REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTRE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU
FACULTE DE GÉNIE ÉLECTRIQUE
ET D'INFORMATIQUE

MEMOIRE

DE FIN D'ETUDE

En vue de l'obtention du diplôme de Master de recherche en informatique

Option :

Systèmes Informatiques

Réseaux, mobilités et systèmes embarqués

Thème

Sécurité informatique basé sur un cryptosystème cas AES

Dirigé Par :

M^{r}: DIB Ahmed

Réalisé Par :

M^{elle} : BOUDAOUD Fetta

M^{elle} : NESSAH Nacéra

M^{elle} : CHOUGAR Melha

Promotion 2012/2013

Remerciements

Nous tenons à exprimer notre profonde gratitude à notre promoteur, ***M^r^ DIB Ahmed*** *pour nous avoir encadrés durant cette année, ainsi que pour ses conseils judicieux. Aussi nous tenons à lui reconnaître le temps précieux qu'il nous a consacré.*

Nos sincères sentiments de gratitude à monsieur ***CHAIEB. Y*** *et* ***HAMMACHE. A*** *pour leurs soutiens.*

Que les membres du jury trouvent ici nos plus vifs remerciements pour avoir accepter d'honorer par leur jugement notre travail.

A tous ceux qui de près ou de loin, ont contribué à la réalisation de ce projet, nos enseignants, nos chères familles et nos amis (es).

Dédicace

On dédie ce modeste travail
à toutes nos familles, nos proches,
à tous nos amis (es) et enfin à toutes les
personnes ayant contribué chacune
à sa manière au bon accomplissement de notre
projet.

Fetta, Nacéra et Melha

Sommaire

Chapitre II La cryptographie

Chapitre III Analyse et Conception

Chapitre IV Implémentation Et Evaluation

La liste des Figures

La liste des tables

Introduction général

La sécurité est devenue un point crucial des systèmes d'informations. Cependant, les organisations sont peu ou pas protégées contre les attaques sur leur réseau ou les hôtes du réseau. L'importance du nombre d'attaques dans le monde, nous donne des raisons visant à démontrer la vulnérabilité des systèmes d'informations, ces derniers se doivent aujourd'hui d'être protégés contre les anomalies de fonctionnement provenant soit d'une attitude intentionnellement malveillante d'un utilisateur, soit d'une faille rendant le système vulnérable.

De ce fait, de nombreuses solutions de protection, aussi différentes les unes des autres, ont vu le jour. Ces dernières, afin qu'elles soient efficaces, doivent être bien choisies, bien placées et bien configurées suivant les caractéristiques du réseau mis en place. Exemple : la mise en place d'un pare-feu qui est devenue indispensable afin d'interdire l'accès aux paquets indésirables. On peut, de cette façon, proposer une vision restreinte du réseau interne vu de l'extérieur et filtrer les paquets en fonction de certaines caractéristiques telles qu'une adresse ou un port de communication.

Cependant, ce système de forteresse est insuffisant s'il n'est pas accompagné d'autres protections. Citons la protection physique des informations par des accès contrôlés aux locaux, la protection contre les failles de configuration par des outils d'analyse automatique des vulnérabilités du système, ou encore la protection par des systèmes d'authentification fiables pour que les droits accordés à chacun soient clairement définis et respectés, ceci afin de garantir la confidentialité et l'intégrité des données. Donc de nouvelles exigences se sont apparues : assurer la confidentialité des messages ne suffit plus, il faut également assurer leur intégrité et leur authenticité.

Alors d'autres mécanismes de sécurités sont indispensables tels que le chiffrement des données qui fut inventé pour assurer la confidentialité des données. Il est assuré par un système de clé (algorithme) appliqué sur le message. Ce dernier est décryptable par une clé unique correspondant au cryptage. Dans la cryptologie, on distingue la cryptographie et la cryptanalyse. La première définit et étudie les systèmes utilisés, alors que la seconde cherche à valider ou à casser ces systèmes.

Au travers de ce travail, nous aborderons en détails un algorithme de cryptage. Et nous verrons la manière de crypter en elle-même aussi ses conséquences et ses faiblesses afin de l'améliorer, Pour cela, nous avons organisé ce projet en quatre chapitres selon le plan méthodologique suivant : Dans le premier chapitre, nous verrons les concepts généreux de la sécurité informatique, le deuxième sera consacré pour la cryptographie et la comparaison des différents algorithmes existants, le troisième : la conception de l'algorithme AES et les modifications porté sur ce dernier , et en fin la réalisation de cette algorithmes avec quelques applications.

Chapitre I

Généralités sur la sécurité dans les réseaux informatiques

Chapitre I Généralités sur la sécurité dans les réseaux informatiques

I.1 Introduction:

Ces dernières années, la sécurité des systèmes informatiques connectés à Internet est devenue un problème très préoccupant. L'accès par Internet à une masse croissante d'informations actualisées en temps réel ainsi que la possibilité de les traiter automatiquement, font que de plus en plus d'entreprises ouvrent leurs systèmes d'informations à leurs partenaires ou leurs fournisseurs, il est donc vital d'analyser les risques qu'encourent ces entreprises, de connaître les ressources qu'elles doivent protéger et de maîtriser le contrôle d'accès et les droits des utilisateurs de leurs systèmes d'informations.

Dans ce qui suit, nous parlerons de la sécurité en générale ainsi que des différentes menaces qui pèsent sur les systèmes informatiques.

I.2 La sécurité informatique :

L'ensemble des données et des ressources matérielles et logicielles d'une entreprise représente un patrimoine essentiel de celle-ci, il convient donc de le protéger, et c'est à ce point qu'intervient la sécurité informatique.

La sécurité informatique est l'ensemble des moyens mis en oeuvre afin d'assurer d'une manière satisfaisante que les ressources citées précédemment ne soient utilisées que dans le cadre prévu et minimiser le nombre de vulnérabilités d'un système contre les menaces accidentelles ou intentionnelles.

I.3 Objectifs de la sécurité informatique :

La sécurité informatique vise généralement cinq principaux objectifs (critères):

- **Confidentialité :**

Toute entreprise possède des données de grandes valeurs (très importantes pour le bon fonctionnement et la survie de cette entreprise), et donc il faut veiller au caractère privé de ces données, c'est-à-dire qu'elles devraient être confidentielles. Ces données sont sensibles et représentent l'objectif principal des attaques, alors comment s'y prendre pour contrôler l'accès à ces informations sensibles ?

La confidentialité consiste à assurer que seules les personnes autorisées à manipuler ces ressources aient accès, donc les rendre inintelligibles et inaccessibles par d'autres personnes qui ne possèdent pas ce privilège.

- **Intégrité :**

Certaines données ne devraient pas être modifiées par n'importe quel utilisateur. On prend par exemple un étudiant ayant accès à un certain champ d'une base de données dans lequel il peut

entrer sa note, et qui ne peut être lue par un autre car la note est cryptée, mais si un étudiant met le contenu crypté d'un autre étudiant sur ce champ alors la note est modifiée et pourtant la confidentialité est réalisée (c-à-d : les données sont toujours cryptées). L'intégrité consiste à assurer la conformité de l'information, elle permet aux utilisateurs d'avoir la certitude que l'information est correcte et qu'elle n'a pas été modifiée par un individu non autorisé.

Les attaques contre l'intégrité sont difficiles à prévoir car elles sont généralement perçues après qu'elles se soient réellement produites et que le système soit compromis.

- **Disponibilité :**

Pour un utilisateur, la disponibilité d'une ressource est la probabilité de pouvoir mener correctement à terme une session de travail.

La disponibilité d'une ressource est indissociable de son accessibilité : il ne suffit pas qu'elle soit disponible, elle doit être utilisable avec des temps de réponse acceptables. Ce service est assuré généralement en faisant des copies de sauvegardes des données où du système d'information, mais dans certaines organisations où la perturbation des fonctions du réseau ou des systèmes informatiques est omniprésente, il ne sera probablement pas suffisant de faire régulièrement des copies de sécurité des données. Les services de disponibilité vont au-delà de la simple copie de sécurité. En fait, on peut diviser ces services en deux groupes principaux. Dans le premier, nous retrouvons des services de contingentement, c.-à-d. les services qui sont requis pour empêcher les personnes, que leurs intentions soient malicieuses ou non, de sur-utiliser les ressources du réseau, comme l'espace disque, la mémoire, la largeur de bande, etc., de telle sorte que ces ressources ne soient plus disponibles pour les autres utilisateurs.

Par ailleurs, un deuxième groupe de services de disponibilité assure le maintien des fonctions du réseau lorsqu'il y a une panne de matériel ou de logiciel; ce groupe est désigné sous l'appellation «tolérance aux pannes».

- **Authentification :**

La première étape afin de protéger les ressources d'un système informatique est de pouvoir vérifier l'identité des utilisateurs, cette vérification s'appelle l'authentification.

L'authentification permet de vérifier l'identité annoncée et de s'assurer de la non-usurpation de l'identité d'une entité. C'est-à-dire qu'elle permet de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être. Un contrôle d'accès peut permettre (par exemple par le moyen d'un mot de passe qui devra être crypté) l'accès à des ressources uniquement aux personnes autorisées. Et plus l'utilisateur doit fournir de

renseignements de ce type, plus faibles sont les risques qu'une autre personne parvienne à se faire passer pour cet utilisateur légitime.

- **Non-répudiation :**

La non-répudiation est le fait de ne pouvoir nier ou rejeter qu'un événement (action, transaction) a eu lieu. A ce critère de sécurité sont associées les notions d'imputabilité, de traçabilité et éventuellement d'auditabilité.

- L'**imputabilité** se définit par l'affectation certaine d'une entité à une action ou à un événement. L'imputabilité est réalisée par l'ensemble des exigences garantissant l'enregistrement des informations pertinentes sur l'individu agissant.
- La **traçabilité** est la fonction de sécurité qui comprend, le cas échéant, bien évidemment, l'imputation, mais qui mémorise l'origine d'un message, d'un événement, d'une information ou d'une donnée. Elle permet, par exemple, de retrouver l'adresse à partir de laquelle ces données ont été envoyées.
- L**'auditabilité** se définit par la capacité d'un système à garantir la présence des informations nécessaire à une analyse ultérieure d'un événement (courant ou exceptionnel) dans le but de déterminer s'il y a effectivement eu violation de la sécurité, et dans ce cas, quelles informations ou autres ressources ont été compromises. C'est également la fonction destinée à déceler et à examiner les événements susceptibles de constituer une menace pour la sécurité.

I.4 Présentation de l'insécurité informatique

I.4.1 Les menace :

La menace est l'éventualité alarmante que quelque chose se produise, et qui pourra porter atteinte à un système informatique, en d'autres termes, une menace est un événement ou action susceptible de violer la sécurité d'un système informatique.

Les principales menaces effectives auxquelles un système d'information peut être confronté sont :

- **Un utilisateur du système :** l'énorme majorité des problèmes liés à la sécurité d'un système d'information est l'utilisateur, généralement insouciant.
- **Une personne malveillante (interne ou externe) :** une personne vient à s'introduire sur le système, légitimement ou non, et à accéder ensuite à des données ou à des programmes auxquels elle n'est pas censée avoir accès.

- **Un programme malveillant :** c'est un logiciel destiné à nuire ou à abuser des ressources du système. Il est installé (par mégarde ou par malveillance) sur le système, ouvrant la porte à des intrusions ou modifiant les données ; des données personnelles peuvent être collectées à l'insu de l'utilisateur et être réutilisées à des fins malveillantes ou commerciales.
- **Un sinistre** (vol, incendie, dégât des eaux) : une mauvaise manipulation ou une malveillance entraînant une perte de matériel et/ou de données.

I.4.2 Vulnérabilité des systèmes informatiques :

La vulnérabilité d'un système, appelée parfois faille de sécurité ou brèche d'un système est un bogue particulier dont l'exploitation permet d'effectuer des actions qui ne sont pas possibles dans le cadre d'une utilisation normale d'un logiciel. Ces failles sont dues aux faiblesses dans la conception ou à la mauvaise configuration du système d'exploitation, des protocoles réseaux ou des applications utilisateurs, et sont caractérisées par la difficulté de leur exploitation et par le niveau de compétence technique requis pour les exploiter. Les failles les plus redoutables sont celles permettant l'exécution de code à distance, c'est-à-dire permettant à un individu malveillant d'exécuter un programme malicieux sur l'ordinateur de sa victime via Internet, même si celle-ci se trouve à l'autre bout de la planète.

I.4.3 Les contre-mesures :

La contre-mesure est un ensemble d'actions ou outils matériels ou logiciels permettant de sécuriser un système face aux menaces. Pour se faire, il est indispensable d'identifier les vulnérabilités de celui-ci face aux menaces et de prévoir la façon de procéder de l'agresseur pour ensuite concevoir les solutions nécessaires et de se doter de moyens efficaces afin de réduire au maximum les vulnérabilités exploitées par l'attaquant (c-à-d renforcer la sécurité du système) et donc minimiser le risque d'être attaqué.

I.4.4 Les risques:

Le risque est la probabilité qu'une menace particulière puisse exploiter une vulnérabilité donnée du système. Traiter le risque c'est prendre en compte les menaces et les vulnérabilités.

Il est important de mesurer les risques, non seulement en fonction de la probabilité ou de la fréquence de leurs survenances, mais aussi en mesurant leurs effets possibles. Ces effets, selon les circonstances et le moment où ils se manifestent, peuvent avoir des conséquences négligeables ou catastrophiques.

- Données irrémédiablement perdues ou altérées, ce qui les rend inexploitables.

- Données ou traitements durablement indisponibles, pouvant entraîner l'arrêt d'une production ou d'un service.
- Divulgation d'informations confidentielles ou erronées pouvant profiter à des sociétés concurrentes ou nuire à l'image de l'entreprise.
- Déclenchement d'actions pouvant provoquer des accidents physiques ou induire des drames humains

I.4.4.1 Facteurs du risque :

Il y'a risque lorsqu'il y'a combinaison de menace et de vulnérabilité, et ces deux composants forment la base du risque. Ainsi, s'il n'y a pas de menace, il n'y a aucun risque, et de même s'il n'y a pas de vulnérabilité, il n'y a aucun risque.

I4.4.2 Niveaux des risques :

Le risque peut être qualitativement défini selon trois niveaux :

- **Mineur :** La vulnérabilité expose l'entreprise à un risque, mais il est improbable que ''quoi que se soit'' puisse se produire. Il faut si possible, prendre des mesures pour supprimer cette vulnérabilité, mais il ne faut pas que le coût de cette action soit trop important par rapport à une réduction minime du risque.
- **Moyen :** La vulnérabilité présente un risque important pour la confidentialité, l'intégrité, la disponibilité des informations de l'entreprise, des systèmes ou des sites physiques. Il y a une réelle possibilité que cela puisse arriver. Il est recommandé de supprimer cette vulnérabilité.
- **Majeur :** La vulnérabilité présente un danger réel pour la confidentialité, l'intégrité et la disponibilité ''des informations, des systèmes ou des sites physiques''. Il faut prendre des mesures immédiates pour supprimer cette vulnérabilité.

I.4.5 Les attaques :

Tout ordinateur connecté à un réseau informatique est potentiellement exposé à une attaque.

Une « **attaque** » est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins généralement préjudiciables.

Sur internet des attaques ont lieu en permanence, à raison de plusieurs attaques par minute sur chaque machine connectée. Ces attaques sont pour la plupart lancées

automatiquement à partir de machines infectées (par des virus, chevaux de Troie, vers, etc.), à l'insu de leur propriétaire.

Afin de contrer ces attaques il est indispensable de connaître les principaux types d'attaques afin de mettre en œuvre des dispositions préventives.

Les motivations des attaques peuvent être de différentes sortes :

- Obtenir un accès au système.
- Voler des informations, tels que des secrets industriels ou des propriétés intellectuelles.
- Recueillir des informations personnelles sur un utilisateur.
- Récupérer des données bancaires.
- S'informer sur l'organisation (entreprise de l'utilisateur).
- Troubler le bon fonctionnement d'un service.
- Utiliser le système de l'utilisateur comme « rebond » pour une attaque.
- Utiliser les ressources du système de l'utilisateur, notamment lorsque le réseau sur lequel il est situé possède une bande passante élevée.

I.4.5.1. Les formes d'attaques :

Il en existe plusieurs, parmi elles on retrouve :

- **Attaque de modification**

a. **Les virus :**

Linux et Mac OS font partie de la famille des systèmes Unix, c'est sur Unix que sont apparus les premiers virus vers 1975. Tout de suite, les concepteurs d'Unix ont mis en place les barrières qui ont sécurisé Unix et depuis, c'est très rare qu'on entende parler de virus sur Unix. C'est donc la sécurité intrinsèque du système qui le protège. Par contre, Microsoft n'a pas pris les mêmes précautions. Pour faire le DOS, il a fallu faire des simplifications considérables et la notion de sécurité a été complètement éludée. Donc toutes les versions qui ont suivi, la sécurité a été un emplâtre que l'on rejouait et non une caractéristique fondamentale du système.

Un virus est un petit programme qui infecte d'autres programmes. Il insère son code dans celui de l'application ciblée afin de pouvoir prendre les commandes au moment de l'exécution des fichiers infectés. Cette définition simple permet d'identifier l'une des principales actions exécutées par les virus, à s'avoir *l'infection*...

Les virus ont des formes très différentes, et des conséquences aussi diverses, ils utilisent différentes voies pour infecter les systèmes comme les disquettes, les clés USB, le téléchargement de programmes via Internet, les emails,…etc.

b. **Les vers (Worms) :**

Un ver, par fois appelé virus de mail peut s'auto-reproduire et se déplacer à travers un réseau en utilisant les mécanismes réseau, en se servant par exemple des programmes de messagerie pour se répandre à grande vitesse, en s'envoyant automatiquement à tout ou partie des personnes présentes dans le carnet d'adresses. Leur premier effet est de saturer les serveurs de messagerie, mais ils peuvent également avoir des actions destructrices pour les ordinateurs contaminés. Ils sont particulièrement redoutables, car le fait de recevoir un mail d'une personne connue diminue la méfiance du destinataire, qui ouvre alors sans se soucier, le fichier joint.

c. **Le cheval de Troie :**

Un cheval de Troie se trouve généralement en pièce jointe d'un simple email, ou encore cachés dans un programme en libre téléchargement, ces fichiers peuvent se révéler être en fait un programme de type **cheval de Troie** (autrement appelé **troyen** ou **trojan**), qui permet à votre "agresseur" de prendre le contrôle à distance de votre machine, et d'avoir un accès libre en lecture, écriture ou suppression à la totalité des fichiers présents sur votre disque dur...

Un cheval de troie est défini comme étant un petit programme qui se substitue généralement à celui qui permet d'effectuer le login et demande à l'utilisateur son identifiant et mot de passe. Ce dernier fournit ces informations en croyant avoir à faire à son propre environnement d'exécution. Le mot de passe est directement capté et mémorisé par le cheval de troie qui le transmet par message électronique à un serveur de messagerie anonyme auquel se connectera le fraudeur. Entre temps, l'utilisateur n'a pas pu se connecter puisque le véritable programme de connexion ne s'est pas exécuté. Il a vu apparaitre à son écran le

message du type « erreur, mot de passe incorrect ». Il pense automatiquement qu'il a effectué une erreur de saisie, il se relogue et redonne son mot de passe, qui cette fois sera traité par le véritable programme de login.

d. Porte dérobée :

Lorsqu'un pirate informatique arrive à accéder à un serveur à l'aide d'une des techniques présentées dans cette section, il souhaiterait y retourner sans avoir tout recommencer. Pour cela, il laisse donc des portes dérobées (backdoor) qui lui permettra de reprendre facilement le contrôle du système informatique.

Il existe différents types de portes dérobées :

- Création d'un nouveau compte administrateur avec un mot de passe choisi par le pirate.
- Création de compte ftp
- Modification des règles du pare-feu pour qu'il accepte des connexions externes.

Dans tous les cas, l'administrateur per le contrôle total du système informatique. Le pirate peut alors récupérer les données qu'il souhaite, voler des mots de passe ou même détruire des données.

❖ Attaque par saturation (Denis de service)

Les attaques par saturation sont des attaques informatiques qui consistent à envoyer des milliers de messages depuis des dizaines d'ordinateurs, dans le but de submerger les serveurs. Cette technique de piratage est assez simple à réaliser, elle est jugée comme de la pure malveillance, et ne fait que bloquer l'accès aux sites, sans en altérer le contenu.

a. Le TCP-SYN flooding

Le TCP-SYN flooding est une variante du flooding qui s'appuie sur une faille du protocole TCP. En effet, on envoie un grand nombre de demande de connexions au serveur (SYN) à partir de plusieurs machines. Le serveur va envoyer un grand nombre de paquet SYN-ACK et attendre en réponse un paquet ACK qui ne viendra jamais. Si on envoie les paquets plus vite que le timeout des « demi-connexions » (connexions autorisées mais non terminé), le serveur sature et finit par se déconnecter.

b. Smurf

Le smurf est une attaque qui s'appuie sur le ping et les serveurs de broadcast. On falsifie d'abord son adresse IP pour se faire passer pour la machine cible. On envoie alors un ping sur un serveur de broadcast. Il le fera suivre à toutes les machines qui sont connectées qui renverront chacune un « pong » au serveur qui fera suivre à la machine cible. Celle-ci sera alors inondée sous les paquets et finira par se déconnecter.

c. Débordement de tampon

Cette attaque se base sur une faille du protocole IP. On envoie à la machine cible des données d'une taille supérieure à la capacité d'un paquet. Celui-ci sera alors fractionné pour l'envoi et rassemblé par la machine cible. A ce moment, il y aura débordement des variables internes.

Suite à ce débordement la machine se bloque ou se redémarre.

d. Ping de la mort

Le ping de la mort consiste à envoyer une suite de fragments d'une requête de type écho ICMP. Une fois à nouveau assemblés par la pile IP/TCP du système cible, ces fragments forment un paquet d'une taille supérieure à la taille maximale autorisée (65 507 octets) et peuvent faire déborder les variables internes, provoquant un comportement anormal du système. Plus aucun système récent n'est vulnérable à ce type d'attaque.

❖ Attaques de répudiation

La répudiation est une attaque contre la responsabilité. Autrement dit, la répudiation consiste à tenter de donner de fausses informations ou de nier qu'un événement ou une transaction se soient réellement passé.

a. IP spoofing

Cette attaque va se dérouler en plusieurs étapes :

- ✓ Trouver la machine de confiance (son adresse IP)

- ✓ Mettre hors service cette machine de confiance (avec un SYN Flooding par exemple) pour éviter qu'elle ne réponde aux paquets éventuellement envoyés par le serveur cible.
- ✓ Prédire les numéros de séquence TCP du serveur cible (un numéro de séquence initial est généré à chaque nouvelle connexion TCP).

b. Spoofing ARP

- ✓ Comme son nom l'indique, l'attaque ARP spoofing s'appuie sur le protocole ARP(Address Resolution Protocol), qui implémente le mécanisme de résolution d'une adresse IP (32 bits) en une adresse MAC (48 bits) pour rediriger le trafic réseau d'un ou plusieurs systèmes vers le système pirate. Lorsqu'un système désire communiquer avec ses voisins sur un même réseau, des messages ARP sont envoyés afin de connaître l'adresse MAC des systèmes voisins et d'établir ainsi une communication avec un système donné. Sachant que chaque système possède localement une table de correspondance entre les adresses IP et MAC des systèmes voisins, la faiblesse d'authentification du protocole ARP permet à un système pirate d'envoyer des paquets ARP réponse au système cible indiquant que la nouvelle adresse MAC correspondant à l'adresse IP d'une passerelle est la sienne. Le système du pirate reçoit donc tout le trafic à destination de la passerelle. Il lui suffit d'écouter ou de modifier passivement le trafic et de router ensuite les paquets vers leur véritable destination

I.4.5.2. Les phases d'une intrusion :

Il y a beaucoup de chemins qu'un attaquant peut prendre afin d'accéder à un système ou l'exploiter. Les étapes de base sont les suivantes :

Figure I.1 : les différentes phases d'une attaque.

a. La phase de reconnaissance :

La phase de reconnaissance implique le rassemblement d'un maximum d'informations sur une cible potentielle (un système, une machine...), à l'insu de cette cible. Ce processus est appelé *collecte d'informations.*

A l'issue de cette phase, sont rassemblées toutes les informations disponibles sur une organisation pour utilisation ultérieure lors d'une attaque. En général, un hacker passe les 90% de son temps à dresser un profil de l'organisme cible et 10% seulement du temps pour lancer l'attaque. Comme mentionné plut haut, l'analyse du trafic réseau *(network sniffing)* est aussi une méthode de reconnaissance qui permet la collecte d'informations utiles telle que les adresses IP, les numéros de port les noms des machines et autres services disponibles dans un réseau ou un système. Le Social Engineering est aussi une méthode redoutable de collecte d'informations.

