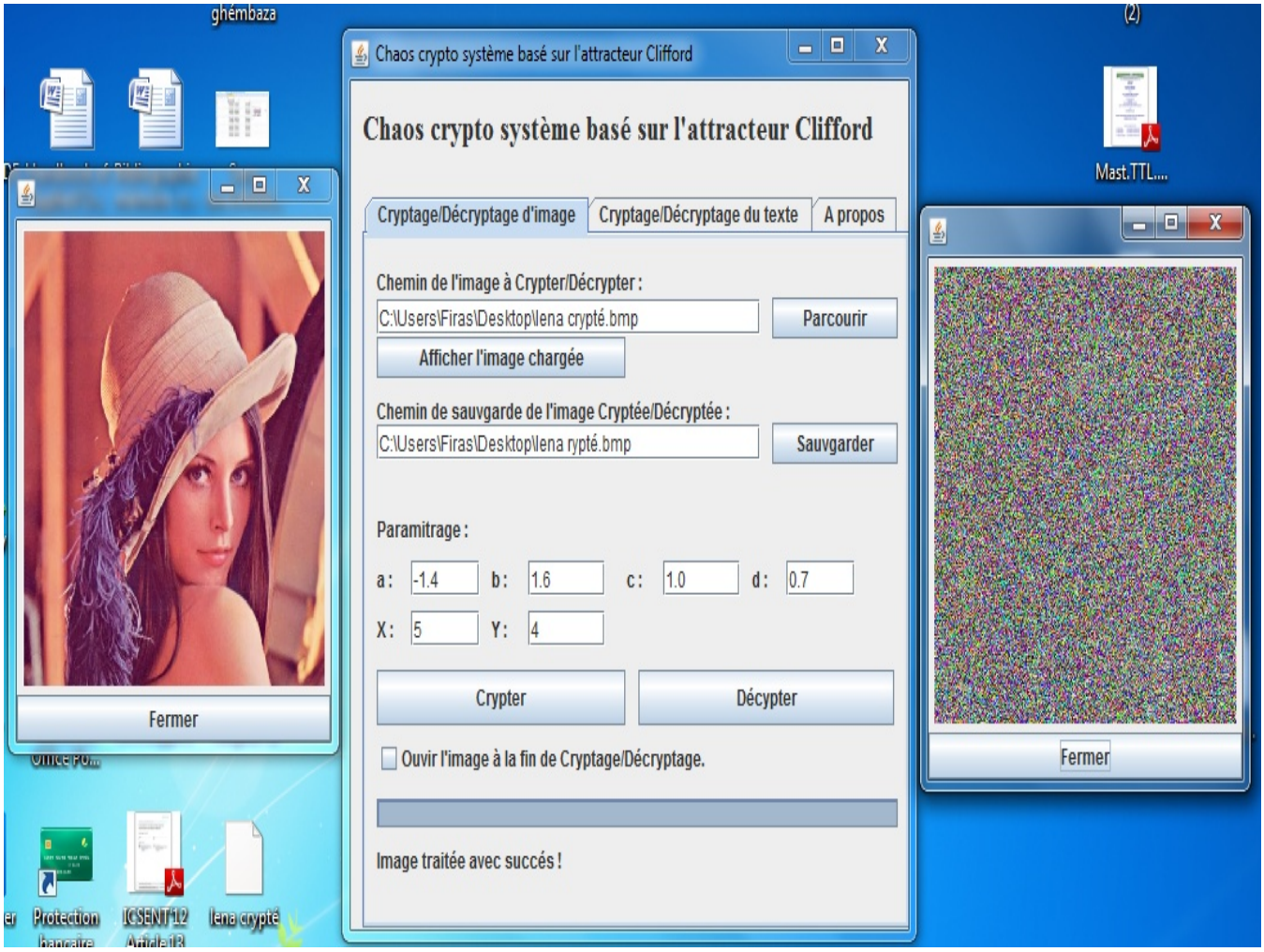


Figure III.6 Cryptage d'image

Une légère modification de clés ne donne pas le même résultat.

