REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITÉ **S**AAD **D**AHLAB **B**LIDA 1

Faculté des Sciences
Département : Informatique

Mémoire de Fin d'Etude pour l'Obtention du Diplôme de Master en Informatique

OPTION : Sécurité des Systèmes d'Information

Présenté par :
CHABNI Chahinez
ELAHCENE Amina

Thème :

Etude, Conception et Développement d'un Système Cryptographique pour le CSIRT ELIT

Organisme d'accueil : ELIT -El Djazïar **I**nformation **T**echnology.

Mme Boumahdi	**Présidente**
Mme Ghebghoub	**Examinatrice**
Mme AROUSSI Sana	**Promotrice**
Mme Hammouche	**Encadreur**

Promotion : 2019-2020

Remerciements

*Nous remercions **ALLAH** le tout puissant et miséricordieux, qui nous a donné la force et la patience d'accomplir ce travail.*

*Un grand merci à madame **AROUSSI Sana** notre promotrice pour ça patience, sa disponibilité, son soutien et ses encouragements, et surtout ces judicieux conseils qui ont contribué à améliorer notre réflexion et structurer notre travail.*

*Nos vifs remerciements vont également aux **membres du jury** pour l'intérêt qu'ils ont porté à notre recherche en acceptant d'examiner notre travail et de l'enrichir par leurs propositions.*

Afin de n'oublier personne, nos vifs remerciements s'adressent à tous ceux qui nos 'ont aidée à la réalisation de ce modeste mémoire.

Nous adressions nos sincères remerciements à tous nos professeurs qui nous ont formés durant notre parcours scolaire.

A tous, nous présentons notre gratitude et notre respect.

Dédicace

Je tiens c'est avec grande plaisir que je dédie ce modeste travail :

A l'être le plus chère de ma vie, ma mère.

A mon père pour son soutien, son affection et la confiance qu'il mon accordée

A mon cher mari

A Mme AROUSSSI Sana notre promotrice

A mes chères frères et sœurs

A Ma binôme Amina

A mes chères amies Soumia, faiza, Imene, Anfel

A tous mes amis, mes collègues

A toute personne qui occupe une place dans mon cœur

Chahinez

Dédicace

Ce travail est dédié

A mes chers parents ma source de volonté, leur prière, encouragement, sacrifices, aides, et soutenir …m'ont vraiment m'aidé pour que je puisse continuer mon parcours, que Dieu le tout Puissant vous préserve, vous accord la santé et le plus haut de paradis Incha'Allah.

A Mme AROUSSSI notre promotrice.

A Ma sœur Yousra

A Mes frères Walid et Abd El Rahmene.

A Ma binôme Chahinez qui m'a soutenu et encouragé toute au long de ce travail.

A tous mes amies et surtout Selma, Yousra et Selma.

A tous ceux qui m'ont aidé et encouragé.

A tous mes collègues.

Je vous aime tous.

Amina

Résumé

Un CSIRT (Computer Security Incident Response Team), comme son nom indique, est une équipe d'experts en sécurité informatique organisées pour prévenir et réagir en cas d'incident informatique**.** Elle assure notamment une veille sécurité (les nouvelles attaques, les nouveaux logiciels malveillants, les dernières vulnérabilités) et en aval, elle analyse et traite les incidents de sécurité. L'une des fonctions principales de cette équipe est la coopération et l'échange d'informations entre ses membres et avec ses clients. Les données échangées relatives à un incident sont classées critiques et doivent toujours être envoyées sous forme crypté**.** C'est pourquoi, chaque CSIRT doit disposer un système cryptographique pour sécuriser ses communications en permettant de préserver la confidentialité des échanges et de s'assurer que les données sensibles stockées ou échangées soient uniquement lisibles par le destinataire et qu'en aucun cas elles ne puissent être lues par une autre personne.

Pour ce faire, nous avons développé un système cryptographique hybride qui combine la rapidité de la cryptographie symétrique avec la sécurité fournie par la cryptographie asymétrique. En effet, notre système permet de crypter les données avec l'algorithme symétrique AES à une clé secrète qui elle-même sera cryptée avec l'algorithme asymétrique RSA en utilisant une paire de clés publique-privée. Ces clés ainsi que les certificats, générées par l'autorité de certification, sont partagées via le protocole SSH. Tout cela a pour but de renforcer la sécurité au niveau du CSIRT ELIT.

Mots – clés : Gestion des incidents, CSIRT, système cryptographique symétrique, asymétrique, hybride, AES, RSA, Autorité de certification, SSH.

ABSTRACT

CSIRT (Computer Security Incident Response Team), as its name suggests, is a team of computer security experts organized to prevent and react to computer incident. In particular, it ensures security watch (veille) (new attacks, new malware, latest vulnerabilities), it analyzes and treaty security incidents. One of the main functions of this team is cooperation and the exchange of information between its members and with its clients. Data exchanged relating to an incident are classified as critical and should always be sent in encrypted form. Therefore, each CSIRT must have a cryptographic system to secure its communications allowing to preserve the confidentiality of exchanges and to ensure that the sensitive data stored or exchanged are only readable by the recipient and that in no case can they be read by another person. To do this we have developed a hybrid cryptosystem that combines the rapidity of symmetric cryptography with the security of asymmetric cryptography. Indeed, our system allows encrypting data with the AES symmetric algorithm. Symmetric key will be encrypted with the RSA asymmetric algorithm using a public and private key. These keys and the certificates are generated by the certification authority are shared via the SSH protocol. All of this are used to reinforce the security of CSIRT ELIT.

Keywords: Incident management, CSIRT, symmetric, asymmetric, hybrid cryptosystem, AES, RSA, Certification authority, SSH.

ملخص

فريق الاستجابة لحوادث أمن المعلوماتية، هو فريق من خبراء أمن الكمبيوتر يعمل على منع حوادث الكمبيوتر والاستجابة لها. كما يضمن المراقبة الأمنية (الهجمات الجديدة، والبرامج الضارة الجديدة، وأحدث نقاط الضعف) ، ويقوم بتحليل الحوادث الأمنية والتعامل معها.

تتمثل إحدى الوظائف الرئيسية لهذا الفريق في التعاون وتبادل المعلومات بين أعضائه وعملائه. يتم تصنيف البيانات المتبادلة المتعلقة بالحادثة على أنها معلومات سرية ويجب دائمًا إرسالها في شكل مشفر. لهذا السبب توفر كل CSIRT على نظام تشفير لتأمين اتصالاته وهذا للحفاظ على سرية التبادلات والتأكد من أن البيانات الحساسة المخزنة أو المتبادلة لا يمكن قراءتها إلا من قبل المستلم. في أي حال من الأحوال لا يمكن قراءتها من قبل شخص آخر. للقيام بذلك، قمنا بتطوير نظام تشفير هجين يجمع بين سرعة التشفير المتماثل والأمان الذي يوفره التشفير غير المتماثل. في الواقع، يسمح نظامنا بتشفير البيانات باستخدام خوارزمية AES بمفتاح سري الذي يتم تشفيره في حد ذاته باستخدام خوارزمية RSA غير المتماثلة باستخدام زوج مفاتيح عام وخاص.

يتم إنشاء هذه المفاتيح والشهادات من قبل سلطة تصديق الشهادات بحيث يتم تمريرها عبر بروتوكول SSH. وهذا كله من اجل تعزيز الأمان على مستوى CSIRT.

الكلمات المفتاحية: إدارة الحوادث، فريق الاستجابة لحوادث أمن المعلوماتية CSIRT، نظام تشفير هجين، AES، RSA، سلطة تصديق،SSH ، متماثل، غير متماثل.