La reconnaissance permet donc de découvrir des informations utiles (collecte d'informations) pour conduire une attaque ultérieure. Par exemple, collecter le type du serveur web et du système d'exploitation, afin exploiter d'éventuelles vulnérabilités et avoir des accès.

b. Phase de scan :

C'est l'utilisation des informations collectées lors de la phase de reconnaissance, pour examiner le réseau. Les outils pouvant être utilisés par les hackers peuvent inclure :

dialers, scanneurs de ports, scanneurs de vulnérabilités, mappers et sweppers. A ce stade, les hackers sont entrain de chercher toute information susceptible de les aider à commettre une attaque.

c. Phase d'accès :

C'est la phase où les vrais hackers prennent place. Les vulnérabilités découvertes durant les phases de reconnaissance et de scan sont maintenant exploitées pour avoir un accès.

d. Phase de maintien de l'accès :

Une fois le hacker arrive à pénétrer dans un système, il va vouloir maintenir cette possibilité d'accès pour de futures attaques. Dans certains cas, les hackers *renforcent le*

système contre d'autres attaquants ou contre le personnel de sécurité par la sécurisation exclusive de leurs accès avec les backdoors et les trojans. Une fois le système est approprié parle hacker, il peut être utilisé pour lancer des attaques additionnelles. Dans ce cas, le système approprié est appelé système *Zombie.*

e. Phase d'effacement de traces :

Une fois l'attaque terminée, la hacker efface ses traces et ainsi, supprimer toute évidence du hacking et donc éviter d'être découvert par le personnel de sécurité, ce qui lui permettra de continuer à utiliser le système ultérieurement.

Les hackers tentent de supprimer toutes les traces comme les fichiers log et les alarmes (générées par les systèmes de détection d'intrusions). Un exemple des activités de cette phase inclue la *stéganographie (qui est l'art de dissimuler des données dans d'autres données*), les protocoles de tunneling et la modification des fichiers log...

I.5 Politique de sécurité réseau

La politique de sécurité réseau est un document générique qui définit des règles à suivre pour les accès aux réseaux informatiques, détermine comment les politiques sont appliquées et présente une partie de l'architecture de base de l'environnement de sécurité du réseau. Ces documents à caractère non technique donnent aux responsables de l'entreprise les axes à suivre.

Voici quelques types de documents :

.1 Guides

Il s'agit de documents détaillant comment implémenté les politiques de sécurité. Ils sont considérés comme des documents complémentaires aux politiques.

.2 Standards

Il s'agit de documents de standardisation de normes et méthodes émanant d'organismes internationaux tels que l'ISO (International Standardization Organization), l'IETF (Internet Engineering Task Force), l'IEEE (Institute of Electrical andElectronics Engineers), etc.

.3 Procédures

Il s'agit de documents à caractère opérationnel et technique, qui décrivent de manière claire et précise les étapes à suivre pour atteindre un objectif de sécurité donné. Une politique de sécurité réseau est donc indépendante de tout produit ou technologie. Elle est avant tout constituée d'une suite de règles et de principes répondant aux besoins de sécurité de l'entreprise. Les documents de sécurité peuvent être représentés par une structure pyramidale représentant le positionnement respectif de chaque document.

I.6 Mécanismes de Sécurité

Nous avons constaté que les attaquants disposent de plusieurs moyens pour réussir leurs attaques. La disponibilité des outils d'attaques et la richesse des sources d'informations accentuent le risque des intrusions. Par conséquent, les administrateurs sécurisent de plus en plus leurs systèmes informatiques. Ils s'appuient sur diverses solutions comme :

I.6.1 Cryptage, Signature électronique et Certificat

- **Cryptage**

Le cryptage est un procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de chiffrement ou de déchiffrement.

- **Signature numérique** (**signature électronique**)

La signature est un mécanisme permettant de garantir l'intégrité d'un document électronique et d'en authentifier l'auteur, par analogie avec la signature manuscrite d'un document papier. (Ajout d'informations cryptées à une unité de données afin de prouver la source et l'intégrité de cette unité de données).

- **Certificat [6] :**

Un certificat est un document contenant une affirmation certifiée, un certificat est une sorte de pièce d'identité par exemple le passeport ou l'extrait de naissance. Un certificat numérique est une information attachée à une clé publique, et qui permet de vérifier que cette clé est authentique, ou valide.

Un certificat numérique comporte trois éléments:

- ✓ Une clé publique
- ✓ Une information de certification (“l’identité” de l’utilisateur, comme son nom, son adresse e-mail, etc.).
- ✓ Une ou plusieurs signatures numériques.

I.6.2 Notarisation [19] :

La notarisation est la certification des différentes étapes de l'évolution d'un document électronique en vue de :

- ✓ Permettre de garantir le contenu, l’origine, la date et la destination d'un message électronique lors d’un échange entre deux machines.
- ✓ Archiver de façon sécurisée des documents numériques

La notarisation électronique permet la vérification et l'archivage des preuves d'échanges et d’archivages électroniques par un tiers de confiance agréé (à la manière d'un notaire). Cette technique améliore la sécurité des échanges et de l'archivage électronique.

I.6.3 Horodatage (timestoping)

L’horodatage protège de toute contestation concernant le contenu d’un fichier et sa date d’émission ou de réception.

L’utilisation de l’horodatage est comme preuve de :

- ✓ Non altération : d’une archive, d’un contrat...
- ✓ Respect de délais légaux : de rétractation, de prise d’effet d’un contrat (assurance, crédit, abonnement, contrat de formation)…
- ✓ Antériorité : dépôt de candidature à un appel d’offre, dépôt de brevet…
- ✓ Accusé de réception opposable : mise en demeure, résiliation/reconduction d’un contrat...
- ✓ Traçabilité des actions : exigences réglementaires type Bâle 2, SOX…

- ✓ Facture électronique : en raison de l'obligation de pouvoir garantir l'authenticité.

I.6.4 Parfeu (filtrage) [13]

Le parfeu est un élément du réseau informatique, logiciel et/ou matériel, qui a pour fonction de sécuriser un réseau domestique ou professionnel en définissant les types de communication autorisés ou interdits. Le principe de base de la sécurité d'un réseau, intranet, repose sur l'installation d'un ou plusieurs firewalls qui peuvent être logiciels ou matériels. L'idée principale d'un firewall est la connexion sécurisée du réseau interne avec l'Internet (ou un autre réseau local non sûr).

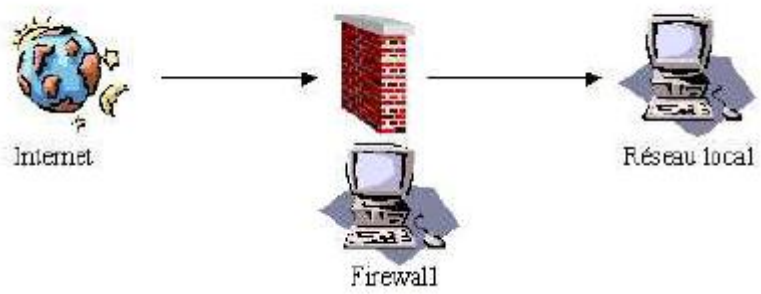


Figure I.2 : Placement d'un firewall

Un firewall permet donc de délimiter les environnements publics et privés afin de protéger son réseau. On arrive à mieux gérer les flux entrants et sortants et ainsi séparer son réseau intranet du réseau internet.

Un pare-feu fonctionne sur des triplets (client/service/ condition). Ainsi, chaque « client » du firewall a accès à certains services sous certaines conditions. Le pare-feu peut bloquer un trafic particulier, ou en laisser passer un autre. On peut donc protéger le réseau d'intrusions non autorisées, tout en permettant aux employés un accès aux services Internet tels que l'e-mail, le web ou autre. Dans la pratique, on peut configurer un firewall de manière à le rendre plus ou moins stricte.

I.6.4.1 Types de firewall

- **Firewalls bridge**

Les firewalls bridge agissent comme de vrais câbles réseau avec la fonction de filtrage en plus, d'où leur appellation de firewall. Ils ne disposent pas d'adresse IP sur leurs interfaces, et ne font que transférer les paquets d'une interface a une autre en leur appliquant les règles prédéfinies. Cette absence d'adresse IP est particulièrement utile, car cela signifie que le firewall est indétectable sur le réseau. En effet, quand une requête ARP est émise sur le câble réseau, le firewall ne pourra pas répondre. Ses adresses Mac ne circuleront jamais sur le réseau, et comme il ne fait que « transmettre » les paquets, il sera totalement invisible sur le réseau. Cela rend impossible toute attaque dirigée directement contre le firewall, étant donné qu'aucun paquet ne sera traité par ce dernier comme étant sa propre destination. Donc, la seule façon de le contourner est de passer à travers ses règles de « drop ». Ces firewalls se trouvent typiquement sur les Switchs.

- **Firewalls logiciels**

Les pare-feux sont présents à la fois dans les serveurs et les machines, on peut les classer en plusieurs catégories

- ✓ **Firewalls personnels** Ils sont pour la plupart commerciaux et ont pour but de sécuriser un ordinateur particulier. Souvent payants, ils peuvent être contraignants et quelque fois très peu sécurisés. En effet, pour rester accessible à l'utilisateur final, ils s'orientent plus vers la simplicité d'utilisation, et donc mettent de côté l'aspect technique.

- ✓ **Firewalls plus « sûre »** Ils se trouvent généralement sous Linux, car ce Système d'Exploitation offre une sécurité réseau plus élevée et aussi un contrôle plus précis. Ils ont généralement le même comportement que les firewalls matériels des routeurs, à la seule différence qu'ils sont configurables à la main.

Ces firewalls logiciels ont néanmoins une grande faille : ils n'utilisent pas la couche bas réseau. Pour récupérer des paquets qui auraient été normalement « droppés », il suffit de passer outre le noyau (en utilisant une librairie particulière).

Néanmoins, cette faille signifie qu'on s'est déjà introduit sur l'ordinateur en question ; ce qui induit une intrusion dans le réseau, où une prise de contrôle physique de l'ordinateur, donc qui est synonyme de faille.

- **Firewalls matériels**

Ils se trouvent souvent sur des routeurs achetés dans le commerce par de grands constructeurs comme Cisco ou Nortel.

Intégrés directement dans la machine, ils font office de « boite noire », et ont une intégration parfaite avec le matériel. Leur configuration est souvent relativement ardue, mais leur avantage est que leur interaction avec les autres fonctionnalités du routeur est simplifiée par leur présence sur le même équipement réseau. Souvent relativement peu flexibles en terme de configuration, ils sont aussi peu vulnérables aux attaques, car présent dans la « boite noire » .

De plus, étant souvent très liés au matériel, l'accès à leur code est assez difficile, et le constructeur a eu toute latitude pour produire des systèmes de codes « signés » afin d'authentifier le logiciel (système RSA ou assimilés). Ce système n'est implanté que dans les firewalls haut de gamme, car cela évite un remplacement du logiciel par un autre non produit par le fabricant, ou toute modification de ce dernier, rendant ainsi le firewall très sûr.

Son administration est souvent plus aisée que les firewalls bridges, les grandes marques de routeurs utilisant cet argument comme argument de vente. Leur niveau de sécurité est de plus très bon.

I.6.4.2 Types de filtrage

- **Firewalls à filtrage de paquets**

Ce type de firewall travaille sur la composition même des paquets réseaux réseau. Ils analysent les paquets entrants/sortants suivant leurs types, leurs adresses source et destination ainsi que les ports utilisés, chaque paquet d'informations entrant ou sortant est accepté ou rejeté selon des règles établies par l'utilisateur.

- **Firewalls Proxy**

Les firewalls proxy (ou firewalls applicatifs) ont un mode de fonctionnement différent des firewalls à filtrage de paquets. Ils masquent les ressources internes du réseau, ce par feu empêche l'extérieur de connaître les adresses internes du réseau.

Chaque application passe alors par le firewall proxy et envoie sa requête non pas au serveur qu'elle désire atteindre mais au firewall qui la retransmettra. Inversement, les communications émises depuis Internet à destination des systèmes internes ne les atteignent pas directement mais sont préalablement traitées par le firewall.

Il est à noter que ces firewalls sont des gros consommateurs de ressources informatiques.

- **Les Proxy « SOCKS »**

Ce type de firewall ne travaille pas sur les flux applicatifs mais rétablisse, à chaque connexion, la connexion vers l'extérieur. Ce type de firewall est peu utilisé désormais. Il est à noter que ces firewalls ne réalisent pas d'authentification des utilisateurs même s'ils ont la capacité d'enregistrer les coordonnées de l'utilisateur qui a demandé la connexion.

I.6.5 Antivirus [20]

Un antivirus est un logiciel informatique destiné à identifier et à effacer des logiciels malveillants, également appelés virus, Chevaux de Troie ou vers selon les formes.

- **Fonctionnement d'un antivirus**

L'antivirus analyse les fichiers entrants (fichiers téléchargés ou courriers électroniques) et, périodiquement, la mémoire vive de l'ordinateur et les périphériques de stockage comme les disques durs, internes ou externes, les clés USB et les cartes à mémoire Flash.

Le logiciel antivirus peut procéder de deux manières différentes :

- ✓ Il analyse les fichiers, en comparant leur contenu aux virus d'un dictionnaire de virus connus. Les virus détectés sont signalés selon la méthode définie par l'utilisateur.

- ✓ Il surveille les processus suspects sur un hôte susceptible d'être infecté. Cette surveillance comprend la saisie de données, la surveillance des ports et d'autres méthodes.

I.6.6 Sonde et Pot de miel

- **Sonde**

Une sonde est un point de collecte de données sur Internet. La plupart du temps, elle repose sur la récupération des fichiers de journalisation des routeurs sur Internet ou des pare-feux. L'approche par sonde est très intéressante car elle a mis en évidence le caractère excessivement malin de plusieurs programmes sur Internet.

- **Pot de miel**

Un pot de miel se définit comme un système informatique connecté à un réseau,

Volontairement vulnérable à une ou plusieurs failles et visant à attirer les attaquants afin d'étudier leur comportement. En théorie, aucune activité en provenance ou à destination de ce système ne devrait être enregistrée. Dans le cas contraire, il s'agit au mieux d'une erreur accidentelle, au pire d'une tentative d'attaque intentionnelle.

I.6.7 Mot de passe [18]

Une personne peut être authentifiée par une combinaison d'une identification et d'un mot de passe, (code secret personnel).Le mot de passe doit posséder certaines caractéristiques qui sont : non trivial, difficile à deviner, régulièrement modifié. Cependant si l'attaquant accède au fichier de mot de passe, il pourra s'introduire dans le système sécurisé.

- ➢ **Choix d'un mot de passe [18]**

Choisir un bon mot de passe n'est pas si évident que ça en a l'air. Il faut respecter quelques règles :

- ✓ Ne jamais choisir un mot du langage courant. Des logiciels spéciaux de type dictionary cracking sont spécialisés dans ce domaine.

- ✓ Ne jamais prendre un mot qui est proche de vous : Votre prénom, le nom de jeune fille de votre femme, le nom du chien, des enfants, de votre hobby préféré...
- ✓ Ne jamais prendre un mot inférieur à 6 lettres. Des logiciels spéciaux de type brute force cracking sont spécialisés dans ce domaine.
- ✓ Un mot de passe ne doit jamais être écrit quelque part. La première chose que fait un pirate, est de fouiller dans vos affaires : Regarder dans votre agenda, sous l'écran, sous le clavier, dans votre poubelle, rechercher un fichier du type "mdp.txt" dans votre disque dur, etc.

I.6.8 Systèmes de détection d'intrusions [18]

Système de détection d'intrusions (IDS) est un équipement permettant de surveiller l'activité d'un réseau ou d'un hôte donné, afin de détecter toute tentative d'intrusion et éventuellement de réagir à cette tentative. Les IDS peuvent se classer selon deux catégories majeures selon qu'ils s'attachent à surveiller le trafic réseau ou l'activité des machines.

I.6.8.1 IDS Réseau :

Ces outils analysent le trafic réseau ; ils comportent généralement une sonde qui " écoute " sur le segment de réseau à surveiller et un moteur qui réalise l'analyse du trafic afin de détecter les signatures d'attaques ou les divergences face au modèle de référence. Les IDS Réseau à base de signatures sont confrontés actuellement à deux problèmes majeurs qui sont le développement de l'utilisation du cryptage et le développement des réseaux commutés. En effet, il est d'une part plus difficile " d'écouter " sur les réseaux commutés et le cryptage rend l'analyse du contenu des paquets presque impossible. La plupart des IDS sont aussi dits IDS inline car ils analysent le flux en temps réel. Pour cette raison, la question des performances est très importante car de tels IDS doivent être de plus en plus performants afin d'analyser les volumes de plus en plus importants pouvant transiter sur les réseaux.

I.6.8.2 IDS Système :

Les IDS Systèmes analysent le fonctionnement ou l'état des machines sur lesquelles ils sont installés afin de détecter les attaques. Ils sont très dépendants du système sur lequel ils sont installés. Il faut donc des outils spécifiques en fonction des systèmes déployés. Ces IDS peuvent s'appuyer sur des fonctionnalités d'audit propres au système d'exploitation ou non

pour vérifier l'intégrité du système et générer des alertes. Il faut cependant noter qu'ils sont incapables de détecter les attaques affectant les couches réseaux de la machine ; typiquement les Déni de service comme SYN FLOOD ou autre.

I.6.9 Fichiers historiques :

Fichier historique permet d'enregistrer tout ou une partie des actions effectuées sur le système. L'analyse de ses informations permet de détecter d'éventuelles intrusions. Les systèmes d'exploitation génèrent des fichiers historiques, certaines applications aussi. Les différents évènements du système sont enregistrés dans un journal, qui devra être analysé fréquemment, voire en permanence. Sur les réseaux, il est indispensable de disposer d'une base de temps commune pour estampiller les évènements.

Les types d'informations à collecter sur les systèmes pour permettre la détection d'intrusions : On y trouve les informations sur les accès au système (qui a accédé, quand et comment), les informations sur l'usage fait du système (utilisation du processeur, de la mémoire ou des entrées/sorties) et les informations sur l'usage fait des fichiers. Le fichier historique doit également permettre d'obtenir des informations relatives à chaque application (le lancement ou l'arrêt des différents modules, les variables d'entrée et de sortie et les différentes commandes exécutées), Les informations sur les violations éventuelles de la sécurité (tentatives de commandes non autorisées) ainsi que les informations statistiques sur le système seront elles aussi nécessaires.

I.6.10 VPN :

Un réseau privé virtuel (VPN) est l'extension d'un réseau privé qui inclut les liaisons avec des réseaux partagés ou publics tels qu'Internet. Avec un réseau VPN, il est possible de transmettre des données entre deux ordinateurs par le biais d'un réseau partagé ou public en émulant une liaison privée point à point.

Ces réseaux offrent deux avantages majeurs :

- ✓ De hautes performances en termes de bande passante, autrement dit des communications à très haut débit et de très grande qualité.
- ✓ La sécurité et la confidentialité des données.

I.6.10 .1 Fonctionnalités des VPN :

Il existe 3 types standards d'utilisation des Vpn :

- **Vpn d'accès [17]**

Le Vpn d'accès est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau privé. L'utilisateur se sert d'une connexion Internet pour établir la connexion Vpn. Il existe deux cas:

- L'utilisateur demande au fournisseur d'accès de lui établir une connexion cryptée vers le serveur distant : il communique avec le Nas (Network Access Server) du fournisseur d'accès et c'est le Nas qui établit la connexion cryptée.
- L'utilisateur possède son propre logiciel client pour le Vpn auquel cas il établit directement la communication de manière cryptée vers le réseau de l'entreprise.

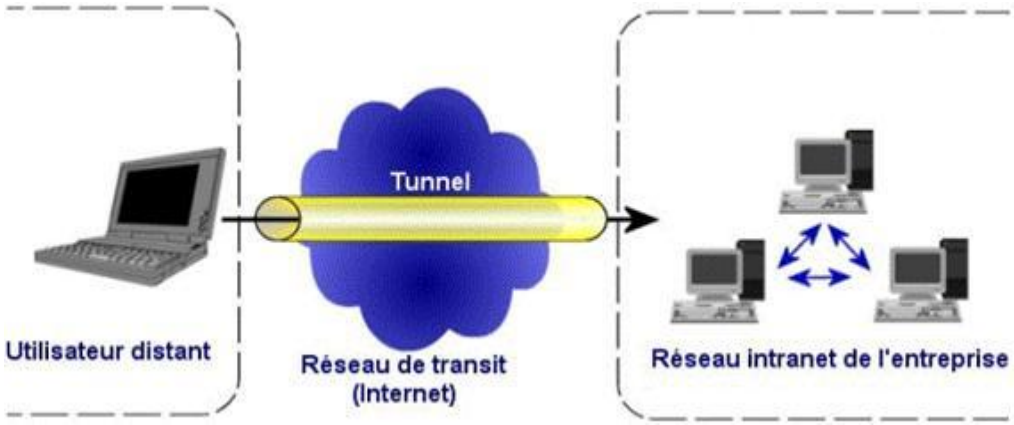


Figure I.3 : VPN d'accès

- **Intranet Vpn**

L'intranet Vpn est utilisé pour relier au moins deux intranets entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants.

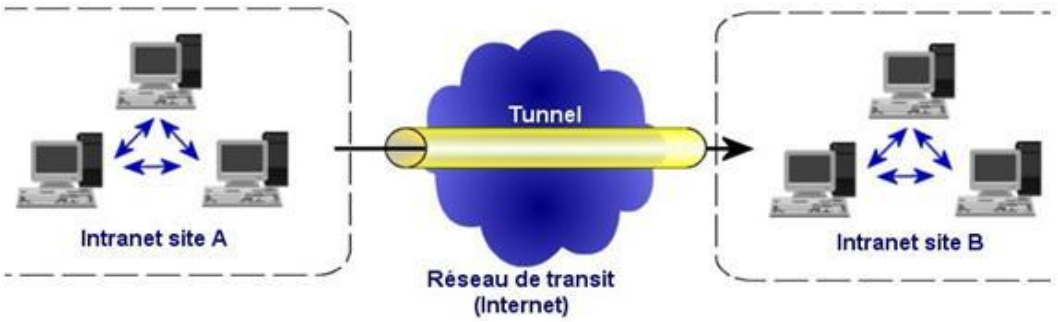


Figure I.4 : VPN intranet.

- **L'extranet VPN**

Une entreprise peut utiliser le VPN pour communiquer avec ses clients et ses partenaires. Elle ouvre alors son réseau local à ces derniers. Dans Ce cadre, il est fondamental que l'administrateur du VPN puisse tracer les clients sur le réseau et gérer les droits de chacun sur celui-ci.

I.7 Conclusion :

Le présent chapitre a été entièrement dédié à l'étude des différents types de menaces, et des techniques utilisées par les pirates pour violer la sécurité des réseaux. Les menaces comme les intrusions, fusent de partout ; de l'extérieur comme de l'intérieur de l'entreprise. Elles sont commises par des vrais pirates (*qui sont engagés par la concurrence*), par des anciens employés licenciés (*par vengeance*) ou par de simples adolescents (*par défi ou par envie de jouer*). Dans tous les cas, ça reste des actions dangereuses pour l'entreprise et donc, il faut s'en protéger au plus vite.