Dans l'exemple suivanton va changer la valeur d'a=1.4 par la valeur a=1.1. Le résultat de décryptage est donné par la figure suivante :

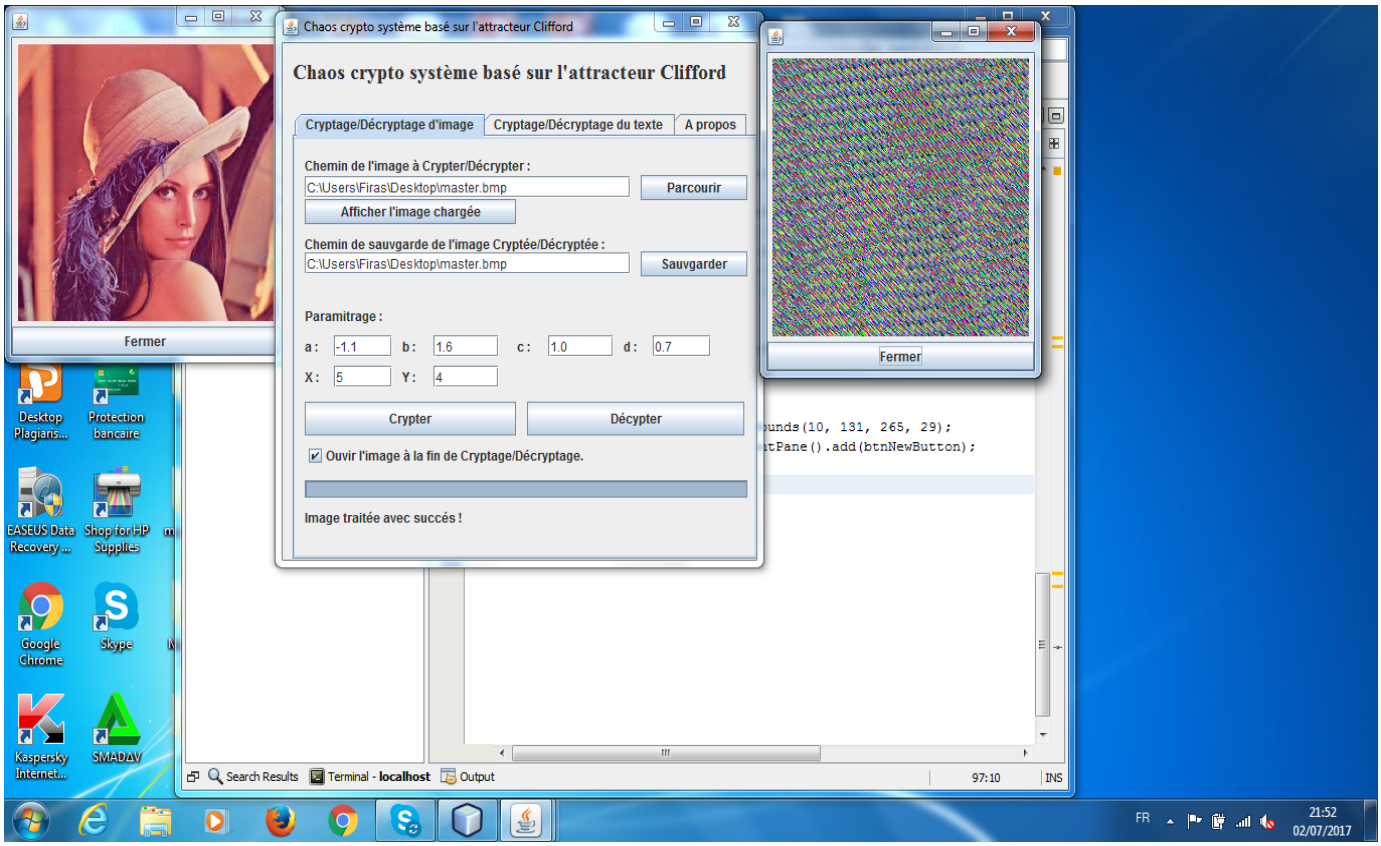


Figure III.7 décryptage avec modification des valeurs initiales

V.2.2 Cryptage/Décryptage du texte:

Le même principe utilisé pour crypter et décrypter une image sera utilisé pour crypter et décrypter un texte.