Tables des matières

Tables des figures

Liste des tableaux

Liste des acronymes

Acronymes	Signification
ACL	Access Control Lists
AES	Advanced Encryption Standard
ARC4	Alleged RC4
CA	Autorité de certification
CC	Coordination Center
CERT	Computer Emergency Response Team
CID	Confidentialité, Intégrité, Disponibilité
CPU	Central Processing Unit
CSIRT	Computer Security Incident Response Team
CSS	Feuilles de style en cascade »
DARPA	Defense Advanced Research Projects Agency
DES	Data Encryption Standard
DNS	Domain Name System
DOS	Denial-of-Service
ECC	Elliptic Curve Cryptography
ELIT	EL djazaïr Information Technology
ENISA	European Network and information Security Agency
FFOM	Forces, Faiblesses, Opportunités et Menaces
FIRST	Forum of Incident Response and Security Teams
FTP	File Transfer Protocol
GnuPG	GNU Privacy Guard
HTML	HyperText Markup Language »
HTTPS	HyperText Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IDEA	International Data Encryption Algorithm
IDS	Intrusion Detection System
IP	Internet protocol
IR	Infrarouge
ISO	International Organization for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
JS	Java Script
LDAP	Lightweight Directory Access Protocol
MIT	Massachusetts Institute of Technology
MitM	Man-in-the-Middle
NIST	National Institute of Standard and Technology
PCA/PRA	Plan de Continuité/Reprise d'Activité
PEST	Politique, Économique, Socioculturel et Technologique
PGP	Pretty Good Privacy
PHP	Hypertext Preprocessor

phpseclib	PHP Secure Communications Library
PIC	Protection des Infrastructures Critiques
PIIC	Protection de l'Infrastructure d'Information Critique
PKI	Public Key Infrastructure
PME	Petites et Moyennes Entreprises
RA	Autorité d'enregistrement
RC4	Rivest Cipher 4
RC5	Rivest's Cipher 5
RSA	Rivest - Shamir – Adleman
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SOC	Security Operations Center
SSH	Secure Shell Protocole
SSL	Secure Sockets Layers
TLS	Transport Layer Security
URL	Uniform Resource Locator
VPN	Virtual Private Network
XOR	eXclusive OR

Introduction Générale

De nos jours, la sécurité informatique devenue un problème majeur qui préoccupe les organisations et les entreprises à cause des incidents de sécurité de leurs systèmes d'information. Ces incidents de sécurité qui représentent tout événement ne faisant pas partie des opérations standards et pouvant provoquer une interruption de service ou altérer sa qualité, sont de plus en plus nombreux et multiformes. De plus, aucune organisation/entreprise ne peut affirmer maîtriser entièrement (à 100%) son système d'information et encore moins sa sécurité. Pour cela, disposer d'une équipe spécialisée en sécurité informatique (appelée aussi équipe de réponse aux incidents de sécurité informatique ou CSIRT pour Computer Security Incident Response Team) aide toute organisation/entreprise à réduire, voire à prévenir, les incidents majeurs et à protéger un patrimoine précieux.

Spécialisée dans les technologies de l'information et de la communication, EL Djazaïr Information Technology (ELIT) est une société algérienne assurant, entre autres, la sécurité des systèmes d'information via une plateforme de sécurité à la pointe de la technologie. Elle met à la disposition de ses utilisateurs un portail CSIRT ELIT pour le signalement des incidents de sécurité de l'information. Le CSIRT ELIT est composé d'une équipe pluridisciplinaire d'experts (malwares, test d'intrusion, veille, lutte contre la cybercriminalité…) chargée de prévenir et de réagir en cas d'incidents de sécurité informatique. Pour ce faire, les membres d'équipe coopèrent et échangent des informations (entre eux et avec utilisateur) contenant les déclarations des incidents qui sont classés très critiques. Malheureusement, ces échangent ne sont pas sécurisées et les messages passent en clair ce qui entraine des problèmes de confidentialités d'intégrité et des données. Un certain nombre de questions se posent Comment ces échanges doivent être sécurisés pour assurer au mieux la sécurité et l'intégrité des données ? Comment puissions-nous échanger certaines de nos données avec d'autres personnes de confiances ? C'est pourquoi le CSIRT ELIT doit déposer d'un système cryptographique permettant de préserver la confidentialité des échanges et 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. C'est dans ce contexte que s'inscrit notre problématique.

Ainsi, l'objectif de notre travail est de concevoir et d'implémenter un système cryptographique pour le CSIRT ELIT afin de résoudre les problématiques de la confidentialité et l'intégrité des données échangées entre le CSIRT ELIT et ses différents utilisateurs.

Notre mémoire est divisé en deux parties comme ceci :

- **Dans la partie 1 :** nous présentons notre étude bibliographique qui est organisé en trois chapitres :

- **Le chapitre 1,** où nous donnons un aperçu sur les incidents de sécurité
- **Le chapitre 2,** où nous présentons les équipes de réponse aux incidents de sécurité informatique (CSIRT).
- **Le chapitre 3,** dans lequel nous étudions les systèmes cryptographiques.

- **Dans la partie 2 :** nous détaillons la conception et le développement de notre solution en deux chapitres :

- **Le chapitre 4**, concerne la conception d'un système cryptographique hybride pour le CSIRT ELIT.
- **Le chapitre 5**, décrit l'implémentation de notre application.

En conclusion générale, nous synthétisons les deux parties de notre mémoire, en faisant ressortir les limites de notre solution ainsi d'exposer des axes d'ouvertures pour l'améliorer.

PARTIE 1 : ETUDE BIBLIOGRAPHIQUE

CHAPITRE I : INCIDENTS DE SECURITE

I.1 Introduction

La notion d'incident est très large et couvre des domaines variés : incident technique, incident fonctionnel, incident de sécurité. D'une manière générale, un incident peut être définit comme un événement causant des dommages. Ce chapitre a pour but de présenter globalement les incidents de sécurité informatiques, leur classification et comment les contrôler, afin de minimiser l'impact négatif des incidents critiques sur les activités métiers.

I.2 Définition d'un incident

En général, un incident est un risque qui perturbe le bon déroulement des activités et des missions de l'établissement. Autrement dit, c'est un événement qui menace la posture de sécurité d'une organisation CID (**C**onfidentialité**, I**ntégrité**, D**isponibilité**)** [1] :

a. **Confidentialité :** est la prévention de la divulgation non autorisée, intentionnelle ou non intentionnelle, de contenus.
b. **Intégrité :** est la garantie que le message envoyé est le message reçu et que ce dernier n'est pas modifié intentionnellement ou non.
c. **Disponibilité :** fait référence aux éléments qui créent la fiabilité et la stabilité dans les réseaux et les systèmes. Il garantit que la connectivité est accessible en cas de besoin, permettant aux utilisateurs autorisés d'accéder au réseau ou aux systèmes [2].

Autres définitions existent dans la littérature, les plus intéressants :

- **Celle de l'ISO (International Organization for Standardization) 27000 :** un incident est un ou Un ou plusieurs événements intéressant la sécurité de l'information, indésirable(s) ou inattendu(s) présentant une probabilité forte de compromettre les opérations liées à l'activité de l'organisme et de menacer la sécurité de l'information [3].
- **Celle de l'ITIL (Information Technology Infrastructure Library)[1]:** un incident est tout événement ne faisant pas partie du fonctionnement standard d'un service et qui cause, ou peut causer, une interruption ou une diminution de la qualité de ce service [3].