Chapitre II

La cryptographie

II.1 Introduction :

L'idée de coder un message dans le but de le rendre inintelligible à toute tierce personne ne date pas aujourd'hui. Les « messages secret » ont joué un rôle important dans tous les conflits depuis que l'homme sait écrire, et sont habituellement associés aux guerres et aux agents secrets.

Le but de ce chapitre, est de présenter les méthodes de la cryptographie. Il intéressera le lecteur qui connaît peu ou pas le domaine et qui souhaiterait comprendre le fonctionnement et les mécanismes mis en œuvre en cryptographie.

II.2 Cryptologie

La cryptologie est la science du secret, ne peut être vraiment considéré comme une science que depuis peut de temps. Cette science englobe la cryptographie, la cryptanalyse et la stéganographie.

II.2.1 Cryptographie :

La cryptographie est l'étude des techniques mathématiques qui permettent d'assurer certains services de sécurité. Elle est définie comme étant une science permettant de convertir des informations «en clair » en informations cryptées (codées), c'est-à-dire non compréhensible, et puis, a partir de ces informations, de restituer les informations originales**[1]**.

La cryptographie est l'étude des méthodes donnant la possibilité d'envoyer des données de manière confidentielle sur un support donné.

II.2.2 Cryptanalyse :

La cryptanalyse est la science de reconstitution du texte en clair sans connaitre la clé. Une cryptanalyse réussie peut fournir soit le texte en clair, soit la clef. La cryptanalyse peut également mettre en évidence les faiblesses d'un cryptosystème qui peuvent éventuellement faciliter les attaques contre celui-ci. Lorsqu'une méthode de cryptanalyse permet de déchiffrer un message chiffré à l'aide d'un cryptosystème, on dit alors que l'algorithme de chiffrement a été « cassé ». On distingue habituellement quatre méthodes de cryptanalyse :

- ✓ Une attaque sur texte chiffré seulement consiste à retrouver la clé de déchiffrement à partir d'un ou plusieurs textes chiffrés ;
- ✓ Une attaque sur texte clair connu consiste à retrouver la clé de déchiffrement à partir d'un ou plusieurs textes chiffrés, connaissant le texte en clair correspondant ;
- ✓ Une attaque sur texte clair choisi consiste à retrouver la clé de déchiffrement à partir d'un ou plusieurs textes chiffrés, l'attaquant ayant la possibilité de les générer à partir de textes en clair ;
- ✓ Une attaque sur texte chiffré choisi consiste à retrouver la clé de déchiffrement à partir d'un ou plusieurs textes chiffrés, l'attaquant ayant la possibilité de les générer à partir de textes en clair.

II.2.3 La stéganographie [9] :

La stéganographie est une méthode de cryptage utilisée depuis longtemps pour le cryptage des messages. Des fichiers peuvent être cachés dans une image. Les nouvelles technologies permettent de camoufler également de la musique au format MP3 ou des images. Le grand avantage de ce système est que le contenu caché dans ce document ne peut pas être détecté par l'œil humain. Cet outil était gratuit mais il est désormais payant. Les fonctionnalités de ce procédé sont très intéressantes ; elles permettent par exemple de mettre un mot de passe pour protéger l'image qui camoufle votre fichier. Le décodage apparaît et procède bit par bit. La personne qui reçoit l'image doit donc utiliser ce même logiciel et connaître le mot de passe de protection du fichier. Autrement, elle ne pourra voir que l'image écran.

II.2.3.1 Présentation de la stéganographie

Le mot "stéganographie" est un composé de deux racines grecques : Stegano, qui signifie "caché" ou "secret" et graphie, "écriture" ou "dessin". En juxtaposant ces deux termes, vous obtenez "écriture cachée". La stéganographie est donc la technique qui permet de transmettre des informations de façon cachée.

Cela ne signifie pas que les informations sont invisibles mais qu'elles sont codées. On parle de cryptographie. Il existe des données qui remontent à la Grèce ancienne, que leurs auteurs ont voulu protéger d'une façon sûre. Ils ont trouvé le moyen de coder leurs données en les transformant en un autre type de données pour qu'elles ne soient pas comprises de tous. Le principe qui nous intéresse est le même.

Avec la stéganographie, les données sont stockées. Elles sont certes transformées mais sont conservées sans altération. Les données peuvent être cachées dans des fichiers au format MP3, par exemple. Il est même possible d'utiliser d'autres moyens. Toutes les déclinaisons sont permises.

De nos jours, vous pouvez donc envoyer par email une image, une photographie, une musique, dans laquelle un texte est caché. Le destinataire du message doit posséder le même logiciel afin d'être en mesure de décrypter le code protégeant le message. Le message pourra apparaître clairement et être lu.

Cette méthode existait déjà en version papier pendant la Seconde Guerre mondiale. Des messages secrets circulaient ainsi entre les mains des militaires, au grand jour.

II.3 Les type de cryptographie :

II.3.1 Cryptographie classique :

Dans la cryptographie classique, la méthode et la clé de chiffrement ainsi que celles de déchiffrement sont connues par l'émetteur et le destinataire. L'émetteur et le destinataire doivent se mettre préalablement d'accord sur la clé. Ce qui pose le problème de l'échange des clés, par exemple, dans un réseau de N entités susceptibles de communiquer secrètement, il faut distribuer $C^2_n = N(N-1)/2$ clés.

La plupart des méthodes de chiffrement classiques reposent sur deux principes essentiels: la substitution et la transposition . La substitution consiste à remplacer certaines lettres par d'autres ou par des symboles. La transposition signifie qu'on permute les lettres du message afin de le rendre inintelligible.

II.3.1.1 Code de César :

Le code de César est la méthode de cryptographie la plus ancienne communément admise par l'histoire. Il consiste à substituer chaque lettre de l'alphabet par celle obtenue après un décalage des lettres. Par exemple, si on remplace A par D, on remplace alors B par E, C par F, D par G, etc ...

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

Tab II.1 : Chiffrement de César

Il n'y a que 26 façons différentes de chiffrer un message avec le code de César. Donc, il est très facile de le casser, en testant de façon exhaustive toutes les possibilités. Son inconvénient très facile a cassé avec une technique de force brute (uniquement 26 cas à essayer).

II.3.1.2 Le carré de Polybe :

Polybe (150 av. JC) était un écrivain grec. C'est lui qui a inventé le premier chiffre de substitution. Le carré de Polybe est basé sur une grille comme celle-ci :

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	IJ	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Tab II.2 La grille de Polybe

Chaque lettre est codée par 2 chiffres. Exemple : S=43. Les lettres I et J ne sont pas différenciés. "BONJOUR" sera chiffré par "12343324344542"

II.3.1.3 Chiffrement par substitution [10] :

Le chiffrement par substitution consiste à remplacer dans un message une ou plusieurs entités (généralement des lettres) par une ou plusieurs autres entités.

On distingue plusieurs types de crypto systèmes par substitution :

- ✓ La substitution mono-alphabétique consiste à remplacer chaque lettre du message par une autre lettre de l'alphabet. Comme le chiffrement par décalage.

- ✓ La substitution poly-alphabétique consiste à utiliser une suite de chiffres mono-alphabétique réutilisée périodiquement. Comme exemple le chiffrement de Vigenère.
- ✓ La substitution homophonique permet de faire correspondre à chaque lettre du message en clair un ensemble possible d'autres caractères.
- ✓ La substitution de polygramme consiste à substituer un groupe de caractères (polygramme) dans un message par un autre groupe de caractères.

- Au moyen d'une table (système de Playfair)

- Au moyen d'une transformation mathématique (système de Hill)

- ➢ **Les faiblesses de la méthode de substitution :**

Dans le chiffrement par substitution, la clé est simplement la permutation des 26 lettres alphabétiques. Le nombre de clés est 26 ! Une recherche exhaustive de la clé est donc impossible.

II.3.1.4 Chiffrement par Transposition (permutation) [11] :

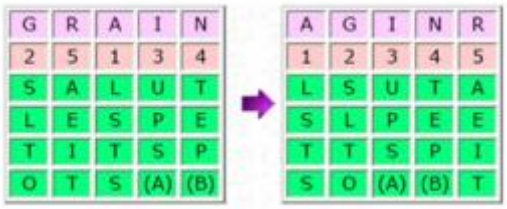
Elles consistent, par définition, à changer l'ordre des lettres. C'est un système simple, mais peu sûre pour de très brefs messages car il y a peu de variantes. Ainsi, un mot de trois lettres ne pourra être transposé que dans 6 (=3!) positions différentes. Par exemple, "col" ne peut se transformer qu'en "col", "clo", "ocl", "olc", "lco" et "loc".

Lorsque le nombre de lettres croît, il devient de plus en plus difficile de retrouver le texte original sans connaître le procédé de brouillage. Ainsi, une phrase de 35 lettres peut être disposée de 35! = 1040 manières différentes. Ce chiffrement nécessite un procédé rigoureux convenu auparavant entre les parties.

Une transposition rectangulaire consiste à écrire le message dans une grille rectangulaire, puis à arranger les colonnes de cette grille selon un mot de passe donné (le rang des lettres dans l'alphabet donne l'agencement des colonnes).

Exemple :

A la table II.3, on a choisi comme clef GRAIN pour chiffrer le message SALUT LES PETITS POTS. En remplissant la grille, on constate qu'il reste deux cases vides, que l'on peut remplir avec des nulles (ou pas, selon les désirs des correspondants).



Tab II.3 : Application d'une transposition

II .3.1.5 Chiffrement de Vernam (masque jetable)

Le chiffrement par la méthode du masque jetable consiste à combiner le message en clair avec une clé présentant les caractéristiques très particulières suivantes :

- ✓ La clé doit avoir la même longueur que le message à chiffrer.
- ✓ Les caractères composant la clé doivent être choisis de façon totalement aléatoire.
- ✓ Chaque clé, ou « masque », ne doit être utilisée qu'une seule fois (d'où le nom de *masque jetable*).

Le principe est alors de combiner clé et message par un XOR bit à bit, le résultat modulo 26 donne le rang de la lettre de texte chiffré.

- ✓ **Exemple :** Si le message est :

MASQUEJETABLE

Et que le morceau de masque (clé) utilisé est :

TBFRGFARFMIKL

Alors le texte chiffré est :

GCYIBKKWZNKWQ

Puisque l'on a :

(M⊕T) mod 26=G

(A⊕B) mod 26=C

(S⊕F) mod 26=Y

II.3.2 La cryptographie moderne :

Si le but de la cryptographie classique est d'élaborer des méthodes permettant de transmettre des données de manière confidentielle, la cryptographie moderne s'intéresse en fait plus généralement aux problèmes de sécurité des communications. Le but est d'offrir un certain nombre de services de sécurité comme la confidentialité, l'intégrité, l'authentification des données transmises. La cryptographie moderne se compose de deux grandes parties : La cryptographie symétrique et la cryptographie asymétrique à base de clés.

Avant de les aborder, il est commode de définir la notion de clé qui sera utilisée tout au long de cette partie.

Une clé: Paramètre constitué d'une séquence de symboles et utilisé, avec un algorithme cryptographique, pour transformer, valider, authentifier, chiffrer ou déchiffrer des données **[4]**.

II.3.2.1 Historique de la cryptographie moderne [12] :

Pendant de nombreuses années, la cryptographie était exclusivement réservée au domaine militaire et diplomatique. La littérature sur le sujet était donc très peu abondante. La première publication fondamentale dans le domaine a été l'article de C laude Shanon 1949/ « the communication thery of secrcy systems ».Dans lequel il jette les bases mathématiques d'un système de communication chiffrée, à partir de la définition d'un nouveau modèle : L a théorie de l'information. Une contribution importante a été ensuite celle de feistel, avec la publication au débit des année 1970 de ses travaux sur les schémas de chiffrement itératifs par blocs qui ont conduit en 1977 ans la proposition de l'algorithme DES comme standard de chiffrement à clé secrète l'accroissement de la sécurité du DES.

L'accroissement de la puissance des ordinateurs ayant remis en cause de la sécurité du DES, il a été remplacé en 2000 par un nouveau standard appelé AES. Cet algorithme est l'aboutissement de recherches récentes notamment dans le domaine de la cryptanalyse. En 1976, après la publication par Diffie et Hellman de l'article : « New Direction in

Cryptography », un nouveau concept révolutionnaire de la cryptographie, qu'est la cryptographie à clé publique, a été introduit.

Plus récemment pour faire face aux nouvelles menaces par le développement des réseaux et la numérisation massive des documents, la cryptographie a dû offrir de nouvelles fonctionnalités : garantie de l'authenticité des messages (provenance et contenu), réalisé par les algorithmes de signature numérique.

Ainsi, la cryptographie moderne offre deux grandes catégories de procédés cryptographiques :

- Algorithmes de chiffrement : servent à protéger la confidentialité des données.
- Algorithmes de signatures : garantissent la provenance et l'intégrité des messages.

II 3.2.2 Chiffrement symétrique ou à clé secrète :

Le principe de chiffrement symétrique se base sur le partage d'une même clé *K* de chiffrement entre deux entités communicantes (voir la figure 8).

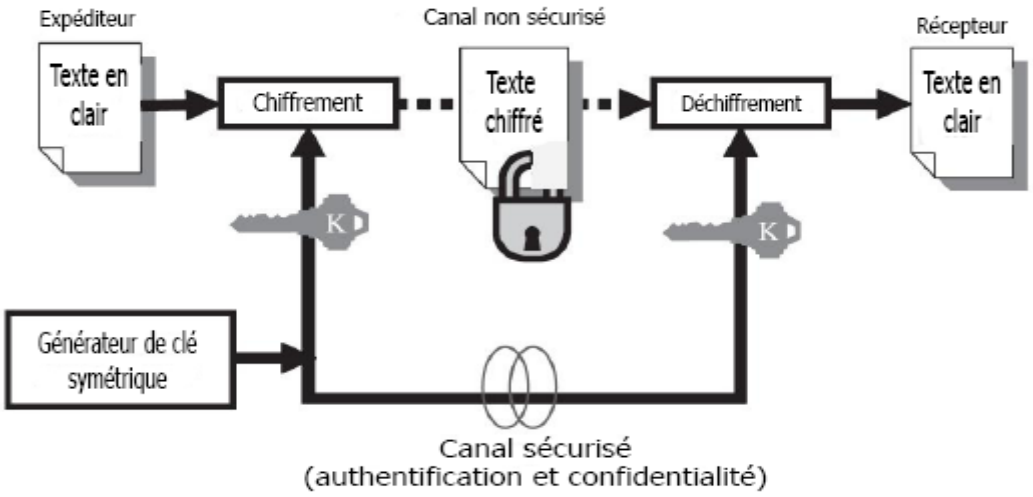


Figure II.1 : Chiffrement symétrique [5].

Les algorithmes de cryptographie symétrique se décomposent en deux sous ensembles, les algorithmes de chiffrement en chaine (en continue) et les algorithmes de chiffrement par blocs.

II.3.2.2.1 Chiffrement en chaine (Flot) :

Ce système chiffre les données bit par bit quelle que soit la longueur du message à coder sans besoin de les découper et/ou attendre la réception entière des données.

La technique utilisée dans cette classe consiste à chiffrer le message à transmettre en effectuant un XOR avec la clé de chiffrement.

Soit ***M*** le message à chiffrer, ***K*** la clé de chiffrement, et $\oplus$ l'opération booléenne XOR, le chiffrement correspondant est :

$M \oplus K = MK$ ou ***MK*** est le message chiffré.

Le déchiffrement se fera alors par :

$$MK \oplus K = M \oplus K \oplus K = M$$

Exemple D'algorithme de chiffrement par flot :

- ✓ **RC4 :**

Est l'acronyme **Revest Cypher** conçu en 1987 par Rivest et dédié aux applications logicielles. Il est largement déployé notamment dans le protocole SSL/TLS et la norme WEP pour les réseaux de sans fil, IEEE 802.11. RC4 présente certaines faiblesses dues à son initialisation, qui est relativement faible, et qui ne prévoit pas de valeur initiale pour la resynchronisation. Employé par exemple avec le protocole de resynchronisation choisi dans la norme IEEE 802.11, RC4 s'avère extrêmement fiable.

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

II.3.2.2.2 Chiffrement par bloc :

Le chiffrement par blocs consiste à fractionner un message ***M*** en blocs de n bits. Ces blocs seront ensuite chiffrés par un algorithme de chiffrement ***F*** et une clé ***k*** extraite d'une clé maître ***K***.

Soient ***M*** le message à chiffrer et ***K*** la clé de chiffrement dont sont extraites les clés k_i et ***F*** la fonction de chiffrement. ***M*** sera découpé en ***r*** blocs de ***n*** bits. Pour chaque bloc b_x de ***M***, le chiffrement se fera de la manière suivante :

$$C_1 = F(k_1 , b_x)$$

F est ensuite itérée avec une nouvelle clé extraite de la clé maître ***K*** pour garantir la sécurité de l'algorithme de chiffrement, ainsi :

$$C_2 = F(k_2 , C_1)$$
$$C_y = F(k_y , C_{y-1})$$

Le déchiffrement se fait avec une fonction ***G***, inverse de la fonction ***F*** et les différentes clé k_i partagées extraites de la clé commune ***K***, de la manière suivante :

$$C_{y-1} = G(k_y , C_y) = G(k_y , F(k_y , C_{y-1}))$$

$$b_x = G(k_1 , C_1)$$

La cryptographie symétrique par blocs est la technique de cryptographie symétrique la plus répandue, utilisée entre autre par les algorithmes de cryptographies comme DES, AES.

1.) L'Algorithme DES (Data Encryption Standard) :

L'algorithme DES, **D**ata **E**ncryption **S**tandard, a été créé dans les laboratoires de la firme IBM Corp. Il est devenu le standard du NIST en 1976 et a été adopté par le gouvernement en 1977 **[21]**. C'est un algorithme de chiffrement symétrique (chiffrement par bloc) basé sur le schéma de *Feistel* qui transforme un bloc de 64 bits en autre bloc de 64 bits avec une clé secrète de 56 bits au moyen de permutations et de substitutions.
La clé du DES est en fait constituée de 64 bits, dont les 56 bits sont générés aléatoirement et utilisés dans l'algorithme. Les huit autres bits peuvent être utilisés pour la détection d'erreurs (dans une transmission par exemple). Chacun des huit bits est utilisé comme bit de parité des sept groupes de 8 bits.

1.1) Chiffrement de DES :

Les grandes lignes de l'algorithme sont les suivantes :

- Fractionnement du texte en blocs de 64 bits (8 octets) ;
- Permutation initiale des blocs ;
- Découpage des blocs en deux parties: gauche et droite, nommées L et R respectivement ;
- Etapes de permutation et de substitution répétées 16 fois (appelées **rondes**) ;
- Recollement des parties gauche et droite puis permutation initiale inverse.

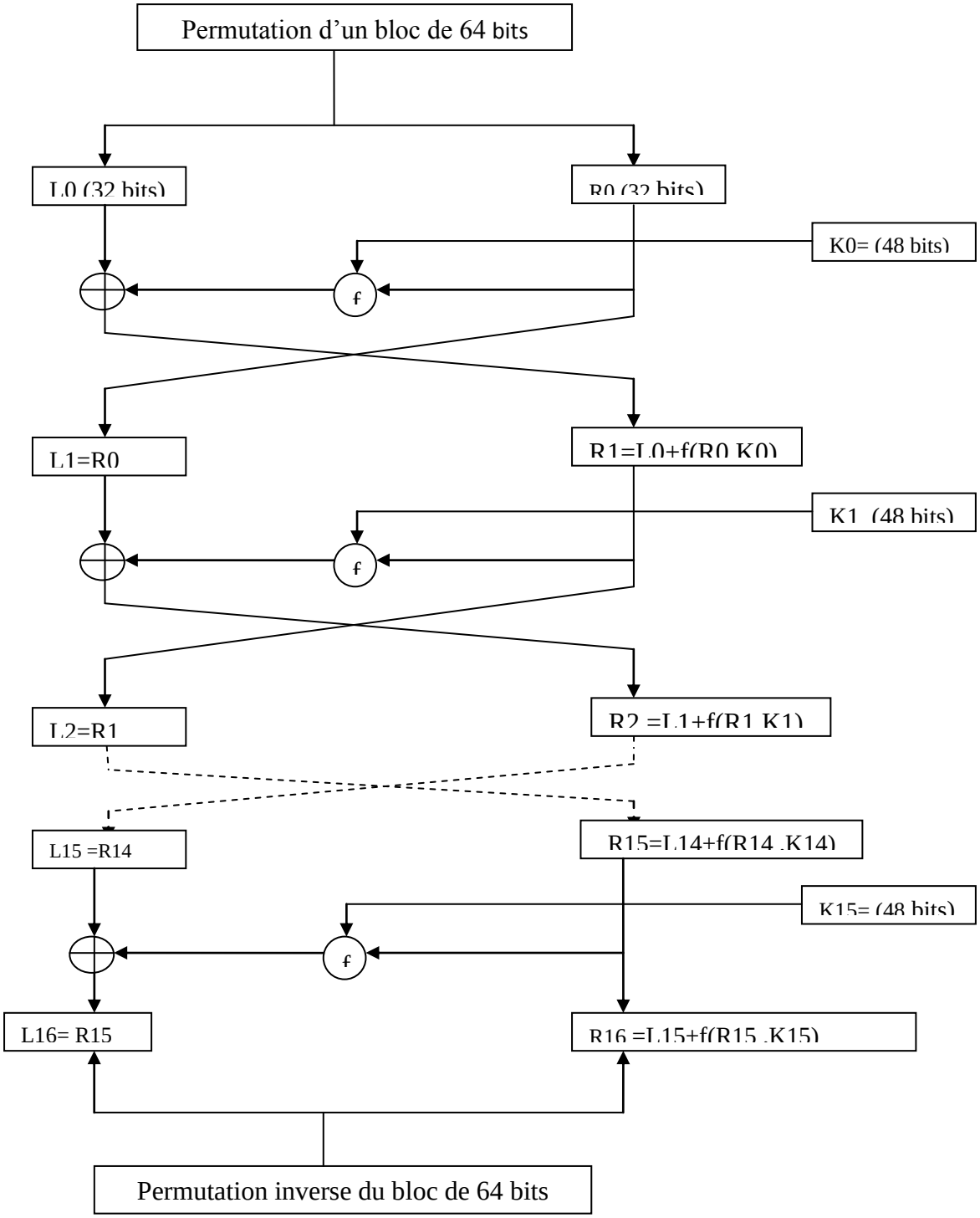


Figure II.2. DES avec ses opérations de chiffrement

1.1.1) Permutation initiale :

Chaque bit d'un bloc de 64 bits est soumis à la permutation initiale pouvant être représentée par le tableau suivant :

58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7

Tab II.4 permutation initiale PI

Ce tableau de permutation indique, en parcourant le tableau de gauche à droit, puis de haut en bas par exemple : la permutation initiale déplace le bit 58 jusqu'a la première position, le bit 50 jusqu'à la second position, etc.

