République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur Et de La Recherche Scientifique

Université de Ghardaïa

N° d'ordre :
N° de série :

Faculté des Sciences et Technologies
Département des Sciences et Technologie

Mémoire présenté en vue de l'obtention du diplôme de

MASTER

Domaine : *Sciences et Technologies*
Filière : Automatique
Spécialité : *Automatique et système*

Par : FENNICHE Khadidja

OULD MOHAMED Mohamed El-Kébir

Thème

Cryptage d'Image avec un Système Chaotique "Tent-Logistic 1D"

Soutenu publiquement le 20/06/2018

Devant le jury :

Benaouicha KARIM	M.A.A	Univ. Ghardaïa	**Président**
Ladjal BOUMEDIENNE	M.A.A	Univ. Ghardaïa	**Examinateur**
Biteur KADA	M.A.A	Univ. Ghardaïa	**Examinateur**
Mohamed ARIF	M.A.A	Univ. Ghardaïa	**Encadreur**

Année universitaire 2017/2018

DEDICACE

Je dédie ce modeste travail :

A Mes chers parents (Mohamed souleymane, fatimetou abdrabou) pour leur encouragement pendant toute la durée du stage, pour leurs sacrifices et leur réconfort moral.

A mes frères : hameda, raby, sidaty, brahim et maaini

A mes sœurs : minetou, mariem et momo

A mes cousins et Ainsi que tous les membres de ma famille.

Et à un personne que j'aime beaucoup « fatimetou sid ahmed aida»

Mes amis : med lemin, sidi elhadi, med moustafa, bekar amar, sidi med ejiwene, sidaty abdrabou.

Tous mes camarades de la section Automate

Et mon binôme fenich khadija

Et à Toutes les personnes qui m'ont apporté Aide et Assistance de près ou de loin.

kebir

Dédicace

Je dédie ce travail à

Toute ma famille mon père ma mère. Mes frères et mes sœurs et ces enfants.

Mes amis et toute la famille FENNICHE .

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, et l'encadreur Mr ARIF MOHAMED d'avoir dirigé cette mémoire ainsi que pour leurs efforts, leurs conseils et leurs encouragements. Je remercie les membres du jury 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.

Table des matières

Chapitre 03 : Cryptage chaotique

Chapitre 04 : Résultat et discussion

Liste Tableau

Liste de figure

Liste des abbréviation explicétées

Introduction générale

Introduction générale

La protection et la sécurité d'information est devenue 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 les pare-feux et la cryptographie. Cette dernière englobe plusieurs techniques et méthodes telles que la cryptographie à clé publique, la cryptographie à clé privée, la cryptographie quantique et la cryptographie basée sur chaos.

L'histoire de la cryptographie est déjà longue. 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 quatre chapitres, le premier chapitre parle sur la gestion de la sécurité des informations. Le deuxième chapitre est consacré à la présentation de la cryptographie symétrique et asymétrique. Le troisième chapitre aborde les systèmes chaotiques et Le dernier chapitre présent la méthode de chiffrement basé sur chaotique cascade.

Chapitre 01:
La sécurité de l’information

1. Introduction

L'information est aujourd'hui la sève de l'entreprise. C'est ce qui fait à la fois sa force et son existence. Fichiers, bases de données, méthodes de travail et de fabrication, fiches des salariés et informations industrielles sont autant d'informations qui composent la structure et la base d'une entreprise. Il s'agit là son capital intellectuel, ou plutôt capital informationnel. Toute perte d'information peut porter un coup fatal à une entreprise ou même à une nation.
Si ces informations venaient à être perdues, volées ou à tomber dans les mains d'une autre entreprise, la donnée n'aurait plus de raison d'exister car elle ne serait plus exclusive. L'information a aujourd'hui de la valeur de par son côté unique et exclusif pour une entreprise. Il est donc dans l'intérêt de l'entreprise de protéger son patrimoine informationnel. Nous allons essayer de déterminer et détailler ce qu'est la sécurité de l'information.

2. Outil de la sécurité de l'information

Il faut, pour définir la sécurité de l'information, étudier ses deux composants :

- **L'information :** qui peut être présentée quelque soit sa forme de stockage, de traitement ou de transmission. On peut ici parler d'un bout de papier, d'un échange oral, d'un classeur, d'une structure numérique couplée d'une méthode de transmission par les télécommunications …
- **La sécurité :** évaluée par différents critères définis qui permettent de qualifier la sûreté d'une information. [1]

3. Concept lies à la sécurité

S. Zevin définit la sécurité comme étant « la protection de l'information et des systèmes d'information contre tout accès et utilisation non autorisés, divulgation, perturbation, modification ou destruction » [2]. Selon C. Albert, « la sécurité revient à déterminer ce qui doit être protégé et pourquoi, ce qui a besoin d'être protégé et comment le protéger tant qu'il existe » [3]. Ces définitions nous montrent que la sécurité d'un système revient à la définition de ce système et à l'identification de la portée de la sécurité sur la totalité des composants formant le système.

La sécurité représente « la satisfaction des besoins de sécurité des biens essentiels » selon [1]. Les besoins de sécurité créent des ce qui suit, objectifs de sécurité à atteindre et conduisent à mettre en place des mesures pour améliorer la sécurité d'un système. Dans nous traitons les objectifs de sécurité, les mesures de sécurité et les stratégies de

développement de systèmes sécurisés.

3.1. Les objectifs de base de sécurité

- **La confidentialité**

La confidentialité est un objectif de sécurité permettant de protéger l'information au repos et lors de son échange contre toute divulgation et accès non autorisés. La confidentialité doit être assurée techniquement (mécanisme de chiffrement et de contrôle d'accès) et non techniquement (classification des informations et mise en place de politiques de contrôle d'accès) afin de ne donner l'accès qu'à ceux qui sont autorisés. Cet objectif peut porter sur la protection d'un message élémentaire ou d'un champ spécifique à l'intérieur d'un message en recourant à l'objectif support d'authentification et de contrôle d'accès.

Les informations peuvent avoir différents niveaux de confidentialité. Si certaines informations n'ont aucune exigence de confidentialité (information publique qui peut être accessible par tout le monde) d'autres informations doivent être plus étroitement contrôlées et partagées uniquement par les partenaires métier, voire pour les plus sensibles n'être accessible que par certaines personnes.

Un autre aspect de la confidentialité est la protection du flot de trafic contre l'analyse. Cela requiert qu'un attaquant ne puisse observer les sources et destinations, les fréquences ou autres caractéristiques du trafic sur un équipement de communication. [3]

- **La disponibilité**

L'objectif de la disponibilité est de garantir l'accès à un service, à une information ou à une ressource à tout moment pour les personnes autorisées. La disponibilité est assurée techniquement en assurant la protection des ressources et des biens (par exemple, les applications, les systèmes d'hébergement et les équipements réseau) et de s'assurer que ces biens fonctionnent correctement. Toutefois, il ne faut pas oublier que la disponibilité est aussi assurée en mettant en place des procédures et des politiques de sécurité. En effet, les dénis de service (indisponibilité du service) sont causés par les attaques malveillantes qui peuvent résulter de la non-application des politiques et des procédures de sécurité. [3]

- **L intégrité**

D'après l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), l'intégrité est la propriété assurant qu'une information ou un traitement n'a pas été

modifié ou détruit de façon non autorisée. Pour assurer l'intégrité de l'information en transit, on peut utiliser des mécanismes de signature électronique. L'intégrité de l'information au repos est assurée en utilisant des mécanismes de signature de cette information d'une part et en vérifiant par des mécanismes de détection d'intrusion que les systèmes hébergeant l'information fonctionnent d'une façon fiable d'autre part. [4]

3.2. Les objectif support de sécurité

Dans le Tableau 1-1, nous décrivons brièvement les objectifs de sécurité de support nécessaires à la mise des objectifs de sécurité de base. La confidentialité est assurée en mettant en place des mécanismes d'identification, d'authentification, d'autorisation et de chiffrement. L'intégrité est assurée par les mécanismes d'authentification, d'audit, de non-répudiation et de signature. La disponibilité est assurée en mettant en place des mécanismes de contrôle d'accès, d'audit, de redondance, de filtrage (pare-feu).etc.

Tableau 1-1 : Les objectifs de sécurité d'un support [3]

Objectif de sécurité	**Description**
Identification	Cet objectif permet d'attribuer des identifiants aux utilisateurs ou aux services. En particulier, la fédération d'identité permet à un utilisateur d'utiliser le même identifiant pour divers domaines de confiances. L'identification sert à l'audit et la traçabilité des activités
Authentification	Cet objectif permet de valider l'identifiant d'un utilisateur ou d'un service. Ceci est réalisé en présentant la preuve de possession de l'identité (soumission d'un mot de passe, d'une clé secrète,
Contrôle d'accès (Autorisation)	Cet objectif permet de contrôler l'accès à l'information et aux systèmes. Pour réaliser ce contrôle, chaque entité essayant d'obtenir un accès doit d'abord être authentifiée avant que les droits d'accès
Non-répudiation	Cet objectif empêche aussi bien l'expéditeur que le receveur de nier le fait d'avoir transmis ou reçu une information. Lorsqu'un message est envoyé, le récepteur peut prouver que le message a été bien envoyé par l'expéditeur. De même, lorsqu'un message est reçu, l'expéditeur peut
Audit	Cet objectif permet de contrôler le fonctionnement d'un système et de contrôler les mécanismes de sécurité et de conformité afin de détecter leurs défaillances et leurs corriger.

3.3. Les mesures de sécurité

Les mesures de sécurité représentent les différentes solutions de sécurité qui pourront être mises en place pour atteindre les objectifs de sécurité. L'ontologie de sécurité NRL-SO classifie les mesures de sécurité en trois types: les protocoles, les mécanismes et les politiques de sécurité. [5]

1- **Les protocoles de sécurité** : sont définis comme une série d'étapes permettant de réaliser une tâche bien définie. Ces protocoles peuvent être associés aux protocoles fonctionnels qu'ils supportent comme des protocoles de sécurité associés aux protocoles de routage (IPsec est associé à IP), de transport (SSL/TLS est associé à TCP), d'application (DNSsec associé à DNS). [6]
2- **Les mécanismes de sécurité** : représentent la mise en œuvre des protocoles. Nous pouvons trouver des mécanismes de sécurité réseaux (VPN), des mécanismes systèmes (Safehost), des mécanismes de services (Parefeu SOAP). [5]
3- **Les politiques de sécurité :** gouvernent les mécanismes et les protocoles en spécifiant les règles de sécurité à appliquer. Différents types de politiques de sécurité peuvent être définis:
   - ✓ Les politiques de sécurité métier sont définies par les responsables métier. Dans cette catégorie, on trouve par exemple les politiques spécifiant les droits d'accès à l'information.
   - ✓ Les politiques de sécurité applicative et architecturale sont définies par les architectes logiciels. Ces politiques sont utilisées dans la conception des applications. Par exemple, ces politiques intègrent la définition des rôles qui donnent des droits à l'invocation d'opérations dans une application.
   - ✓ Les politiques de sécurité opérationnelles sont définies par les administrateurs réseaux. Ces politiques sont utilisées dans la gestion de l'infrastructure technique comme par exemple la définition du nombre de tentatives de connexion sur un système informatique. [7]

Afin de choisir les meilleures mesures de sécurité à mettre en place, il faut faire une veille sur les mesures de sécurité existantes et choisir parmi ces mesures celles qui sont les plus adéquates au contexte métier et technologique de l'entreprise. Par exemple, les mesures de sécurité suivantes pourront être mises en place pour assurer la confidentialité des données :

- ✓ Des politiques spécifiant les doits d'accès aux données.
- ✓ Des mécanismes de chiffrement ou des mécanismes d'authentification et d'autorisation (Mandatory Access Control 'MAC' [8], Role Based Access Control 'RBAC' [9])
- ✓ Des protocoles de chiffrement tels que les protocoles SSL/TLS pour les données en transit. Assurer la confidentialité des données revient à choisir une ou plusieurs de ces instances, à les combiner en fonction des contextes métier et technologique de l'entreprise.

Dans ce qui suit, nous abordons les stratégies de développement de systèmes sécurisés. En particulier, nous mettons en évidence la notion de patron de sécurité. Un patron de sécurité représente des mesures de sécurité types à déployer pour répondre à un problème connu.

3.4. Les stratégies dans le développement de systèmes sécurisés

Sécuriser un système revient à prendre en compte la sécurité dès les premières phases de la conception. Le développement de systèmes sécurisés, qu'il s'agisse de systèmes d'informations, d'architectures à base de services ou d'applications monolithiques, peut être effectué en utilisant des méthodologies d'analyse des risques, des modèles de conception et des patrons de sécurité. Dans ce qui suit, nous présentons le concept des patrons de sécurité.

De manière générale, un patron constitue une base de savoir et de savoir-faire pour résoudre un problème récurrent dans un domaine particulier. La spécification de ces connaissances réutilisables

1) Permet d'identifier le problème à résoudre par capitalisation et organisation de connaissances d'expériences.
2) Propose une solution possible, correcte, générale et consensuelle pour y répondre
3) Offre les moyens d'adapter cette solution au contexte spécifique. [10]

A partir des spécifications d'un problème récurrent, les patrons permettent d'obtenir les informations et connaissances organisationnelles pour y faire face. Les patrons de sécurité aident les architectes et les développeurs à partager des connaissances sur la sécurité, à définir un nouveau paradigme de conception ou un style d'architecture, à identifier les risques qui ont été traditionnellement identifiés par prototypage ou par

expérience intégrant les visions métier et technologiques de la sécurité. [11]

Dans le Tableau 1-2, nous proposons des exemples de patrons de sécurité :

Tableau 1-2 : Exemples patterns de sécurité

Nom du patron	**Standards et**	**Description**
Communication sécurisée	HTTPS; SSL (TLS), IP sec	Ce patron de sécurité décrit l'utilisation d'une couche de transport sécurisée dans le cadre de la communication client-serveur ou serveur-
Log d'évènements de sécurité	JMX; Java API for Login	Ce patron de sécurité décrit la traçabilité des évènements de sécurité pour des raisons
Passerelle de sécurité SOA	Intégration de services de sécurité au sein d'un ESB	Pour centraliser la sécurité, des services de sécurité peuvent être connectés à un ESB. En utilisant ce patron, nous pouvons simplifier la propagation des identités, renforcer les

4. Gestion de la sécurité

La gestion de la sécurité est un processus permettant d'assurer la sécurité en intégrant les aspects organisationnels et technologiques. Ce processus permet d'identifier les biens à protéger et de développer des stratégies de protection contre les menaces éventuelles. L'objectif principal de la gestion de la sécurité est de cadrer les besoins de sécurité et de définir une stratégie globale afin d'assurer le niveau de sécurité requis sur l'information et les systèmes d'informations de l'entreprise. Dans le cadre de la gestion de la sécurité d'un système d'information, l'Agence Nationale de la Sécurité des Systèmes d'Information de France (ANSSI) a défini dans son référentiel général de la sécurité, six principes à la base de la gestion de la sécurité: [11]

1. Adapter une démarche globale

L'objectif est la cohérence d'ensemble de la démarche de sécurisation des systèmes d'information. Il convient à ce titre de n'oublier aucun élément pertinent, pour éviter toute faille qui réduirait la sécurité globale du système d'information.

2. Adapter la sécurité du système d'information selon les enjeux

Il est recommandé que la sécurité du système d'information soit adaptée aux enjeux du système et aux besoins de sécurité, afin d'y consacrer les moyens financiers et humains

juste nécessaires mais suffisants.

3. Gérer les risques

Il est obligatoire de suivre une démarche qui consiste à :

1) Identifier l'ensemble des risques pesant sur le système.

2) Fixer les objectifs de sécurité, pour répondre de manière proportionnée aux besoins de protection du système et des informations face aux risques identifiés.

3) En déduire les fonctions de sécurité et leur niveau de mise en œuvre pour atteindre ces objectifs.

4. Elaborer une politique de sécurité du système d'information(SSI)

Élaborer une stratégie globale de sécurité permet de définir le cadre d'utilisation du système d'information. Les politiques définissent entre autres les rôles et les responsabilités des différents acteurs, les règles d'utilisation des systèmes et de l'information, les règles permettant de contrôler l'accès sur l'information, les règles d'utilisation des données privées, les règles d'audit, de sauvegarde, etc.