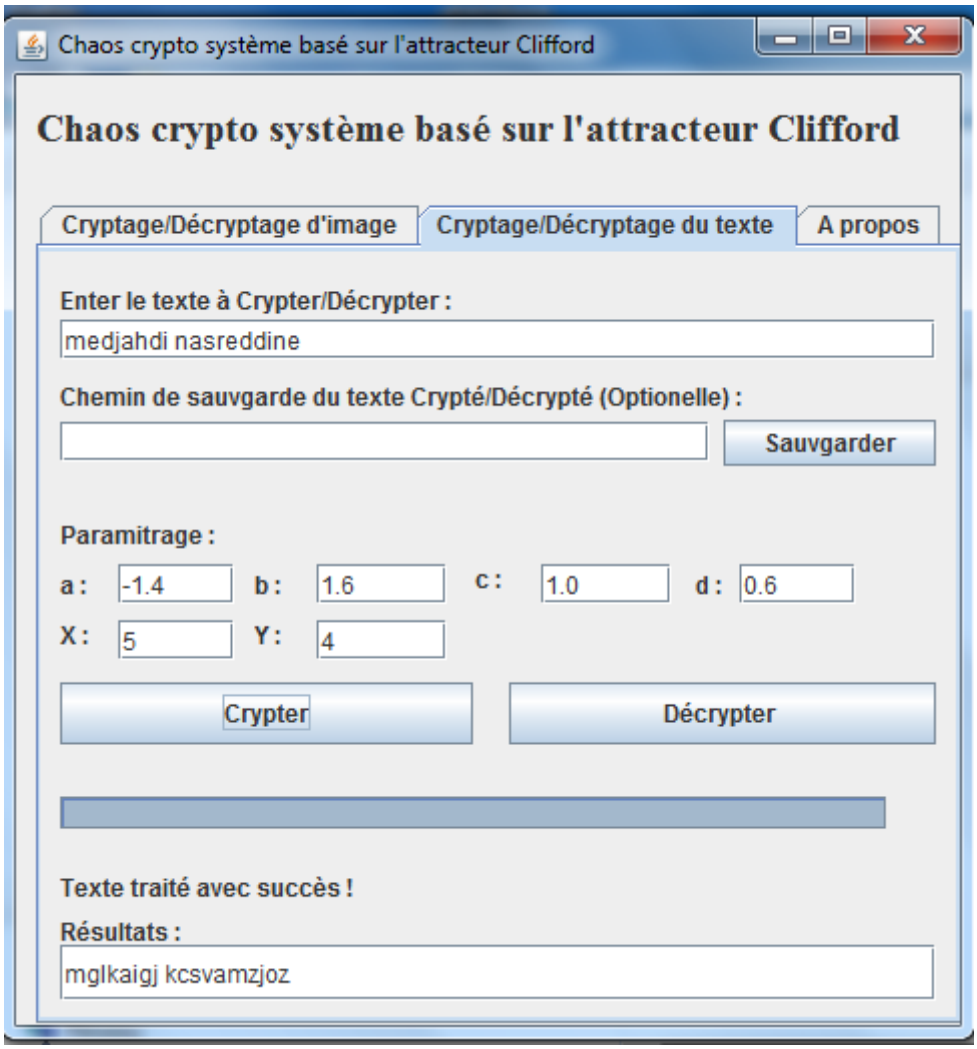


Figure III.8 : cryptage texte

Figure III.9 : décryptage texte

Méme principe que l'image quand nous avons changé l'un de des clés a,b,c ,d ou Xet Y le décryptage n'aboutit pas au résultat correct .

Dans l'exemple suivant on a remplacé a=-1.4 par a=.1.1. le résultat est incorrect