1.1.2) Décomposition en bloc de 32 bits :

Une fois la permutation initiale réalisée, le bloc de 64 bits est décomposé en deux blocs de 32 bits, notés respectivement L0 et R0 pour gauche et droite. On note L0 et R0 l'état initiale de ces deux blocs :

L0							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8

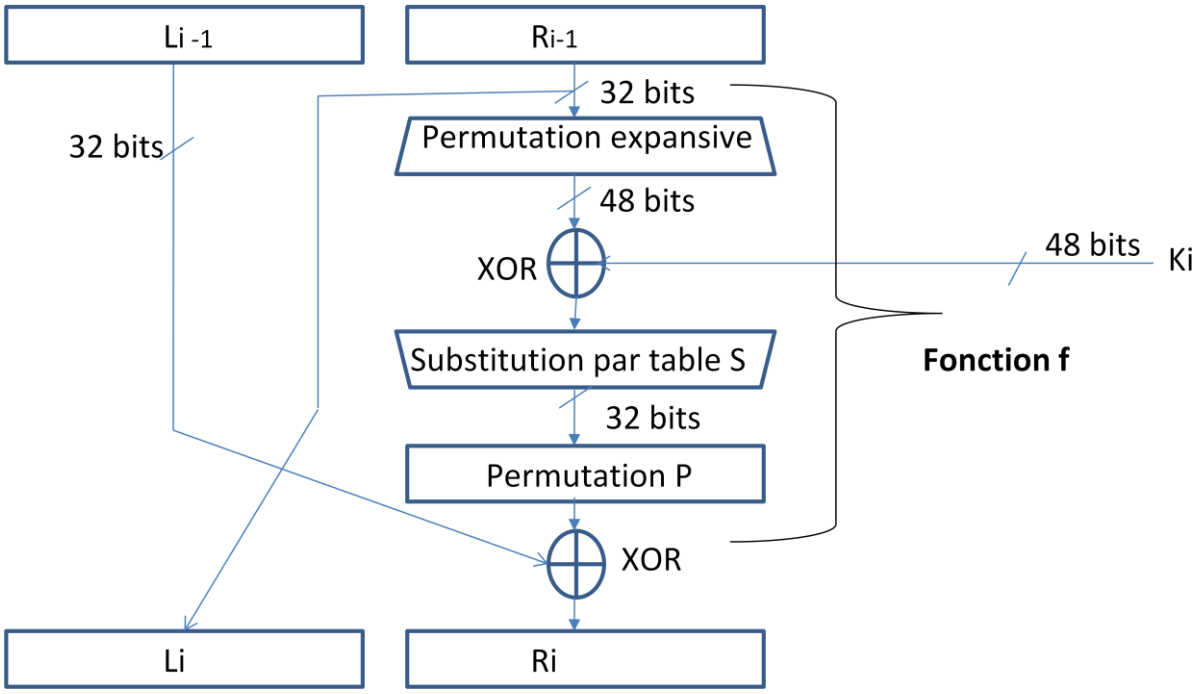
R0							
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Tab II.5 : les blocs gauche et droit de PI

Sachant que L0 contient tous les bits possédant une position paire dans le message initiale, tandis que R0 contient les bits de position impaire.

1.2) Tours de DES :

Les blocs gauches et droits (Li, Ri) sont soumis à un ensemble de transformation itératives appelées round



- $Li = R_{i-1}$
- $Ri = L_{i-1} \oplus f(R_{i-1}, K_i)$

Figure II.3 : les rounds-i de DES

1.2.1) Fonction d'expansion :

Les 32 bit de droite D0 sont étendus à 48 bits grâce à une table d'expansion notée E, dans laquelle les 48 bits sont mélangés et 16 d'entre eux sont dupliques la table donnée ci-dessous.

32	1	2	3	4	5	4	5	6	7	8	9
8	9	10	11	12	13	12	13	14	15	16	17
16	17	18	19	20	21	20	21	22	23	24	25
24	25	26	27	28	29	28	29	30	31	32	1

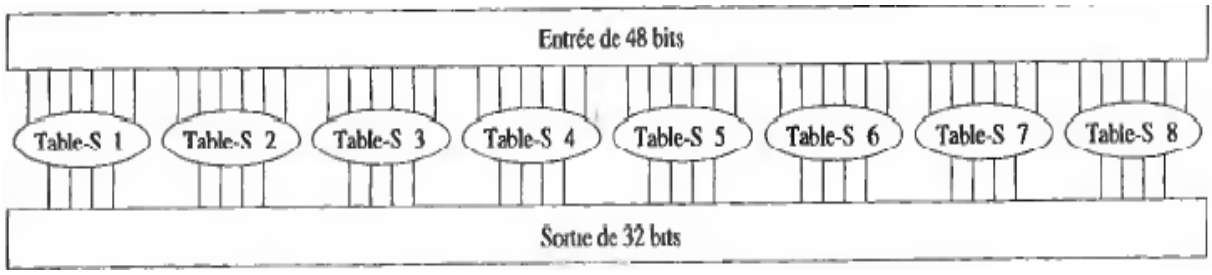
Tab II.6 Table d'expansion E

1.2.2) OU exclusif avec la clé :

Une opération de OU exclusif est effectué entre les 48 bits de matrice résultante (E) et les 48 bits d'une des clés dérivées de la clé principale 56 bits. Le résultat de OU exclusif est une matrice D0 (il ne s'agit pas de D0 de départ) de 48 bits.

1.2.3) Fonction de substitution :

Les 48 bits de résultat de OU exclusif sont ensuite condensés sur 32 bits à l'aide des boites S1 à S8, Chaque table reçoit 6 bits d'entrées et produit 4 bits de sorties, les 48 bits sont devisés en bloc de 6 bits, Chaque bloc est manipulé par une table S différente



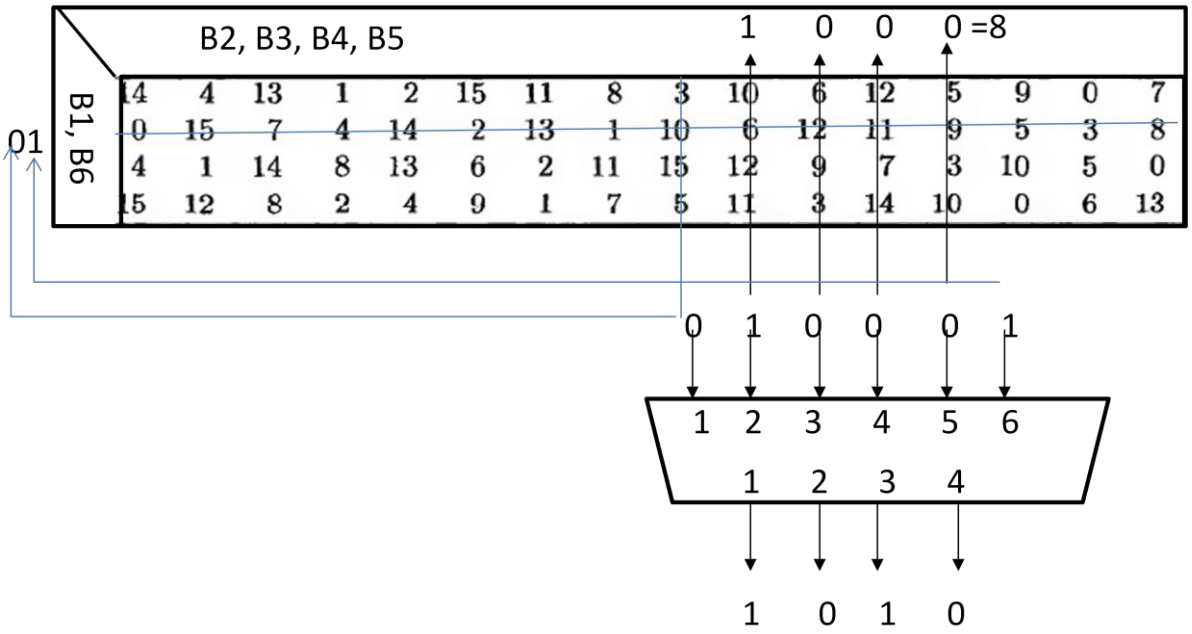
Tab II.7 : S-box de substitution. [23]

Les 6 bits d'entrées de chaque boite de substitution sont définit de la manière suivantes :

- Le premier et le 6^{ime} bit détermine en binaire numéro de ligne de la fonction de sélection (boite de substitution).
- Les autres bits 2 ,3 ,4 et 5 déterminent la colonne.

La sélection d'une ligne se faisant sur deux bits, il y a 4 possibilités (0, 1, 2,3), la sélection de la colonne se faisant sur 4bits, il y a 16 possibilités de 0 jusqu'à 15.

Voici la premier table de substitution Table-S1 est présentée par 4 lignes et 16 colonnes.



Tab II.8 : S1-box

Soit B1, B2, B3, B4, B5, B6 égale à 010001 le 1^{ier} et le 6^{ime} bits donnent 01 c'est-à-dire 1en binaire.les bits 2, 3,4 ,5 donnent 1000 soit 8 en binaire. Donc le résultat de la fonction de sélection est l'intersection de la ligne n° 1 et la colonne n°8, Il s'agit de la valeur 10 soit 1010 en binaire.

Les autres fonctions de sélection sont présentées au- dessus :

S_2																
	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

Tab II.9: S2-box

S_3																
	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

Tab II.10: S3-box

S_4																
	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

Tab II.11: S4-box

S_5	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

Tab II.12 : S5-box

S_6	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

Tab II.13 : S6-box

S_7	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

Tab II.14 : S7-box

S_8	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Tab II.15 : S8-box.

1 .3) Permutation:

Le bloc de longueur 32 bits obtenu de sortie de la table de substitution est enfin soumis à une permutation fixée P avant d'être combiné avec les 32 bits de la partie gauche, Sachant que le résultat de cette opération forme la partie droite du tour actuel.

16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

Tab II.16 : Table de permutation P.

1.4) Ou exclusif :

L'ensemble des résultats en sortie de permutation P est combinée avec la partie gauche G0 de départ par Ou exclusif.

- ✓ **Remarque :**

Toutes les tours (rounds) précédentes sont répétées 16 fois.

1.5) Permutation initiale inverse :

La permutation inverse est la dernière opération avant l'obtention du bloc chiffré, les deux blocs G16 et D16 sont recollés, puis soumis à la permutation initiale inverse, et le résultat en sortie est un bloc de longueur 64 bits.

40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25

Tab II.17 : Table de permutation initiale inverse PI-1

1.6) Génération des clés :

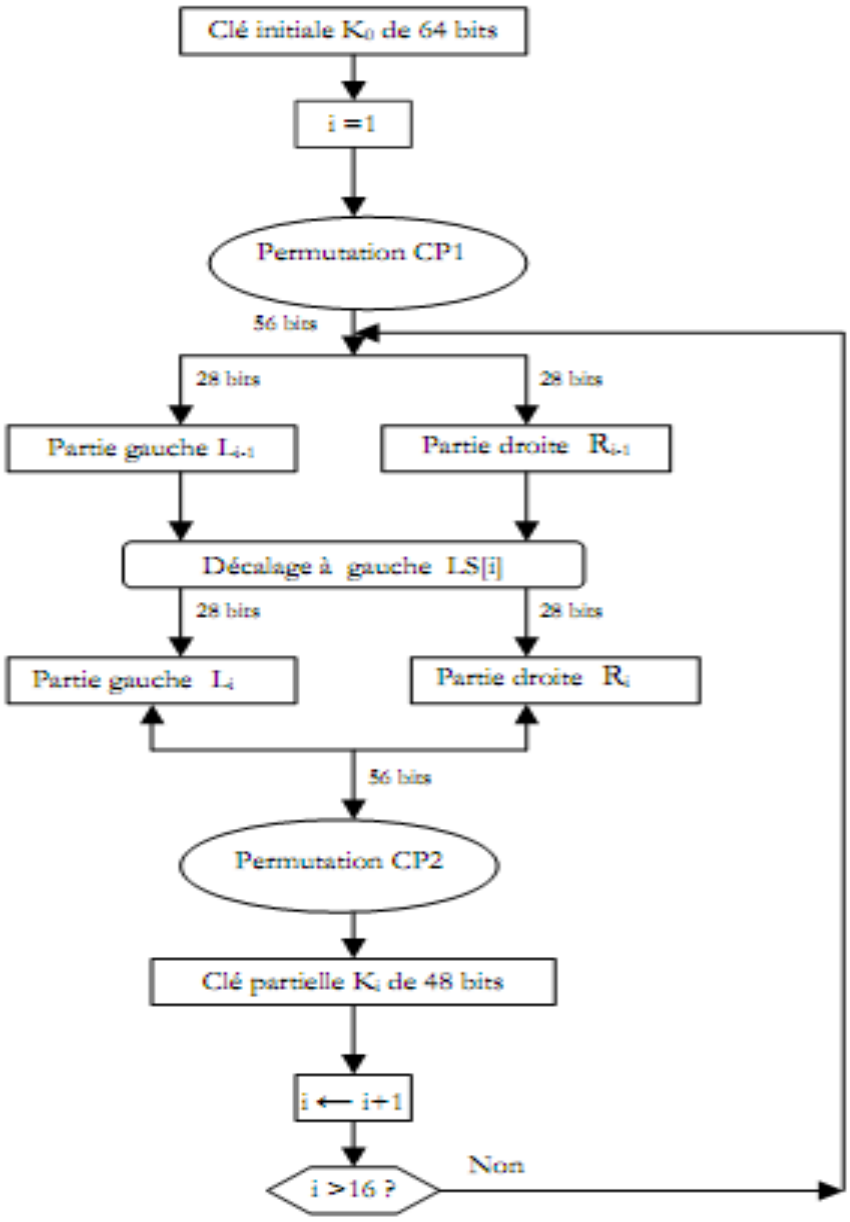


Figure II.4 la diversification des clés en DES [24].

La clé initiale de 64 bits subit à une permutation choisie noté CP-1, est réduite à 56 bits dont les 8 bits de parité servant à vérifier l'intégrité de la clé, La table est présentée ci-dessous :

57	49	41	33	25	17	9	1	58	50	42	34	26	18
10	2	59	51	43	35	27	19	11	3	60	52	44	36
63	55	47	39	31	23	15	7	62	54	46	38	30	22
14	6	61	53	45	37	29	21	13	5	28	20	12	4

Tab II.18 : Table Permutation Choisie CP-1.

La clé résultant de 56 bits est alors devisée en deux blocs (L0, R0) de 28 bits,
Chacun d'eux est décalé à gauche de façon circulaire de un ou de plusieurs bits en fonction du tour actuel.

Ronde	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Nombre de décalages	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Tab II.19 : Nombre de bits de décalages en fonction de tour actuel.

Les deux nouveaux blocs seront regroupés en un bloc de 56 bits avant la nouvelle permutation compressive, noté CP-2, fournissant en sortie une clé K1 sur 48 bits.
Ces 48 bits sont également réordonnée comme indiqué dans la table suivante.

14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

Tab II.20: permutation compressive CP-2.

On répète ces opérations 15 fois pour généré les clés (K2, K3, …K16).

1 .7) Déchiffrement :

Puisque le DES est un processus symétrique le chiffrement est identique au déchiffrement, pour déchiffré on effectue les mêmes opérations que pour le chiffrement sauf que les 16 itérations de la clé doivent être présentées dans l'ordre inverse K16, K15, …K1. Le décalage circulaire sera vers la droite et le nombre de décalage par tour sera : 0, 1, 2, 2, 2, 2, 2, 2, 1, 2, 2, 2, 2, 2, 2, 1.

2.) Le Triple DES :

Triple DES (TDES) aussi appelé 3DES est une variante sécurisée de (DES). Il a d'abord été proposé par IBM en 1978 et défini dans la norme ANSI X9.52. **[25].**

Le Triple DES est un algorithme de chiffrement symétrique par bloc, enchaînant trois applications successives de l'algorithme DES sur le même bloc de données de 64 bits, avec 2 ou 3 clés DES différentes son objectif est de pallier à la faiblisse principale de DES.

- **Chiffrement :**

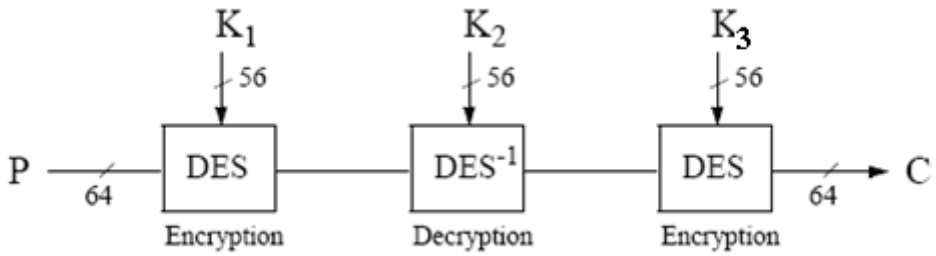


Figure II.5 : Chiffrement de 3DES

E = Encryption Chiffrement DES

D = Decryption Déchiffrement DES

K=Clé

P: plaintext (texte clair)

C : Ciphertext (texte chiffré)

Ciphertext = E_{K3} (D_{K2} (E_{K1} (plaintext)))

Le chiffrement de 3 DES s'effectue en trois étapes:

La premier étape consiste à faire le chiffrement DES avec K1, ensuite un déchiffrement DES avec K2, enfin le chiffrement DES avec K3.

- **Déchiffrement**

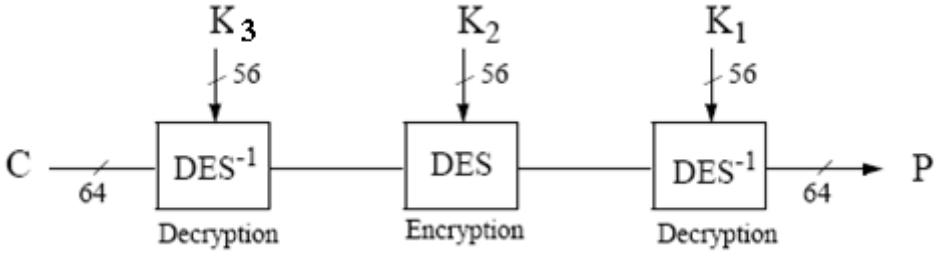


Figure II.6 : Déchiffrement de3 DES

Le déchiffrement consiste à faire l'inverse de chiffrement :

- ✓ **Algorithme AES *(Advanced Encryption Standard*)**:

C'est Standard de chiffrement avancé en français, aussi connu sous le nom de Rijndeal, est un algorithme de chiffrement symétrique Il remporta en octobre 2000 le concours AES, lancé en 1997 par le NIST et devint le nouveau standard de chiffrement pour les organisations du gouvernement des Etats-Unis. Il a été également approuvé par la NSA (National Security Agency) pour les informations top secrètes.

Pour conclure sur cet aspect, on voit que le standard AES répond aux mêmes exigences que le DES mais il est également beaucoup plus sûr et flexible que son prédécesseur. Cet algorithme sera détaille dans le 3^{ime} chapitre.

II.3.2.3 Le chiffrement asymétrique :

Le chiffrement asymétrique appelé aussi chiffrement à clé publique utilise une *paire* de clés pour le cryptage : une clé publique qui chiffre des données et une clé privée ou secrète correspondante pour le déchiffrement. La clé privée doit rester secrète alors que la clé publique doit être diffusée. Un exemple est illustré dans la figure II.7.

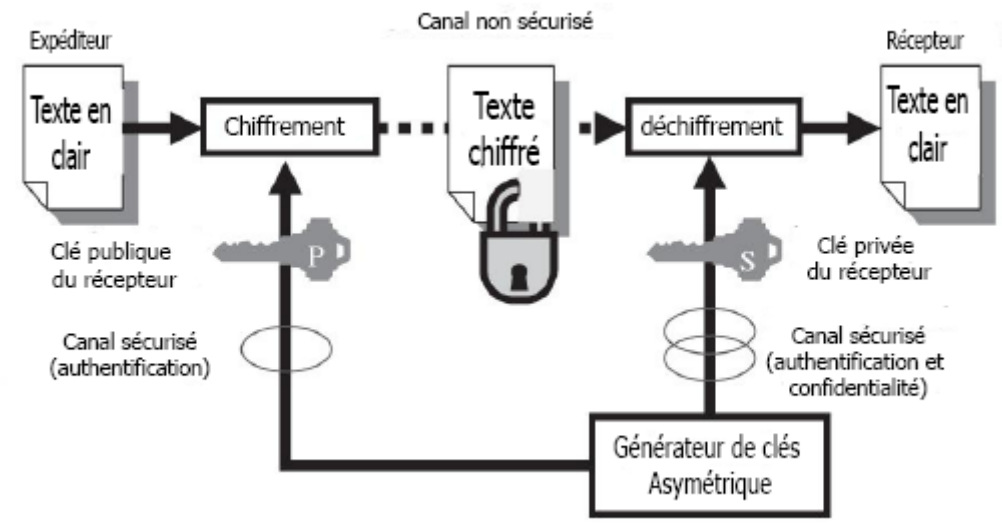


Figure II.7 : Chiffrement asymétrique [5].

Formellement le chiffrement et le déchiffrement de données d'un message entre deux nœuds ***A*** et ***B*** correspondent au mécanisme suivant : soit K_P la clé publique et K_S la clé privée de ***A***, ***F*** la fonction de chiffrement et ***G*** la fonction de déchiffrement. ***A*** diffuse sa clé publique dans le réseau. Soit ***M*** le message que souhaite transmettre ***B*** à ***A***, alors :

$Mk = F(K_P, M)$ où Mk est le message chiffré,

$M \neq G(K_P, Mk)$

B envoie le message M à A qui va ensuite pouvoir le déchiffrer avec sa clé privée :

$M = G(K_S, Mk)$

Parmi les algorithmes asymétriques les plus répondus est RSA :

1) Algorithme RSA

RSA, du nom de ces inventeurs, est un algorithme de chiffrement appartenant à la grande famille "Cryptographie asymétrique".
RSA peut être utilisé pour assurer :

- ✓ la confidentialité : seul le propriétaire de la clé privée pourra lire le message chiffré avec la clé publique correspondante.
- ✓ la non-altération et la non-répudiation : seul le propriétaire de la clé privée peut signer un message (avec la clé privée). Une signature déchiffrée avec la clé publique prouvera donc l'authenticité du message.

Sa robustesse réside dans la difficulté à factoriser un grand nombre.

2) Principe de fonctionnement de RSA :

Si Bob souhaite recevoir des messages en utilisant le RSA, il procède de la façon suivante :

- ✓ **Création des clés :** Bob crée 4 nombres p,q, e et d :
  - p et q sont deux grands nombres premiers distincts. Leur génération se fait au hasard, en utilisant un algorithme de test de primalité probabiliste.
  - e est un entier premier avec le produit (p-1)(q-1).
  - d est tel que ed=1 modulo (p-1)(q-1). Autrement dit, ed-1 est un multiple de (p-1)(q-1). On peut fabriquer d à partir de e, p et q, en utilisant l'algorithme d'Euclide.

- ✓ **Distribution des clés :** Le couple (n,e) constitue la clé publique de Bob. Il la rend disponible par exemple en la mettant dans un annuaire. Le couple (n,d) constitue sa clé privée. Il la garde secrète.
- ✓ **Envoi du message codé :** Alice veut envoyer un message codé à Bob. Elle le représente sous la forme d'un ou plusieurs entiers M compris entre 0 et n-1. Alice possède la clé publique (n,e) de Bob. Elle calcule $C=M^e \bmod n$. C'est ce dernier nombre qu'elle envoie à Bob.
- ✓ **Réception du message codé** : Bob reçoit C, et il calcule grâce à sa clé privée $D=C^d \pmod n$. D'après un théorème du mathématicien Euler, $D=M^{de}=M \pmod n$. Il a donc reconstitué le message initial.

II.4 Fonction de hachage

Une fonction de hachage est une fonction mathématique utilisée pour vérifier l'intégrité des données. En fait Il faut être capable de vérifier que les données n'ont pas été altéré par une personne malveillante pendant l'envoi.

Une fonction de hachage est fondamentale pour la cryptographie à clé publique, Elle convertit une chaine de caractères de longueur quelconque vers une chaine de taille fixe qui varie selon les algorithmes (128 bits pour MD5 et 160 bits pour SHA-1). La chaine produite est appelé empreinte (digest en anglais) ou condensé de la chaine initiale. Cette fonction **H(m)=h** doit être une fonction à sens unique ou "one-way hash function" en anglais C'est-à-dire qu'il doit être facile de trouver **h** à partir de **m,** mais très difficile de trouver **m** à partir de **h**. Elle doit aussi être très sensible pour qu'une petite modification de message entraine une grande modification de l'empreinte. En envoyant le message accompagne de son empreinte, Le destinataire peut ainsi s'assurer de l'intégrité du message en recalculant le résumé à l'arrive et en le comparant à celui reçu. Si les deux résumes sont différents, cela signifie que le fichier à été modifie par une tierce personne.