I.3 Classification des Incidents de Sécurité

La classification des incidents informatiques aide à identifier et acheminer les incidents vers le bon technicien, économisant du temps et des efforts [5]. Quoiqu'il n'existe aucune classification parfaite [4], les incidents dans un environnement informatique peuvent être classifiés de plusieurs façons Différentes. Nous avons choisi celle adoptée par les équipes de réponse aux incidents de sécurité informatique ou CSIRTs (Computer Security Incident Response Team)

[1] ITIL est un ensemble de bonnes pratiques, procédures et méthodes qui servent de lignes directrices pour l'amélioration de la gestion des services dans l'environnement informatique.

qui font l'objet de notre travail et seront détaillés dans le chapitre suivant. Le tableau suivant résumé cette classification [6] :

Classes d'incidents	Descriptions	Exemples
Contenu Abusif	Un courrier électronique non sollicité, la plupart du temps de la publicité qui encombre le réseau, et fait perdre du temps à leurs destinataires.[7]	Spam,
	Discrédits, ou discrimination contre une personne d'un point de vue cyber.	Harcèlement,
Code malicieux	Logiciel intentionnellement introduit dans un système pour un but nocif. L'interaction d'un utilisateur est normalement nécessaire pour activer ce code.	Virus, Ver, Cheval de Troie, Spyware, etc.
Collecte d'informations	Attaque qui consiste à envoyer des requêtes à un système pour découvrir ses failles. Ceci inclut également tout type de processus de test pour collecter des informations sur les hôtes, les services et les comptes, par exemple : requête DNS (Domain Name System), ICMP (Internet Control Message Protocol), SMTP (Simple Mail Transfer Protocol), …	Scanning
	Collecte d'informations sur un être humain sans utiliser de moyens techniques (ex : mensonges, menaces, …).	Ingénierie sociale
Tentatives d'intrusion	Sont des attaques informatiques menées contre des entreprises afin de voler ou consulter des informations sensibles. Elles sont d'une efficacité redoutable : investigations sur la cible, piratage de postes de travail et de serveurs, maintien de portes dérobées afin de conserver un accès au système d'information… Ces tentatives d'intrusion sont les faits des cybercriminels aux intentions très variées : certains sont financés par des États, ou des concurrents, alors que d'autres sont seulement des opportunistes espérant pouvoir revendre les données volées.[8]	Exploiter des vulnérabilités connus, tentatives de connexion.
Intrusions	Une compromission réussie d'un système ou d'une application (service) qui peut être causé à distance par une nouvelle vulnérabilité ou une vulnérabilité inconnue, mais aussi par un accès local non autorisé.	Compromission d'un compte privilégié, Compromission d'un compte non privilégié,

		Compromission d'une application.
Indisponibilité	C'est une attaque touchant la disponibilité des données sensibles et services de la société.	DOS, DDOS(Denial-of-Service), etc.
Sécurité de l'information	Peut être mise en mal par un compte ou une application compromise. Aussi, les attaques qui interceptent et accèdent aux informations pendant leur transmission sont possibles (écoute, usurpation, ou hijacking).	Accès non autorisé aux informations, Modification non autorisée aux informations.
Fraude informatique	Est le fait intentionnel et sans droit d'introduire, de modifier ou d'effacer des données dans un système informatique ou de modifier l'utilisation normale de ces données.	Usage non autorisé des ressources, Droit d'auteur (Copyright),
Autres	Tout incident qui ne fait pas partie des catégories citées ci-dessus.	

Tableau 1 : Les principales classes des incidents de sécurité.

I.3.1 Exemple d'incident

Dans le tableau suivant, nous allons détailler quelques exemples des incidents de sécurité (cités dans le tableau 1) tout en donnant leurs mécanismes de sécurité :

Nom de l'incident	Description	Mécanismes de sécurité
Les virus	Ce sont des programmes malveillants qui ont pour but de se reproduire. Souvent, ils sont gênants pour l'utilisateur, puisqu'ils peuvent détruire des fichiers sur l'ordinateur [9].	Anti-virus, Pare-feu [10]
Les vers	Ce sont des programmes qui se propagent d'ordinateur à ordinateur via un réseau comme l'Internet. Ainsi, contrairement à un virus, les vers n'ont pas besoin d'un programme hôte pour assurer leur reproduction.	Anti-virus [11]

	Leurs poids est très léger, ce qui leur permet de se propager à une vitesse impressionnante sur un réseau, et pouvant donc saturer ce dernier et Espionner l'ordinateur ou il se trouve, offrir un port dérobé aux les pirates informatiques [9].	
Cheval de Troie	C'est un programme ou un code malveillant intégré à une application par ajout ou par modification de son code. Lors de l'exécution de ce programme. Le bout de code malveillant pourra exécuter des commandes spécifiques (récupération de fichiers de mot de passe, etc.) à l'insu de l'utilisateur, reposant sur une porte dérobée « backdoor » [9].	Anti-virus [12]
Le sniffing	C'est une attaque de sécurité réseau courante dans laquelle un programme ou un périphérique prend des informations importantes du trafic réseau d'un réseau spécifique. L'objectif principal du sniffer est de voler des mots de passe, des fichiers (fichiers FTP (File Transfer Protocol), fichiers e-mail) et du texte e-mail [13].	Cryptage du canal en utilisant le protocole HTTPS[2] (sessions cryptées SSL[3]) lors de l'envoi des données, et/ou les réseaux privés virtuels VPNs (**V**irtual **P**rivate **N**etwork),
Exploiter des Vulnérabilités connues	Une tentative pour compromettre un système ou interrompre tout service en exploitant les vulnérabilités avec des identifiants standardisés comme un nom CVE (ex : Buffer overflow, Portes dérobées, etc.) [6].	Un firewall
Tentatives de connexion	Tentatives de connexion multiples (vol ou crack de mots de passe, force brute) [6].	Utiliser des mots de passe « forts ».

[2] **H**yper**T**ext Transfer **P**rotocol **S**ecure.
[3] **S**ecure **S**ockets **L**ayers.

DOS ou DDOS	Les attaques de type Denial-of-Service ont pour but de saturer un routeur ou un serveur afin de le crasher. Ces types d'attaque sont très faciles à mettre en place et très difficile à empêcher pour Récupérer un accès : une attaque de type Denial Of- Service fait, la plupart du temps, partie d'une attaque visant à obtenir le contrôle d'une machine ou d'un réseau [9].	IDS (Intrusion Detection System), firewall ou ACL (Listes de Contrôle D'Accès).
Usage non autorisé des ressources	L'utilisation des ressources à des buts non autorisés, incluant des activités à but lucratif (ex. l'usage d'email pour participer dans des transactions illégales [6].	Plusieurs décisions de la justice pour limiter ces fraudes informatiques.
Droit d'auteur (Copyright)	Vendre ou installer des copies de logiciels commerciaux illégalement ou d'autres matériels sous droit d'auteur (Warez) [6].	
Man-in-the-Middle (MitM)	Les MitM sont un type d'attaque dont le principe est de s'insérer dans les communications entre un serveur et un client [14].	Cryptage des données.
Le crypto jacking	Le crypto jacking exploite plusieurs ordinateurs au moyen de logiciels utilisant un langage de script intégré. Le plus courant est le logiciel Coin Hiveui s'exécute en arrière-plan lorsqu'on navigue sur une page web [16].	- Extensions Chrome qui vérifient les codes des pages web visitées. One Coin et MinerBlock sont deux extensions qui permettent de détecter et bloquer les malwares de minage de cryptomonnaies. - Utiliser les bloqueurs de scripts comme No-Script et ScriptSafe et les bloqueurs de publicité. - La sécurisation du réseau informatique [16].