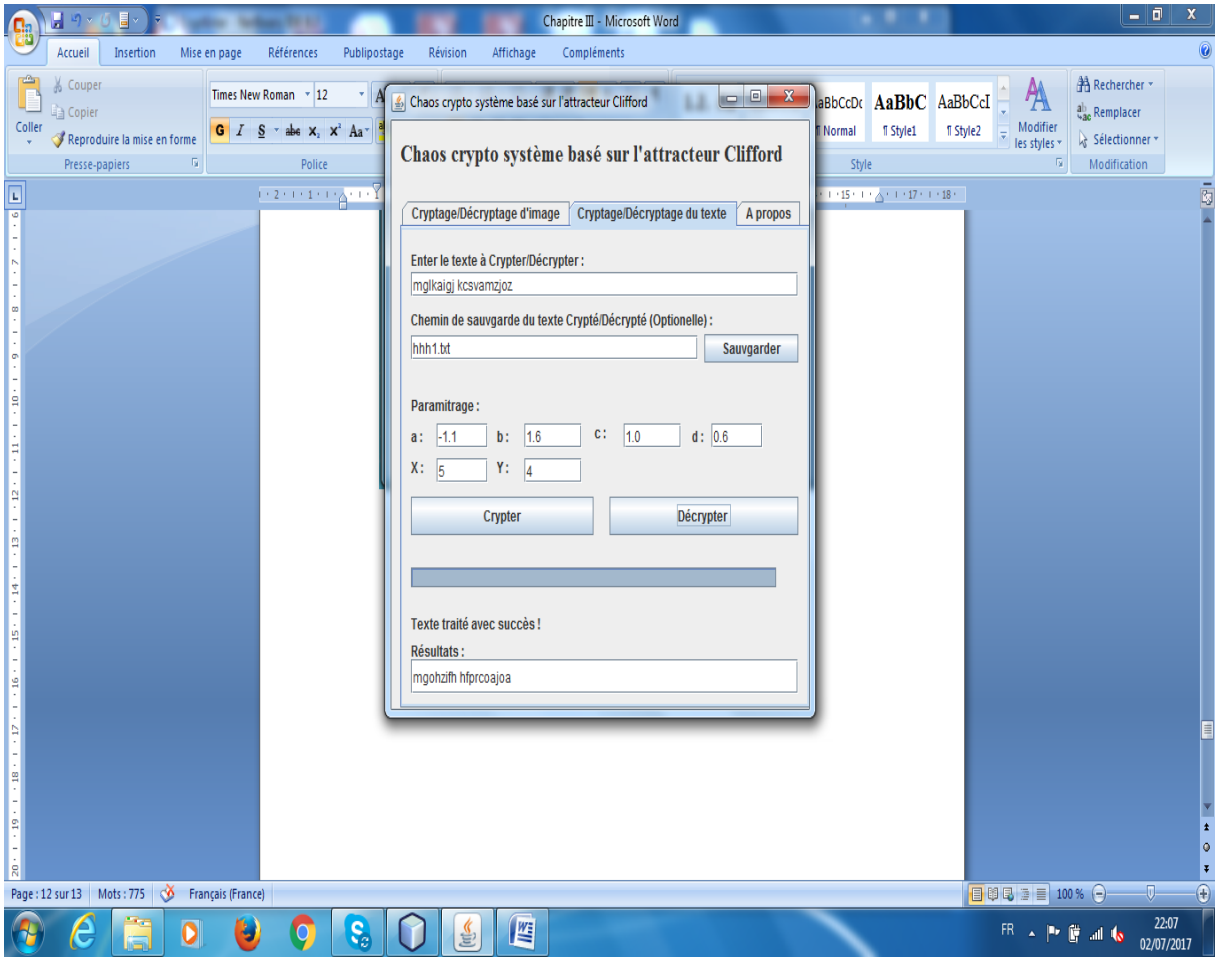


Figure III.10 : décryptage texte

Conclusion

Dans ce chapitre, nous avons présenté dans un premier lieu l’approche de cryptage et décryptage chaotique qui se base sur l’attracteur de Clifford. Ensuite en deuxième lieu, nous avons présenté notre application qui permet de crypter et décrypter des messages textes et images en se basant toujours sur l’attracteur de Clifford.

Conclusion générale

La sécurisation de l'information est aujourd'hui, essentiellement fondée sur des algorithmes de calcul dont la confidentialité dépend du nombre de bits nécessaires à la définition d'une clé cryptographique.

Différentes méthodes cryptographiques existent dans la littérature. On a des méthodes symétriques et d'autres asymétriques, ces deux méthodes sont généralement utilisées conjointement. Bien que cesméthodes ont fait leurs preuves, la puissance croissante des moyens de calcul menace leur confidentialité. Les ordinateurs puissants sont certes capables de crypter et de décrypter rapidement l'information, mais leur vitesse de calcul autorise parallèlement la cryptanalyse, qui a pour objectif de casser un code en découvrant la clé, par exemple en testant toutes les clés possibles.

Au début des années 90 la cryptographie chaotique a émergé. Cette dernière présente un niveau élevé de confidentialité et permet de crypter rapidement un flux important d'information. Le principe du cryptage par chaos consiste à ajouter au message à transmettre un signal chaotique. L'émetteur envoie à un récepteur ce signal chaotique où le message est noyé. Connaissant les caractéristiques du signal chaotique initial, le récepteur sait extraire le message du signal reçu.

Dans ce mémoire, on a développé un système de cryptage chaotique tout en se basant sur l'attracteur de Clifford.

TABLE DES MATIERES

Chapitre I : Généralité sur la cryptographie

Chapitre II : Introduction aux systems chaotiques

Chapitre III : Cryptage chaotique basé sur l'attracteur de clifford

Bibliographies

[1] : http://ram-0000.developpez.com/tutoriels/cryptographie/?page=page_2#L2 .< visité le :07/03/2017>

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

[3] :http://www.bart-konieczny.com/fr/blog/securite-des-applications-web/cryptage-symetrique-et-asymetrique.< visité le :07/03/2017>

[4] :http://www.mi.parisdescartes.fr/~mea/cours/Mi/crypto_synthese .< visité le :22/04/2017>

[5] N.Kouadri Moustefai, Test de validation pour les crypto-systèmes chaotiques, Mémoire de Magister a l'université de sciences et technologies mohamed boudief oran, soutenue en juin 2014.