- ✓ **Noté bien** :

Si la fonction de hachage est associée à une clé privé (chiffrement symétrique), elle permet le calcule d'un **MAC** (**M**essage **A**uthentification **C**ode) pour assure l'intégrité des données et l'authentification de la source, plus précisément il est réalisé au moyen d'une fonction de hachage appliqué au message + la clé privé. Si elle est associée à un

chiffrement asymétrique elle permet le calcule de la signature pour assurer : l'intégrité des données, authentification et non-répudiation de la source.

II.4.1 Présentation des fonctions de la famille MD-SHA [8]

II.4.1.1 MD4 (Message Digest 4)

MD4 est une fonction de hachage conçue par le professeur Ronald Rivest du MIT. La taille de la signature est de 128 bits. L'algorithme a été abandonné au profit du MD5 après la découverte de faiblesses dans sa conception. D'autres attaques encore plus efficaces ont suivi, notamment par le service du chiffre allemand et encore l'équipe chinoise à l'origine de l'attaque sur MD5.

II.4.1.2 MD5 (Message Digest 5)

MD5 est une fonction de hachage cryptographique qui permet d'obtenir pour chaque message une empreinte numérique (en l'occurrence une séquence de 128 bits) avec une probabilité très forte que, pour deux messages différents, leurs empreintes soient différentes. En 1996, une faille grave (possibilité de créer des collisions à la demande) est découverte et indique que MD5 devrait être mis de côté au profit de fonctions plus robustes.

En 2004, une équipe chinoise découvre des collisions complètes. MD5 n'est donc plus considéré comme sûr au sens cryptographique. Leur attaque a permis de découvrir une collision complète sans passer par une méthode de type brute-force. La sécurité du MD5 n'étant plus garantie selon sa définition cryptographique, les spécialistes recommandent d'utiliser des fonctions de hachage plus récentes comme le SHA-256.

MD5 reste encore très utilisé comme outil de vérification lors des téléchargements. Les sites affichent encore souvent la signature en MD5 (128 bits) de leurs fichiers, bien que SHA-1 (160 bits) le remplace de plus en plus.

II. 4.1.3 SHA-1 (Secure Hash Algorithm 1)

SHA-1 a été conçu par la National Security Agency des États-Unis (NSA), et publiée par le gouvernement des États-Unis comme un standard. SHA-1 défini en 1995 et produit un

condensat de 160 bits. SHA-1 est le successeur du SHA-0 (1993) qui a été rapidement mis de côté par le NIST pour des raisons de sécurité insuffisante.

En février 2005, Bruce Schneier a fait état d'une attaque sur la version complète du SHA-1 par l'équipe chinoise de Wang, Yin et Yu. Leur méthode permet de trouver une collision dans le SHA-1 complet de 128 bits avec 2^{69} opérations. Ayant perdu une longueur d'avance dès l'annonce de l'attaque de Wang, SHA-1 a été retiré progressivement des applications cryptographiques au profit de SHA-256 ou des autres fonctions de hachage.

II. 4.1.4 SHA-2 (Secure Hash Algorithm 2)

SHA-2 à été publié récemment et est destiné à remplacer SHA-1. Les différences principales résident dans les tailles de hachés possibles : 256, 384 ou 512 bits. Il sera bientôt la nouvelle référence en termes de fonction de hachage.

En 2005, des problèmes de sécurité de SHA-1 ont été mis en évidence : il existe pour la recherche de collisions une attaque théorique nettement plus rapide que l'attaque générique des anniversaires sur les fonctions de hachage. Bien que l'algorithme de SHA-2 partage des similarités avec celui de SHA-1, ces attaques n'ont actuellement pas pu être étendues à SHA-2. Le NIST a cependant organisé un concours pour sélectionner une nouvelle fonction de hachage, SHA-3. Le concours a débouché fin 2012 sur le choix d'une nouvelle famille de fonctions dont la conception est très différente de SHA-1 et de SHA-2. La nouvelle famille de fonctions est présentée comme un autre choix possible, elle ne remet pas en cause l'utilisation de SHA-2 du moins dans l'immédiat.

II.5 Signature numérique :

Les fonctions de hachage permettent de s’assurer de l’intégrité d’un message mais un autre problème se pose : comment être certain que personne n’a usurpé l’identité de l’expéditeur pour vous envoyer un message ? Ou que l’expéditeur ne va pas nier vous de message qui à envoyé ?.

Le principe de la signature numérique consiste à applique une fonction de hachage sur une portion de message, ensuite le code produit crypté avec la clé privée de l’émetteur et rajouter au message. Lorsque le destinataire reçoit le message, il décrypte ce code grâce à la clé publique de la source puis il compare ce code à un autre code qu’il calcule grâce au message

reçu. Si les deux correspondent, le destinataire sait que le message n'a pas été altéré et que son intégrité n'a pas été compromise. Le destinataire sait aussi que le message provient de l'émetteur puisque seul ce dernier possède la clé privée qui a crypté le code.

II.6 Système PGP

Dans la plupart des applications actuelles, la meilleure solution consiste à utiliser un système hybride, qui combine la cryptographie à clé publique et à clé privé. Le plus connu de ces systèmes est le PGP.

Dans PGP, la cryptographie à clé publique permet une distribution de clés efficace tandis que la cryptographie à clé privé, offre une rapidité de chiffrement consommant le minimum d'énergie.

II. 6.1 Chiffrement PGP

PGP (Pretty Good Privacy) est un programme de cryptage créé par Philip Zimmermann [ZIM94].

Le système de PGP est un système hybride que l'on peut classer dans les systèmes à « clé de session ». PGP est un système qui utilise à la fois le principe du chiffrement à clé privée IDEA et le principe du chiffrement à clé publique RSA.

Considérons les différentes étapes du transfert d'un message crypté avec PGP de l'expéditeur A vers le destinataire B.

(i) A doit envoyer le message crypté à B.

(ii) B crée une paire de clé via l'algorithme RSA. Il transmet sa clé publique à A.

iii) A saisit le texte en clair à envoyer. Ce texte est tout d'abord compressé ce qui offre un double avantage :

-La taille des données à transférer est réduite,

-Les risques de décryptage sont minimisés (la plupart des techniques de cryptanalyse se base sur le texte en clair obtenu. Si le texte obtenu est un texte compressé il est, par exemple, plus difficile de calculer la probabilité de retrouver telle ou telle lettre).

Il faut noter que la compression n'est pas systématique. Si le taux de compression d'un fichier n'est pas satisfaisant ou si le fichier est trop petit, cette étape n'est pas réalisée.

(iv) Puis, A crée aléatoirement une clé secrète. L'expéditeur chiffre le texte avec cette clé. Le texte ainsi chiffré pourra être déchiffré avec la même clé. Dans PGP, le message est alors crypté selon un système symétrique (à clé secrète).

(v) Le destinataire B ne connaissant pas cette clé, elle va lui être envoyée avec le message crypté. Toutefois pour éviter qu'elle soit interceptée, la clé sera également cryptée à l'aide de la clé publique de B. La clé privée secrète est cryptée avec la clé publique de B selon un système asymétrique (à clé publique).

Finalement, le résultat obtenu contient :

-le texte chiffré avec la clé secrète,

-la clé secrète chiffrée avec la clé publique RSA du destinataire.

A la réception du message, le destinataire utilise sa clé privée RSA pour retrouver la valeur de la clé secrète. Il utilise la clé obtenue pour déchiffrer le message reçu.

Toutes ces étapes sont illustrées au-dessus :

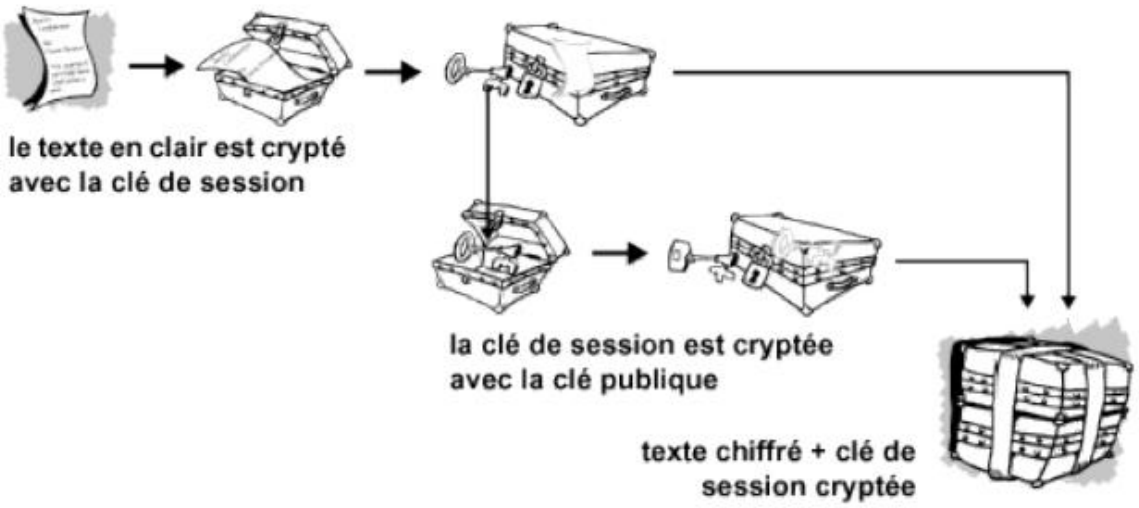


Figure II.8: Fonctionnement de chiffrement PGP [7]

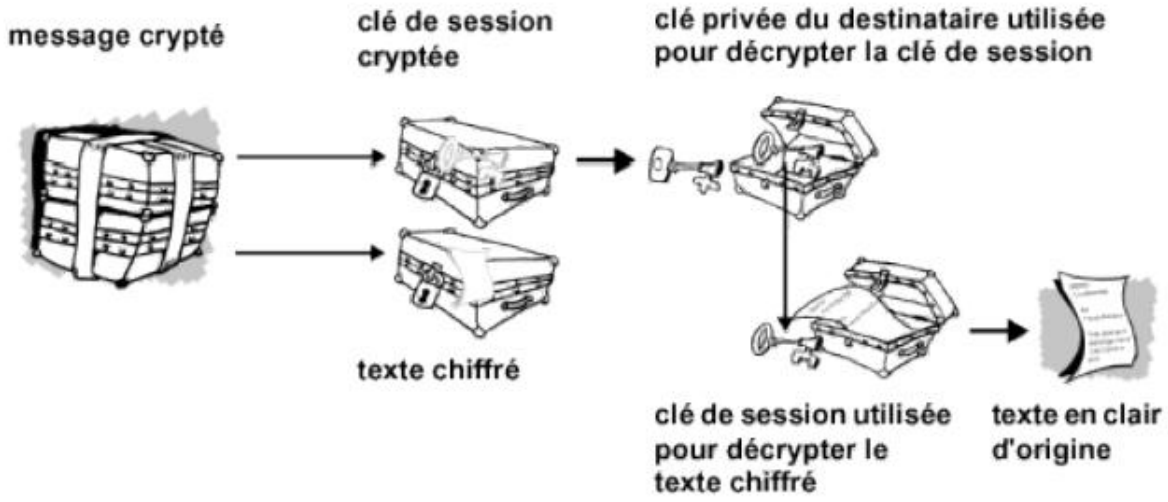


Figure II.9 : Fonctionnement de déchiffrement PGP [7]

II.6.2 Avantages PGP:

-La rapidité : le message est chiffré par un cryptage symétrique. La clé secrète est chiffrée de façon asymétrique. Toutefois le volume de données que représente cette clé est négligeable par rapport au volume de données que représente le message. Par conséquent, le temps de chiffrage global est proche de celui d'un système symétrique.

-Une plus haute sécurité qu'un système à clé symétrique : en effet, dans un système à clé privée standard, le canal d'échange de la clé est le point faible du système. Si l'on désire changer de clé afin de minimiser les risques, cela nécessite de définir un moyen d'échanger cette nouvelle clé, opération difficile à mettre en pratique. Dans PGP en revanche, la clé utilisée pour coder le message est nouvelle pour chaque message. Ce qui implique que pour effectuer une attaque il est nécessaire de casser au choix :

- Autant de clés privées que de messages,
- le système de clé RSA, ce qui rend finalement PGP plus résistant qu'un système à clé privée classique.

II.7 Comparaison des algorithmes symétrique et asymétrique :

Chacune de ces deux primitives de chiffrement possède ses propres avantages et inconvénients. Les systèmes symétriques nécessitent le partage d'un secret entre les interlocuteurs tandis que la découverte des systèmes asymétrique a permis

de s'affranchir de cette contrainte. Mais elle n'a pas pour autant apporté une solution définitive, dans la mesure où tous les algorithmes de chiffrement à clé publique, de par leur lenteur, ne permettent pas le chiffrement en ligne.

Le tableau **Tab II.21** ci-dessous résume les avantages et les inconvénients de chacune d'elles.

Cryptographie symétrique		Cryptographie asymétrique
Avantages	• Vitesse de traitement élevée • Clés relativement courtes. • Permet de concevoir différents mécanismes cryptographiques (fonctions de hachage, …etc.)	• Seule la clé secrète a besoin d'être conservée de manière secrète. • Une paires de clés(publique/secrète) peut être utilisée plus longtemps qu'une clé symétrique. • Assure la non-répudiation dans les schémas de signature numérique ; • Gestion efficace des clés.2n clés sont nécessaires dans un réseau de n utilisateurs.
Inconvénients	• Dans une communication entre deux parties, la clé doit rester secrète des deux cotés. • Complexité de la gestion des clés dans un réseau de n entités, on doit gérer, n*(n-1)/2 clés. • Impossibilité de garantir la propriété de non-répudiation dans les schémas de signature électronique.	• Performances moins bonnes que celles fournies par les systèmes symétriques. • Taille des clés, plus grand que celle des systèmes symétriques. • Nécessité de la mise en place d'infrastructures afin d'éviter les attaques par milieu.

Tab II.21 Comparaison entre le chiffrement, symétrique et asymétrique.

II .7.1 Avantages et inconvénients de chaque algorithme symétrique et asymétrique :

	Algorithme	Avantages	Inconvénients
Algorithmes symétriques	DES	• Chiffrement très rapide • Implémentation matérielle et logicielle et très simple.	• La faiblisse réside dans la longueur de la clé 56 bits,(recherche exhaustive de la clé en 2^{56} essais). • Taille des blocs 64 bits devenu court et présente des risques d'attaques en distinguabilité 2^{32}
	3-DES	• Plus sur puisque l'éspace des clés est beaucoup plus grand.	• Trois fois plus lent que le DES . • Le problème lié à la taille du bloc subsist.
	IDEA	• Implémentation hardware sont simplement légèrement plus rapide	• Il existe un nombre élevé de clés faible ou semi-faible.
	RC4	• Le chiffrement très rapide	• Il existe de large ensemble de clé dites faible • Une faille « Known IV attack » telle que IV signifie Initiale Value
	Blowfish	• Le chiffrement très rapide	• Des failles découvertes mais ne sont pas exploitable.
	AES	• Une recherche exhaustive de la clé n'est en absolument pas envisageable en un temps limité (aucune attaque ne connu à ce jour) • Très efficace en termes de rapidité. • Ces besoin en ressources mémoire sont également très faibles • Il est très flexible d'implémentation, Cela induit une grande variété	• Recherche exhaustive de la clé en 2^{128} essais.

		de plateforme et d'application. • Il est possible de l'implémente aussi bien sous forme logicielle que matérielle	
Algorithme asymétrique	RSA	• Longueur de clés variables 1024,2048bits Utilisé pour la signature	Lenteur quand on veut chiffrer et déchiffrer un nombre important de données (communication téléphoniques, …).

Tab II.22 Avantages et inconvénients de chaque algorithme Symétrique et Asymétrique

II .8 Conclusion

Dans ce chapitre, nous avons étudié les l'évolution de la cryptographie de temps classique au temps moderne, et aussi ses différents algorithmes nécessaires pour la protection des informations personnelles ou privés.

Nous détaillerons dans le chapitre qui va suivre le principe et le fonctionnement de ces algorithmes de chiffrement symétrique AES.

Chapitre III

Analyse et Conception

III.1. Introduction :

Nous avons vu dans ce qui précède les différents concepts de la sécurité informatique et de la sécurité basé sur la cryptographie et on a conclus que le principe de la cryptographie est de s'assurer que les données sensibles stockées ou échangées via des réseaux soient uniquement lisibles par le destinataire et qu'en aucun cas elles ne puissent être lues par une autre personne.

Essentielle aux systèmes d'informations actuels, la cryptographie procure des moyens de protection des données par des algorithmes cryptographiques assurant la confidentialité mais aussi l'authentification et l'intégrité des données. Les algorithmes cryptographiques sont des fonctions mathématiques très difficiles à inverser sans une information particulière, tenue secrète, appelée clé. La sécurité repose donc, en pratique, sur la difficulté à retrouver la clé secrète à partir d'informations publiques. Et l'objectif de la cryptanalyse d'estimer cette difficulté, et ainsi d'évaluer la sécurité des algorithmes cryptographiques.

Dans ce contexte ce travail est réalisé, pour renforcer l'algorithme de chiffrement symétrique

II.2. Présentation du projet :

III.2.1. Description :

Ce projet consiste à la réalisation d'un logiciel de cryptage, qui assure le chiffrement et le déchiffrement de données, en proposant un algorithme de cryptage symétrique, qui repose sur des formules mathématiques.

L'objectif principal de ce projet, est de sécuriser les données à stocker sur une machine ou bien à transmettre sur un réseau, pour faire face à ceux qui ont un but de falsifier ou de détruire ces données en utilisant la technique de cryptographie symétrique vue précédemment.

L'application à réaliser doit garantir les critères de la sécurité informatique tel que :

- La confidentialité des données cryptées.
- L'intégrité des informations décryptées.
- La disponibilité de l'information (les données peuvent être cryptées ou décryptées par le logiciel de façon indépendante du moment et de la machine sur laquelle il est utilisé).

En plus de ces critères, notre application doit offrir une interface conviviale et simple d'utilisation.

- ✓ **Présentation général de l'algorithme AES :**

L'AES (**A**dvanced **E**ncryption **S**tandard) est, comme son nom l'indique, un standard de cryptage symétrique destiné à remplacer le DES (Data Encryption Standard) qui est devenu trop faible au regard des attaques actuelles, c'est une technique de cryptage à clé symétrique

L'algorithme AES utilise une des trois longueurs de clé de codage (mot de passe) suivantes : 128, 192 ou 256. Chaque taille de clé de cryptage utilise un algorithme légèrement différent, ainsi les tailles de clé plus élevées offrent non seulement un plus grand nombre de bits de brouillage de données, mais également une complexité accrue de l'algorithme.

Historiquement, le développement de l'AES a été instigué par le NIST (National Institue of Standards and Technology). Il est également approuvé par la NSA (National Security Agency) pour l'encryptions des informations dites très sensibles.

Cet algorithme suit les spécifications suivantes :

- L'AES est un standard, donc libre d'utilisation, sans restriction d'usage ni brevet.
- C'est un algorithme de type symétrique
- C'est un algorithme de chiffrement par blocs
- Il supporte différentes combinaisons [longueur de clé]-[longueur de bloc] : 128-128, 192-128 et 256-128 bits (en fait, l'AES supporte également des tailles de blocs variables, mais cela n'est pas retenu dans le standard)

- ✓ **Caractéristiques et points forts de l'AES**

Le choix de cet algorithme répond à de nombreux critères plus généraux dont nous pouvons citer les suivants :

- Sécurité ou l'effort nécessaire pour une éventuelle cryptanalyse
- Puissance de calcul qui entraine une grande rapidité de traitement
- Besoins en ressources et mémoire très faibles
- Flexibilité d'implémentation, cela inclut une grande variété de plateformes et d'applications ainsi que des tailles de clés et de blocs supplémentaires

- Compatibilité hardware et software, il est possible d'implémenter l'AES aussi bien sous forme logicielle que matérielle
- Simplicité, le design de l'AES est relativement simple

III.2.2. Principe de fonctionnement cas (AES_128) :

La cryptographie à algorithmes symétriques utilise généralement la même clé (formule de cryptage) pour les processus de chiffrement et de déchiffrement, cette clé est appelée secrète car toute la sécurité de l'ensemble est directement liée au fait que cette clé reste secrète, car on considère l'algorithme de chiffrement connu de tous.

L'algorithme utilisé reçoit en entrée un bloc de 128 bits **(plaintext P)** qu'il transforme en blocs cryptés de 128 bits **(C)** par une séquence de nombre d'opérations **SubByte( ), ShiftRows ( ) ,MixColumns(),AddRoundKey( )**, ou "rounds", à partir d'une clé de 128 bits,

Avec dix ronds, Et le déchiffrement est effectué dans l'ordre inverse. A la fin de ce traitement, le bloc de données en sortie est considéré comme étant crypté en cas de chiffrement, et décrypté en cas de déchiffrement.

III.3. Description de l'algorithme :

L'activité de conception consiste à enrichir la description du logiciel de détails d'implémentation afin d'aboutir à une description très proche d'un programme, pour cela nous allons détailler le fonctionnement des deux opérations: cryptage et décryptage.

III.3.1. L'algorithme de chiffrement :

On découpe les données et les clés en octets et on les place dans des tableaux. Les données comportent td = 16 octets p0, qui sont classés dans un tableau ayant 4 lignes et 4 colonnes. Le tableau est rempli colonnes par colonnes.

De même la clé est découpée en 16 octets, Ces octets sont aussi classés dans un tableau de 4 lignes et 4 colonnes

Le système AES effectue plusieurs tours d'une même composition de transformations.
À partir de la clé initiale **K**, le système crée **nr + 1** clés de tour ayant chacune 16 octets

(nr dans notre cas = 10)

Ces clés seront stockées dans un tableau unidimensionnel **TK** et seront notées.

La procédure suivante décrit le fonctionnement global du système AES. Elle prend en entrée un tableau de données **St (texte clair)** qui est modifié par la procédure et renvoyé en sortie (texte chiffré) :

- **Procédure générale :**

Entrée : le tableau St et la clé K

Sortie : le tableau St modifié AES(St,K)

début

KeyExpansion(K, TK) ;

AddRoundKey(St, TK[0] ;

pour (i = 1 ; i < nr; i + +) **Round**(St, TK[i]) ;

FinalRound(St, TK[nr]) ;

Fin

- **La procedure round :**

Entrée : le tableau d'état St et une clé de tour T

Sortie : le tableau St modifié

Round(St, T)

Début

SubBytes(St) ;

ShiftRows(St) ;

MixColumns(St) ;

AddRoundKey(St, T) ;

Fin

- **La procédure FinalRound :**

Entrée : le tableau d'état St et une clé de tour T

Sortie : le tableau St modifié

FinalRound(St, T)

début

SubBytes(St) ;

ShiftRows(St) ;

AddRoundKey(St, T) ;

Fin

La figure suivante, illustre le processus de chiffrement adopté par notre application dont les étapes sont décrites en détail dans le paragraphe qui suit la figure :

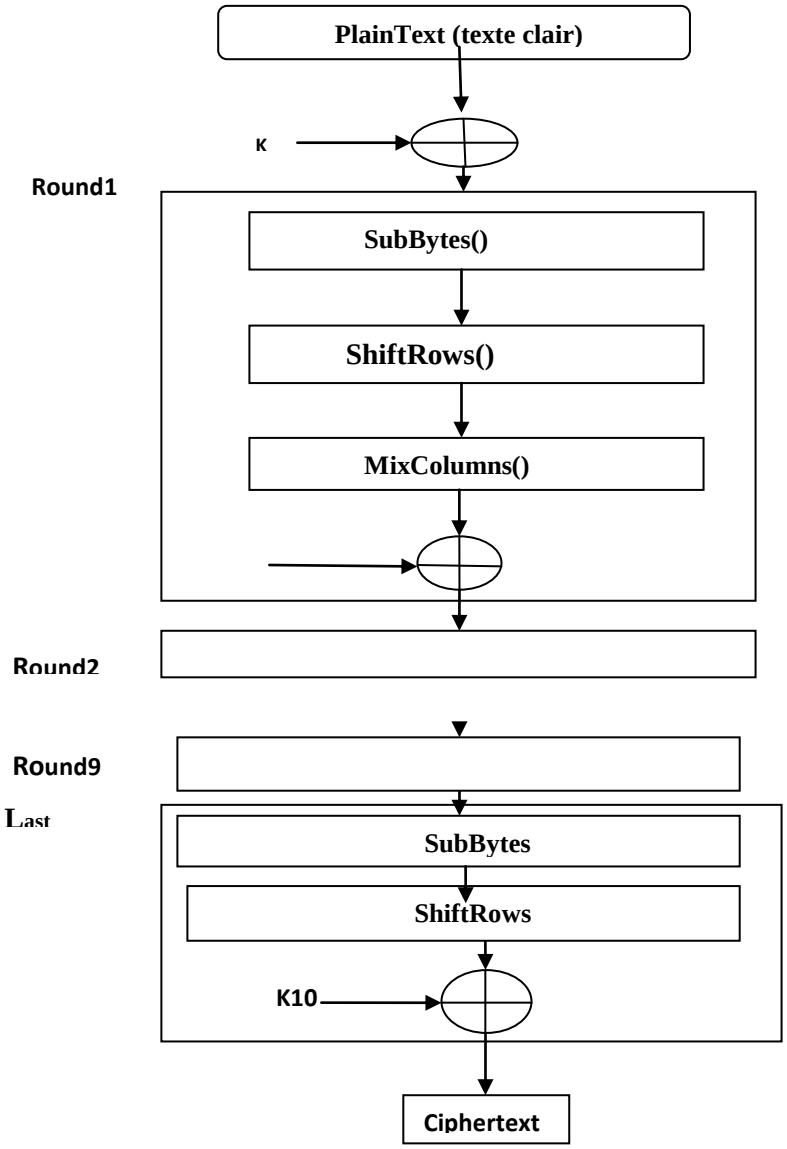


Figure III.1: Processus de chiffrement.