Attaque ransomware	Les ransomwares constituent une menace en croissance rapide pour les fichiers de données des particuliers et des entreprises. Il crypte les fichiers sur un ordinateur infecté et détient la clé pour décrypter les fichiers jusqu'à ce que la victime paie une rançon. En raison des sommes importantes à réaliser, de nouvelles versions apparaissent fréquemment. Cela permet de contourner le logiciel antivirus et d'autres méthodes de détection d'intrusion [17].	Éviter les liens et les pièces jointes par e-mail. Éviter de cliquer sur des liens ou d'ouvrir des pièces jointes dans des spams. Mettre à jour le système d'exploitation, les navigateurs, les logiciels et les plug-ins tiers. Eteindre la machine infectée et arrêter le réseau qui la connecte. [17]

Tableau 2 : Des exemples des incidents de sécurité.

I.3.2 Principaux Mécanismes de sécurité

Les mécanismes et les outils de détection d'incidents permettent d'assurer la sécurité des systèmes informatiques et les rendre plus efficaces. Parmi ces mécanismes et outils, nous décrivons ceux les plus importantes cités dans le tableau 2 :

Mécanisme de sécurité	Description
IDS	Un système de détection d'intrusion est un mécanisme destiné à repérer les adjectifs anormaux ou suspects sur la cible analysée (un réseau ou un hôte). Il permet ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions [9].
Pare-feu	Un pare-feu (en anglais Firewall) est un système permettant de séparer un réseau interne d'un réseau externe. Il permet de filtrer les communications dans les deux sens et ainsi protéger le réseau interne des éventuelles menaces provenant de l'extérieur [9].
VPN	VPN, pour Virtual Private Network désigne un réseau crypté dans le réseau Internet, qui permet à une société dont les locaux seraient géographiquement dispersés de communiquer et partager des documents de manière complètement sécurisée, comme s'il n'y avait qu'un local avec un réseau interne [18].
ACL	Une ACL est une liste de règles permettant de filtrer ou d'autoriser du trafic sur un réseau en fonction de certains critères (IP[4] source, IP[5] destination, port source, port destination, protocole, ...). Une ACL permet de soit autorisée du trafic (permit) ou de le bloquer(deny) [19].
Cryptage	C'est le processus de codification ou de chiffrement des données afin qu'il ne puisse être lu que par une personne ayant les moyens de le ramener à son état d'origine [20].
Antivirus	Un antivirus est un logiciel qui a pour but de détecter et de supprimer les virus d'un système informatique [9].

Tableau 3 : Les mécanismes de sécurité.

[4] Internet Protocol

I.4 Gestion des incidents

La gestion des incidents concerne la prise en charge de tous les incidents informatiques tout au long de leurs cycles de vie [21]. Autrement dit, c'est un processus de gestion des interruptions du service informatique, elle s'étend d'un utilisateur final signalant un problème jusqu'au membre d'une équipe du service d'assistance résolvant ce problème [5]. Il permet de **[22]** :

- Minimiser l'impact des incidents sur les métiers de l'entreprise.
- Fournir un meilleur contrôle des performances, en conformité avec les accords de niveaux de services (SLA).
- Utiliser plus rationnellement le personnel IT.
- Satisfaire l'utilisateur.
- Offrir une meilleure identification des coûts en ayant une plus grande connaissance des dysfonctionnements des services IT.

I.4.1 Le processus de gestion des incidents

Le processus de gestion des incidents peut être résumé de la façon suivante :

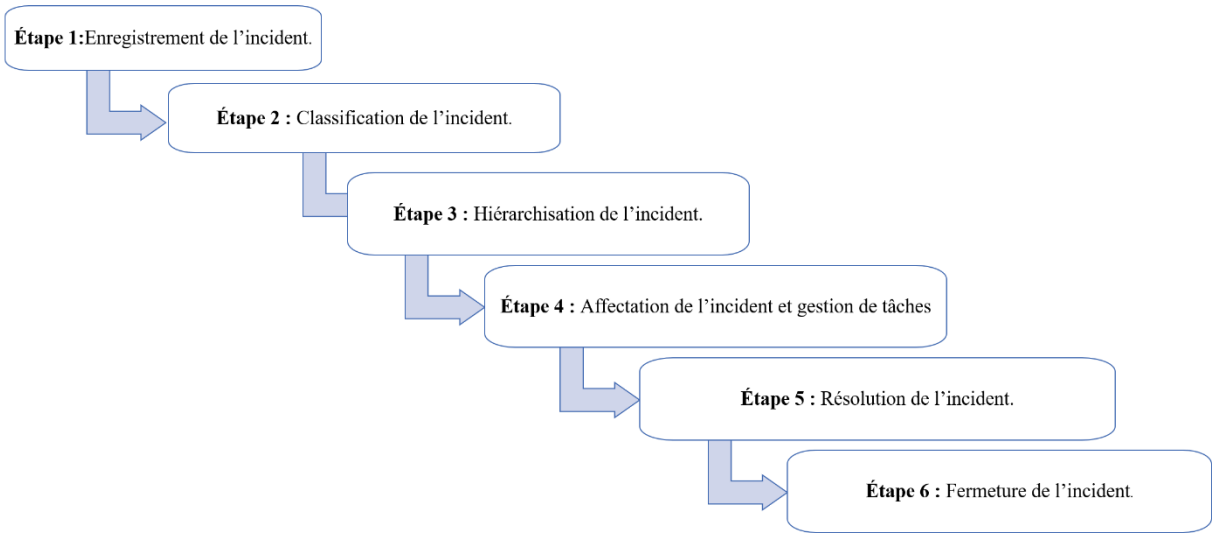


Figure 1 : Le processus de gestion des incidents [5].

1. **Enregistrement de l'incident** : Dans la gestion des incidents, la première étape est de signaler l'incident identifié. Cela peut être fait par les utilisateurs finaux eux-mêmes ou par les agents pour le compte des utilisateurs [23]. Un incident peut être enregistré par appel téléphonique, e-mail, SMS (**S**hort **M**essage **S**ervice), formulaire Web publié sur le portail ou par message sur le chat en direct [5].
2. **Classification de l'incident :** Répartir les incidents dans les catégories et sous-catégories appropriées permet d'identifier facilement le bon groupe et le bon agent [23].
3. **Hiérarchisation de l'incident :** Cette étape permet de définir les priorités d'un incident en fonction de son impact et de son urgence [24].
4. **Affectation de l'incident et gestion de tâches :** A ce niveau, l'incident est automatiquement affecté à un technicien disposant de l'expertise adéquate. L'incident peut être aussi décomposé en sous-activités ou tâches en fonction de sa complexité. Les tâches sont généralement créées lorsqu'une résolution d'incident requiert la contribution de multiples techniciens provenant de différents services [5].
5. **Résolution de l'incident :** Un incident est considéré résolu lorsque le technicien a trouvé une solution temporaire ou permanente au problème [5].
6. **Fermeture de l'incident :** une fois que le problème est résolu, l'incident peut être fermé [5].

En général, ce processus est intégré dans une méthode documentée de gestion des incidents, vulnérabilités et failles de sécurité informatique. On parle ici de « plan de réponse » qui est utilisé dans les environnements et les installations informatiques d'entreprises pour identifier, répondre, limiter et contrer les incidents de sécurité au fur et à mesure qu'ils surviennent [49].