5. Utiliser les produit et prestataires labellises pour leur sécurité

La certification de produits ou prestataires permet d'attester de la confiance que l'on peut accorder à des produits de sécurité et à la compétence des professionnels en matière de SSI.

6. Viser une amélioration continue

Il est recommandé de chercher une amélioration constante de la SSI, par exemple en mettant en place un « Système de Management de la Sécurité de l'Information » (SMSI) pour planifier les actions de sécurisation et les mettre en œuvre puis les vérifier et améliorer la SSI.

4.1. Les standard dans la gestion de sécurité

Le standard ITSEC dl 'Union Européenne

Proposé en 1991, le standard Information Technologie Security Evaluation Criteria de l'Union Européenne a été développé pour réaliser une synthèse entre les travaux de certification sécurité des différents états partenaires. [12]

Les besoins en termes de « cible de sécurité » (i.e. le niveau de certification visé) sont décrits selon 8 groupes de critères : identification et authentification, contrôle d'accès, imputabilité, réutilisation d'objets, fidélité, continuité de service, échange de données

(incluant l'authentification, le contrôle d'accès, la confidentialité des données, l'intégrité des données et la non-répudiation). Ces critères sont également regroupés en neuf familles selon le cycle de vie du projet permettant d'aboutir à un système d'information sécurisé: étude des besoins, conception de l'architecture, conception détaillée, mise en œuvre, configuration et contrôle, langages de programmation et compilateurs, sécurité pour les développeurs, documentation « opérationnelle », environnement opérationnel. Toutefois, si l'ITSEC vise une analyse globale du système support du système d'information, ce standard ne prend pas réellement en compte les aspects organisationnels. L'accent est placé sur les aspects conception, développement et contraintes de mise en œuvre de ressources informatique et non sur l'adaptation de l'organisation pour répondre aux contraintes de la politique de sécurité. De même, ce standard « oublie » les composants « sécurité » d'un réseau ou d'un système informatique. [13]

Les 'Common citerai'

Afin de certifier de manière unifiée dans un cadre international le niveau de sécurité atteint par les systèmes des partenaires dans un environnement distribué, le standard 'Common Criteria' (CC) définit à la fois des critères et une méthode d'évaluation. Ce standard repose sur deux concepts principaux :

- Le profil de protection (PP) représente l'ensemble des besoins et d'objectifs de sécurité pour une catégorie de produits ou systèmes.
- La cible de sécurité (Security Target : ST) décrit les objectifs de sécurité et les besoins associés à une 'cible d'évaluation'.

L'originalité de ce standard est qu'il repose sur un modèle de gestion des risques intégrant différents concepts (Figure 1-1). Le risque porte sur les biens (assets) et est identifié en croisant les menaces et les vulnérabilités. Un risque est réduit en mettant en place de contremesures permettant de réduire les vulnérabilités et donc leur possible exploitation par des menaces. Ce modèle met également en relief la responsabilité des propriétaires dans la définition de la valeur des biens et des contremesures, ce qui permet d'intégrer les contraintes organisationnelles dans la définition des objectifs de sécurité. La méthode développée pour l'évaluation permet de contrôler la conformité de la cible (ST) vis-à-vis d'un ou de plusieurs profils de sécurité (PP).

Toutefois, ce standard vise majoritairement la certification des composants et

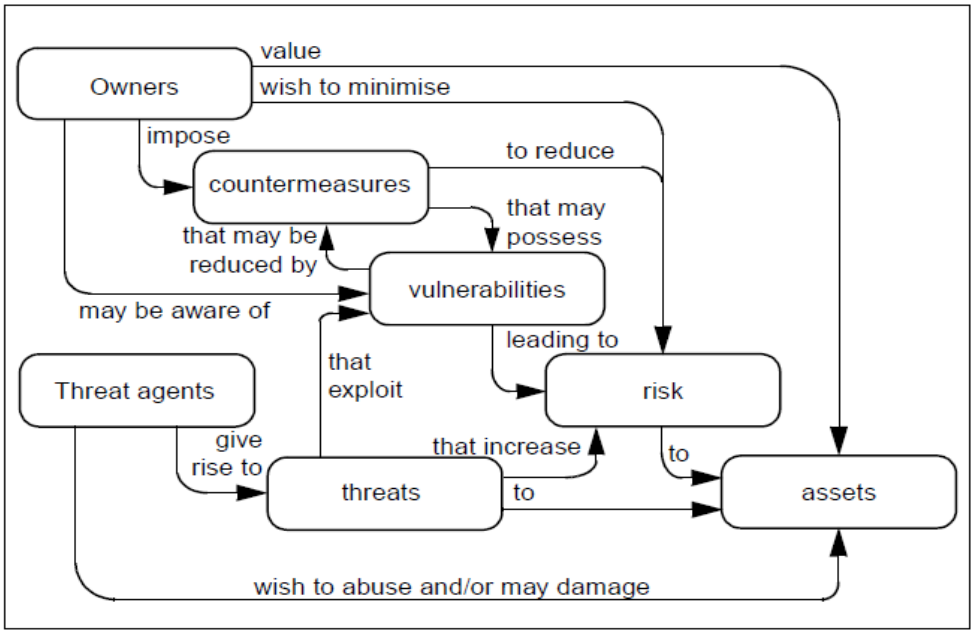


Figure 1.1 : Modèle de concepts de sécurité. [14]

Les standard de l' ISO

L'ISO et l'IEC (International Electrotechnique Commission) ont publié les standards ISO27001/ISO27002 (anciennement ISO 17799). Ces standards établissent les lignes directrices et les principes pour préparer, implémenter, maintenir et améliorer la gestion de la sécurité. A la différence des standards précédents, la sécurité est prise en compte aux niveaux organisationnel et technologique. [15]

Le Tableau 1-3 liste les fonctions offertes par ces standards:

Tableau 1-3 : Fonctions ISO 27001 / ISO 27002

ISO 27001	Gestion de la responsabilité
	Audit Interne
	Amélioration de l'ISMS (Information Security Management System)
ISO 27002	Elaboration d'une politique de sécurité
	Organisation de la sécurité des informations
	Gestion des biens et des actifs
	Sécurité physique et environnementale
	Communications et la gestion des opérations
	Contrôle d'accès
	Systèmes d'acquisition de l'information
	Développement et maintenance
	Gestion des incidents de sécurité des informations
	Gestion de la continuité
	Conformité

Les standards ISO27001/ISO27002 font partie d'une série de standards publiés par l'ISO sur la gestion de sécurité:

- ✓ Le standard ISO27004 fournit les directives pour l'évaluation d'un système de gestion de sécurité.
- ✓ Le standard ISO27005 fournit les directives pour la gestion des risques dans une entreprise.
- ✓ Le standard ISO27006 fournit les directives pour l'accréditation des organismes qui offrent la certification ISO.

Le cadre FISMA du NIST

Dans une même perspective, le NIST (National Institute of Standards and Technologie) a développé des standards pour l'implémentation de la gestion de la sécurité (FISMA : Federal Information Security Management Act). [16]

FISMA est un cadre de gestion qui fait référence à de nombreux documents élaborés par le NIST dans la sécurisation des systèmes d'information. L'objectif du cadre FISMA est la mise en œuvre d'un plan de gestion de la sécurité. Le Tableau 1-5 résume la portée de ce cadre :

Tableau 1-4 : Portée du cadre FISMA

Standards pour la catégorisation de l'information et des systèmes d'information
Standards des exigences de sécurité minimales pour l'information et les systèmes d'information
Directives pour la sélection des contrôles de sécurité appropriés aux systèmes d'information
Guide pour l'évaluation des contrôles de sécurité dans les systèmes d'information et de la détermination de l'efficacité du contrôle de sécurité
Directives pour la certification et l'accréditation des systèmes d'information

Parmi les documents auxquels FISMA fait référence, nous listons ci-dessous ceux qui sont au cœur de ce cadre :

✓ NIST 800-30 : Le guide de gestion des risques pour les systèmes d'informations.

✓ NIST 800-53 : Le guide des contrôles de sécurité dans les systèmes d'information.

✓ FIPS 199 (Federal Information Procession Standard 199): Standards pour la catégorisation de l'information et des systèmes d'information.

Bien que le cadre FISMA s'oriente vers les systèmes en développement et que les standards de l'ISO sont plus destinés aux systèmes en production, nous avons remarqué que ces deux cadres sont assez similaires dans la gestion de la sécurité :

✓ Les deux cadres se basent sur un processus de développement : ISO recommande le processus PDCA (Plan–Do–Check–Act), FISMA propose un cycle de développement plus classique (Initialisation, développement, acquisition/implémentation, opération et maintenance)

✓ Les deux cadres mettent la gestion des risques au cœur de leur démarche.

✓ Les deux cadres soulignent l'importance du support des responsables métier dans l'étude, l'implémentation et le suivi de la gestion de la sécurité.

Les cadres (ITSec/ISO/FISMA) font référence dans le domaine de la gestion de la sécurité et permettent de sensibiliser les responsables métier et technique à la gestion de la sécurité des systèmes d'information. Toutefois, aucun de ces cadres n'a été conçu pour la gestion de la sécurité dans un environnement de services distribués et dynamiques où la collaboration entre les différents partenaires est l'un des principaux objectifs. En effet, ces cadres ne correspondent pas au contexte de collaboration interentreprises et ne définissent pas une plateforme d'intégration des exigences de sécurité dans les modèles des processus métier. [17]

4.2. Les processus d'implémentation de la gestion de la sécurité

La gestion de la sécurité suppose de mettre en œuvre plusieurs études et processus de gestion des risques , de gouvernance de sécurité et d'organisation d'un plan de poursuite d'activité pour prendre en compte les besoins de sécurité, sur l'ensemble du cycle de vie du système d'information et des projets associés. [18]

La gouvernance de la sécurité

Le processus de gouvernance simplifie la gestion d'une stratégie de sécurité globale. Parmi les fonctions principales de la gouvernance, le processus de planification et la détermination des priorités dans l'utilisation des ressources de l'entreprise tient une place importante. Ce processus comprend l'établissement du budget, l'allocation des ressources, ainsi que le support des décisions prises dans le processus de gestion des risques. D'après la spécification 800-39 du NIST, le processus de gestion des risques inclut :

- ✓ L'alignement stratégique des décisions de gestion des risques avec la mission de l'entreprise et les objectifs organisationnels;
- ✓ La vérification de l'application du processus de gestion des risques et de l'attribution des ressources nécessaires à ce processus
- ✓ La vérification que l'exécution du processus de gestion des risques garantit les

objectifs métiers et organisationnels. [18]

Le plan pour suite d'activité

Le plan de poursuite d'activité a pour but de garantir la survie de l'entreprise, en préparant à l'avance la continuité des activités stratégiques. Plus précisément, le plan de poursuite d'activité intègre :

- ✓ Un plan de secours informatique qui garantit la reprise des systèmes désignés comme critique dans le temps minimum fixé.
- ✓ La reprise des données avec le minimum de perte.

Le processus de définition du plan de secours informatique suppose l'engagement de la direction de l'entreprise et utilise l'analyse de risques pour réaliser les activités suivantes :

- Analyse de l'impact de l'indisponibilité des activités sur les objectifs métiers de l'entreprise.
- Choix des stratégies de recouvrement en fonction des contextes métier et technologiques de l'entreprise.
- Mise en place d'un plan de rétablissement des activités et des stratégies de recouvrement suite à des scénarios de risques.
- Sensibilisations des acteurs afin qu'ils puissent agir dans des scénarios de risque.
- Vitrification du plan continuité d'activité

5. Conclusion

Dans ce premier chapitre, nous avons présenté les concepts liés à la sécurité. Nous avons noté que la sécurité est fortement dépendante des besoins et objectifs métiers et qu'il est crucial de bien identifier ces objectifs pour pouvoir mettre en place les mesures de sécurité les plus adaptées au contexte de l'entreprise.

En traitant les concepts de la gestion de la sécurité, nous avons trouvé qu'il est crucial d'élaborer une stratégie de sécurité globale du système. Par conséquent, nous nous sommes référés aux différents standards permettant la définition de cette stratégie (ITSec, standards de l'ISO et standards du NIST). Toutefois, aucun de ces standards ne répond aux exigences liées à la sécurité des environnements distribués et dynamiques tels que les environnements de services. Enfin, la gestion des risques est au cœur de l'implémentation du processus de gestion de la sécurité.

Chapitre 02:
La cryptographie

1. Introduction

La cryptographie est une science très ancienne. Des recherches indiquent qu'un scribe égyptien a employé des hiéroglyphes non conformes à la langue pour écrire un message.

De ce temps-là et au long de l'histoire, la cryptographie a été utilisée exclusivement à des fins militaires. Aujourd'hui, les réseaux informatiques exigent une phase de cryptographie comme mécanisme fondamental afin d'assurer la confidentialité de l'information numérique. Dans ce chapitre nous présentons les notions de base de la cryptographie.

2. Terminologie

- **Texte en clair** : c'est le message à protéger.
- **Texte chiffré** : c'est le résultat du chiffrement du texte en clair.
- **Chiffrement** : c'est la méthode ou l'algorithme utilisé pour transformer un texte en clair en texte chiffré.
- **Déchiffrement** c'est la méthode ou l'algorithme utilisé pour transformer un texte chiffré en texte en clair.
- **Clé** : c'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 quiconque 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'études 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 servit au chiffrement. Ce mot ne devrait donc être employé que dans le contexte de la cryptanalyse.
- **Crypter** : 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.
- **Codé, décodé** : c'est une méthode ou un algorithme permettant de modifier la mise en forme

d'un message sans introduire d'élément secret. [1]

3. Définition de la cryptographie

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

Le fait de coder un message de telle façon à le rendre secret s'appelle chiffrement. La méthode inverse, consistant à retrouver le message original, est appelée déchiffrement

Le chiffrement se fait généralement à l'aide d'une clef de chiffrement, le déchiffrement nécessite quant à lui une clef de déchiffrement. On distingue généralement deux types de clefs :

- ***Les clés symétriques*:** il s'agit de clés utilisées pour le chiffrement ainsi que pour le déchiffrement. On parle alors de chiffrement symétrique ou de chiffrement à clé secrète.
- ***Les clés asymétriques*:** il s'agit de clés utilisées dans le cas du chiffrement asymétrique (aussi appelé *chiffrement à clé publique*). Dans ce cas, une clé différente est utilisée pour le chiffrement et pour le déchiffrement [4]

Qu'entend-on par clef ?

On appelle clef une valeur utilisée dans un algorithme de cryptographie, afin de chiffrer une donnée. Il s'agit en fait d'un nombre complexe dont la taille se mesure en bits. On peut imaginer que la valeur correspondant à 1024 bits est absolument gigantesque. Plus la clef est grande, plus elle contribue à élever la sécurité à la solution. Toutefois, c'est la combinaison d'algorithme complexe et de clefs importantes qui seront la garantie d'une solution bien sécurisée. [3]

Les clefs doivent être stockées de manière sécurisée et de manière à ce que seul leur propriétaire soit en mesure de les atteindre et de les utiliser.