Remarque : Le signe + entouré d'un cercle désigne l'opération de OU exclusif (XOR).

Pour crypter des données, notre algorithme de cryptage suit 5 étapes, qui sont :

1) **Etape SubBytes ( )** :

Il s'agit d'une substitution non-linéaire d'octets : les 128 bits sont répartis en 16 blocs de 8 bits (8 bits=un octet), eux même dispatchés dans un tableau 4×4. Chaque octet est remplacé par

un autre octet choisi dans une table particulière une Boite-S (S-Box). Il utilise une opération sur le corps fini à 256 élément.

La figure suivante montre la transformation SubBytes() appliquer indépendamment à chacun des octets de l'Etat en utilisant une table de substitution

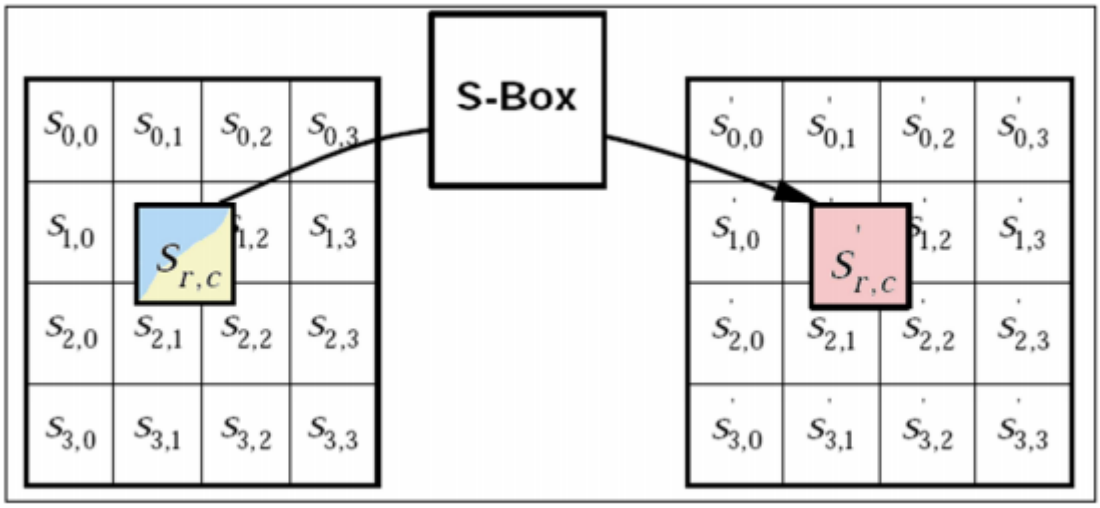


Figure III.2 :SubBytes() applique le S-box pour chaque octet de l'état.

La table S-box utilisée par cette fonction est représentée sous forme d'un tableau de 16 lignes et 16 colonnes en hexadécimales comme montre ci-dessus :

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Table III.1 : S-Box.

Par exemple, si $S_{1,1}$= {53},

$S'_{1,1}$ =SubBytes ($S_{1,1}$)= {ed}.

C'est à dire la valeur de substitution est déterminé par l'intersection de la ligne d'indice «5» et la colonne d'indice «3»

2) ShiftRows ( ) :

Est une fonction opérant des décalages de lignes, (Typiquement elle prend l'entrée en 4 morceaux de 4 octets et opère des décalages vers la gauche sur les trois 3 dernières lignes : la 2ème ligne est décalée d'une colonne, la 3ème ligne de 2 colonnes, et la 4ème ligne de 3 colonnes, Donc $S'_{r,c} = S_{r,(c+r) \bmod 4}$

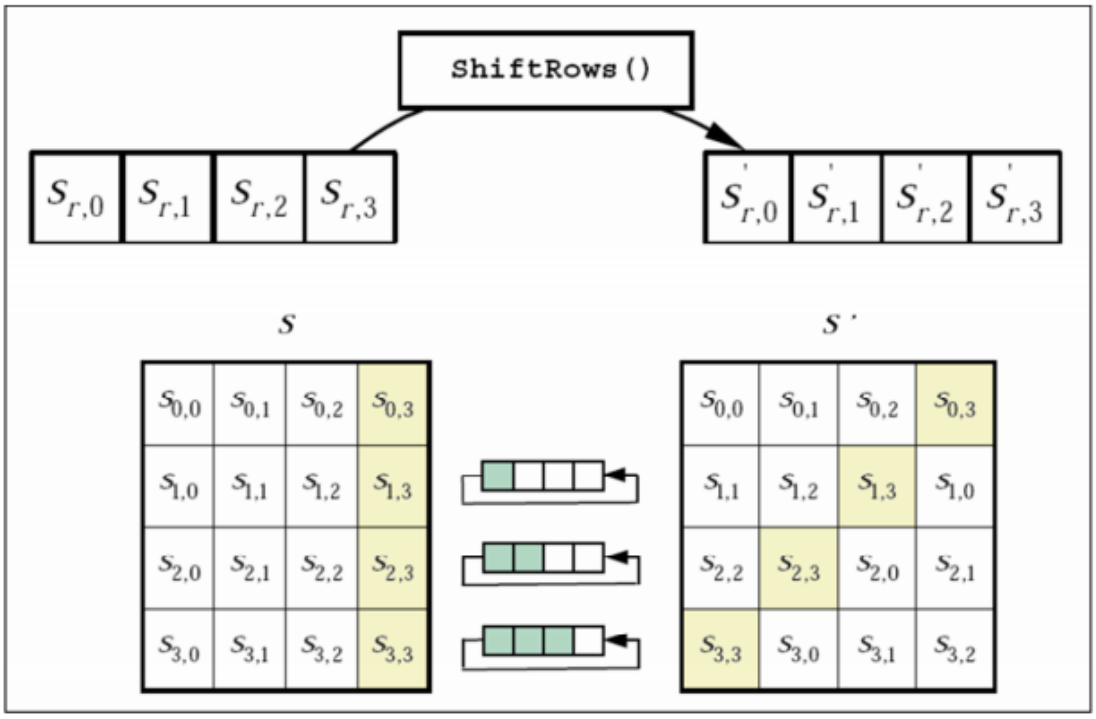


Figure III.3 : ShiftRows ( ) décale cycliquement les trois 3 dernières lignes.

3) MixColumns ( ) application linéaire garantissant une bonne diffusion :

Les colonnes sont traitées comme des polynômes de 4 termes dans GF2^8, l'étape MixColumns consiste alors à effectuer pour chaque colonne une multiplication par un polynôme

$C(X) = 3X^3 + X^2 + X + 2$.fixé suivi d'une réduction modulo le polynôme $X^4 + 1$. Dans MixColumns, on réalise donc l'opération:

$$S'(X) = C(X) \times S(X) mod\ (X^4 + 1) \leftrightarrow \begin{bmatrix} S'_{0,C} \\ S'_{1,C} \\ S'_{2,C} \\ S'_{3,C} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ O3 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} S_{0,C} \\ S_{1,C} \\ S_{2,C} \\ S_{3,C} \end{bmatrix}$$

La figure suivante illustre la transformation appliquée à chaque colonne:

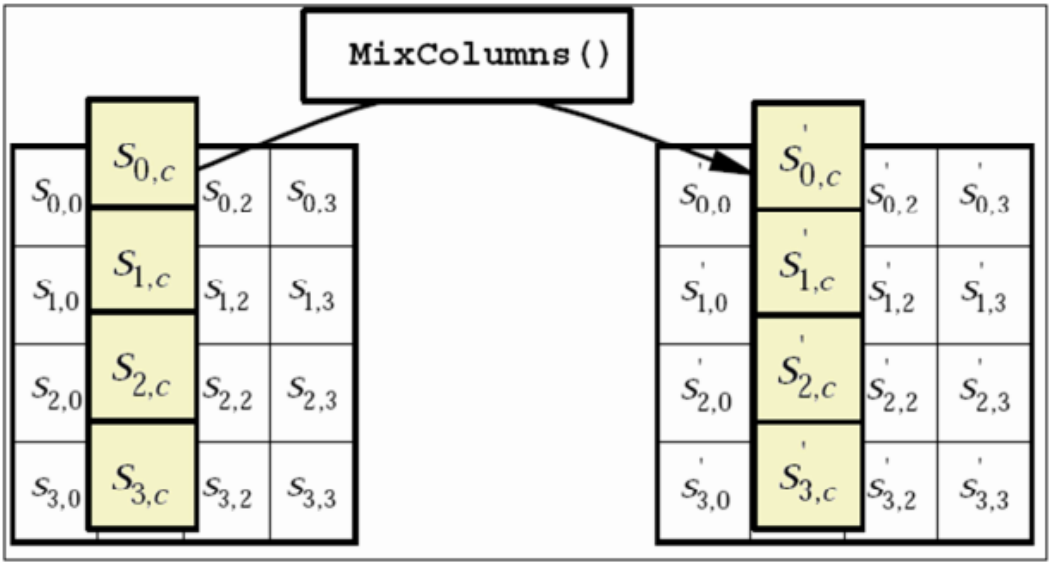


Figure III.4: MixColumn() fonctionne sur la matrice Etat colonne par colonne.

4) AddRoundKey ( ) addition de clés :

L'étape AddRoundKey, consiste à faire un ou exclusif entre les 128 bits la matrice State avec les 128 bits de la clé de ronde, Les dix clés de ronde (une pour chaque ronde) sont calculées à partir de la clé secrète.

XOR(ou exclusif)		Résultat
0	0	0
0	1	1
1	0	1
1	1	0

Table III.2: Ou logique exclusif.

5) Key Expansion « Diversification de la clé » :

La clé de chiffrement K stockée dans une matrice de 4 lignes et 4 colonnes soumet à la routine d'expansion qui génère 4*(Nr+1) mots, le résultat de cette expansion consiste dans un tableau linéaire noté [Wi] avec i variant de 0 à 4*(Nr+1), en voici sa composition.

- Les (Nk=4) premiers mots [$W_O \ldots W_{NK-1}$] contiennent la clé de chiffrement.
- Les mots suivants sont calculés en faisant un « XOR » du mot précédant

W_{i-1} et du mot situe avant la position NK :(W_{i-NK}) .

- Pour les mots situes sur une position qui est un multiple de NK, une transformation est appliquée à [W_{i-1}] avant le « XOR » .Cette transformation correspond à un décalage circulaire vers la gauche de chaque élément d'une colonne verticalement vers le haut nommé « RotWord ( ) » suivie d'une application « SubWord ( ) » qui applique la boite-S Sbox sur chaque élément (octet) de la colonne. Puis d'un″XOR″ avec un vecteur de constantes dépendant du tour noté « Rcon[i] ».

Tel que Rcon[i] contient la valeur [X^{i-1},{00},{00}{00}].

0x01	0x02	0x04	0x08	0x10	0x20	0x40	0x80	0x1B	0x36
0x00	0x00	0x00	0x00	0x00	0x00	0x00	0x00	0x00	0x00
0x00	0x00	0x00	0x00	0x00	0x00	0x00	0x00	0x00	0x00
0x00	0x00	0x00	0x00	0x00	0x00	0x00	0x00	0x00	0x00

Table III .3 Rcon[i]

III.3.2. Déchiffrement «Inverse Cipher » :

Le déchiffrement consiste à appliquer les opérations inverses, dans l'ordre inverse et avec des sous-clés également dans l'ordre inverse de celui du chiffrement.

La figure suivante, illustre le processus de déchiffrement adopté par notre application dont les étapes sont décrites en détail dans le paragraphe qui suit la figure :

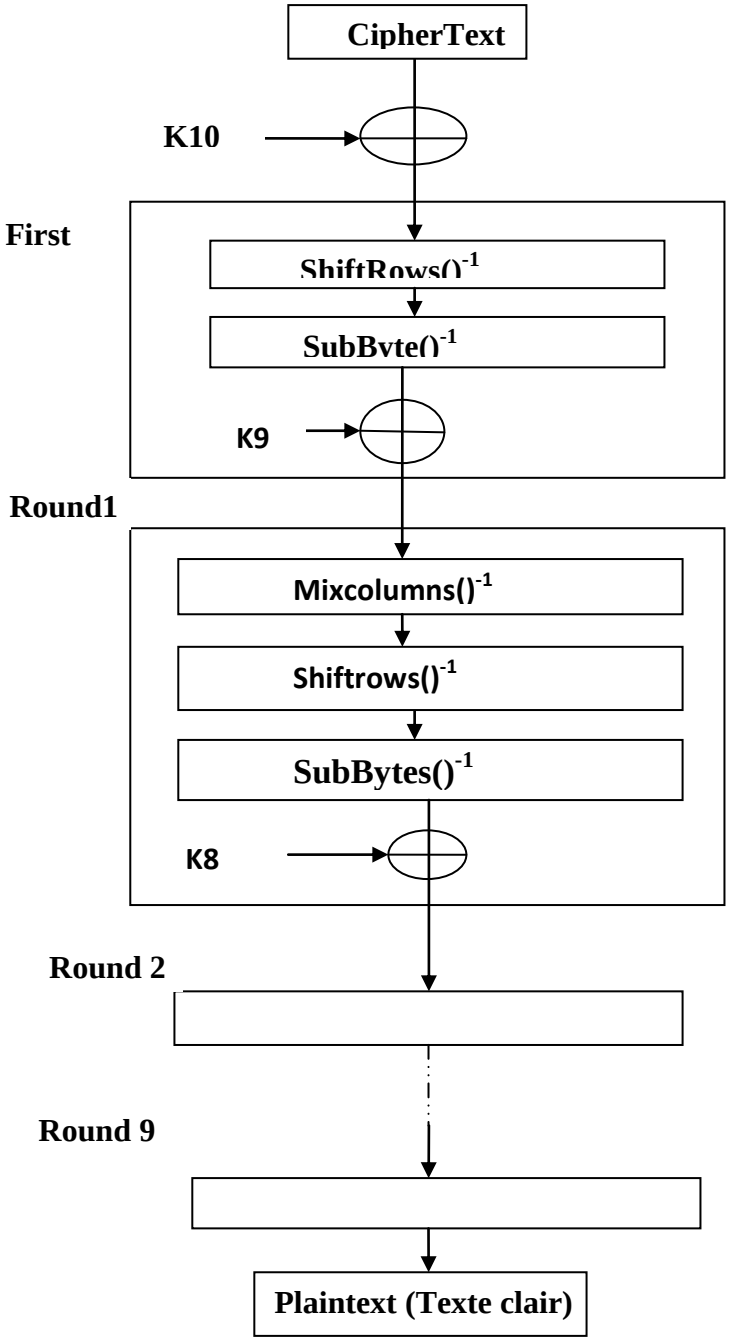


Figure III.5: Processus de déchiffrement.

1) La transformation « InvShiftRows ( ) » :

Est l'opération inverse de ShiftRows Consiste évidemment à effectuer au niveau de la ligne i un décalage cyclique à droite.

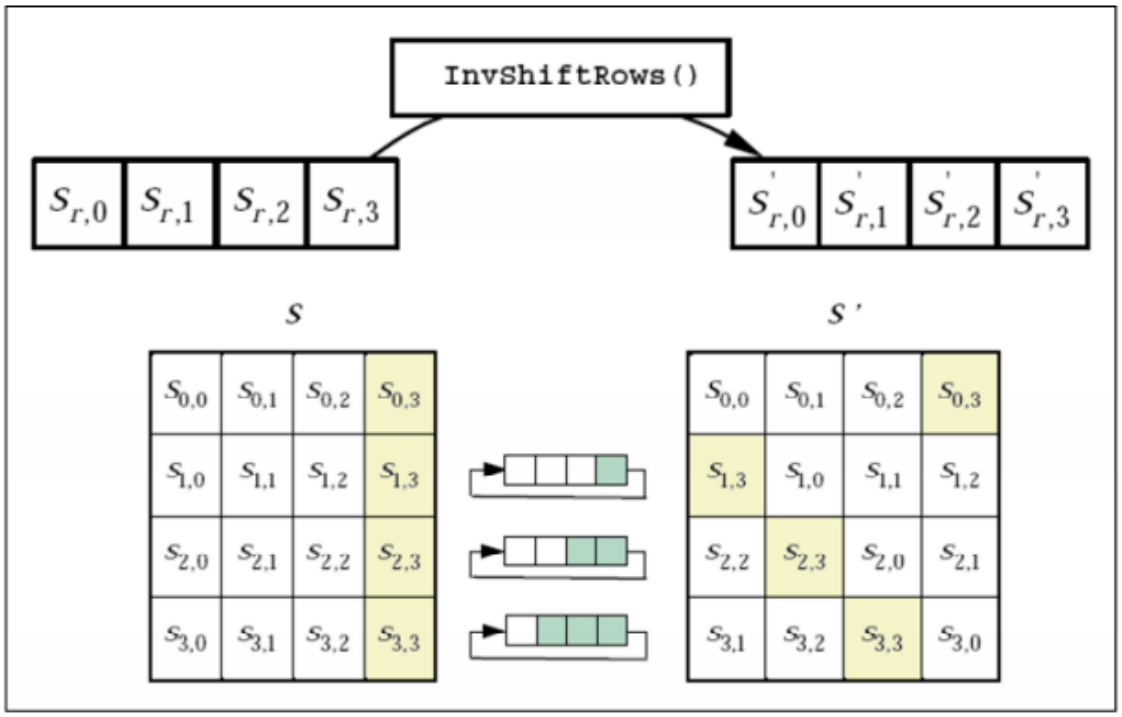


Figure III.6 :InvShiftRows() décale cycliquement les trois dernières lignes de l'Etat.

2) La transformation « InvSubByts ( ) »

InvSubByts ( ) est l'inverse de la transformation SubBytes ( ).

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
	1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
	2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
	3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
	4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
	5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
	6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
	7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
	8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
	9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
	a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
	b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
	c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
	d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
	e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
	f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Table 3. 19: Inverse S-Box.

Pour : S_{IJ}= {ed}

S'_{IJ}=InvSubBytes (S_{IJ}) = {53}

3) La transformation « InvMixColumns »

L'opération inverse de MixColumns consiste à effectuer la même opération mais à partir d'une multiplication par le polynôme $d(X)$=$C^{-1}(X)$donné par la relation:

$$(03X^3 + X^2 + X + 02) \times d(X) \equiv 01\ mod\ (X^4 + 1)$$

On obtient ainsi :

$$d(X) = 0BX^3 + 0DX^2 + 09X + 0E$$

Cette étape revient à effectuer le calcul de produit matriciel suivant:

$$S'(X) = d(X) \times S(X) mod\ (X^4 + 1) \leftrightarrow \begin{bmatrix} S'_{0,C} \\ S'_{1,C} \\ S'_{2,C} \\ S'_{3,C} \end{bmatrix} = \begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \times \begin{bmatrix} S_{0,C} \\ S_{1,C} \\ S_{2,C} \\ S_{3,C} \end{bmatrix}$$

III.3.3 Le fonctionnement de notre application à base de l'algorithme itératif AES :

Dans notre cas en utilise une clé de chiffrement de taille quelconque c'est-à-dire supérieur, inferieur ou égal à 128 (expansion de la clé AES) en a éliminer les condition sur la taille de la clé .

III.3.3.1 Pour chiffrer une donnée :

En utilise une clé de taille quelconque (X) et si la clé utilisé est supérieure à 128 bits en la fragmente en blocs de 128 (À partir d'une clé de 128 bits (un bloc), on cherche à en générer N nouvelles de même taille) et si le dernier bloc ne contient pas 128 bits c'est-à-dire :

X mod 128 ≠ 0 en complète avec des zéros.

N correspond au nombre d'itérations qui seront ensuite appliquées aux données par AES-128

- (On peut aussi avoir une clé initiale de moins de 16 octets, dans ce cas, on la complète avec des 0) et en applique l'algorithme.

Puis le principe de chiffrement appliqué avec chacun des blocs de la clé est identique avec le principe de fonctionnement d'AES jusqu'à l'obtention d'un texte chiffré N fois.

La figure suivante, illustre le processus de chiffrement adopté par notre application basé sur l'algorithme AES

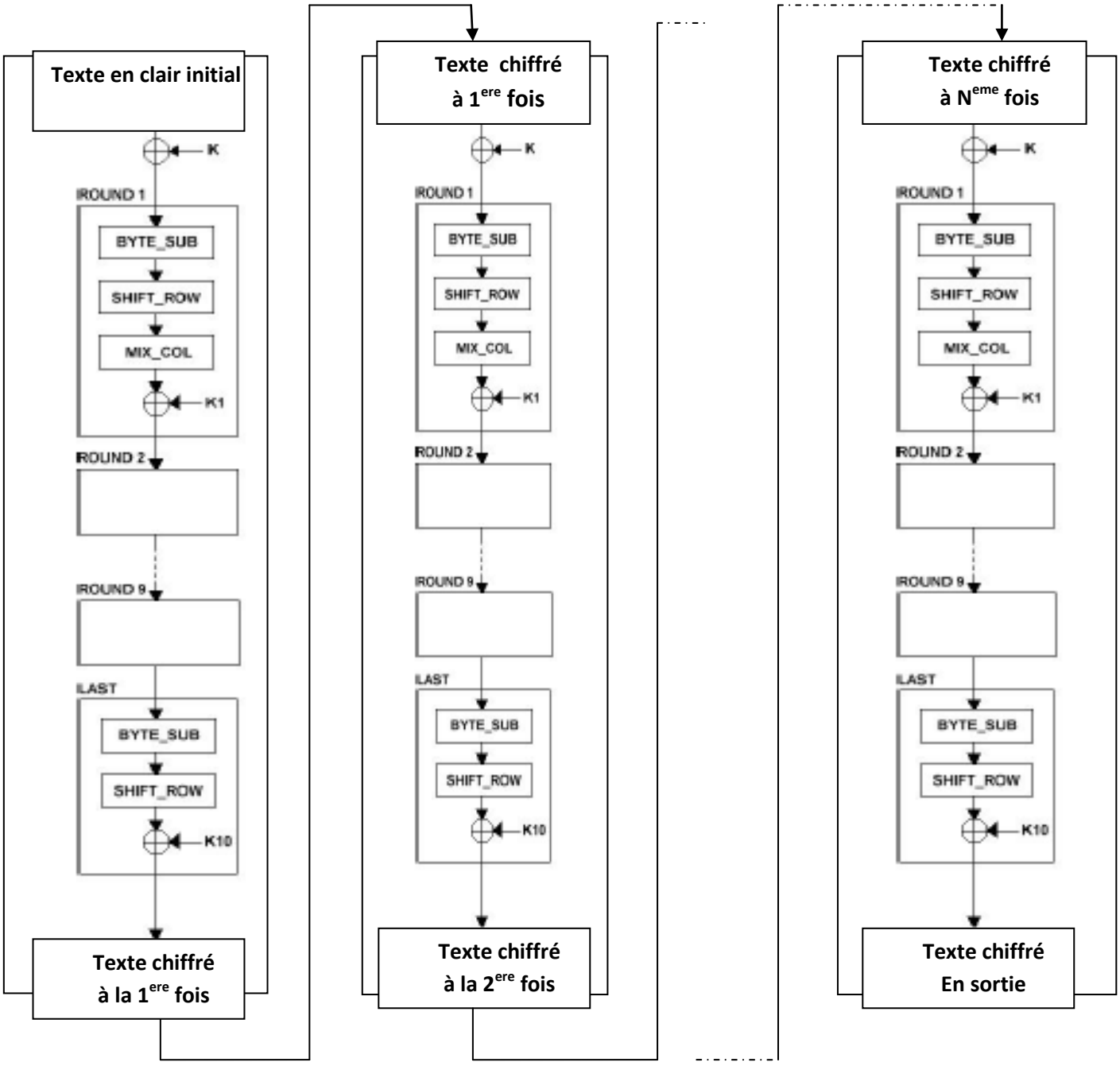


Figure III.7: différentes étapes de chiffrement

III.3.3.2 Pour déchiffrer une donnée :

Le déchiffrement est similaire au chiffrement, il suffit d'inverser l'ordre et l'effet de chacune des opérations et aussi d'inverser l'ordre des blocs de la clé.