I.4.2 Plans de réponse aux incidents

Une bonne équipe de sécurité doit pris en charge un plan de réponse aux incidents qui est formulé, supporté dans toute la société et testé régulièrement. Il est important de se rendre compte qu'avec assez de temps et de ressources, quelqu'un arrivera à briser les protections du système ou réseau le plus sécurisé et non seulement les systèmes qui sont faible et vulnérable. La figure suivante montre les étapes nécessaires à la création d'un plan de réponse aux incidents [25] :

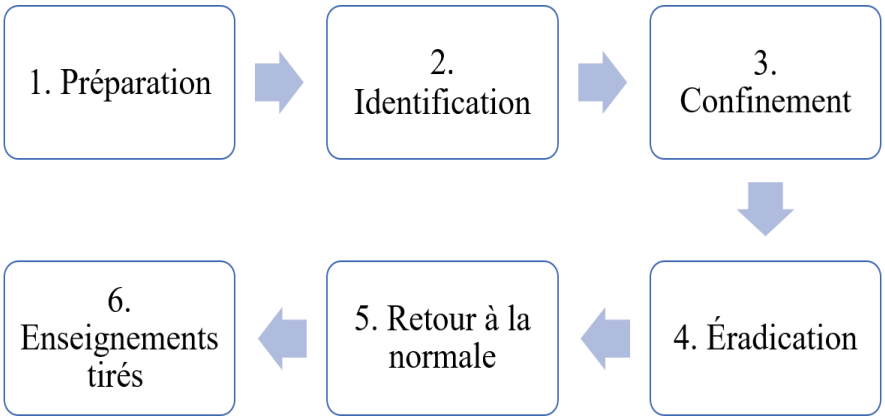


Figure 2 : Un plan de réponse aux incidents [25].

1. Préparation : Définir une politique de sécurité d'entreprise, définir un guide pour gérer les incidents de sécurité y compris comment l'équipe de réponse doit documenter les incidents et les communications internes et externes.
2. Identification : définir le critère qui déclenche l'intervention de l'équipe d'experts en sécurité. Il pourrait s'agir d'un type de problème spécifique ou l'émission d'une alerte qui déclenche un plan de réponse aux incidents.
3. Confinement : Il existe deux types de confinement : long et court. Le confinement à court terme est une réponse immédiate qui permet d'empêcher la menace de se propager et de faire davantage de dégâts. Le confinement à long terme inclut le retour en production de tous les systèmes pour revenir à un fonctionnement normal, mais sans les comptes et backdoors qui ont permis l'intrusion.
4. Éradication : mettre en place un processus de restauration de tous les systèmes affectés.
5. Retour à la normale : déterminer comment remettre tous les systèmes en production après avoir vérifié qu'ils sont propres et dépourvus de tout élément suspect pouvant entraîner un nouvel incident de sécurité.
6. Enseignements tirés : Actualiser le plan de réponse aux incidents en fonction des retours et de toute lacune identifiée.

I.4.3 Les avantages et les limites de la gestion des incidents

Le système de gestion des incidents apporte les avantages suivants [23] :

- Des opérations de travail fluides
- Une meilleure productivité
- Des utilisateurs finaux satisfaits
- Le maintien de niveaux de service uniformes
- L'identification et la prévention proactives des incidents majeurs

Cependant, il peut rencontrer différents problèmes notamment **[22]** :

- Manque d'engagement de la Direction.
- Manque de compétences.
- Ressources insuffisantes.
- Outils logiciels insuffisants ou mal adaptés.
- Utilisateurs et intervenants IT ignorant le processus.

I.5 Conclusion

Dans ce chapitre, nous avons cité les différentes classes d'incidents de sécurité qui représentent tout événement ne faisant pas partie des opérations standard et pouvant provoquer une interruption de service ou altérer sa qualité. Nous avons vu aussi la gestion des incidents qui réagit pour réduire les dégâts, documenter les solutions pour les problèmes récurrents ou

familiers, et établir des rapports. A cet effet, les organisations ou les entreprises pensent à mettre en place une équipe de réponse aux incidents de sécurité informatique ou un CSIRT (Computer Security Incident Response Team) qui se compose des d'experts en sécurité informatique organisées pour réagir en cas d'incident de sécurité. Ces CSIRTs font l'objet du chapitre suivant.

CHAPITRE II : ÉQUIPES DE REPONSE AUX INCIDENTS DE SECURITE INFORMATIQUE (CSIRT)

II.1 Introduction

De nos jours-là, la sécurité des systèmes d'informations et des réseaux de communication devient un enjeu stratégique dans les organisations. Et pour que le niveau de sécurité puisse évoluer dans le bon sens, les organisations pensent aujourd'hui à mettre en place une équipe d'experts en sécurité informatique ou un CSIRT (Computer Security Incident Response Team).

L'apparition du premier CSIRT a coïncidé avec la propagation du premier « ver » informatique développé par un étudiant de l'université américaine de Cornell. En novembre 1988, ce programme informatique commence à se propager dans ARPANET[5], l'ancêtre d'Internet, qui ne comprenait à l'époque qu'environ 60 000 ordinateurs. Avec seulement 3 à 4% de machines contaminées, le réseau devint complètement indisponible pendant plusieurs jours. Pour éliminer ce « ver Internet » (nommé « Morris »), une équipe d'analyse ad hoc fut créée avec des experts de l'institut américaine MIT (Massachusetts Institute of Technology), de l'université de Californie à Berkeley et l'université américaine de Purdue. Ces derniers ont pu procéder au « reverse engineering[6] » du code du ver pour identifier et corriger les failles qu'il exploitait et développer une solution d'éradication. C'est à la suite de cet incident majeur que l'agence américaine DARPA (Defense Advanced Research Projects Agency), a pris la décision de mettre en œuvre une structure permanente appelée « Computer Emergency Response Team / Coordination Center (CERT/CC) » dans le but de disposer d'une équipe capable de répondre à des incidents informatiques et qui pourrait jouer un rôle de coordination avec les administrateurs informatiques des réseaux touchés

Dans ce chapitre, nous allons expliquer le concept de CSIRT en commençant par le définir et citer ses avantages. Ensuite, nous présentons les principaux services offerts par CSIRT aux différents secteurs, puis une étude pour l'approche de création d'un CSIRT. Enfin, nous allons présenter notre cas d'étude qui concerne le CSIRT ELIT.

II.2 Définition d'un CSIRT

Un CSIRT (Computer Security Incident Response Team)[7] ou une équipe de réponse aux incidents de sécurité informatique est une équipe d'experts en sécurité informatique ayant pour mission principale de répondre aux incidents en proposant les services nécessaires au traitement des attaques et en aidant leurs parties prenantes à restaurer les systèmes qui en ont fait l'objet [26].

Le CSIRT peut offrir en outre les avantages suivants [26] :

- La centralisation de la coordination en matière de sécurité informatique au sein de l'organisation (point de contact).

[5] ARPANET- est le premier réseau à transfert de paquets développé aux États-Unis par la DARPA. Le projet fut lancé en 1966, mais ARPANET ne vit le jour qu'en 1969.

[6] Représente l'étude et l'analyse d'un système pour en déduire son fonctionnement interne.

[7] L'acronyme CSIRT est principalement utilisé en Europe comme synonyme du terme protégé CERT (Computer Emergency Response Team/ Equipe de réponse aux urgences informatique) et déposé aux États-Unis par le CERT|CC : centre de coordination (Coordination Center, CC) du CERT [26].

- La centralisation et la spécialisation du traitement et de la réponse aux incidents informatiques.
- La disponibilité d'une expertise permettant de soutenir les utilisateurs et de les aider à la restauration de leur système après un incident de sécurité.
- La gestion des aspects juridiques et la protection des preuves en cas d'action en justice.
- Le suivi des évolutions dans le domaine de la sécurité.
- L'incitation des parties prenantes à coopérer en matière de sécurité informatique (sensibilisation).

II.3 Services fournis par un CSIRT

Un CSIRT peut proposer un très large éventail de services, mais aucun CSIRT n'en propose actuellement la gamme complète. La sélection des services les mieux adaptés apparaît donc comme une décision essentielle [27].