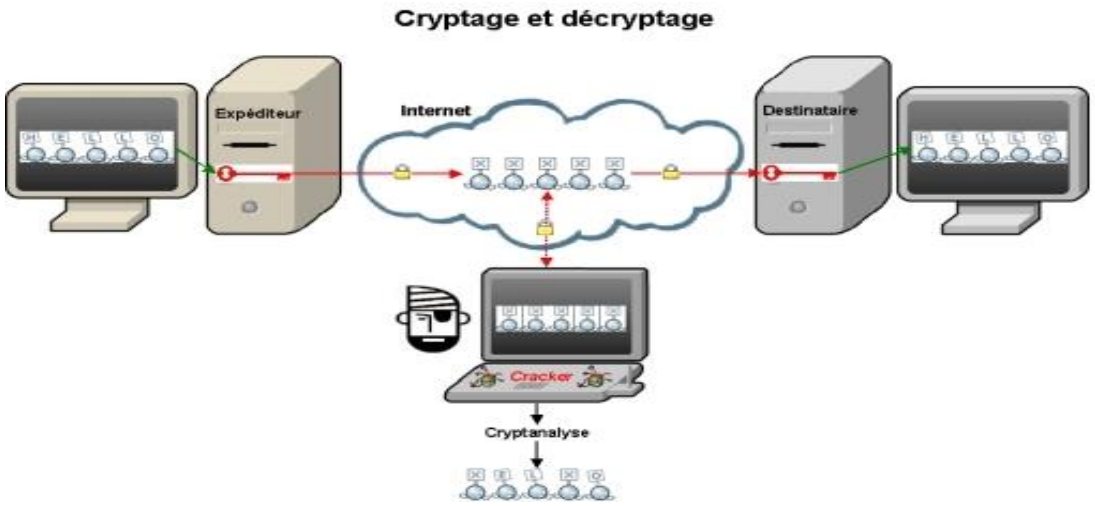


Figure 2.1 : Schéma de cryptographie[6]

4. But de cryptographie

cryptographie permet de résoudre quatre problèmes différents :

- **La confidentialité**. Le texte chiffré ne doit être lisible que par les destinataires légitimes. Il ne doit pas pouvoir être lu par un intrus.
- **L'authentification**. Le destinataire d'un message doit pouvoir s'assurer de son origine. Un intrus ne doit pas être capable de se faire passer pour quelqu'un d'autre.
- **L'intégrité.** Le destinataire d'un message doit pouvoir vérifier que celui-ci n'a pas été modifié en chemin. Un intrus ne doit pas être capable de faire passer un faux message pour légitime.
- **La non répudiation**. Un expéditeur ne doit pas pouvoir, par la suite, nier à tort avoir envoyé un message. [4]

5. Mécanisme de la cryptographie

Un algorithme de cryptographie ou un chiffrement est une fonction mathématique utilisée lors du processus de cryptage et de décryptage. Cet algorithme est associé à une clef (un mot, un nombre, ou une phrase). Afin de crypter une donnée avec des clés différentes le résultat du cryptage variera également. La sécurité des données cryptées repose entièrement sur deux

éléments : l'invulnérabilité de l'algorithme de cryptographie et la confidentialité de la clef.

Un système de cryptographie est constitué d'un algorithme de cryptographie, ainsi que de toutes les clefs et tous les protocoles nécessaires à son fonctionnement. [3]

6. cryptage Classiques

6.1. 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.

Tableau 2-1 substitution mono-alphabétique

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

Exemple:

Texte claire : «la cryptographie»

Texte Crypté : «iweqbgndtqwgkcy»

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

L'illustration la plus simple qui corresponde à ce principe est l'utilisation d'une fonction à base de ou exclusif (XOR).

6.2. 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.

6.3. Cryptage par produit: C'est la combinaison de chiffrement par substitution et chiffrement par transposition. La plupart des algorithmes à clés symétriques utilisent le chiffrement par produit. On dit qu'un « round » est complété lorsque les deux transformations ont été faites une fois (substitution et transposition). Ces successions des rondes portent également le nom de réseaux S-P de Shannon.[2]

7. Algorithmes de la cryptographie

7.1. Algorithmes symétriques (clef secrète)

Un algorithme symétrique est un algorithme qui permet de transformer un texte en clair en texte chiffré en utilisant une clé et de retransformer le texte chiffré en texte en clair en utilisant la même clé. Le secret de la communication est uniquement assuré par la clef qui est utilisée lors de la phase de chiffrement et de déchiffrement. L'algorithme utilisé ne fait pas partie du secret.

On parle d'algorithmes symétriques car c'est la même clef qui sert à la fois au chiffrement et au déchiffrement du message.

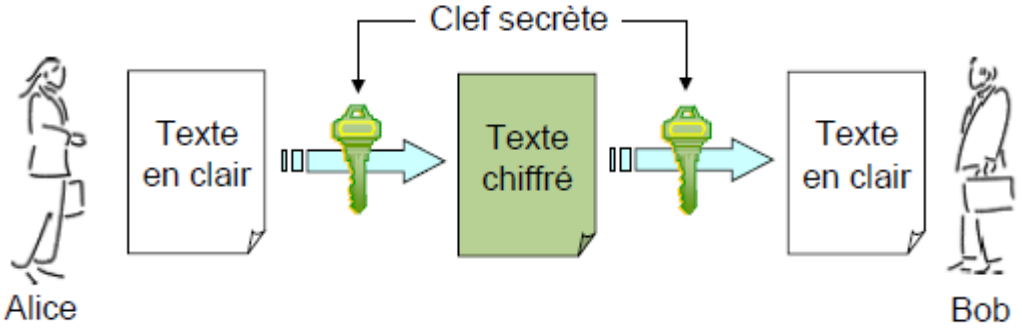


Figure 2.2 : Principe de l'algorithme symétrique[7]

Les algorithmes symétriques sont de deux types :

- *Les algorithmes de chiffrement en continu,* qui agissent sur le message en clair un bit à la fois.

- *Les algorithmes de chiffrement par bloc,* qui opèrent sur le message en clair par groupes de bits appelés bloc. [3]

Algorithmes de chiffrement en continu

Qui opèrent sur le message en clair un bit à la fois. Le principe consiste à générer un flux

pseudo aléatoire et de le combiner avec l'information bit à bit par l'opération XOR. A la réception, on applique le même mécanisme, et on restitue l'information.

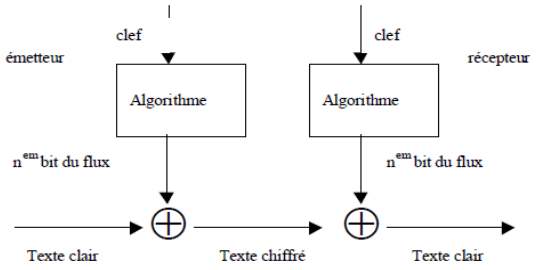


Figure 2.3: Chiffrement en continu

Algorithmes de chiffrement par bloc

Qui opèrent sur le message en clair par groupe de bit. La taille typique des blocs est 64 bits, ce qui est assez grand pour interdire l'analyse et assez petit pour être pratique

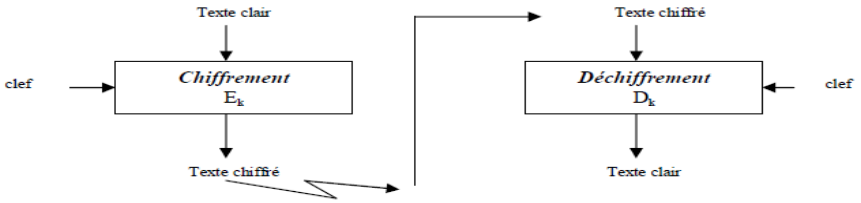


Figure 2.4: Chiffrement par bloc

Les algorithmes de chiffrement par blocs peuvent être utilisés suivant différents modes, dont les deux principaux sont le mode ECB (Electronique Code Boock) et le mode CBC (Chipher Block Chaining). [3]

1- *Le mode ECB (Electronique Code Book) :*

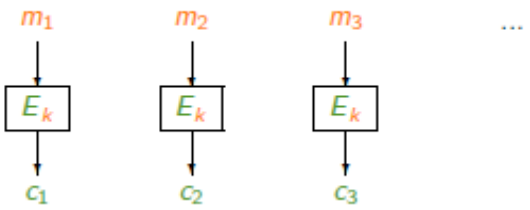


Figure 2.5: Le mode ECB

Chiffrement : Chaque bloque clair m_i est chiffré indépendamment et donne un bloc chiffré

$$c_i = E_k (m_i).$$

Déchiffrement : Chaque chiffré est déchiffré indépendamment pour donner le clair correspondant

$$m_i = D_k (c_i).$$

Avantage : Ce mode permet le chiffrement en parallèle des différents blocs composant un message.

Inconvénient : Même bloc de message en clair sera toujours chiffré en un même bloc de message chiffré. Or, dans le chiffrement sur un réseau par exemple, les données à chiffrer ont des structures régulières facilement repérables par un cryptanalyse, qui pourra donc obtenir beaucoup d'informations. D'autre part, un attaquant actif pourra facilement manipuler les messages chiffrés en retirant, répétant ou inter changeant des blocs. Un autre inconvénient qui s'applique au chiffrement par blocs en général, est l'amplification d'erreur : si un bit du message chiffré est modifié pendant le transfert, tout le bloc de message en clair correspondant sera faux.[5]

2 - Le mode CBC (Cipher Block Chaining) :

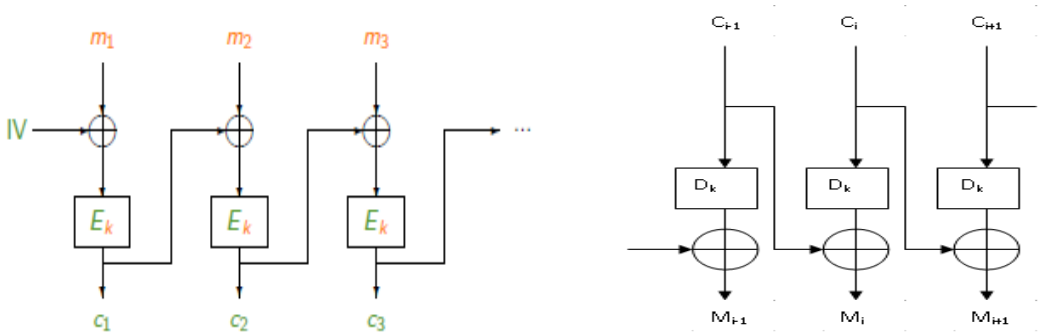


Figure 2.6 : Chiffrement et Déchiffrement CBC

Chiffrement : Un vecteur d'initialisation IV est généré aléatoirement

$C_i = E_k (M_i \oplus C_{i-1})$.

Le vecteur IV est transmis avec les blocs chiffrés.

Déchiffrement : $M_i = C_{i-1} \oplus D_k(C_i)$.

Avantage : La structure du message en clair est masquée par le chaînage. Un attaquant ne peut plus manipuler le cryptogramme, excepté en retirant des blocs au début ou à la fin. Un inconvénient est qu'il n'est plus possible de paralléliser le chiffrement des différents blocs (le déchiffrement reste parallélisable).

Inconvénient : On pourrait craindre que le chaînage de bloc n'entraîne une propagation d'erreur importante. De fait, une erreur d'un bit sur le message en clair affectera tous les blocs chiffrés suivants. Par contre, si un bit du message chiffré est modifié au cours du transfert, seul le bloc de message en clair correspondant et un bit du bloc de message en clair suivant seront endommagés : le mode CBC est dit auto réparateur. [5]

Exemple des algorithmes symétrique

Chiffrement par bloc

		DES	3DES	IDEA	RC4	RC5 et RC6	Blowfish	AES
Nom réel		Data Encryption Standard	Triple Data Encryption Standard	International Data Encryption Algorythm	Rivest Cipher 4	Rivest Cipher 5/6	Blowfish	Advanced Encryption Standard
Date		1973	1978	1992	1987	1994	1993	1998
Longueur	Clé	64 bits (56 effectifs)	192 bits (168 effectifs)	128 bits	jusqu'a 256 bits	entre 0 et 2040 bits	entre 40 et 448 bits	128, 192, 256 bits
	Bloc	64 bits	64 bits	64 bits	Flux	32, 64, 128 bits	64 bits	128 bits

7.2. Algorithme asymétriques (clef publique)

Les algorithmes symétriques vus sont tous fiables mais ils posent un problème, c'est celui de l'échange de la clé : comment transmettre de manière fiable à mon interlocuteur la clé de chiffrement utilisée pour déchiffrer le message que je lui envoie ? Il y a bien sûr le téléphone, mais il y a aussi les écoutes téléphoniques.

Les algorithmes asymétriques ont été inventés pour pallier précisément le problème de transmission sécurisée de la clef.

On parle d'algorithmes asymétriques car ce n'est pas la même clef qui sert au chiffrement et au déchiffrement. Dans le cas de ces algorithmes, on parlera alors de clé privée et de clé publique. Ces deux clés, clé privée et clé publique, sont intimement liées par une fonction mathématique complexe.

Les algorithmes asymétriques possèdent 2 modes de fonctionnement;

- Le mode chiffrement dans lequel l'émetteur chiffre un fichier avec la clé publique du destinataire pour chiffrer. Le destinataire utilise sa clé privée pour déchiffrer le fichier. Dans ce mode, l'émetteur est sûr que seul le destinataire peut déchiffrer le fichier.

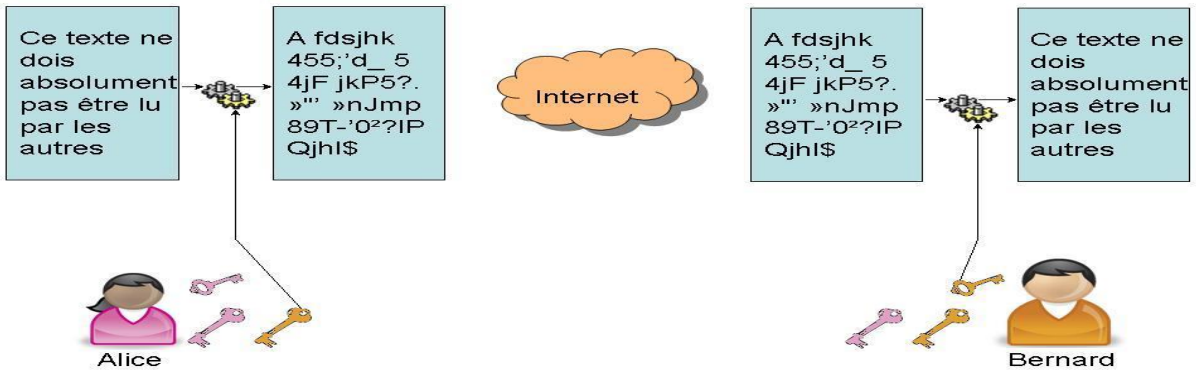


Figure 2.7: Chiffrement avec l'algorithme asymétrique[8]

- Le mode signature dans lequel l'émetteur signe un fichier avec sa propre clé privée. Le destinataire utilise la clé publique de l'émetteur pour vérifier la signature du fichier. Dans ce mode, le destinataire est sûr que c'est bien l'émetteur qui a envoyé le fichier.

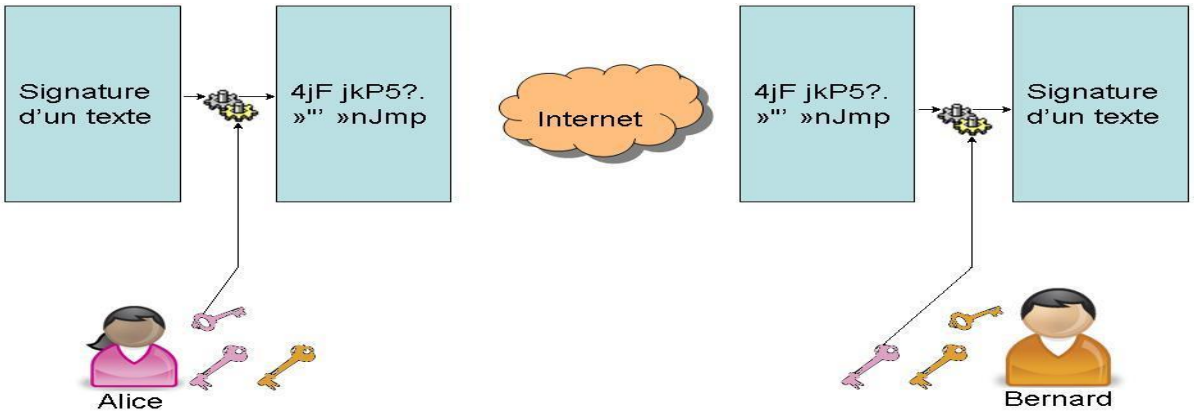


Figure 2.8: Signature avec l'algorithme asymétrique

Donc pour résumer :

- L'émetteur chiffre avec la clé publique du destinataire, le destinataire déchiffre avec sa clé privée.
- L'émetteur signe avec sa clé privée, le destinataire vérifie la signature avec la clé publique de l'émetteur. [3]

8. Conclusion

Dans ce chapitre, nous avons montré les inconvénients et les avantages de chaque type d'algorithme de chiffrement en plus nous avons cité les différents algorithmes de cryptage classiques et modernes. Dans le chapitre suivant, nous allons présenter les différentes méthodes de cryptage chaotiques.