Le schéma suivant illustre le fonctionnement de déchiffrement d'une d'un texte crypté avec notre algorithme :

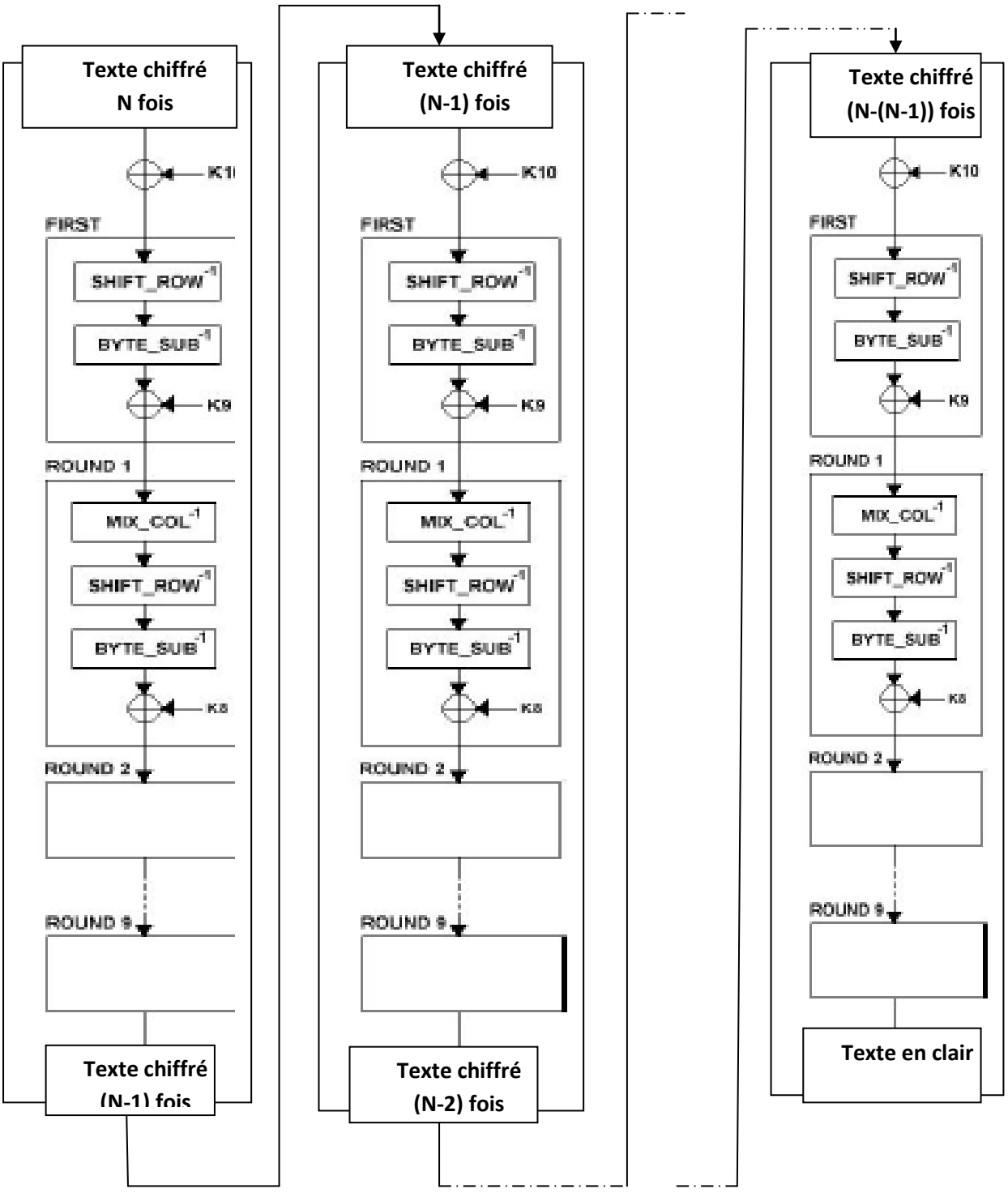


Figure III.8 : différentes étapes de déchiffrement.

III.4. Conclusion :

Ce chapitre est d'une grande importance pour la suite du travail, du fait qu'il projette les notions théoriques vues dans notre étude, et qu'il traite la conception du logiciel à réaliser, sans laquelle la réalisation ne pourra se faire.

Nous y avons d'abord décrit le fonctionnement général de notre algorithme, puis expliqué son fonctionnement détaillé en faisant appel à des schémas illustrant le déroulement de ces processus.

Donc à ce stade on est assez armé pour mettre sur pied notre application, ce qui va être l'objet du chapitre suivant toute en exposant l'environnement de développement.

Chapitre IV

Implémentation

Et

Réalisation

IV.1 Introduction :

La réalisation consiste à mettre en œuvre notre système. Ainsi, cette étape se présente en aval à la conception. Après avoir bien définit notre application dans le chapitre précèdent, nous allons traduire ces structures dans un langage de programmation.

Dans ce chapitre nous présentons l'environnement sous lequel nous avons effectué le développement de notre logiciel, et une description de ce logiciel qui a pour objectif de crypter différents fichiers à transmettre via des canaux de communication. Ainsi la présentation de quelques résultats obtenus après la réalisation de ce logiciel.

IV.2 Présentation de l'environnement de travail (matériel et logiciel):

IV.2.1 L'environnement matériel :

L'application que nous avons réalisée a été développée sur un micro-ordinateur portable acer. Ce dernier possède les caractéristiques suivantes :

Un microprocesseur Intel(R) Pentium(R) CPU P6200 @ 2.13GHz

Mémoire (RAM) : 2 Go

Type du système : Système d'exploitation 32 bits

IV.2.2 L'environnent logiciel :

IV.2 .2.1 Présentation du langage de programmation utilisé (java) :

Java est un langage de programmation orienté objet mis au point en 1991 par la firme SUN. Il est caractérisé par les points suivants :

- **Java est indépendant de toute plate-forme** : Une application développée en java fonctionne (sans aucune modification, même pas une recompilation) dans n'importe quel environnement disposant d'une MJV (Machine Virtuelle Java).
- **Java est un langage orienté objet** : Dans ce type de programmation, on ne manipule pas des fonctions et des procédures, mais des objets qui s'échangent des messages. Le principal avantage, outre le fait que l'on peut créer des objets de toutes natures représentant les véritables objets du problème à traiter, est chaque objet peut être mis aux point séparément.

- **Java est extensible à l'infini :** Java est écrit en java. Idéalement, toutes les catégories d'objets (appelées classes) existant en java sont définies par extension d'autres classes, en partant de la classe de base la plus générale : la classe Object. Pour étendre le langage, il suffit donc de développer de nouvelles classes. Ainsi, tous les composants écrits pour traiter un problème particulier peuvent être ajoutés au langage et utilisés pour résoudre de nouveaux problèmes comme s'agissait d'objets Standards.
- **Java est un langage à haute sécurité :** Contrairement à C++, Java a été développé dans un souci de sécurité maximale. L'idée maitresse est qu'un programme comportant des erreurs ne doit pas pouvoir être compilé. Ainsi, les erreurs ne risquent pas d'échapper au programmeur et de passer les procédures de tests. En détectant les erreurs à la source, on évite qu'elles se propagent en s'amplifiant.
- **Java est un langage compilé :** Java est un langage compilé, c'est-à-dire qu'avant d'être exécuté, il doit être traduit dans le langage de la machine sur laquelle il doit fonctionner. Cependant, contrairement à de nombreux compilateurs, java traduit le code source dans le langage d'une machine virtuelle, appelée JVM (Java Virtual Machine). Le code produit, appelé bytecode, ne peut pas être exécuté directement par le processeur de la machine. Le bytecode est ensuite confié à un interpréteur qui le lit et exécute.

IV.3 Présentation de l'environnement de développement :

NetBeans est un environnement de développent intégré (IDE) qui permet de programmer et concevoir les interfaces utilisateur de manière visuelle. Pour ce faire, il offre de nombreux outils de conception visuelle qui permettent de concevoir les interfaces utilisateur avec rapidité et efficacité en attachant des événements et en modifiant les dispositions.

Pour la réalisation de notre application, nous avons utilisés la version 6.9 (NetBeans 6.9).

- **Outils de conception visuelle de NetBeans :**

NetBeans fournit des outils permettant de concevoir et de programmer visuellement les classes Java, ce qui nous conduit à produire de nouveaux composants, ces outils sont organisés comme la montre la figure suivante :

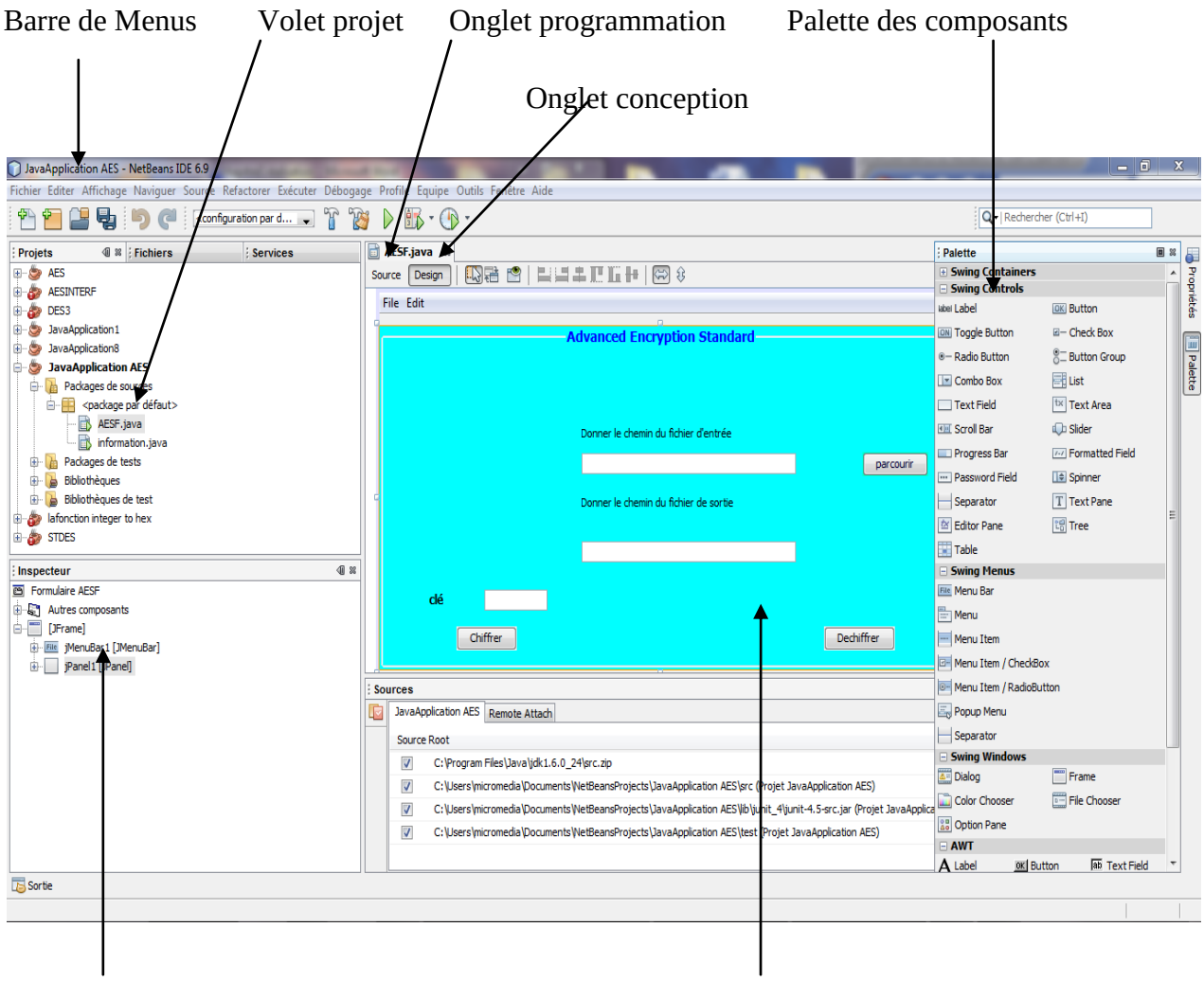


Figure IV.1 Environnement de développent NetBeans.

- **Volet Project :** contient tous les packages de projet, et pour chaque package on trouve les classes crées avec les quelles l'application et réalisé.
- **Palette des composants** : la palette des composants contient des composants visuels et non visuels qu'on peut faire glisser dans l'inspecteur ou dans l'arborescence des composants.
- **Volet inspecteur** : L'arborescence des composants apparait dans le volet inspecteur au dessous du volet projet. Elle affiche une vue structurée de tous les composants du fichier source et de leurs relations.

IV.4 Présentation du logiciel

AES avec expansion de clé est un logiciel de cryptage et de décryptage de données, permet à l'utilisateur de crypter des fichiers ayant n'importe qu'elle extension (.txt, .docx, .pdf, .jpg, png, .exe, .mp3, …).

IV.4.1 Présentation des interfaces de notre application :

Nous allons maintenant présenter les différentes interfaces du logiciel ainsi que son fonctionnement.

IV.4.1.1 Interface d'authentification :

Le but de cette interface est d'authentifier l'utilisateur du logiciel pour offrir une certaine privatisation de l'utilisation de ce logiciel, et ainsi empêcher toute tentative d'utilisation illégale des personnes ne possédant pas le droit de l'utiliser.

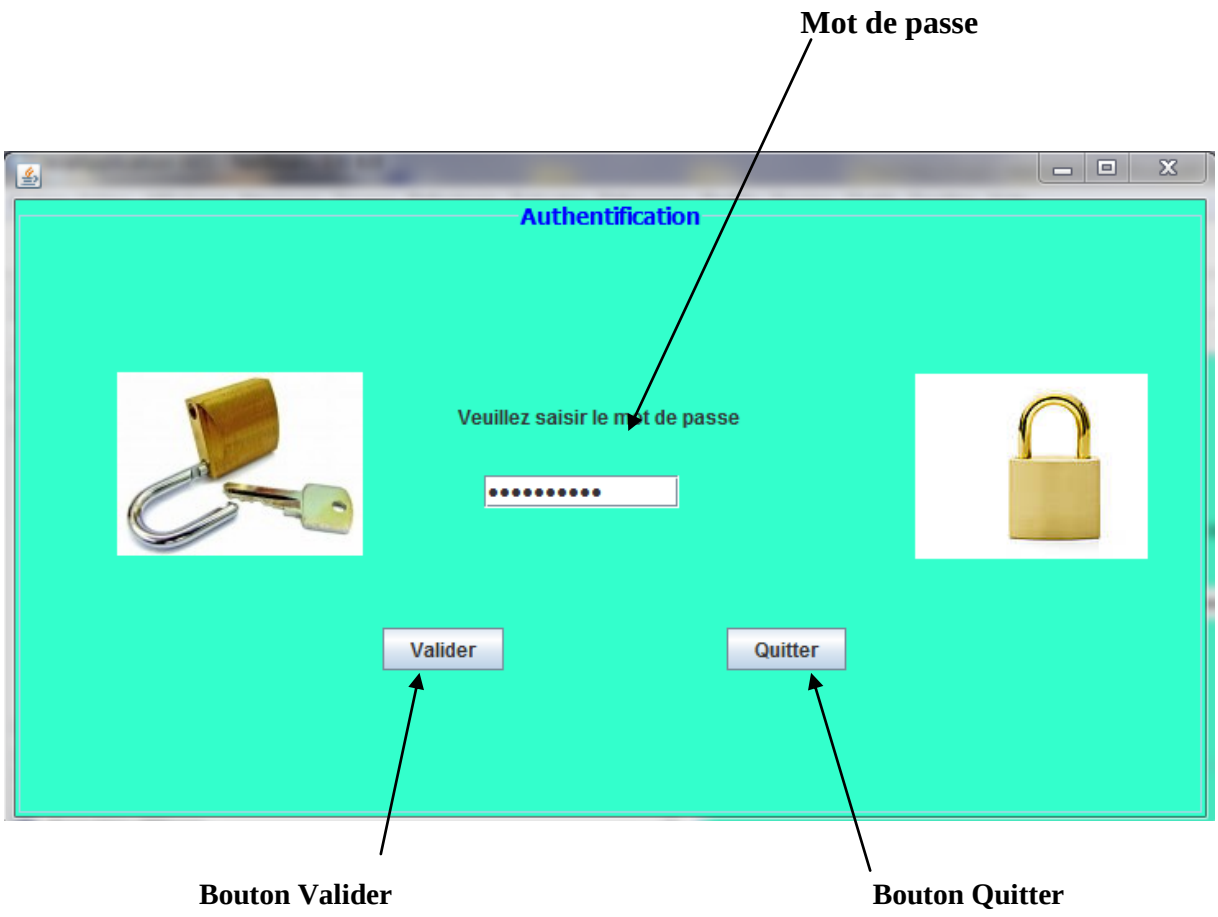


Figure IV.2 : Interface Authentification.

IV.4.1.2 Interface d'accueil :

C'est l'interface principale de notre logiciel, elle est conçue de sorte qu'elle offre une simplicité d'utilisation. Cette interface permet l'accès aux différentes opérations du logiciel à partir de la barre du menu principal, qui comporte deux sous-menus différents.

Menu Action **Menu A propos**

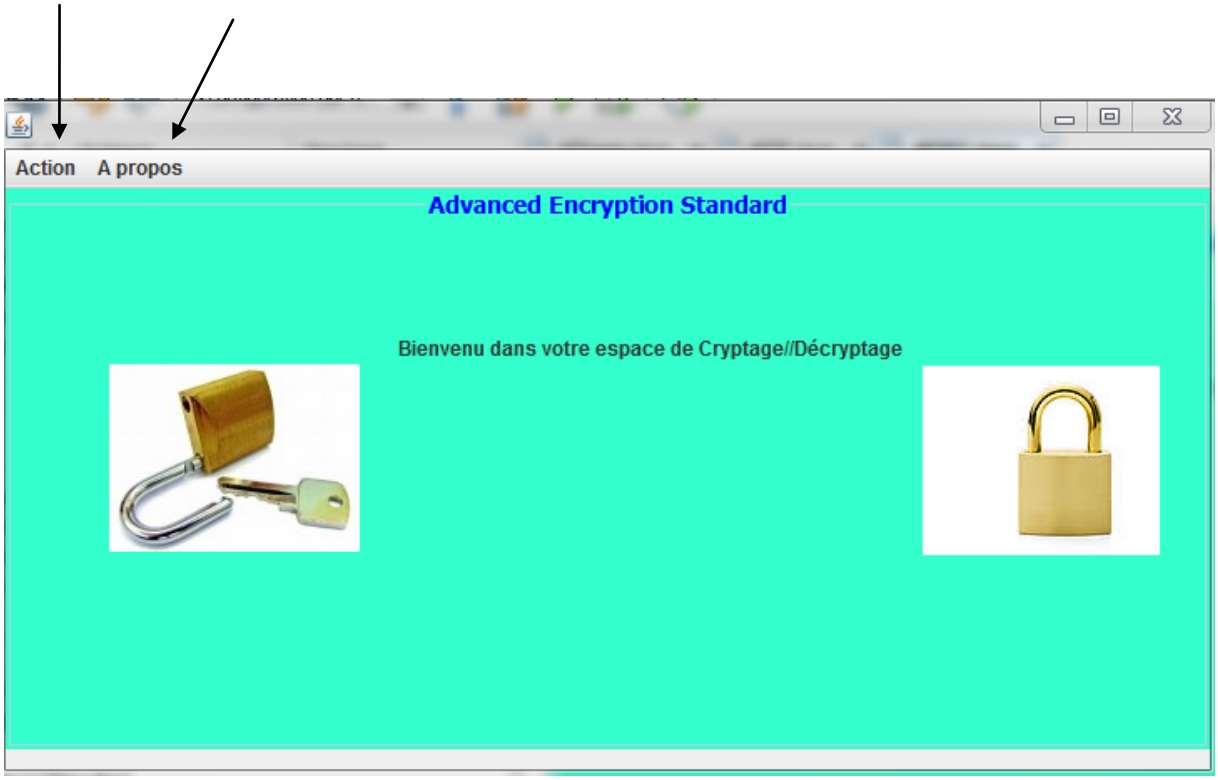
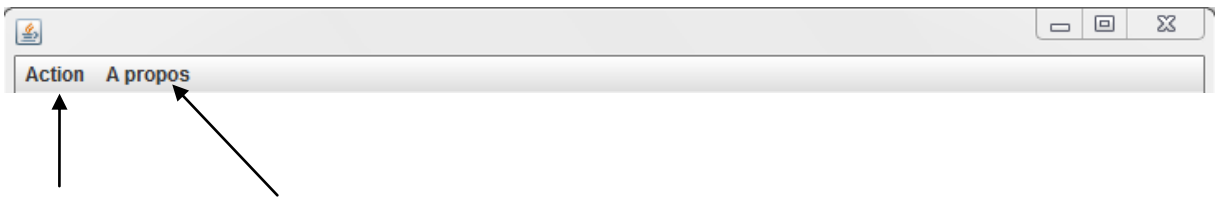


Figure IV.3: Interface d'accueil.

IV.4.1.3 Présentation du menu principal :



Menu Action **Menu A propos**

Le menu principal de ce logiciel comporte deux sous-menus différents :

- **Le sous-menu Action :**

Permet à l'utilisateur de choisir une opération.

- **Crypter/Décrypter fichier :** lancer la fenêtre de cryptage/décryptage du fichier comme le montre dans la figure IV.4.
- **Quitter :** permet de quitter l'application.

- **Le sous-menu A propos :**
  - **A propos de l'application :** Affiche la fenêtre donnant les informations générales sur l'application.