Le tableau ci-dessous résume la liste des services que peut proposer un CSIRT :

Services de bases	Services réactifs	Services proactifs	Traitement des artefacts	Gestion de la qualité de la sécurité
Exemples des sous-services fournis	• Alertes et avertissements. • Traitements des incidents de sécurité. • Analyse des incidents. • Appui à la réponse aux incidents. • Coordination de la réponse aux incidents. • Réponses aux incidents sur place. • Traitements des vulnérabilités. • Analyse des vulnérabilités. • Réponse aux vulnérabilités. • Coordination des réponses aux vulnérabilités.	• Annonces. • Veille technologique. • Audits ou évaluations de la sécurité. • Configuration et maintenance de la sécurité. • Développement d'outils de sécurité. • Services de détection des intrusions. • Diffusion d'informations relatives à la sécurité.	• Analyse des artefacts. • Réponse aux artefacts. • Coordination des réponses aux artefacts.	• Analyse des risques. • Continuité de l'activité et reprise après sinistre. • Consultance en matière de sécurité. • Sensibilisation. • Education/formation. • Évaluation ou certifications des produits.

Tableau 4 : Les services fournis par un CSIRT.

Dans ce qui suit, nous allons décrire brièvement ces services.

II.3.1 Services réactifs

Les services réactifs visent à gérer les incidents et à réduire les dommages qui en découlent. Les services les plus importants sont :

a. Alertes et avertissements : ce service consiste à diffuser des informations décrivant une attaque, une vulnérabilité de sécurité, une alerte d'intrusion ou un virus informatique, et à recommander des mesures à court terme pour remédier aux problèmes qui en découlent.

b. Traitement des incidents de sécurité : ce service consiste en un certain nombre d'étape d'un processus depuis la déclaration de l'incident jusqu'à sa résolution.

c. Analyse des incidents : ce service consiste essentiellement à examiner toutes les informations disponibles, ainsi que les éléments probants ou artefacts relatifs à un incident ou un événement donné. L'analyse a pour but de déterminer l'ampleur de l'incident, l'étendue du dommage causé, la nature de l'incident et les stratégies de réponse ou solutions temporaires.

d. Réponse aux incidents sur place : le CSIRT fournit une assistance directe à ses parties prenantes en facilitant sur place la reprise après sinistre. Le CSIRT procède lui-même à l'examen physique des systèmes affectés et procède à leur réparation et leur restauration.

e. Appui à la réponse aux incidents : par téléphone, par courriel, par télécopie ou par l'envoi de documentation, le CSIRT fournit à distance des conseils permettant au personnel local de procéder lui-même à la restauration.

f. Coordination de la réponse aux incidents : le CSIRT joue le rôle de coordinateur des différents services impliqués dans le traitement des incidents :

- ✓ Chaînes fonctionnelles et hiérarchiques.
- ✓ Juridique, police / gendarmerie.

g. Traitement des vulnérabilités : le traitement des vulnérabilités comprend la réception des informations et signalements concernant des vulnérabilités au niveau des matériels et des logiciels, l'analyse de la nature, du fonctionnement et des conséquences des vulnérabilités, et l'élaboration de stratégies de réponse permettant de détecter les vulnérabilités et d'y remédier.

h. Analyse des vulnérabilités : le CSIRT procède à l'examen technique des vulnérabilités et à leur analyse, tant au niveau matériel que logiciel.

i. Réponse aux vulnérabilités : ce service vise à déterminer la réponse la plus adéquate pour atténuer la vulnérabilité ou y remédier.

j. Coordination de la réponse aux vulnérabilités : le CERT avertit les différents départements de l'entreprise ou les parties prenantes de l'existence de la vulnérabilité, et fournit des informations sur les moyens d'y remédier ou d'en atténuer les effets.

II.3.2 Services proactifs

Les services proactifs permettent de prévenir les incidents par des actions de sensibilisation et de formation :

a. **Annonces :** ce service vise à annoncer les alertes d'intrusion, les avertissements de vulnérabilité et les bulletins de sécurité pour permettre aux parties prenantes de protéger leurs systèmes et réseaux contre les problèmes récemment détectés, avant même qu'ils puissent être exploités.
b. **Veille technologique** : le CSIRT assure le service de veille technologique à ses clients en s'appuyant sur l'observation et l'analyse de l'information scientifique, technique et technologique, et de son impact sur l'environnement économique, commercial et financier.
c. **Audits ou évaluations de sécurité** : ce service assure l'examen approfondi de l'infrastructure de sécurité d'une organisation sur la base des exigences fixées par celle-ci ou par d'autres normes. Il peut également procéder à l'examen des pratiques organisationnelles en matière de sécurité.
d. **Configuration et maintenance des outils de sécurité, des applications, des infrastructures et des services :** ce service précise ou donne des indications quant à la manière de configurer et d'entretenir en toute sécurité les outils et peut procéder à des mises à jour et à la maintenance au niveau des outils et des services de sécurité : IDS, filtres, pare-feu, VPN ou autres mécanismes d'authentification.
e. **Développement d'outils de sécurité :** ce service porte sur le développement de tout outil nouveau spécifiquement destiné à répondre aux besoins ou aux souhaits des parties prenantes ou du CSIRT lui-même. Il peut s'agir, par exemple, de la mise au point de correctifs de sécurité spécialement conçus pour les logiciels utilisés par les parties prenantes. Ce service peut également prévoir le développement d'outils ou de scripts destinés à étendre la fonctionnalité des outils de sécurité déjà en place. : dispositif supplémentaire en vue du branchement d'un scanner de vulnérabilité ou de réseau, par exemple.
f. **Services de détection d'intrusion :** les CSIRTs qui offrent ce type de service examinent les journaux IDS [8], les analysent et remonte l'information aux clients.
g. **Diffusion d'informations relatives à la sécurité :** le CSIRT relaie un certain nombre d'informations qu'il reçoit en priorité. En général, il s'agit :
    - Des avis de vulnérabilité diffusés notamment par d'autres CSIRT, des éditeurs de logiciel, des équipementiers.
    - Des informations précises et des statistiques sur les incidents traités par le CSIRT.
    - Des alertes lorsque certains évènements dans l'actualité font augmenter considérablement le risque d'attaque sur le SI.
    - Des éléments de veille juridique.

[8] IDS : Intrusion Detection System- est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte). Il permet ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions.

II.3.3 Traitement des artefacts

Ce service comprend l'analyse de tout fichier ou objet présent dans un système et susceptible de participer à un acte malveillant (traces de virus, vers, script, cheval de Troie, etc.) [26].

a. **Analyse des artefacts** : Le CSIRT procède à l'examen technique de l'artefact détecté sur le système. Cette analyse peut couvrir l'identification du type de fichier et de structure de l'artefact, la comparaison d'un nouvel artefact par rapport à des artefacts existants ou à d'autres versions pour établir les similitudes et les différences, ou une rétroingénerie (désassemblage du code) pour déterminer le but et la fonction de l'artefact.
b. **Réponse aux artefacts** : Ce service a pour but de définir les actions les plus adéquates pour détecter et éliminer les artefacts présents dans un système, ainsi que les mesures destinées à prévenir leur installation.
c. **Coordination de la réponse aux artefacts :** Ce service prévoit le partage et l'analyse des résultats et des stratégies de réponse à un artefact donné avec des chercheurs, des CSIRT, des fournisseurs et d'autres experts en sécurité

II.3.4 Services de gestion de la qualité de la sécurité

Les services inclus dans cette catégorie ne relèvent pas spécifiquement du traitement des incidents, mais ils visent à améliorer la sécurité générale d'une organisation.