Chapitre 03 :
Cryptage Chaotique

1. Introduction

Le terme chaos a été introduit avec sa signification actuelle en 1976 par Jim York, 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 ressuscitée en 1961 par le météorologue américain Edward Lorenz, professeur de mathématique au MIT (Massachusetts Institute of Technologie) 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.

2. Théorie chaotique

2.1. Rappel Historique

La notion de fonctions chaotiques apparaît au début du XXème siècle dans les travaux d'Henri Poincaré sur la physique des corps. Cependant, il faut attendre les années 60, avec l'apparition de l'ordinateur, pour que cette notion soit approfondie. En effet, il fallait réaliser un nombre immense d'opérations de calcul, ce qui n'était pas possible avant les années 60.

En 1963, le météorologue Edward Lorenz prouve le caractère chaotique des conditions météorologiques, un infime changement de l'état initial pouvant entraîner une évolution totalement différente (ce qui lui inspira le fameux postulat du battement d'aile de papillon). Avec cette découverte les travaux d'Henri Poincaré connurent un regain d'intérêt et en 1975 le mathématicien James York emploie pour la première fois le terme de « chaos ».

Plusieurs domaines d'applications variés utilisent les principes de la théorie du chaos pour étendre et mieux comprendre les phénomènes liés à ses applications. Nous citons: la psychologie, la sociologie, la biologie, la physique, l'économie, la sécurité de l'information, etc.

2.2. 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. [1, 2]

a) La non-linéarité

Un système chaotique est un système dynamique non linéaire. Un système linéaire ne peut pas être chaotique. La notion de système dynamique est relative à tous les systèmes dont l'évolution dépend du temps. 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. [1, 2]

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. [1, 2]

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 est ce fait, assez répandu. Quelques caractéristiques permettent de comprendre qualitativement les points marquants de ces systèmes. [1, 2]

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 différent 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 limitant 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 différent 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.

2.3. Cartes chaotiques

Parmi les nombreuses cartes chaotiques de la littérature, nous présentons très brièvement ci- dessous seulement les équations de quatre cartes chaotiques très utilisées en pratique qui sont : la carte d'ARNOLD la carte Logistique, la carte PWLCM (Piece Wise Linear Chaotic Map) et la carte Skewtent. Ces cartes possèdent plusieurs bonnes propriétés: réalisation simple, et généralement assez bonne propriété cryptographique.

2.3.1. La carte logistique

Une suit logistique est une suite simple, dont la récurrence n'est pas linéaire est donnée par la relation suivante : $x_{n+1} = r x_n (1 - x_n)$ (1)

x est la variable dynamique prenant des valeurs entre 0 et 1 non inclus et r est le paramètre du système. Selon la valeur de *r*, la suite peut être un point fixe, une suite *périodique* de période 2, 4, 8,..., et 64 pour *r* = 3,569692, ou une suite *chaotique* pour *r* compris entre 3,56996 et 4.

2.3.2. Carte PWLCM (Piece Wise Linear Chaotic Map)

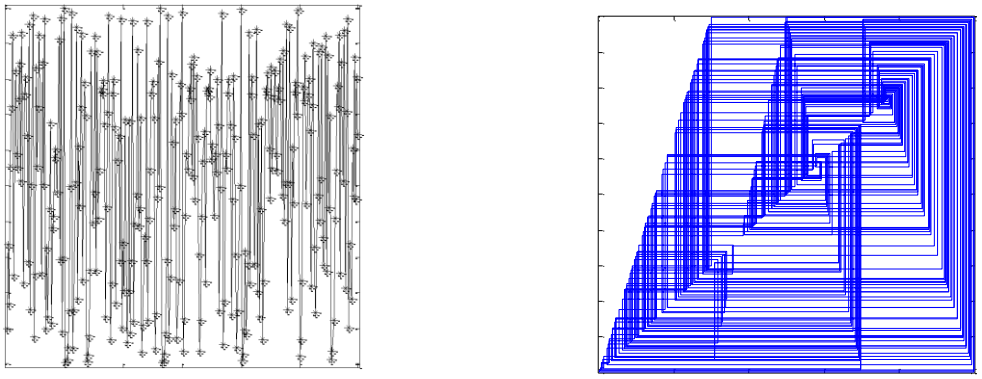
La carte chaotique **P**iece **W**ise **L**inear **C**haotic **M**ap (**PWLCM**) est composée de plusieurs segments linéaires par morceaux dont l'équation est donnée par :

$$x(n) = f[x(n-1), p]$$

$$x(n) = \begin{cases} x(n-1) \times \frac{1}{p} & si\ 0 \le x(n-1) < p \\ [x(n-1) - p] \times \frac{1}{0.5-p} & si\ p \le x(n-1) < 0.5 \\ F[1 - x(n-1)] & si\ 0.5 \le x(n-1) < 1 \end{cases} \quad (2)$$

$p \in [0, 0.5]$ est le paramètre de contrôle et $x(0) \in [0, 1[$ est la valeur initiale.

La figure 3. 1 (a) ci-dessous représente la forme temporelle de la fonction PWLCM pour 300 itérations, utilisant une valeur initiale $x(0)$ égale à 0.6, et une valeur de paramètre p est égale 0.3. La figure 3.1 (b), représente l'attracteur, courbe [x(n), x(n+1)] de la carte PWLCM (tracé pour 1000 itérations)



(a) **(b)**

Figure 3.1. : Carte PWLCM : (a) Séquence $x(n)$; (b) Attracteur

La carte PWLCM est caractérisée par :

1. une densité invariante et uniforme;
2. une réalisation simple du point de vue matériel et logiciel.

2.3.3. La carte d'ARNOLD

La carte chaotique appelée la carte d'ARNOLD en reconnaissance de mathématicien russe Vladimir I. Arnold, qui l'a découverte en utilisant une image d'un chat. C'est une démonstration et une illustration simple et élégante de certains des principes de chaos, une évolution apparemment aléatoire d'un système.

Si nous considérons $X=\begin{pmatrix} x \\ y \end{pmatrix}$, une matrice de taille n × n, la transformation d'Arnold T est :

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = T \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x+y \\ x+2y \end{pmatrix} \ mod\ n \qquad (3)$$

x' et y' est la nouvelle position du pixel, x et y est la position originale du pixel.

2.3.4. La carte Skew tent

La carte Skew tent est une carte linéaire par morceaux, décrite par l'équation suivante:

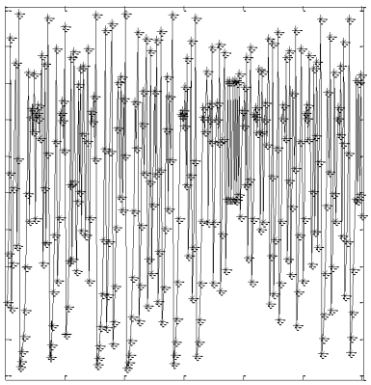
$$x(n) = f(x(n-1), p) = \begin{cases} \frac{x(n-1)}{p} & si\ 0 \le x(n-1) \le p \\ \frac{1-x(n-1)}{1-p} & si\ p \le x(n-1) \le 1 \end{cases} \quad (4)$$

Où $x(n) \in [\ 0,1\ [$, et p le paramètre de contrôle qui varie dans l'intervalle suivant :

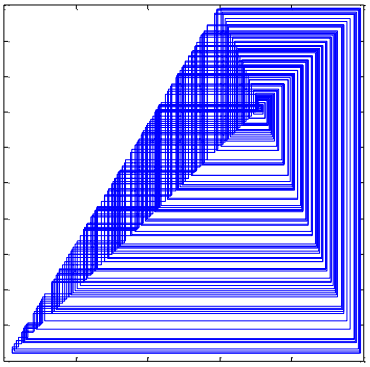
$$0 < P < 1$$

L'histogramme de cette carte est pratiquement uniforme comparé à celle de la carte Logistique. [3]

La figure 3.2 (a) représente la séquence temporelle x(n) générée par la carte Skew tent avec p égale à 0.6, et la figure 3.2 (b), représente son attracteur.



(a)



(b)

Figure 3 .2: La carte Skew tent, (a) Séquence x(n), (b) Attracteur

2.4. Intérêt et description de la technique de perturbation de l'orbite chaotique

En précision finie, pour un système de N bits de quantification, le nombre maximum de niveaux chaotiques différents est 2^N. Cette limitation de l'espace des valeurs (supposée infini pour le chaos analogique) entraîne des cycles périodiques des différentes orbites chaotiques, ayant chacune une longueur maximale forcement largement inférieure à 2^N (propriétés quasi chaotique), donc la dynamique des signaux chaotiques est dégradée.[4]

Par ailleurs, à chaque condition initiale, il existe une orbite chaotique formée généralement de deux parties : une branche transitoire de longueur l et un cycle de période c.

Notons aussi que le cas *l=0* ou *l=c* est possible. Lorsque *l=0*, l'orbite est un simple cycle de longueur *c*, et lorsque *c=1*, l'orbite chaotique converge vers un point fixe (voir figure 3.3 et figure 3.4).

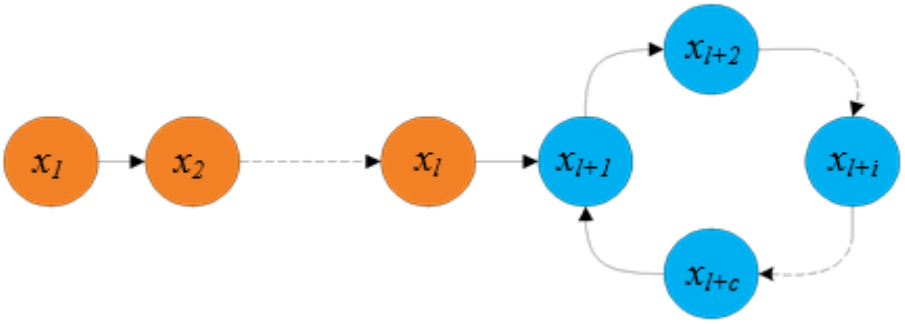


Figure 3.3 : Orbite chaotique de longueur *l+c*

La figure 3.4, montre un exemple explicatif, dans le cas N=4, de deux orbites chaotiques obtenues pour deux conditions initiales différentes.

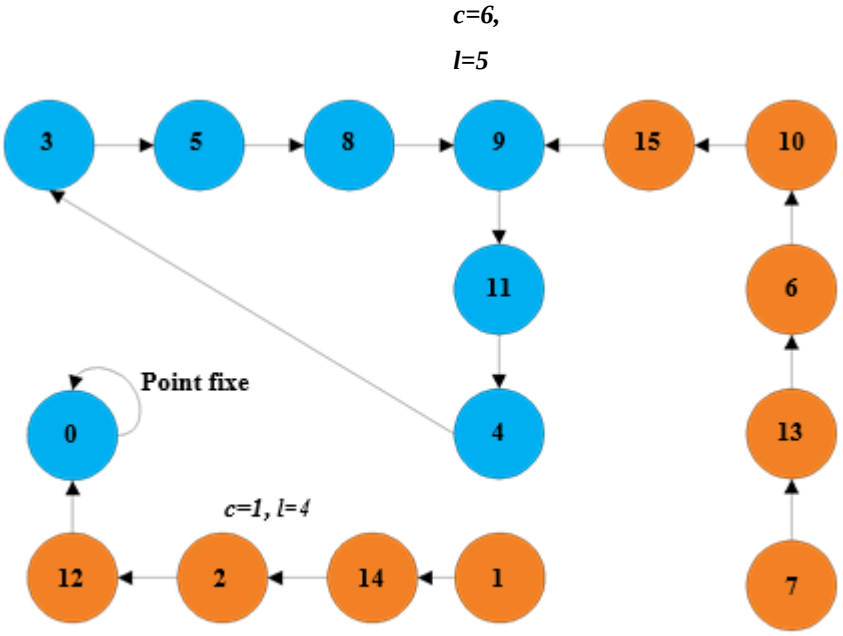


Figure 3.4 : Deux orbites chaotiques différentes pour deux conditions initiales différentes, avec *N=4*

Afin de contourner l'effet de la précision finie sur la dynamique chaotique, deux techniques sont utilisées : la technique de cascade et la technique de perturbation de l'orbite chaotique. La première technique permet effectivement une expansion de la longueur des cycles mais sans aucun contrôle. La seconde technique permet non seulement d'avoir un cycle de longueur très grande, mais aussi d'imposer une longueur minimale de cycle, dépendant directement du signal perturbateur.

La méthode de perturbation trouve son fondement sur le fait qu'aucun cycle stable n'existe pas, c.-à-d. si le système chaotique décrit, à un moment donné, un cycle donné, il peut, par application d'une perturbation, quitter ce cycle immédiatement pour aller vers un autre cycle. Le choix de la séquence perturbatrice est effectué selon les règles suivantes : elle devrait avoir une longue longueur de cycle contrôlable et une distribution uniforme; elle ne devrait pas dégrader les bonnes propriétés statistiques de la dynamique chaotique, donc l'amplitude du signal perturbateur doit être nettement plus petite que celle du signal chaotique, de sorte que le rapport R entre les deux amplitudes maximales, soit supérieur ou égal à 40 dB :

$$R = 20 \times \log\left[\frac{Amplitude\ maximal\ du\ signal\ chaotique}{Amplitude\ maximal\ du\ signal\ perturbateur}\right] \geq 40dB \qquad (4)$$

Un bon candidat pour la génération des séquences perturbatrices est le registre à décalage à réaction à longueur maximale. En effet, ce dernier est caractérisé par : une bonne fonction d'auto-corrélation, par une distribution presque uniforme, par un cycle de longueur maximale égale à $2^k - 1$ (k est le degré du polynôme primitif utilisé) et une implémentation logicielle ou matérielle facile.

Partons de l'équation du générateur de base :

$$X(n) = F[X(n-1)] \in 2^N - 1 \qquad n = 1,2.. \ (5)$$

où chaque valeur X(n) est représentée par N bits :

$$X(n) = x_{N-1}(n)x_{n-2}(n) \dots \ x_i(n) \ \dots x_0(n), \ x_i(n) \in A_b = [0,1], \ i = 0,1,2, \dots, N-1$$

Soit Δ le cycle minimal du générateur de séquences chaotiques sans perturbation. La perturbation est appliquée si n=m× Δ $m = 0,1,2, \dots$(c.à.d. pour $n=0$ et toutes les Δ itérations, donc est l'horloge du registre RDR). La séquence perturbée s'écrit selon l'équation suivante :

$$x_i = \begin{cases} F[x_i(n-1)] & k \le i \le N-1 \\ F[x_i(n-1) \oplus Q_i(n) & 0 \le i \le k-1 \end{cases} \quad (6)$$

où $F[x_i(n-1)]$ représente le i[éme] bit de $F[X(n-1)]$ et $Q_i(n)$ représente la séquence de perturbation (sortie du RDR) telle que :

$$Q_{k-1}^{+}(n) = Q_{k(n)} = g_0 Q_0(n) \oplus g_1 Q_1 \oplus \dots \oplus g_{k-1} Q_{k-1}(n), \text{ n = 0, 1, 2 ....} \quad (7)$$

avec :

$[g_0, g_1, \dots, g_{k-1}]$ sont les coefficients du polynôme primitif du registre et $[Q_0, Q_1, \dots, Q_{k-1}]$ Représente la valeur initiale non nulle du registre. Notons que la séquence perturbatrice est Appliquée sur les k bits de poids faibles de $F[X(n-1)]$.

si $n \neq m \times \Delta \quad m = 0,1,2,\dots$, la sortie du générateur de séquences chaotiques n'est pas Perturbée, donc :

$$X(n) = F[X(n-1)] \quad (8)$$

La période du système chaotique perturbé est donnée par :

$$L = \sigma \times \Delta \times (2^k - 1) \quad (9)$$

où σ est un entier positif. La période minimale est alors :[5]

$$L_{min} = \Delta \times (2^k - 1) \quad (10)$$

3. L'utilisation du chaos dans cryptographie informatique

Avec la découverte de la possibilité de synchronisation, des chercheurs ont étudié d'autres techniques de contrôle des systèmes chaotiques. Ils ont constaté qu'en utilisant des petites Perturbations on pouvait contrôler le chaos et diriger sa trajectoire dans un endroit souhaité de l'espace de phase. Ce fait a donné naissance à des techniques de cryptage ou de communication Sécurisée. En effet le transmetteur envoie des faibles perturbations pour diriger la trajectoire d'un système chaotique dans le récepteur vers des régions spécifiques de l'espace de phase qui correspondent à un élément de l'alphabet. Les perturbations sont générées de manière à diriger la trajectoire sur les régions correspondant aux lettres de notre message, décodé par le récepteur.