IV.4.1.4 Interface de Cryptage/Décryptage du fichier :

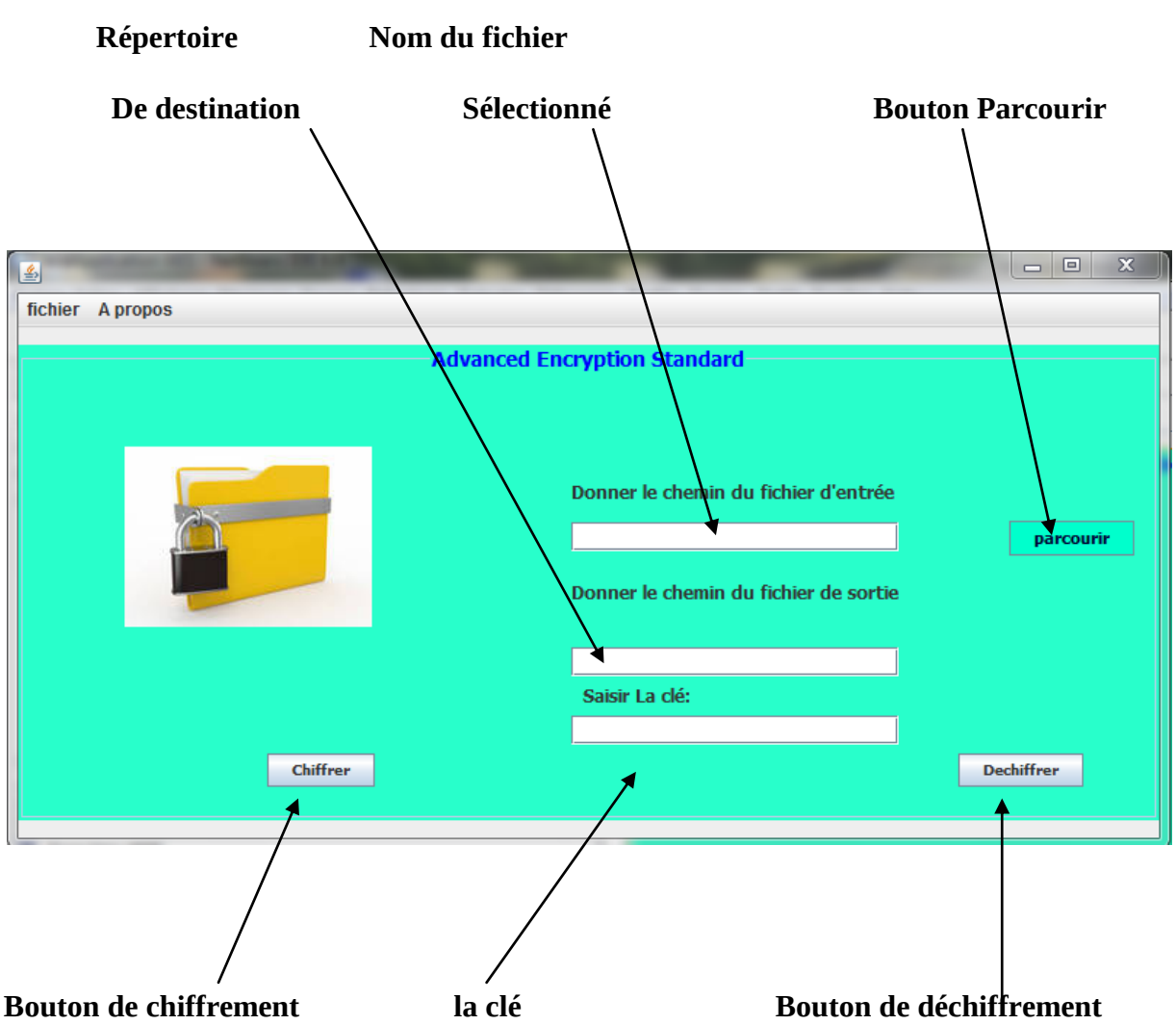


Figure IV.4 : Interface de Cryptage/Décryptage du fichier.

Si l'utilisateur veut crypter ou décrypter un fichier, il le sélectionne en cliquant sur le bouton «Parcourir…», qui lui permet de choisir un fichier à partir d'un répertoire. Après la sélection du fichier que l'on désire crypter/décrypter, le nom du fichier apparaît dans le champ «donner le chemin du fichier d'entrée» de l'interface «Crypter/Décrypter le fichier», ensuite l'utilisateur passe à la dernière étape du cryptage/décryptage en cliquant sur le bouton «Chiffrer» ou « Déchiffrer ».

IV.4.1.5 Interface pour choisir le fichier à Crypter/Décrypter :

La Figure IV.5 suivante représente l'interface engendrée par le bouton de « Parcourir ».

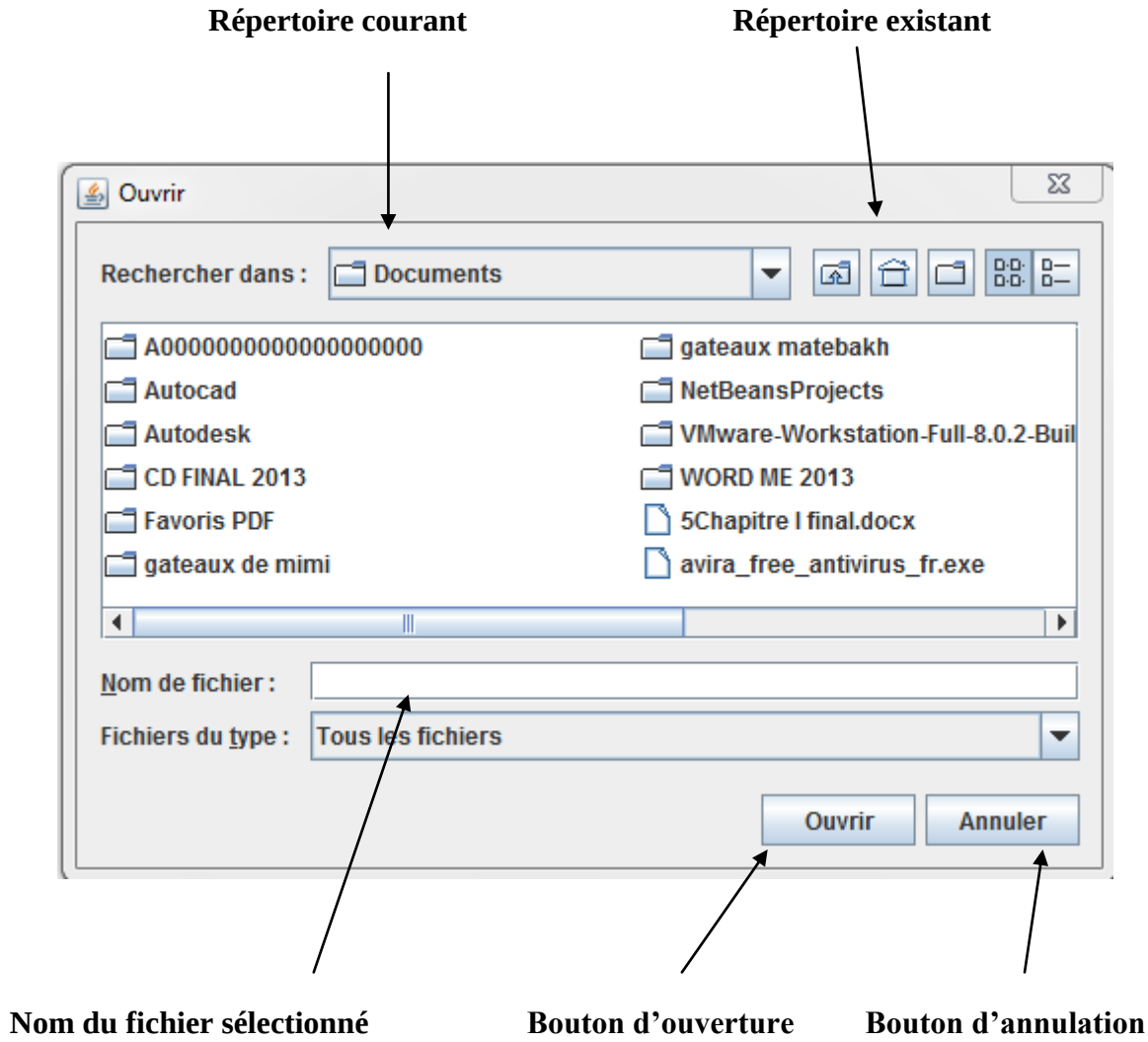


Figure IV.5 Interface pour choisir le fichier à Crypter/Décrypter.

IV.5 Exemples d'utilisation :

Afin d'évaluer la performance de notre logiciel, nous allons utiliser le fichier «Exemple.docx » pour le crypter.

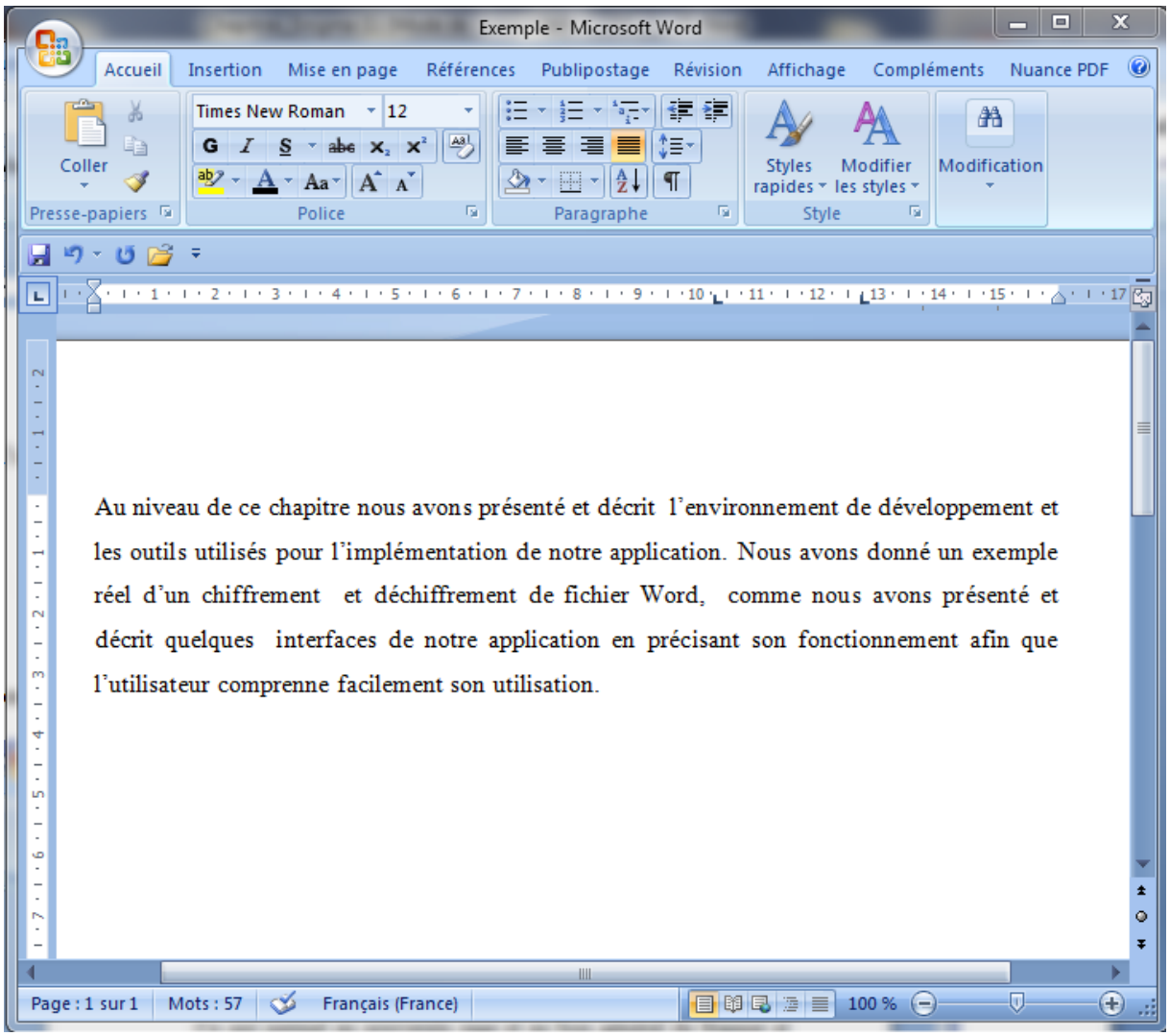


Figure IV.6 Le fichier à crypter.

Pour crypter ce fichier on clique sur le bouton « Crypter/Décrypter le fichier » de sous-menu « Action » à partir de la fenêtre principale, L'interface de Cryptage/Décryptage du fichier s'affiche. Puis on choisi le fichier à crypter à partir de la fenêtre «Cryptage/Décryptage du fichier » en cliquant sur le bouton « Parcourir ».

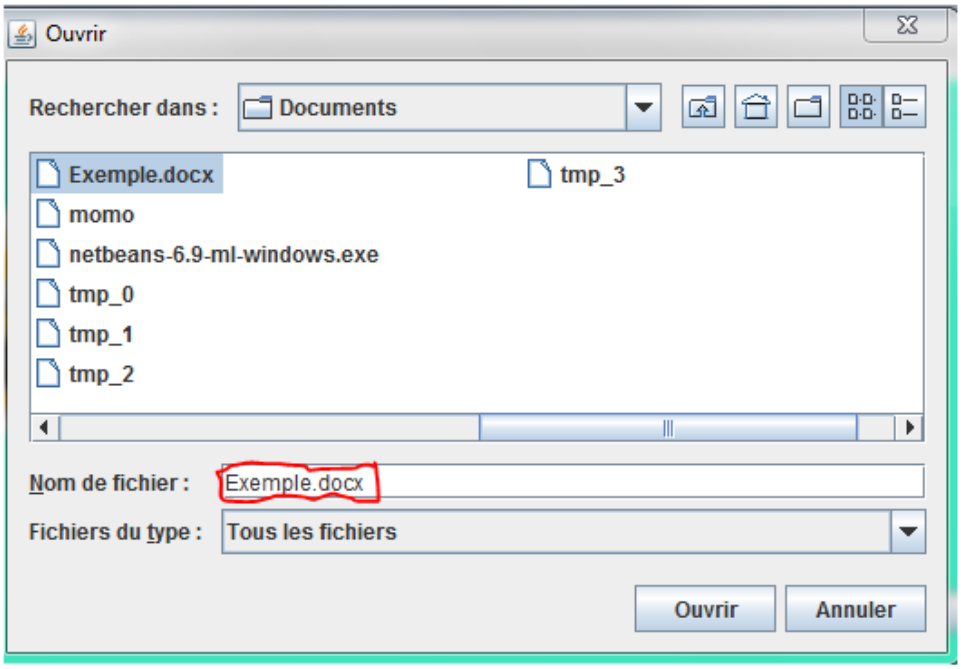


Figure IV.*7* Le fichier sélectionné

Une fois le fichier est sélectionné, le nom du fichier s'affiche dans le champ « donnée le chemin du fichier d'entrée », on spécifie le répertoire est le nom du fichier Crypté dans le champ « donnée le chemin du fichier de sortie », on Saisit la clé de chiffrement, puis on valide avec le Bouton « chiffrer ».

Figure IV.8 validation de l'opération de cryptage.

Quand le système termine le cryptage du ce fichier, l'application renvoi le message informatif suivant :

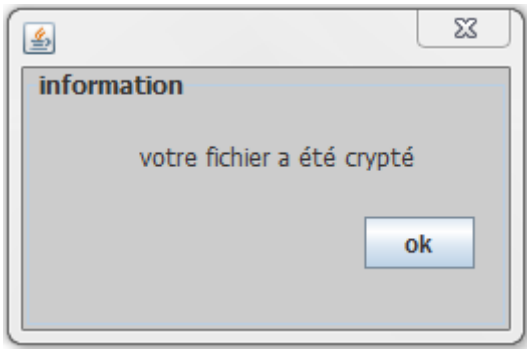


Figure IV.9 message d'information.

A la fin du cryptage, on ouvre le fichier crypté avec l'éditeur de texte de Windows «Bloc note», et on trouve le contenu suivant :

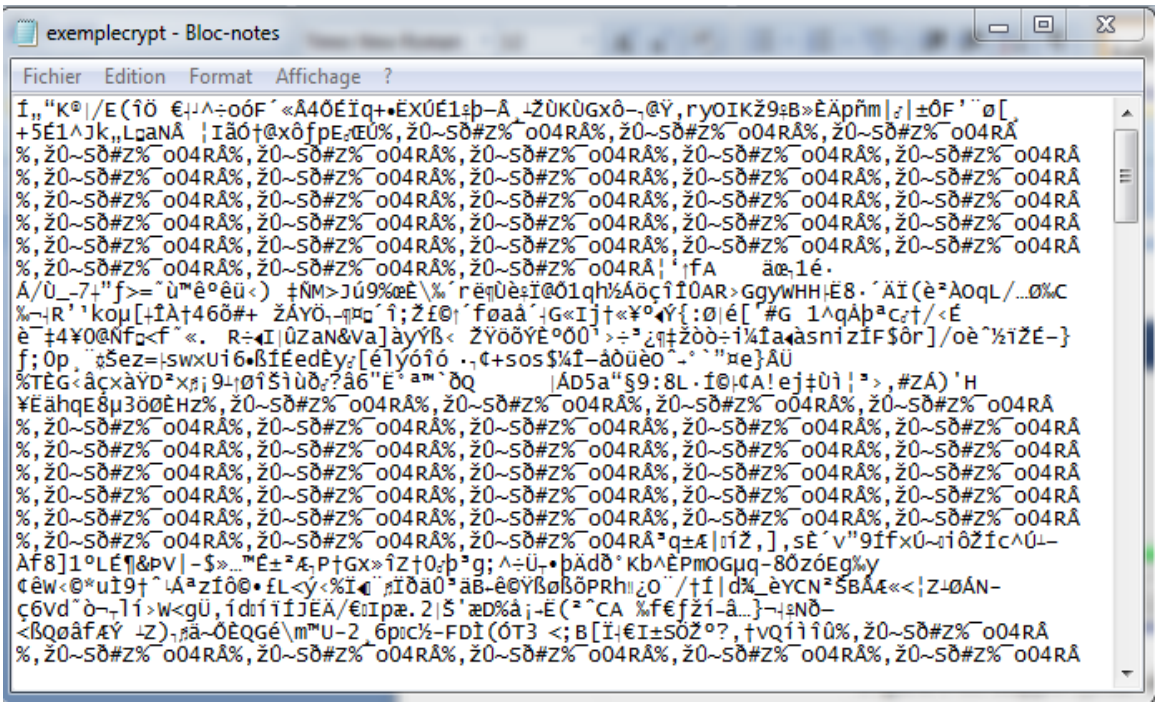


Figure IV.10 Contenu du fichier crypté.

IV.6 Conclusion :

Au niveau de ce chapitre nous avons présenté et décrit l'environnement de développement et les outils utilisés pour l'implémentation de notre application. Nous avons donné un exemple réel d'un chiffrement et déchiffrement de fichier Word, comme nous avons présenté et décrit quelques interfaces de notre application en précisant son fonctionnement afin que l'utilisateur comprenne facilement son utilisation.

Conclusion général :

Par le biais de ce travail, nous avons pu réaliser un système de chiffrement basé sur un algorithme de cryptographie symétrique AES (advanced encryption standard) consistant à l'améliorer en définissant une clé non restreinte en ce qui concerne le nombre de ses caractères. Ainsi, après la construction de ce système de chiffrement évolutionniste dont des applications sur différents messages ont été réalisés, illustrant le bon fonctionnement de ce système, l'amélioration été élaborées dont le but d'avoir un chiffrement plus sûr. Ce qui a permis l'obtention d'un autre système de chiffrement distincts plus résistants que le premier.

La nouvelle technique de chiffrement augmente considérablement la résistance de notre système, cependant elle présente l'inconvénient d'augmenter la taille de la clé secrète. En fait, nous risquons d'avoir une taille de clé aussi longue que le message. Donc nous avons fragmenté la clé en blocs pour régler ce problème. Quand à la fragmentation elle possède l'avantage d'avoir une clé de taille petite comparativement a celle de sa fusion.

Le trafique des clés secrètes a toujours assez limité l'utilisation des algorithmes symétriques, des efforts restent a fournir pour laisser la porte grande ouverte a ce genre de systèmes qui sont plus rapides que les autres types de systèmes.

Liste des Abréviations

DOS : Disk Operating System

ACK : ACKnowledged

IP : Internet Protocol

ARP: Adress Resolution Protocol

ISO: International Standard Organization

IETF: Internet Engineering Task Force

IEEE: Institute of Electrical andElectronics Engineers

RSA : Rivest Shamir Adleman

SOCKS

USB : Universal Serial Bus

IDS: Integrated Data Storage

VPN : Vertual Private Network

XOR : eXclusive OR

DES : Data Encryption Standard

AES : Advanced Encryption Standard

SSL/ TLS : Secure Socket Layer/ Transport Layer Security

WEP : Wired Equivalent Privacy

RC4 :Rivest Cypher 4

TDES : Triple Data Encryption Standard

ANSI : Americain National Standard Institute

MD: Message Digest

SHA: Secure Hash Algorithm

MAC: Message Authentification Code

NSA: National Security Agency

NIST: National Institute of Standard And Technology

PGP: Pretty Good Privacy

IDEA: International Data Encryption Algorithm

Bibliographie

[1] : www.securiteinfo.com, « Le Grand Livre de SecuriteInfo.com »,19 février 2004

[4] : Securite dans les Reseaux de Capteurs Sans-Fil,mémoir,béjaia 2008,

[5] : ZNAIDI Wassim, thèse doc, Quelques propositions de solutions pour la sécurité des réseaux de capteurs sans fil. INSA lyon 2010,

[6] : une introduction à la cryptographie ; support du cour ,universitées de nante

[7] : www .apprendre-en ligne.net

[8] : T.Peyrin, Analyse de fonctions de hachage cryptographiques, Thèse de Doctorat ENS, Versailles, novembre 2008.

[9] : Auteurs Alexandre GOMEZ-URBINA Copyright © 2010 Micro Application 20-22, rue des Petits-Hôtels 75010 Paris1ère Édition - Février 2010

[10] : F.Omary / Thèse en Informatique / 2006 / Faculté des Sciences Rabat

[11] : Université de LiègeFaculté sdes Sciences Appliquées Cryptographie et Sécurité informatique INFO0045-2 Notes de cours provisoires 2009 - 2010 Renaud Dumont

[12] : Bruno Martin, Codage, Cryptograhie et Applications.1ere édition, 2004.Presses polytechniques et Universitaires Romandes.

[13] : Amakou Mbata,Olivier persent ,Firewall,parfeu,mur de feu ;PARIS decembre 2006

[17] : http://www.frameip.com/vpn/#2.2_-_Fonctionnalit%C3%A9s_des_Vpn

[18] : http://www.securiteinfo.com/conseils/introsecu.shtml

[19] : https://fr.wikipedia.org/wiki/Notarisation_%C3%A9lectronique

[20] : http://www.futura-sciences.com/fr/definition/t/informatique-3/d/antivirus_10999/

[22] : Eric ALATA, Observation, caractérisation et modélisation de processus d'attaques sur Internet, thèse de Doctorat , l'Institut National des Sciences Appliquées de Toulouse,2007

Résumé :

L'évolution rapide des réseaux informatiques, privés ou publics engendre un volume toujours plus important de données sauvegardées et transmises, générant ainsi de nouveaux besoins en matière de sécurité. Dans un mode où l'entreprise dépend de plus en plus de son système informatique, la sécurité est donc devenue une préoccupation primordiale.

Ce travail a pour objectif d'étudier et de réaliser un cryptosystèmes accomplissant l'algorithme AES (chiffrage, déchiffrage, et expansion de clé) permettant ainsi d'exécuter des cryptages plus sûrs et plus robustes, il présente, entre autres, une plus grande résistance aux attaques par dictionnaires de clés. Les autres attaques ne sont pas applicables dans son cas. Grâce à une organisation et modification soigneuse d'AES.
Mots clés :algorithme symétrique, cryptographie, cryptanalyse, clé, AES, DES, ……etc.

Abstract

The quick change of the data-processing networks, private or public generates a volume increasingly more important safeguarded and transmitted data, thus generating new needs as regards safety. In a mode where the company depends more and more on its computing system, safety thus became a paramount concern.

This work aims to study and carry out a cryptosystèmes achieving algorithm AES (figuring, deciphering, and expansion of key) thus making it possible to carry out surer and more robust encodings, it presents, inter alia, a greater resistance to the attacks by dictionaries of keys. The other attacks are not applicable in its case. Thanks to an organization and careful modification of AES.
Key words: symmetrical algorithm, cryptography, cryptanalyse, key, AES, DES, ….; etc