a. Analyse des risques : les CSIRTs sont en mesure d'apporter une valeur ajoutée à l'analyse et à l'évaluation des risques et d'améliorer ainsi la capacité de l'organisation d'apprécier les menaces réelles, de procéder à une évaluation qualitative et quantitative réaliste des risques pour son patrimoine informationnel, et de jauger les stratégies de protection.
b. Plan de continuité d'activité et reprise après sinistre : les CSIRTs qui présentent ce service participent à la planification et l'intégration d'un plan de continuité et de reprise d'activité (PCA/PRA) après un sinistre touchant la sécurité de l'information.
c. Consultance : le CSIRT peut fournir des conseils et des orientations concernant les pratiques de sécurité les mieux adaptées à l'activité des parties prenantes.
d. Sensibilisation : le CSIRT joue également un rôle préventif. L'objectif est de sensibiliser différentes populations (utilisateurs finaux, responsables, correspondants sécurité, informaticiens, etc.) à la sécurité informatique.
e. Éducation/formation : ce service consiste à fournir des formations contenant toutes les informations utiles en matière de prévention, de détection, de signalement et de réponse aux incidents de sécurité informatique.
f. Évaluation ou certification des produits : le CSIRT peut procéder à des évaluations portant sur des outils, des applications ou tout autre service, en vue de s'assurer de la sécurité des produits et de leur conformité à des normes de sécurité considérées comme acceptables par le CSIRT ou l'organisation concernée.

II.4 Différents Contextes de Création d'un CSIRT

Un CSIRT peut être créés dans différents contextes ou secteurs comme illustré dans la figure suivante [26] :

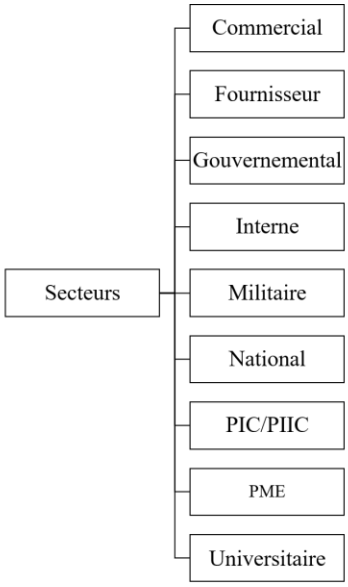


Figure 3 : Secteurs auxquels les services du CSIRT sont destinés [26].

- **CIRST dans le secteur commercial :** propose des offres de veille, de réponse à incidents à leurs clients.
- **CSIRT dans le secteur des fournisseurs :** développe et propose des solutions qui permettent d'en supprimer les vulnérabilités et de minimiser les effets négatifs éventuels de leurs failles.
- **CSIRT gouvernemental :** fournit des services aux organismes publics et, dans certains pays, aux citoyens.
- **CSIRT interne :** intervient pour aider et conseiller l'ensemble du groupe, et ses filiales voire ses clients en cas d'incident de sécurité.
- **CSIRT dans le secteur militaire :** fournit des services à des organisations militaires chargées de l'infrastructure informatique nécessaire à la défense.
- **CERT national :** constitue le point de contact du pays dans le domaine de la sécurité.
- **CSIRT dans le secteur de la PIC/PIIC[9] :** couvre l'ensemble des secteurs informatiques critiques nationaux et protège les citoyens du pays concerné.
- **CSIRT dans le secteur des PME (petites et moyennes entreprises) :** offre ses services à l'intérieur de sa propre branche d'activité ou à des groupes d'usagers analogues.
- **CSIRT dans le secteur universitaire :** fournit de services destinés aux établissements de l'enseignement supérieur.

[9] Protection des Infrastructures Critiques et/ou Protection de l'Infrastructure d'Information Critique (PIIC)

II.5 Approche de création d'un CSIRT

Après avoir comprendre le concept de CSIRT, ses avantages et les services qui peuvent l'offrir aux, différents secteurs, l'étape suivante consiste à étudier les approches adoptées lors de la création du CSIRT. Dans [26], l'agence européenne de sécurité d'information et de réseau ENISA (European Network and information Security Agency) recommande une approche générale de création (Figure 4) basant sur une étude plus approfondie de l'environnement, des parties prenantes ainsi que leurs missions. Une description plus approfondie dans les paragraphes qui vont suivre sur ces différentes démarches et qui peuvent servir à l'élaboration du plan d'activités / de projet [26].

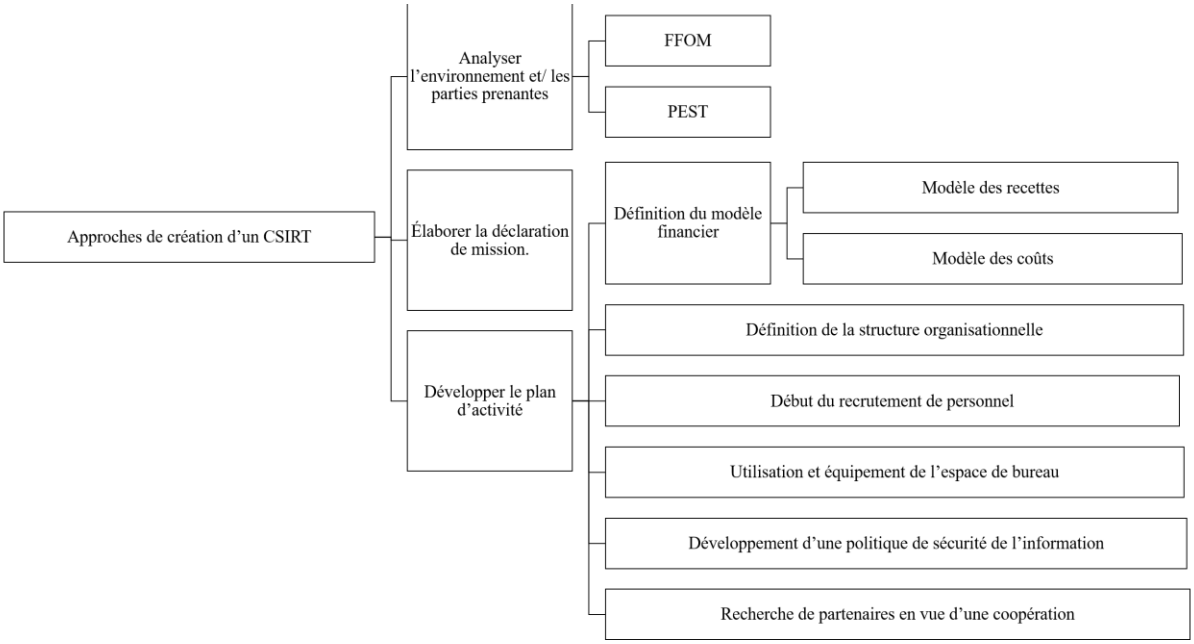


Figure 4 : Approches de création d'un CSIRT [26].

II.5.1 Analyser l'environnement et les parties prenantes

Il est très important de connaître les stratégies de communication, les besoins des parties prenantes[10], les voies de communication les mieux adaptées à la transmission des informations qui leur sont destinées, y compris les facteurs internes et externes pouvant affecter les activités d'organisation. Les théories de gestion décrivent plusieurs approches possibles de l'analyse du groupe cible, les plus importantes sont [26] :

- **FFOM** (**F**orces, **F**aiblesses, **O**pportunités et **M**enaces) : est un outil de planification stratégique qui combine à la fois les forces, les faiblesses, les opportunités et les menaces propre à une organisation commerciale.

[10] Le terme désormais bien établi (au sein des communautés CSIRT), un client particulier étant désigné comme « une partie prenante ».