Jusque là nous avons seulement étudié le cryptage des signaux en temps réel dans le cadre d'un système de communication. Nous allons maintenant nous intéresser au cas des signaux représentant des données informatiques comme un texte, une image ou un fichier quelconque qui peuvent être stockés. Remarquons dans un premiers temps que tout ce que

l'on a vu pour les signaux analogiques peut être aussi appliqué à des signaux numériques. Par exemple, on pourrait considérer les octets d'un fichier comme un échantillonnage d'un signal temporel et on peut échantillonner le signal chaotique et appliquer les mêmes techniques de masquage ou modulation sur ces données. En plus la synchronisation ne poserait pas un problème car il suffit de poser les conditions initiales comme une clé secrète pour le décryptage. Mais dans le cadre de ce rapport nous allons étudier des algorithmes qui utilisent le chaos d'une manière plus intelligente.

Nous allons d'abord voir la méthode de Baptisât qui consiste à utiliser la trajectoire de la suite logistique dans son espace de phase qui est découpé en plusieurs régions correspondant à des éléments de l'alphabet. Puis nous allons voir une différente technique qui utilise l'attracteur de Lorenz pour crypter une image.[6]

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. [7]

Tableau 3-1: Correspondance entre la théorie du chaos et la cryptographie.

. **Théorie du chaos**	**Cryptographie**
Système chaotique	Système pseudo-aléatoire
Transformation non linéaire	Transformation nom linéaire
Nombre infini d'états	Nombre fini d états
Nombre d itération	Nombre fini d itérations
Etat initial	Plainte xt
Etat final	Ciphentext
Condition initial (s) et /ou paramètre(s)	Clé(s)
Indépendance asymptotique des états initiaux et finaux	Confusion
Sensibilité la condition initiale (s) et paramètre(s)	Diffusion

5. conclusion

Dans ce chapitre nous donnons une brève historique sur le développement de chaos, puis nous définissons le cryptage chaotique et donne différentes cartes de chaos et expliquons les différentes étapes mathématiques pour réaliser cette méthode. Dans le chapitre qui suit nous donnerons des applications de cette méthode sur des images à 2D et expliquons les résultats obtenus.

Chapitre 04 :
Résulta et discussion

1 Introduction

Un système dynamique est un concept en mathématiques où une règle fixe décrit la dépendance temporelle d'un point dans un espace géométrique [1]. Au cours des dernières décennies, les chercheurs ont augmenté leur attention aux systèmes dynamiques, en particulier aux cartes chaotiques qui sont dessystèmes dynamiques traditionnelles. Les cartes chaotiques ont des propriétés ergodiques et imprévisibles. Ils peuvent générer des séquences chaotiques totalement différentes utilisant des paramètres différents ou les valeurs initiales. Les cartes chaotiques sont des outils utiles dans les applications mathématiques, dans les sciences d'ordinateur et dans l'ingénierie. Surtout dans les applications de sécurité, les cartes chaotiques montrent d'excellentes performances en générateurs pseudo-aléatoire de nombres (PRNGs) [4,5], aux données et cryptage d'image [6 - 8].

De nombreuses cartes chaotiques ont été développées récemment [9, 10]. Ils peuvent être classés en deux catégories: 1-D et des cartes chaotiques de haute dimension (HD). Les cartes chaotiques 1-D sont des systèmes mathématiques qui simulent les évolutions d'une variable unique sur des pas discrets dans le temps. Exemple inclure la carte logistique, la carte de tente, la carte de Gauss et la transformationDyadique. [9]

Ces cartes chaotiques 1-D ont généralement simple structures et sont faciles à mettre en œuvre. Ils ont d'excellentes propriétés chaotiques et ont été utilisés pour différentes applications de sécurité [7]. Cependant, ils ont plusieurs faiblesses de sécurité:

1) leurs portées chaotiques sont limitées [8];

2) ils ont un petit nombre des paramètres;

3) leurs sorties sont faciles à prévoir avec faibles coûts de calcul [11] - [13].

D'autre part, les cartes chaotiques HD modélisent les évolutions d'au moins deux variables. Les exemples sont lacarte de Hénon [14], système de Lorenz [14], système de Chen et Lee [15] et systèmes hyper chaotiques [16]. Par rapport aux cartes chaotiques 1-D, Cartes HD chaotiques ont généralement une meilleure performance chaotique et leurs orbites chaotiques sont plus difficiles à prédire [17]. Cependant, Les cartes HD chaotiques ont des coûts de calcul élevés et sont difficiles à implémenter dans le matériel. Ces faiblesses limitent la performance dans certaines applications basées sur le chaos, en particulier dans les applications en temps réel. Pour surmonter la performance limitée des cartes chaotique 1-D et la difficulté de mise en œuvre des cartes HD chaotiques, nous avons proposé un Système Chaotique en Cascade (CCS) en tant que général Cadre chaotique 1-D. CCS relie deux cartes chaotiques 1-D (cartes de Semences) en série. Les graines de la sortie de la première

carteestliée auxgraines de l'entrée de la deuxième carte. La sortie de la seconde on est réinjecté dans l'entrée du premier pour les itérations récursives, et c'est aussi la sortie de CCS. Les simulations et l'analyse de sécurité sont fournies pour démontrer que le système de cryptage des données peut crypter différentes données avec un haut niveau de sécurité et surpasser plusieurs algorithmes de pointe. En résumé, nos principales contributions dans ce travail sont les suivantes:

1) Nous présentons le CCS qui est un cadre général chaotique avec une structure simple et efficace.

2) La performance chaotique de CCS est étudiée théoriquement et expérimentalement.

3) Nous proposons un PRNG basé sur le CCS.

4) Les propriétés aléatoires du PRNG proposé sont évaluées en utilisant deux normes d'essai.

5) Cryptage et performance de sécurité de la proposition système de chiffrement de données sont analysés.

2. Contexte

Cette partie passe brièvement en revue trois cartes chaotiques traditionnelles. Ils seront utilisés comme cartes de semences pour le CCS.

2.1.Carte logistique

La carte Logistique est une carte chaotique discrète 1D largement utilisée dans de nombreuses applications. Il a été prouvé avoir une bonne chaotique performance [18] et peut générer des séquences chaotiques avec gamme de [0, 1] en étirant et en retirant une initiale valeur d'entrée comprise entre [0, 1]. Mathématiquement, la carte Logistique est définie :

$$X_{n+1} = ax_n(1 - X_n)$$

où*a* est un paramètre avec une plage de [0, 4].

2.2. Carte des tentes

La carte tente est une autre carte chaotique discrète 1-D qui effectue les opérations d'étirement et de pliage. Quand sa contribution est inférieur à 0.5, il étire la sortie dans la plage de [0, 1]. Sinon, lorsque son entrée est supérieure ou égale à 0,5, La carte de tente plie sa valeur d'entrée dans la plage [0, 0.5] et puis l'étend dans la plage de [0, 1] pour générer sa sortie. Sa représentation mathématique est définie

$$x_{n+1} = \begin{cases} ux_n & si\ x_n < 0.5 \\ u(1 - x_n) & si\ x_n \geq 0.5 \end{cases}$$

où le paramètre *u* est dans la plage de [0, 2].

2.3. Carte Sine

La carte Sine est une autre carte chaotique couramment utilisée à des comportements chaotiques similaires à la carte logistique. Mais sa définition mathématique est totalement différente, comme indiqué

$$x_{n+1} = rsin(\pi x_n)$$

où le paramètre *r* est compris entre 0 et 1, x_n est l'itératif sorties / entrées avec une plage de [0, 1]. Lorsque $r \in [0.867, 1]$, la carte Sine a des comportements chaotiques.

3. CCS

Motivé par des structures en cascade dans les circuits électroniques, cette section propose un CCS. Il peut générer de nouvelles cartes 1-D chaotiques en utilisant une combinaison de deux cartes chaotiques 1-D existantes.

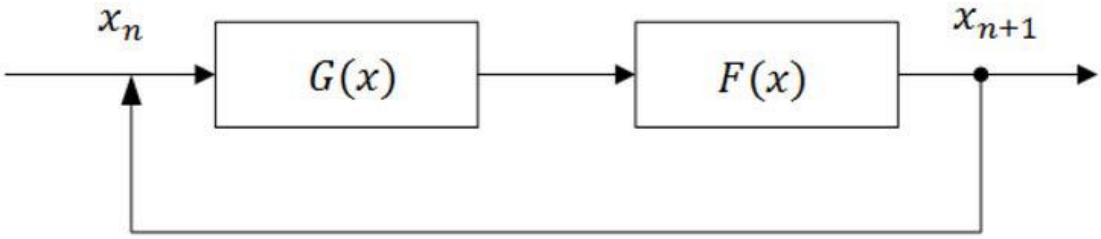


Figure1 : Structure de CCS

3.1. CCS

La figure 1 montre la structure de CCS, où G (x) et F (x) sont deux cartes de semences. CCS relie deux cartes de semences en série. La sortie de G (x) est introduite dans l'entrée de F(x), et celle la sortie de F(x) est ensuite réinjectée dans l'entrée de G(x) pour itérations récursif.

Mathématiquement, le CCS proposé est défini dans le suivant, où G(x) et F(x) sont deux cartes de graines

$$x_{n+1} = \Gamma(x_n) = F\big(G(x_n)\big).$$

Toute carte chaotique 1-D existante peut être utilisée comme carte de semis de CCS. Les utilisateurs ont la possibilité de définir des cartes de graines F(x) et G(x) comme des cartes chaotiques identiques ou différentes.

1) Quand F(x) et G(x) sont les mêmes cartes chaotiques 1-D, à savoir F(x) = G(x), CCS change pour :

$$x_{n+1} = F(F(x_n)) \text{Ou} x_{n+1} = G(G(x_n))$$

CCS devient une structure qu'une carte chaotique 1-D est en cascade avec lui-même. Par exemple, lorsque F(x) et G(x) sont deux cartes Sine, CCS est un carte Double-Sine.

2) Lorsque F(x) et G(x) sont sélectionnés comme cartes chaotiques différents, à savoir F(x) ≠ G(x), CCS devientune autre Structure chaotique 1-D définie par :

$$x_{n+1} = G(F(x_n))$$

Modification des paramètres de F(x) et G(x) ou même l'ordre de deux cartes de semences, CCS donne unecarte chaotique 1-D différente. Par exemple, la Tente-Logistique et Logistique-Tente les cartes sont complètement différentes.

CCS offre aux utilisateurs une grande flexibilité pour générer un grand nombre de NCM utilisant différents paramètres de F(x) et G(x). Par rapport à leurs cartes de graines correspondantes, des cartes chaotiques généré par CCS sont complètement différentes, et ont plus paramètres et comportements chaotiques plus complexes.

De plus, la structure de CCS de la Figure 1 peut être davantage étendue en trois ou plus de trois cartes de graines en cascade. Ça offre aux utilisateurs encore plus de flexibilité dans la sélection des cartes de semences. Les cartes chaotiques résultant ont beaucoup plus compliqué et chaotique comportements et plus de paramètres, et donc ils peuvent avoir de meilleures performances chaotiques et générer plus aléatoire et des séquences de sortie imprévisibles. D'autre part, cependant, en cascade plus de cartes de semences peut entraîner de nombreux côtés effets, y compris retard important, difficulté matérielle mise en œuvre, et la complexité de l'analyse de la performance.

3.2. Analyse de comportement chaotique

Reliant deux cartes chaotiques G(x) et F(x) en série, les séquences de sortie de CCS ont la structure de G(x), F(x), outous les deux. CSS contient tous les paramètresde ses cartes de graines. Ainsi, il a plus de paramètres et propriétés complexes que ses cartes de semences.Parce que CCS est un cadre généralisé de systèmes chaotiques,en utilisant différentes cartes chaotiques comme ses cartes de graines, ou mêmechanger l'ordre de ses cartes de semences, CCS donne des résultats totalement différentsdes cartes chaotiques. Analyser ou prouver directement le chaotique, la performance de CCS devient extrêmement difficile.

Supposons x_0 et y_0 sont deux valeurs initiales extrêmement proches deCCS. Après la première itération, la différence | x1 -y1 | estDéfini par

$$|X_1 - Y_1| = |\Gamma(X_0) - \Gamma(\mathrm{Y}_0)| = \frac{\left|F\left(G(x_0)\right) - F\left(G(y_0)\right)|G(x_0 - G(y_0)|\right|}{|G(x_0 - G(y_0)||x_0 - y_0|}|x_0 - y_0|$$

Pour $x_0 \to y_0\ ona G(x_0) \to G(y_0)$;alors

$$\left|\frac{dF}{dx}|G(x_0)\right| \approx \lim_{G(x_0)\to G(y_0)} \frac{\left|F\left(G(x_0)\right) - F(G(y_0))\right|}{|G(x_0) - G(y_0)|}$$

$$\left|\frac{dG}{dx}|x_0\right| \approx \lim_{x_0\to y_0} \frac{|G(x_0) - G(y_0)|}{|x_0 - y_0|}$$

Donc

$$|x_1 - y_1| \approx \left|\frac{dF}{dx}|G(x_0)\right| \left|\frac{dG}{dx}|x_0\right| |x_0 - y_0| .$$

$$|x_1 - y_1| = |\Gamma(x_0) - \Gamma(y_0)|$$

$$= \frac{\left|F\left(G(x_1)\right) - F\left(G(y_1)\right)\right||G(x_1) - G(y_1)|}{|G(x_1) - G(y_1)||x_1 - y_1|}|x_1 - y_1|$$

$$\approx \left|\frac{dF}{dx}|G(x_1)\right| \left|\frac{dG}{dx}|x_1\right| \left|\frac{dF}{dx}|G(x_0)\right| \left|\frac{dG}{dx}|x_0\right| |x_0 - y_0| .$$

$$|x_n - y_n| = |\Gamma(x_{n-1}) - \Gamma(y_{n-1})|$$

$$\approx \left|\prod_{i=0}^{n-1} \frac{dF}{dx}|G(x_i)\right| \left|\prod_{i=0}^{n-1} \frac{dG}{dx}|x_i\right| |x_0 - y_0|$$

$$\Delta\Gamma(x) \approx \left\{\left|\prod_{i=0}^{n-1} \frac{dF}{dx}|G(x_i)\right| \left|\prod_{i=0}^{n-1} \frac{dG}{dx}|x_i\right|\right\}^{\frac{1}{n}}$$

$$= \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln \left|\frac{dF}{dx}|G(x_i)\right| + \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln \left|\frac{dG}{dx}|x_i\right|$$

$$\lambda_{F(x)} = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln \left|\frac{dF}{dx}|x_i\right|$$

$$\lambda_{G(x)} = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln \left|\frac{dG}{dx}|x_i\right|$$

$$\lambda_{\Gamma(x)} = \lambda_{F(x)} + \lambda_{G(x)}.$$

Par conséquent, LE de CCS est une combinaison des valeurs LEde ses deux cartes de semences. Lorsque λ (x)> 0, les trajectoires des deux séquences de sortie de CCS divergent considérablement comme le nombredes itérations augmente, et CCS devient chaotique.

La plus grandevaleur LE positive signifie la divergence plus rapide de deux trajectoires,résultant en une meilleure performance chaotique. Les comportements chaotiquesde CCS sont résumés comme suit.

1) Quand $\lambda_{F(x)} > 0$et $\lambda_{G(x)} > 0$, $\lambda_{\Gamma(x)} > 0$, $\lambda_{\Gamma(x)} > \lambda_{F(x)}$et $\lambda_{\Gamma(x)} > \lambda_{G(x)}$Lorsque les deux cartes de graines sont chaotiques,CCS est chaotique et a une meilleure performance chaotique que ses cartes de graines.