[6] Hassan Noura. Thése doctoras .Conception et simulation des generateurs, crypto-systemes et fonctions dehachage bases chaos performants. Electronique. UNIVERSITE DE NANTES, 2012. Français.

[7] http://www.juliensalort.org.2016. < visité le :26/04/2017>

[8] A. Ali-pacha1, N. Hadj-Said1, . M'hamed2,A . belghoraf1, chaos crypto-système basé sur l'attracteur de Clifford, 5th international conférence Sciences of electronic, technologie of information and télécommunications ,March 22-26 2009 –Tunisie.

[9] Ghada Zaibi.Thése doctoras , sécurisation par dynamiques chaotiques des réseaux locaux sans _l au niveau de la couche mac. autre [cs.oh]. Universite toulouse le mirail - toulouse ii, 2012. francais.

[10] Nada Rebhi, Mohamed Amine Ben Farah, Abdennaceur Kachouri & Mounir Samet Analyse de sécurité d'une nouvelle méthode de cryptage chaotique, 4th international conference:sciences of electronic,technologies of information and télcommunications march 25-29, 2007 – Tunisia.

[11] Mohamed Zakarya Baba Ahmed , Anane mohamed , Fatima Z.Benmansour, Conception d'un crypto système pour les transmissions de données chiffrées, International Conférence on

Software Engineering and New Technologies ,Faculté de technologie, université Abou Bekr belkaid bp 230, chetouane, Tlemcen 13000, 14 November 2014 Algérie.

[12]: http://www.cryptage.org/applications-cryptographie.html. .< visité le :27/04/2017>

Et https://ar.wikipedia.org/wiki/theorie-chaos- .< visité le :02/05/2017>

LISTE DES FIGURES

LISTE DES TABLEAUX

LISTE DES EQUATIONS

Résumé

Dans le domaine des télécommunications, où les échanges d'informations multimédias se développent rapidement, il est indispensable de pouvoir disposer de systèmes sécurisés pour protéger les données à caractère personnel ou confidentiel et assurer la sécurité des données. La nécessité de protection des informations numériques devient alors obligatoire, en particulier pour les images et les textes d'ou le développement d'outil de protection efficace des données transférées et des communications contre les intrusions arbitraires. Le cryptage des données est très souvent le seul moyen efficace pour répondre à ces exigences. Dans ce contexte, nous avons utilisé des systèmes chaotiques qui sont des systèmes déterministes non linéaires et très sensibles aux conditions initiales et en utilise les attracteurs Clifford dans notre mémoire. Les aptitudes de notre approche pour la confusion, la sensibilité à l'image nette et à la clef ont été testées. Les résultats obtenus montrent l'efficacité de cette implémentation contre les attaques avancées.

Abstract

In the field of telecommunications, where the exchange of multimedia information is developing rapidly, it is essential to have secure systems to protect a personal or confidential data and ensure the security of data transfers. The need to protect digital information becomes compulsory especially for images and texts. It is therefore necessary to develop an effective protection tool of transferred data and communications against arbitrary intrusions. Data encryption is very often the only effective way to meet these requirements. In this context, We used chaotic systems that are nonlinear deterministic systems and are very sensitive to initial conditions and uses the Clifford attractors in our memory. The abilities of this proposed tool for the confusion, sensitivity to the sharp images and to the key were tested. The results show the effectiveness of this implementation against advanced attacks.

ملخص

في مجال الاتصالات، حيث تبادل المعلومات الوسائط المتعددة تنمو بسرعة، فمن الضروري أن يكون أنظمة آمنة لحماية الحاجة إلى حماية المعلومات الرقمية تصبح إلزامية، وخاصة بالنسبة .البيانات في شخصية أو سرية، وضمان أمن البيانات وتشفير البيانات .للصور، وبالتالي تطوير النصوص أداة الحماية الفعالة للبيانات والاتصالات ضد الاختراقات التعسفية نقلها وفي هذا السياق، استخدمنا أن الأنظمة الفوضوية هي أنظمة .وغالبا ما يكون الطريقة الفعالة الوحيدة لتلبية هذه الاحتياجات ، تم اختبار حساسية للصورة حادة .حتمية لاخطية وحساسة للغاية للشروط الأولية ويستخدم الجذابون كليفورد في ذاكرتنا .وأظهرت النتائج فعالية هذا التنفيذ ضد الهجمات المتقدمة .ومفتاح مهارات نهجنا إلى الارتباك