2) Lorsque $\lambda_{G(x)} \leq 0$, $\lambda_{F(x)} \leq 0$et$\lambda_{\Gamma(x)} \leq 0$, CCS ne fait pas avoir de comportement chaotique quand aucune carte de graines n'est chaotique.

3) Lorsque $\lambda_{G(x)} > 0$ et $\lambda_{F(x)} \leq 0$, ou $\lambda_{F(x)} > 0$et $\lambda_{G(x)} \leq 0$, nous avons :

$$\lambda_{\Gamma(x)} \begin{cases} > 0 \ si \lambda_{F(x)} + \lambda_{G(x)} > 0 \\ \leq 0 \ si \lambda_{F(x)} + \lambda_{G(x)} \leq 0 \end{cases}$$

Lorsqu'il n'y a qu'une seule carte de semences qui est chaotique, CCSsera chaotique si et seulement si λF(x) + λG(x)> 0.En général, le CSC est chaotique quand il y a au moins une carte de graine dans la gamme chaotique. Il a une meilleure performance chaotiquelorsque les deux cartes de graines sont chaotiques.

4. PRNG PROPOSÉE

Parce que les cartes chaotiques ont des propriétés d'ergodicité, d'imprévisibilité, et sensibilité aux valeurs initiales des paramètres, ils sont des candidats idéaux pour concevoir un PRNG. La performance chaotique des cartes chaotiques détermine le caractère aléatoire performance des PRNG. Les cartes chaotiques générées par CCS montrent mieux performances chaotique que les cartes de semences existantes, et donc ils sont plus adaptés aux PRNG.

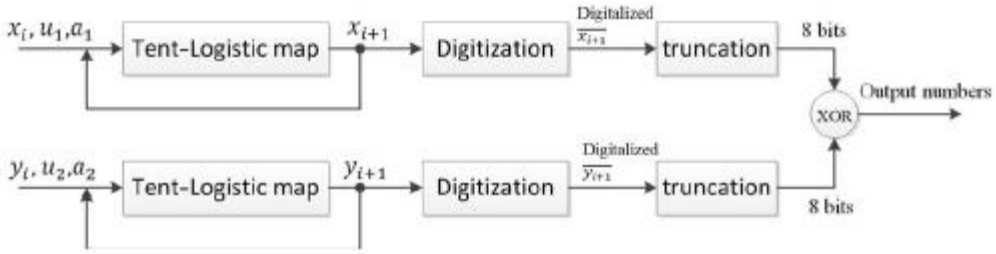


Figure 2 : Structure de TLPRNG.

Cette section utilise la carte Tente-Logistique comme exemple de NCM générés par CCS pour concevoir un nouveau PRNG, puis analyse sa propriété aléatoire.

Le PRNG proposé s'appelle Tent-Logisticmap-based PRNG (TLPRNG). Son schéma fonctionnel est illustré à la Figure 2 Supposons que $\{x_i$, i = 1, 2,. . . , N$\}$ et $\{y_i$, i = 1, 2,. . . , N$\}$ sont deux séquences chaotiques générées par la carte Tent-Logistic avec différentes valeurs initiales et paramètres, TLPRNG est défini

$$TLPNG(i) = X(i) \oplus Y(i)$$

où$\oplus$ est l'opération XOR, X(i) et Y(i) sont binaires 8 bits nombres définis par

$$X(i) = T\lceil \bar{x_i} \rfloor k_1 : (k_1 + 7)$$

$$Y(i) = T\lceil \bar{y_i} \rfloor k_2 : (k_2 + 7)$$

où$T[m]_{k_1:(k_1+7)}$est une fonction pour tronquer le bit binaire m flux de l'emplacement de bit k1 à l'emplacement (k1 + 7). xi et yi sont des flux binaires de 52 bits convertis par les sorties xi et yi. [25]

k1 et k2 sont deux entiers Défini par

$$k_1 = (x_i \times 10^{10} mod\ 6) + 39$$

$$k_2 = (y_i \times 10^{10} mod\ 6) + 39$$

Dans chaque itération, la séquence binaire de 8 bits est générée parTLPRNG. Dans TLPRNG, nous utilisons deux sorties de la Tente-Logistique carte avec différentes valeurs initiales et paramètres pour générer nombres pseudo-aléatoires. Comme on peut le voir sur la figure 2, en utilisant deux sorties de différentes orbites chaotiques pour générer numéros pseudo-aléatoires peuvent assurer que TLPRNG est capable degénérer des nombres pseudo-aléatoires avec des tailles suffisamment grandes et un excellent caractère aléatoire.

5. SYSTÈME DE CRYPTAGE DE DONNÉES PROPOSÉ

Comme une simple technologie de sécurité des données, le cryptage des données attire des attentions croissantes. Il transforme les données en un format de données sans signification. Au cours des dernières décennies, de nombreuses données technologies de cryptage ont été développés. Les exemples comprennent la norme de cryptage numérique (DES), cryptage avancé standard (AES), cryptage de données en réseau [30], et beaucoup autres algorithmes de chiffrement [7], [31]. En raison des propriétés de sensibilité aux paramètres et valeurs initiales, ergodicité, et l'imprévisibilité, les cartes chaotiques sont de bons outils pour le cryptage des données. Les cartes chaotiques avec d'excellents comportements chaotiques Avoir des avantages de sécurité pour le cryptage des données.

Parce que le système CCS a une bonne performance chaotique, il est adapté pour chiffrement de données.

Dans ce travail, en simulant la carte Tente-Logistique comme exemple de CCS, nous présentons une nouvelle carte basée sur la carte Tent-Logistic algorithme de chiffrement de données (TL-DEA). Beaucoup de DEA existants sont conçus pour crypter les données dans le format binaire tels que DES et AES. Les données avec d'autres formats devraient être transformées dans le format binaire avant le cryptage. Ceci peut être inefficace pour certaines données avec une grande taille telle que haute résolution d'images / vidéos. Mais TL-DEA peut directement crypter différents types de données. Les simulations et l'analyse de sécurité sont fournies pour démontrer ses performances de chiffrement.

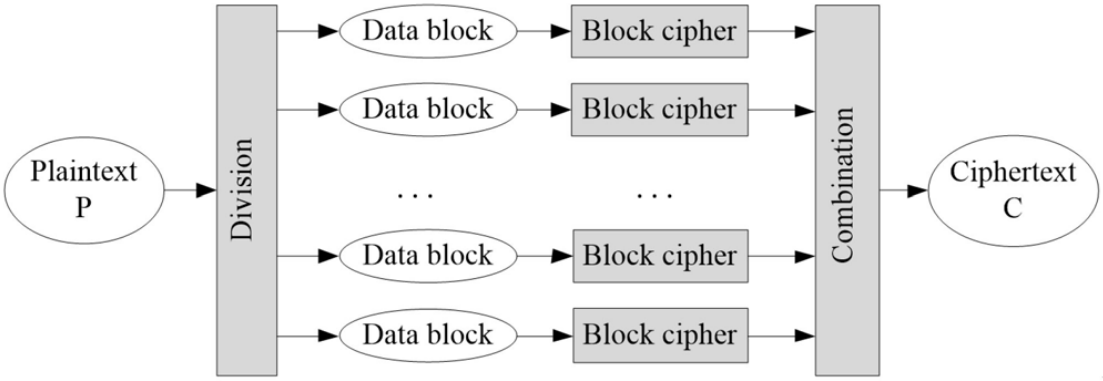


Figure 3: Proposition de TL-DEA.

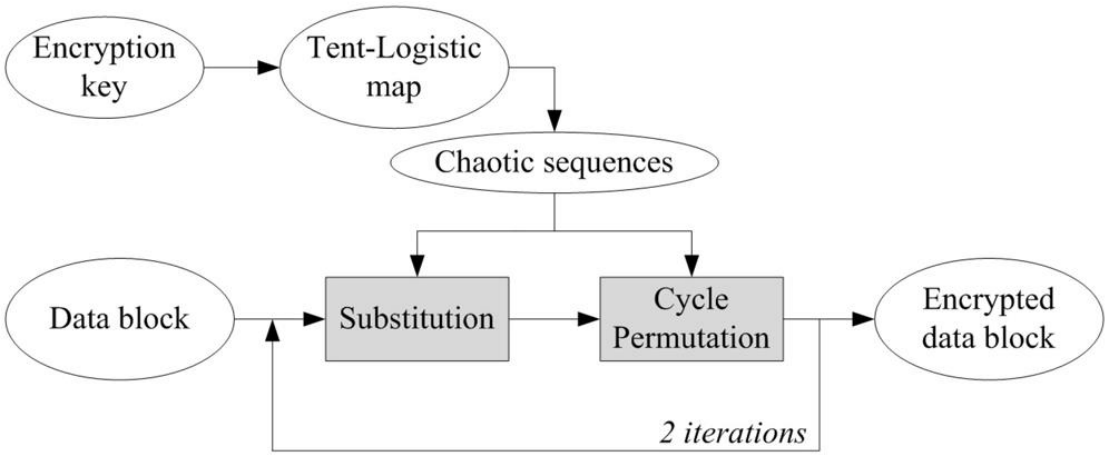


Figure 4 : Schéma fonctionnel du chiffrement par bloc.

Algorithme 1 Génération de valeurs initiales et de paramètres

Input: Security key K with length of 256 bits
1: Initial value $x_0 \leftarrow (\sum_{i=1}^{52} K_i 2^{52-i})/2^{52}$
2: parameter $u \leftarrow (\sum_{i=53}^{104} K_i 2^{104-i})/2^{52}$
3: parameter $a \leftarrow (\sum_{i=105}^{156} K_i 2^{156-i})/2^{52}$
4:$T \leftarrow (\sum_{i=157}^{208} K_i 2^{208-i})/2^{52}$
5: $R_1 \leftarrow \sum_{i=209}^{232} K_i 2^{232-i}$
6:$R_2 \leftarrow \sum_{i=233}^{256} K_i 2^{256-i}$
7**: for** i =1 **to** 2 **do**
8: $x_{Oi} \leftarrow (x_{Oi} + R_i T)$ mod 1
9: $u_i \leftarrow 1.8 + (u + R_i T)$ mod 0.2
10: $a_i \leftarrow 3.8 + (a + R_i T)$ mod 0.2
11: **end for**
Output: Initial Conditions (x_{O1}, u_1, a_1) and (x_{O2}, u_2, a_2)

5.1. TL-DEA

Le schéma de principe du TL-DEA proposé est représenté en Figure 3. Le texte en clair P indique les données originales tandis que le **Ciphertext C** signifie les données cryptées. L'opération de division est de diviser le texte en clair dans de nombreux blocs de données avec une longueur fixe. Le chiffrement par bloc est ensuite utilisé pour chiffrer chaque donnée bloqué individuellement. L'opération de combinaison consiste à combiner tous les blocs de données cryptés dans une séquence de données cryptées obtenir le texte chiffré.

Le chiffrement de bloc est représenté sur la figure 4 La clé de chiffrement est de fournir les conditions initiales de la carte Tente-Logistique. Deux tours de processus de substitution et de permutation dans TL-DEA sont de garantir de bonnes propriétés de confusion et de diffusion.

1) Analyse de clé: La clé de sécurité dans TL-DEA est avec longueur de 256 bits. Il est utilisé pour produire deux groupes de valeurs et paramètres tels que décrits dans l'algorithme 1. La carte Tente-Logistique les utilise ensuite pour générer deux séquences chaotiques.

Algorithme 2 Permutation de cycle

Input: Data block H and chaotic sequence S. Both are with length
of L
1: Rearrange H, S with size of M C N , where L = M × N.
2: Sort each row of S and get the row index matrix I. Then Sorted_$S_{m,n}$= $S_m I_{m,n}$, where m,n ∈ $[1, M] \times [1, N]$
3: **for** j=1 to N **do**
4:**for** i = 1 to M **do**
5: Find value j in the row of I, get its position (i, j_i).
6:**end for**
7: connect values of H in positions $(1, j_1)(2, j_2), \ldots \ldots (M, j_M)$ Into a circle, and shift them by j positions to upperdirection.
8: **end for**
9: Rearrange the permutation result into length of L
Output: The permuted result C.

2) **Substitution**: Le processus de substitution est conçu pour changer les valeurs de données dans le texte en clair en utilisant ses deux précédentes valeurs de données voisines et une valeur aléatoire de la séquence chaotique. Supposons qu'un bloc de données P est avec une longueur de L, un séquence chaotique S avec la longueur de L est générée par la Tente-Logistique carte, S = $\{x_1, x_2, \ldots, x_L\}$. Relier chaque donnée à son précédent un et reliant les premières données avec le dernier sont à faire le bloc de données sous la forme d'un cercle. Ensuite, le processus de substitution pour chaque bloc de données est défini comme

$$H_i = \begin{cases} (P_i + P_L + P_{L-1} + \lfloor S \times 20^{20} \rfloor_i) mod Fsii = 1 \\ (P_i + C_{i-1} + P_L + \lfloor S \times 20^{20} \rfloor_i) mod Fsii = 2 \\ (P_i + C_{i-1} + C_{i-2} + \lfloor S \times 20^{20} \rfloor_i) mod Fsii \in [3, L] \end{cases}$$

où F est le nombre d'échelles d'intensité autorisées dans le texte en clair. Par exemple, F = 2 si le texte en clair contient uniquement des données binaires données et F = 256 si le texte en clair est représenté en 8 bits décimales,l'opération est au sol.

3) **Permutation de cycle**: La permutation de cycle est de mélanger toutes les positions de données, comme indiqué dans l'algorithme 2.

Par exemple, supposons que la matrice d'index de ligne I est la suivante:$I = \begin{vmatrix} 2 & 14 & 3 \\ 1 & 32 & 4 \\ 3 & 24 & 1 \\ 1 & 43 & 2 \end{vmatrix}$

La figure 4 montre les opérations détaillées utilisant l'index matrice I. Premièrement, nous recherchons la valeur d'index 1 dans toutes les lignes de I, et obtenir les positions (1, 2), (2, 1), (3, 4), et (4, 1), puis nous nous connectons les données dans ces positions dans le bloc de données H dans un cercle et déplacez-les d'une position vers la direction supérieure. En Seconde, nous recherchons la valeur d'index 2 dans I, et obtenons des positions (1, 1), (2, 3), (3, 2) et (4, 4), connecter les données dans ces positions H dans un cercle, puis les déplacer de 2 positions à la partie supérieure direction. Répéter les mêmes procédures jusqu'à ce que la maximum valeur de l'indice dans I. Après une permutation de cycle, les données peuvent être séparées de toutes ses données voisines.

Répéter la substitution et encercler la permutation une fois de plus temps avec une autre séquence chaotique, le bloc de données crypté Est obtenu.

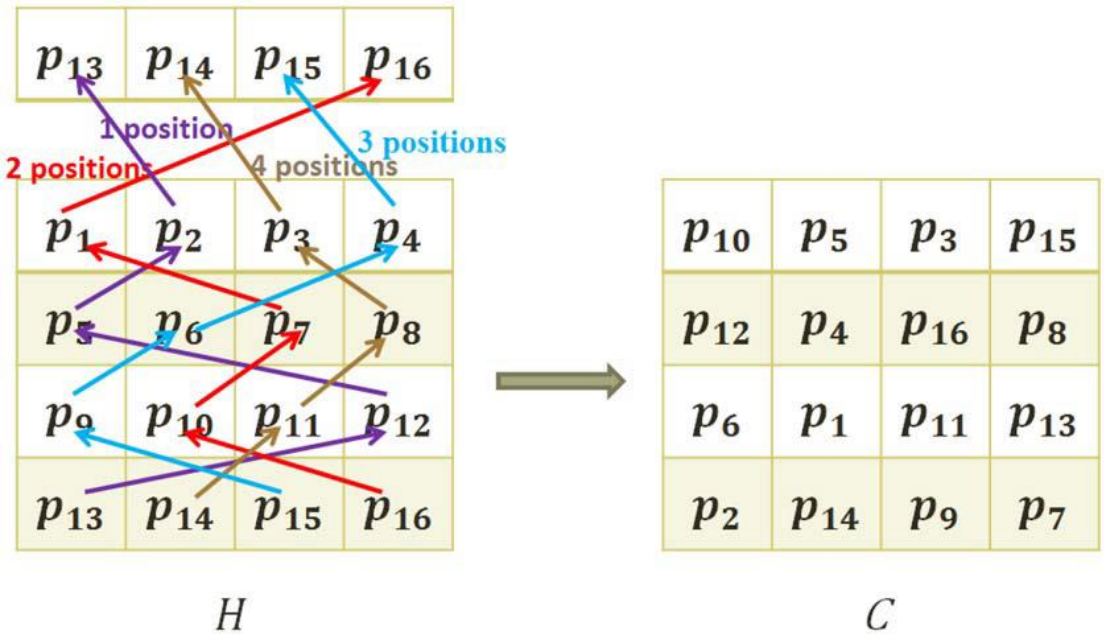


Figure 5 : Exemple de permutation de cycle.

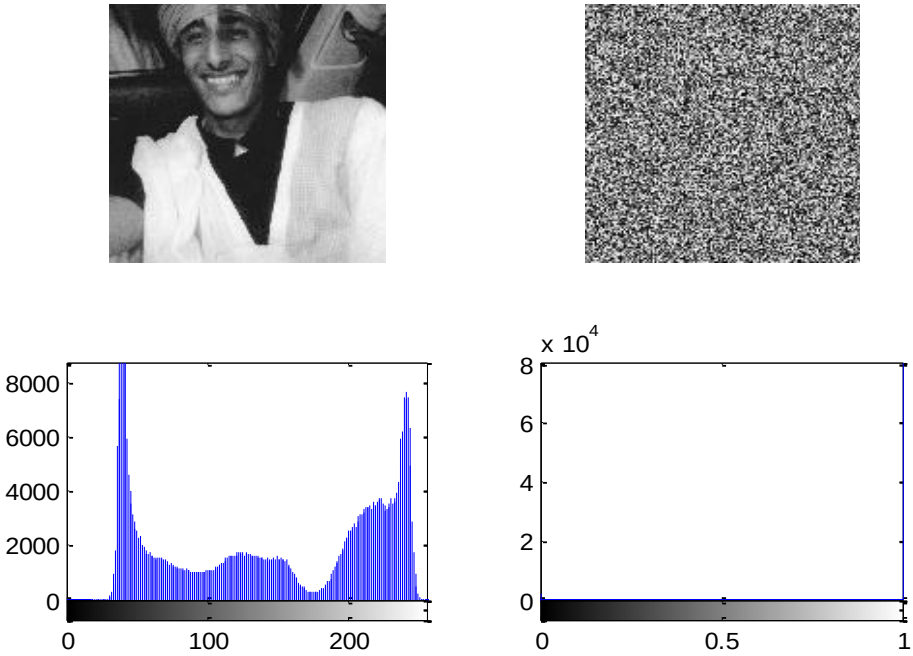


Figure 6 Chiffrement des résultats de données binaires. (a) Plaintext. (b) Texte chiffré. (c) Séquences de données segmentées à partir du texte en clair et du cpertext.

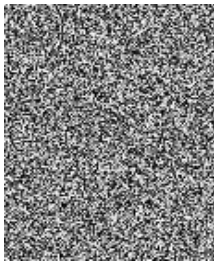
5.2. Résultats de la simulation

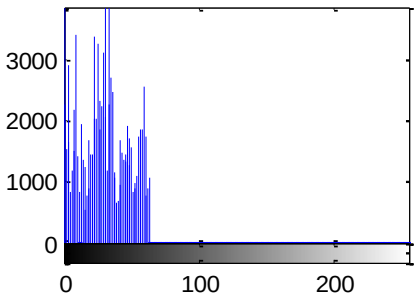
Un bon algorithme de cryptographie devrait être capable de crypter différents types de texte en clair dans le texte chiffré ressemblant à du bruit. Dans nos expériences, les données binaires et les données décimales 8 bits (par exemple, des images) sont utilisés comme texte en clair pour tester le cryptage performance du TL-DEA proposé. La simulation est faite avec MATLAB R2010a sous système Windows 7.

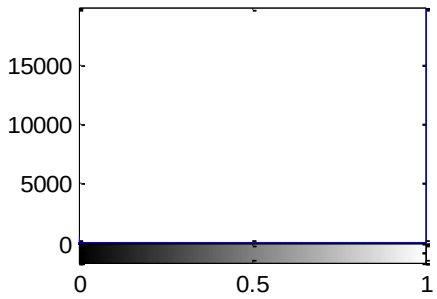
Pour chiffrer les données binaires, nous utilisons une image binaire comme exemple. Parce qu'une image binaire est représentée comme une matrice 2-D, il peut être traité comme un bloc de données et appliqué avec le bloc chiffré directement. Les résultats de chiffrement sont montrés sur la figure 6. Nous pouvons voir que les données binaires 0 et 1 dans le texte chiffré distribuer au hasard dans toutes les positions. Il n'y a pas d'information à propos des données d'origine.

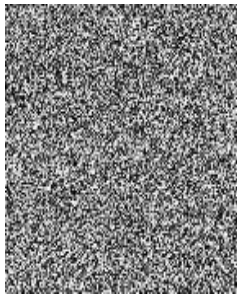
TL-DEA peut également crypter des données avec d'autres formats tels que les images numériques et vidéos. Leurs pixels sont généralement représentés par 8 bits ou plus. TL-DEA peut crypter directement eux au niveau du pixel, ce qui est plus efficace et pratique que ceux du niveau de bits. La Figure 7 montre le cryptage résultats d'images numériques. Comme on

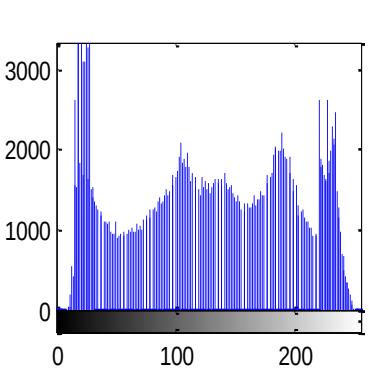
peut le voir, le crypté les images ressemblent visuellement à du bruit avec des distributions de données uniformes. Les données d'origine sont protégées avec un haut niveau de Sécurité.

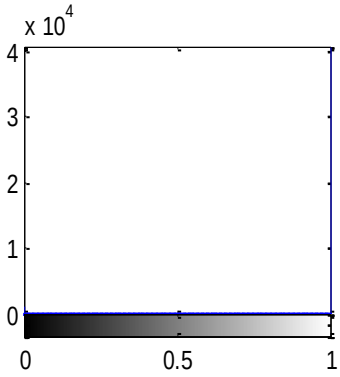












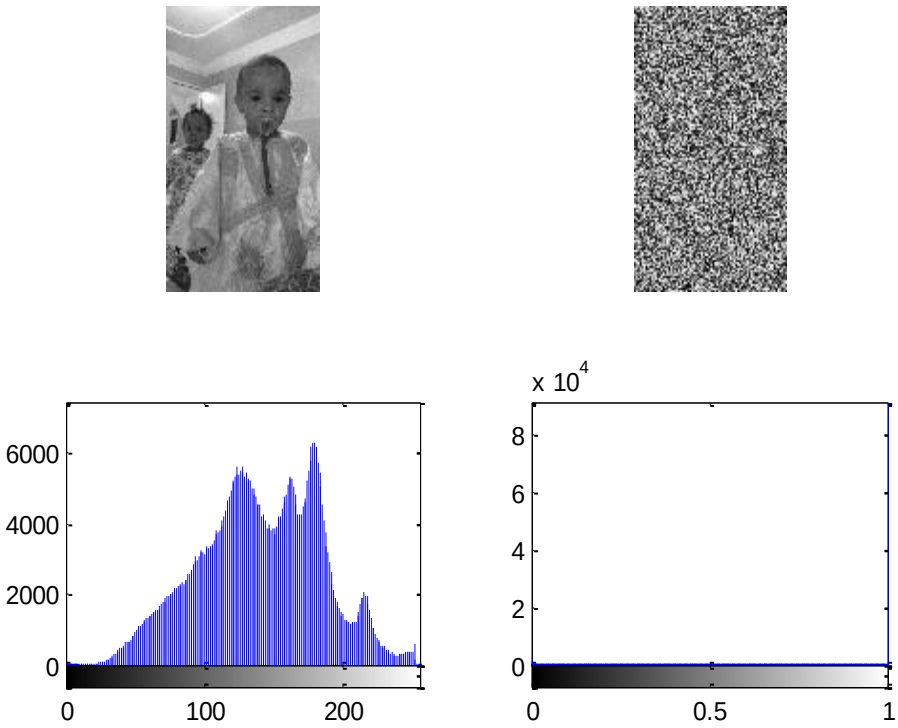


Figure 7 : Cryptage de différentes d'image

5.3. Analyse de sécurité

La sécurité est la propriété la plus importante d'une cryptographie système. Un bon système de cryptographie devrait avoir la capacité résisté à différentes attaques bien connues. Pour montrer les performances de sécurité du TL-DEA proposé, nous utilisons des images numériques représentées par 8 bits comme exemples à effectuer une analyse de sécurité, y compris le test de sensibilité clé, analyse d'attaque différentielle, ainsi que le bruit, et la perte de données attaques.

1) Test de sensibilité de clé: Un algorithme de chiffrement devrait être sensible à ses clés de sécurité. La sensibilité clé peut être testée dans les processus de cryptage et de décryptage: 1) clé de cryptage sensibilité, ce qui signifie qu'un léger changement dans le cryptage les clés donnent un texte chiffré complètement différent et 2) le décryptage la sensibilité des touches, ce qui signifie que le texte en clair d'origine peut être récupéré seulement lorsque les clés de sécurité correctes sont utilisées, et qu'un léger changement des clés de sécurité se traduira par un résultat de déchiffrement non reconnu.

Les principaux résultats de l'analyse de sensibilité sont présentés sur la figure 14. K2 et K3 sont deux clés de sécurité différentes qui sont généréesà partir de la clé de sécurité K1 avec un changement de bit. Comme on peut le voir, lorsqu'une image en texte clair P [Figure 8 (a)] est crypté en utilisant K2 et K3 avec seulement une différence de bit, nous obtenons deux totalement des résultats cryptés différents, comme le montrent les figures 8 (b) et (c). La figure 8 (d) montre leurs différences. D'un autre côté, quand une image cipertexte [Fig. 8 (b)] est déchiffré par deux touches avec une différence de bit, nous obtiendrons également deux totalement résultats différents décryptés comme montré sur les figures 8 (f) et (g). Seulement la clé de sécurité correcte peut reconstruire le texte en clair d'origine comme représenté sur la figure 8 (e). Par conséquent, le TL-DEA proposé est sensible à ses clés de sécurité dans le cryptage et le décryptage processus.

2) Analyse d'attaque différentielle: un système de cryptographie avec une excellente propriété de diffusion peut résister à différentiel attaques. Pour évaluer quantitativement la propriété de diffusion de TL-DEA, nous utilisons le nombre de taux de changement de pixel (NPCR) et intensité modifiée moyenne unifiée (UACI). Mathématiquement, le NPCR et l'UACI de deux images C1 et C2 sont définis comme

$$NPCR(C_1, C_2) = \sum_{i=1}^{M}\sum_{j=1}^{N}\frac{D(i,j)}{L} \times 100\%$$

$$UACI(C_1, C_2) = \sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|C_1(i,j) - C_2(i,j)|}{T \times L} \times 100\%$$

$$D(i,j) = \begin{cases} 0, & siC_1(i,j) - C_2(i,j) \\ 1, & siC_1(i,j) - C_2(i,j) \end{cases}$$

où C1 et C2 sont deux images cryptées qui sont générées à partir de deux images en clair avec une différence de pixel, T dénote la plus grande intensité de pixel autorisée et L dénote le nombre total de pixels dans l'image. Le NPCR mesure le pourcentage de pixels différents entre deux images cryptées tout en UACI teste les intensités changées.

Les images en texte brut proviennent de l'USC-SIPI jeu de données d'image. Pour chaque image de test, il est défini sur un pixel à zéro pour générer une nouvelle image de test, puis TL-DEA avec le même La clé de sécurité est appliquée aux deux images. Les deux cryptés les résultats sont ensuite mesurés par NPCR et UACI. Les spectacles du tableau V la mesure résulte. Comme on peut le voir, les valeurs moyennes de

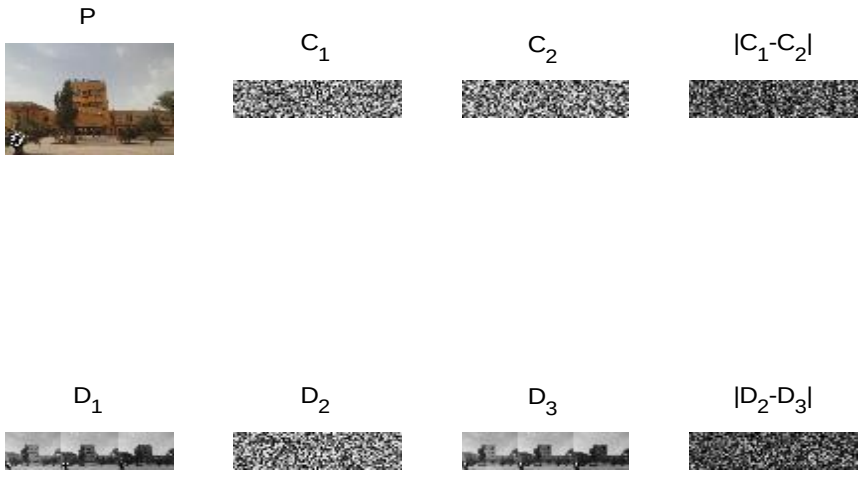


Fig. 14. Analyse de sensibilité de clé. (a) Image du texte en clair P. (b) Image du Cipertext C1 avec K1. (c) Cipertexte image C2 avec K2. (d) Différence entre le cpertext images, | C1 - C2 |. (e) Image décryptée D1 de C1 avec K1. (f) Décrypté image D2 de C1 avec K2. (g) Image décryptée D3 de C1 avec K3. (h) Différence entre images décryptées, | D2 - D3 |.

TABLEAU 1 : RÉSULTATS NPCR ET UACI DE TL-DEA AVEC LE PLAINTEXT IMAGES DE L'USC-SIPI IMAGE DATASET

Nom du fichier	NPCR %	UACI %
Ghard.bmp	99.6063	33.5162
Cameraman.tiff	99.6216	33.4507
Kids.tiff	99.6336	33.4761
Forest.tiff	99.6239	33.4663
Trees.tiff	99.5725	33.5110
Univ.bmp	99.6075	33.4335
Kh.jpj	99.6102	33.4139
Onion.PNG	99.6670	33.5390
Biye.jpj	99.6091	33.4562
Kebir.jpj	99.5531	33.3567
Moyenne	**99.6115**	**33.4840**

NPCR et UACI sont 99,6098% et 33,4384%, respectivement. Ils sont extrêmement proches des valeurs théoriquement idéales de Le NPCR et l'UACI (99,609% et 33,464%) se

sont révélés dans [32]. Ce démontre que TL-DEA a d'excellentes propriétés de diffusion et est capable de résister à une attaque différentielle.

3) Bruit et attaques de perte de données: Presque toutes les transmissions de données les canaux sont des canaux de bruit [33]. Lorsque les données sont en cours transmis sur les canaux de bruit, ils sont facilement contaminés par le bruit. Il existe également une perte de données lors de la transmission de données et le stockage. Par conséquent, il est important pour un cryptage algorithme capable de résister au bruit et aux attaques de perte de données. Pour tester la performance contre le bruit et la perte de données attaques, nous comparons TL-DEA avec trois cryptage existants algorithmes: l'AES [34], Liao et al. [35], et Les algorithmes de Wu et al. [36]. Nous cryptons d'abord une image en clair.

6. CONCLUSION

Dans Ce chapitre on asimulé un nouveau CCS. Le système est capable de pour générer un grand nombre de différentes cartes chaotiques 1-D en utilisant une combinaison de deux cartes chaotiques 1-D existantes. Trois exemples de MR générés par le SCC ont été introduits et analysé. Les résultats de l'évaluation et de la comparaison ont montré que les cartes chaotiques nouvellement générées sont plus imprévisible et avoir une meilleure performance chaotique, plus paramètres et propriétés chaotiques plus complexes que celles existantes cartes chaotiques

Montrer comment le CSC proposé peut bénéficier à l'applications basées sur le chaos, en utilisant la carte Tent-Logistic comme exemple de NCM de CCS, nous avons introduit TLPRNG et TL-DEA. Nous avons également évalué la performance de TL-DEA en ce qui concerne le chiffrement de données et l'analyse de sécurité. Les résultats ont montré que TL-DEA est capable de protéger différents types de données avec un haut niveau de sécurité et de résister attaque différentielle, ainsi que des attaques de bruit et de perte de données.

Conclusion générale

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.

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 cascade. Montrer comment le CSC proposé peut bénéficier à l'application basées sur le chaos, en utilisant la carte Tent-Logistic comme exemple de NCM de CCS, nous avons introduit TLPRNG et TL-DEA. Nous avons également évalué la performance de TL-DEA en ce qui concerne le chiffrement de données et l'analyse de sécurité. Les résultats ont montré que TL-DEA est capable de protéger différents types de données avec un haut niveau de sécurité et de résister attaque différentielle, ainsi que des attaques de bruit et de perte de données.

Références bibographique

Références Biographies

Chapitre 01 :

[1] ANSSI. *EBIOS: Expression des Besoins et Identification des Objectifs de Sécurité*. [En ligne]. 2010. Disponible sur : < http://www.ssi.gouv.fr/ > (consulté le 8 juin 2010)

*[2] NIST. *Standards for Security Categorization of Federal Information and Information Systems*. [En ligne]. 2004. Disponible sur : < http://csrc.nist.gov > (consulté le 10 septembre 2009)

[3] Stallings W. *Sécurité des réseaux : applications et standards*. Paris : Vuibert, 2002. ISBN : 9782711786534.

[4**]** ANSSI. *Agence nationale de la sécurité des systèmes d'information*. [Enligne].Disponible sur : < http://www.ssi.gouv.fr/ > (consulté le 5 mai 2012)

[5] Kim A., Luo J., Kang M. « Security ontology for annotating resources ». *On the Move toMeaningful Internet Systems 2005: CoopIS, DOA, and ODBASE*. 2005. p. 1483–1499.

[6] Schneier B. *Applied cryptography : protocols, algorithms, and source code in C*. 2nd ed.New York : Wiley, 1996. ISBN : 9780471128458.

[7] BUECKER A. et al. *Understanding SOA Security Design and Implementation*. [Enligne2007.Disponible sur : <http://www.redbooks.ibm.com/abstracts/sg247310.html > (consulté le 4 septembre 2010)

[8] Samarati P., De Vimercati S. « Access control: Policies, models, and mechanisms ».*Foundations of Security Analysis and Design*. 2001. p. 137–196.

[9] Ferraiolo D., Cugini J., Kuhn D. R. « Role-based access control (RBAC): Features and motivations ». In : *Proceedings of 11th Annual Computer Security Application Conference*. Washington : IEEE Computer Society Press, 1995. p. 241–48.

[10] Hachani wafa. *Patrons de conception à base d'aspects pour l'ingénierie des systèmes d'information par réutilisation*. Thèse Doctorat. GRENOBLE : Université Joseph Fourier,2006.

[11] Steel C. *Core security patterns best practices and strategies for J2EE, Web services, and identity management*. Upper Saddle River, NJ : Prentice Hall PTR, 2006. ISBN :9780131463073.

[12] *EEC, Information Technology Security Evaluation Criteria (ITSEC), Rapport Technique*. [En ligne]. Disponible sur : <http://csrc.nist.gov/publications/secpubs/itsec.txt> (consulté le 15 septembre 2009)

[13] MATHIEU H. *Modélisation conjointe de l'infrastructure et des processus pour l'administration pro-active de l'entreprise distribuée*. Thèse Doctorat. Lyon : INSA de Lyon, 2004. 252 p.

[14] ISO/IEC. *Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model* .[En ligne]. 1998.Disponible sur : < www.commoncriteriaportal.org > (consulté le 9 décembre 2009)

[15] ISO/IEC, The International Organisation for Standardisations and The International Electrotechnique Commission. *ISO/IEC 27002:2005*. [En ligne]. 2005. Disponible sur :

[16] NIST. *Fédéral Information Security Management Act (FISMA) Implémentation Project*. [En ligne]. Disponible sur :<http://csrc.nist.gov/groups/SMA/fisma/index.html (consulté le 7 décembre 2010)

[17] Biennie F., Mathieu H. « Technisa Solutions vs. Global BPR Investment ». *Schedae Informaticae*. 2005. Vol. 14, p. 13-34.

[18] Vacca J. *Managing information security*. Burlington MA : Elsevier, 2010. ISBN :9781597495332.

Chapitre 02 :

[1]:http://ram0000.developpez.com/tutoriels/cryptographie/?page=page_2#L2
< visité le :07/03/2017>

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

[3]Gada Zaibi. Thèse doctorats , sécurisation par dynamiques chaotiques des réseaux locaux sans _l au niveau de la couche mac. autre [cs.oh]. Universités Toulouse le Mirail -Toulouse ii, 2012. français.

[4] A. Menezes, P. VanOorschot, S. Vanstone,Handbook of applied cryptography, 1997 by CRC Press

[5] Touradj Ebrahimi, Franck Leprévost, Bertrand Warusfel, Cryptographie et sécurité des systèmes et réseaux, Hermès -Lavoisier 2006.

Chapitre 03 :

.[1] 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.

[2] Hassan Noura. Thése doctorats .Conception et simulation des générateurs, crypto-systèmes et fonctions détachage bases chaos performants.
Electronique. UNIVERSITE DE NANTES, 2012. Français.

[3] Billings, L. et Böll, E.M. (2001). Probability density functions of some skew tent maps,

Chaos Solutions Fractals, Volume 12, pages 365–376.

[4] El Assad, S., et Noura, H. (2011). Generator of chaotic sequences and corresponding generating system, Extensions internationals Brevets France n° FR20100059361 et FR201052288. Dépôt 28/03/2011. WO2011121218 (A1) 6/10/2011 et EP2553567,(A1) 06/02/2013. Publications : CN103124955(A) 29/05/2013 ; JP2013524271(A) 17/06/2013 ; US2013170641(A1) 4/07/2013.

[5] El Assad, S., Farajallah, M. et Vladeanu, C. (2008). Chaos-based Block Ciphers: An Overview", IEEE, 10th International Conference on Communications, COMM-2014, Bucharest, Romania, May 2014, pages 23-26. Invited talk

[6] Kapitaniak, T., Bindley, J. et Czolczynski, K. (2000). Controlling chaos and bifurcations in engineering systems, chapitre Chaos in mechanical systems and its control, pages 71–88. CRC Press, Taylord and Francis.

[7] http://www.juliensalort.org.

Chapiter 04:

[1] E. Ott, Chaos dans les systèmes dynamiques. New York, NY, États-Unis: Cambridge Univ. Presse, 2002.

[2] Q. Tao, Z. Sun et K. Kong, "Développer des algorithmes d'apprentissage via optimisé «IEEE Trans. Syst., Homme, Cybern. B, Cybern., Vol. 42, non. 1, pp. 140-149, février 2012.

[3] K.-Y. Lian, T.-S. Chiang, C.-S. Chiu, et P. Liu, "Synthèse de floue conceptions à base de modèles pour la synchronisation et la sécurisation des communications pour Systèmes chaotiques, "IEEE Trans System, Homme, Cybern B, Cybern., Vol. non. 1, pp. 66-83, février 2001.

[4] S.-L. Chen, T. Hwang et W.-W. Lin, "amélioration Randomness en utilisant "IEEE Trans Circuits System II, Exp. Mémoires, vol. 57, non. 12, pages 996-1000, déc. 2010.

[5] T. Addabbo et al., «Une classe de congruence non linéaire à période maximale générateurs dérivés de la carte chaotique de Rényi, "IEEE Trans. Syst. I, Reg. Papiers, vol. 54, no. 4, pages 816-828, avril 2007.

[6] R. Bose et S. Pathak, «Un nouveau système de compression et de cryptage utilisant un codage arithmétique à modèle variable et un système chaotique couplé, " IEEE Trans. Circuits Syst. I, Reg. Papiers, vol. 53, no. 4, pp. 848-857, Avril 2006.

[7] K.-W. Wong, Q. Lin et J. Chen, "Codage arithmétique simultané et le cryptage en utilisant des cartes chaotiques, "IEEE Trans Circuits System II, Exp. Mémoires, vol. 57, non. 2, pp. 146-150, février 2010.

[8] Y. Zhou, L. Bao, et C. L. P. Chen, "Un nouveau système chaotique 1D pour cryptage d'image, "Signal Process., volume 97, pages 172-182, avril 2014.

[9] R. C. Hilborn, le chaos et la dynamique non linéaire: une introduction pour Scientifiques et ingénieurs, 2e éd. New York, NY, États-Unis: Oxford Univ. Presse, 2001.

[10] Y. Wu, Y. Zhou et L. Bao, "Système chaotique à commutation de roues discrètes et applications, "Circuits IEEE Trans. I, Reg. Papiers, à être publié

[11] D. Arroyo, R. Rhouma, G. Alvarez, S. Li et V. Fernandez, «Sur la sécurité d'un nouveau schéma de chiffrage d'image sur une carte chaotique treillis, "Chaos, volume 18, numéro 3, septembre 2008, article ID 033112.

[12] H. C. Papadopoulos et G.W. Wornell, «Estimation du maximum de vraisemblance d'une classe de signaux chaotiques, "IEEE Trans. Inf. Théorie, volume 41, non. 1, pp. 312-317, janv. 1995.

[13] X. Wu, H. Hu et B. Zhang, "estimation de des séquences symboliques générées par le système de chaos ", Chaos Soliton. vol. 22, non. 2, pages 359-366, oct. 2004.

[14] G. Chen et X. Yu, Contrôle du chaos: théorie et applications, vol. 292. Berlin, Allemagne: Springer, 2003.

[15] H.-K. Chen et C.-I. Lee, "Anti-contrôle du chaos dans le mouvement du corps rigide" Chaos Soliton. Fract., Vol. 21, non. 4, pages 957 à 965, 2004.

[16] C. Shen, S. Yu, J. Lu et G. Chen, «Une méthodologie systématique pour la construction de systèmes hyperchaotiques avec plusieurs positifs Lyapunov Exposants et la mise en œuvre du circuit », IEEE Trans. Circuits Syst. I, Reg. Papiers, vol. 61, no. 3, pp. 854-864, mars 2014.

[17] T. Gao et Z. Chen, «Un nouvel algorithme de cryptage d'image sur hyper-chaos », Phys., Lettonie A, volume 372, n ° 4, pp. 394-400, janvier 2008.

[18] Y. Zhou, L. Bao et C. L. P. Chen, «Cryptage d'image en utilisant un nouveau système de commutation paramétrique, "Signal Process., volume 93, numéro 11, pp. 3039-3052, 2013.

[19] G. Jakimoski et K. P. Subbalakshmi, «exposant discret de Lyapunov et cryptanalyse différentielle, "IEEE Circuits Circuits II, Exp. vol. 54, no. 6, pages 499-501, juin 2007.

[20] J. Amigo, L. Kocarev et J. Szczepanski, "exposant discret de Lyapunov". et la résistance à la cryptanalyse différentielle, "IEEE Trans. Circuits Syst. II, Exp. Mémoires, vol. 54, no. 10, pages 882 à 886, oct. 2007

[21] A. Muchnik et S. Y. Positselsky, «l'entropie de Kolmogorov dans le contexte de la théorie de la calculabilité, "Theor, Comput, Sci., volume 271, numéro 12, pp. 15-35, 2002.

[22] R. Frigg, "En quoi l'entropie de Kolmogorov-Sinaï est-elle une mesure pour un comportement chaotique? Combler le fossé entre les systèmes dynamiques théorie et théorie de la communication, "Brit. J. Philos. Sci., Vol. 55, non. 3, pp. 411-434, 2004.

[23] J. Gao, J. Hu et W.-W. Tung, "Mesures d'entropie pour le signal biologique analyses, "Dyn. non linéaire, vol. 68, non. 3, pp. 431-444, 2012.

[24] C.-Y. Li, J.-S. Chen, et T.-Y. Chang, "Un pseudo-aléatoire basé sur le chaos générateur de nombres utilisant la méthode de réensemencement basée sur la synchronisation, "dans Proc. IEEE Int. Symp. Circuits Syst., Pp. 3277-3280, île de Kos, Grèce, 2006.

[25] Norme IEEE pour l'arithmétique en virgule flottante, norme IEEE 754-2008, 2008, pp. 1-70.
[26] I. Lawrence et al., "SP 800-22 Rév. 1a. Une suite de tests statistiques aléatoires et des générateurs de nombres pseudo-aléatoires pour les applications cryptographiques " Nat. Inst. Supporter. Technol., Gaithersburg, MD, États-Unis, Tech. NIST Rep. SP 800-22, 2010.

[27] P. L'Ecuyer et R. Simard, "TestU01: Une bibliothèque C pour les tests empiriques des générateurs de nombres aléatoires, "ACM Trans. Math. Softw., Vol. 33, non. 4, p. 22, 2007.

[28] J. M. Bahi, X. Fang, C. Guyeux, et Q. Wang, "Qualité aléatoire" des générateurs chaotiques CI: Applications à la sécurité internet, "in Proc. 2ème Int. Conf. Evol. Internet (INTERNET), 2010, pp. 125-130.

[29] Q. Wang, C. Guyeux et J. M. Bahi, «Un nouveau nombre pseudo-aléatoire générateur basé sur des itérations chaotiques discrètes », dans Proc. 1er Int. Conf. Evol. Internet (INTERNET), 2009, pp. 71-76.

[30] J. Lu et G. Chen, «Un modèle de réseau dynamique complexe variant dans le temps. et ses critères de synchronisation contrôlés, "IEEE Trans. Autom. Contrôle, vol. 50, non. 6, pages 841 à 846, juin 2005.

[31] Y. Zhou, K. Panetta, S. Agaian, et C. L. P. Chen, "(n, k, p) -Gray code pour les systèmes d'image, "IEEE Trans. Cybern., Vol. 43, non. 2, pp. 515-529, Avril 2013.

[32] C. Fu et al., «Un système de chiffrement d'image numérique basé sur le chaos avec une stratégie de diffusion améliorée, "Opt. Express, vol. 20, non. 3, pp. 2363-2378, 2012.

[33] R. C. Gonzalez et R. E. Woods, Traitement d'images numériques, 3e éd. Harlow, Royaume-Uni: Prentice-Hall Inc., 2007.

[34] Advanced Encryption Standard (AES), FIPS PUB 197, 2001.

[35] X. Liao, S. Lai, et Q. Zhou, "Un algorithme de cryptage d'image roman basé sur la transmission d'onde auto-adaptative, "Signal Process., vol. 90, non. 9, pp. 2714-2722, 2010.

[36] Y. Wu, G. Yang, H. Jin, et J. P. Noonan, "cryptage d'image en utilisant le carte chaotique logistique bidimensionnelle, "J. Electron. Imagerie, vol. 21, non. 1, 2012, Art. ID 013014.

Résume

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. 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 utilisant les cascades 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.

Les mots clé : Cascade, cryptage, décryptage, chaotique, symétrique, asymétrique.ect

Abstract

In the field of telecommunications, where the exchange of multimedia information is developing rapidly, it is essential to have secure systems to protect 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 . 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 Cascade 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

Key words: cascade, encrypting , unencrypting ,chaotic, symmetric,insymmétric.ect ,.

ملخص

في مجال الاتصالات حيث تبادل المعلومات المتعددة تنمو بسرعة ,فمن ضروري ان يكون انظمة امنة لحماية الحاجة حيث حماية الرقمية الزميه ,من اجل ضمان امن تشفير البيانات و صور فبالتالي تم تطوير انظمة فعالة لحماية البيانات ضد اختراقات تعسفية واستخدمنا انظمة فوضوية و من بينها نظام لكاس كاد حيث اظهرت نتائج فعالة ضد اي هجمات متقدمة

الكلمات المفتاحية: كاس كاد, تشفير, عدم تشفير, تشويش, متماثل, غير متماثل....