- **PEST (P**olitique, **É**conomique, **S**ocioculturel et **T**echnologique**) :** utilisé pour mieux connaître les parties prenantes et, plus précisément, le contexte politique, économique, socioculturel et technologique dans lequel le CSIRT est appelé à fonctionner.

II.5.2 Élaborer la déclaration de mission

L'étape qui fait suite à l'analyse des besoins est l'élaboration de la déclaration de mission qui décrit la fonction essentielle de l'organisation au sein de la société en termes de produits et de services fournis aux parties prenantes. C'est une étape nécessaire et extrêmement importante au moment du démarrage. Elle permet de faire connaître clairement l'existence et le rôle du nouveau CSIRT. Par exemple,

CSIRT peut aider à mettre en œuvre des mesures proactives visant à réduire les risques et répondre aux incidents qui survient [26].

II.5.3 Développer le plan d'activité

Lors de la mise en œuvre d'un CSIRT, les organisations suivent les étapes écrites ci-dessous [26] :

a. Définition du modèle financier

Une série de services de base initiaux ont été sélectionnés à l'issue de l'analyse. Il convient de définir des conditions de prestation des services en question qui soient à la fois adaptées et payables. Pour cela, deux modèles existent :

- Modèle des coûts : basé sur la fixation des heures de service et le nombre (et la qualité) des effectifs à y affecter.

- Modèle des recettes : qui détermine comment les services planifiés peuvent-ils être financés ? Plusieurs scénarios sont envisageables, parmi lesquels :

L'utilisation de ressources existantes, les cotisations en vendant les services du CSIRT aux parties prenantes et la subvention au gouvernement ou à un organisme officiel.

b. Définition de la structure organisationnelle

La structure organisationnelle adéquate d'un CSIRT dépend largement de la structure déjà en place au sein de l'organisation.

Un CSIRT type définit les rôles suivants au sein de son équipe :

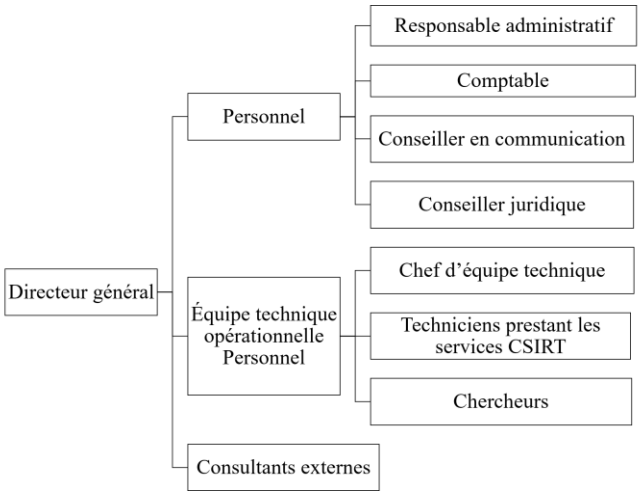


Figure 5 : La structure organisationnelle d'un CSIRT [26].

c. Début du recrutement de personnel : La réussite d'un CSIRT et son efficacité dépend à 90 % des professionnels de la sécurité qui les composent et les pilotent. Donc, la formation et le recrutement de vrais experts qui vont savoir analyser et traiter les incidents de sécurité est une des étapes les plus importantes lors de mise en place un CSIRT.

d. Utilisation et équipement de l'espace de bureau

Étant donné que les CSIRT traitent souvent des informations très sensibles, il vaut mieux :

- Confier à leur équipe le soin d'assurer la sécurité physique des locaux, ainsi que la sécurité du matériel informatique (consolider tous les systèmes, utiliser des logiciels de sécurité…),
- Prendre en compte des règles concernant les canaux de communication (formulaires électroniques pour le signalement des incidents, mettre un numéro téléphonique dédié à la disposition des parties prenantes…),
- Mettre en œuvre d'un système (ou des systèmes) de localisation des enregistrements (base de données de contact contenant les coordonnées des membres de l'équipe, d'autres équipes, etc.).

e. Développement d'une politique de sécurité de l'information

Une politique de sécurité de l'information « sur mesure » est mise en place selon le type de CSIRT. Outre la description des procédures et processus opérationnels et administratifs souhaités, elle devra veiller au respect des lois et normes applicables, notamment en matière de responsabilité du CSIR

f. Recherche de partenaires en vue d'une coopération

Il est recommandé de prendre contact avec d'autres CSIRT, afin d'être introduit auprès de leurs communautés. Ces dernières se montrent généralement très disposées à aider les nouvelles équipes à démarrer. La coopération entre les différents CSIRT a pour mission de

mettre en place un forum d'échange d'expériences et de connaissances, et d'aider à la création de nouveaux CSIRT et à la formation de leur personnel.

II.6 Etude du CSIRT ELIT

Spécialisée dans les technologies de l'information et de la communication, EL djazaïr Information Technology (ELIT) est une société algérienne comptant plus de 300 ingénieurs informaticiens, plus de 40 clients et des infrastructures hautement disponibles et sécurisées. Au-delà des aspects reconnus au domaine IT, les réseaux informatiques, le développement des sites web, la messagerie électronique, etc., ELIT assure la sécurité des systèmes d'information via une plateforme de sécurité à la pointe de la technologie et ce, avec une ressource humaine 100% algérienne [29].

II.6.1 Définition de CSIRT ELIT

CSIRT ELIT est un CSIRT interne formé d'une équipe pluridisciplinaire d'experts (malwares, test d'intrusion, veille, lutte contre la cybercriminalité…) chargée de prévenir et de réagir en cas d'incidents de sécurité informatique. Elle assure la veille sécuritaire en amont ainsi que l'analyse et le traitement des incidents en aval [28].

Les principaux objectifs du CSIRT ELIT sont [28] :

- Centralisation des demandes d'assistance suite aux incidents de sécurité.
- Traitement des alertes et réaction aux attaques informatiques.
- Établissement et maintenance d'une base de connaissance.
- Coordination et échange avec les autres CSIRTs.
- Sensibilisation.

II.6.2 Avantages du CSIRT ELIT

De ce fait, Le CSIRT ELIT permet de [28] :

- Renforcer la sécurité du système d'information.
- Assister les sociétés du Groupe Sonelgaz dans le traitement des incidents de sécurité de l'information.
- Bénéficier de l'expertise externe à travers une collaboration avec les différents CSIRTs internationaux pour l'échange et le partage des :
    - Vulnérabilités apparues dans le monde.
    - Rapports de résolution des incidents de sécurité.
    - Nouvelles sur la sécurité dans le monde.
    - Nouveaux outils de sécurité.

- Diminuer l'impact des incidents liés à la sécurité informatique pouvant toucher les systèmes d'information du Groupe.
- Accroître l'image de marque de la société.

II.6.3 Organisation du CSIRT ELIT

Le CSIRT ELIT est composé (Figure 6) :

- **D'une équipe de veille** qui a une activité continue, en grande partie itérative visant à une surveillance active des environnements sécuritaire, technologique, énergétique, commercial, etc. Cette équipe offre plusieurs fonctionnalités, prenant en charge la diffusion et le traitement des dernières informations et actualités dans les domaines de veille supportés par la solution, l'archivage de l'actualité récoltée des différents types de veille traités, le filtrage avancé sur les différents types de veille, etc [29].
- **D'une équipe SOC (Security Operations center)** qui permet d'assurer la sécurité de l'information [50].
- **D'un service helpdesk** qui permet de prendre en charge les clients. Un Help Desk a pour but de fournir des informations et des solutions techniques aux clients. En général, il est composé d'équipes de techniciens supports. Il appartient à ces derniers de trouver les solutions les mieux adaptées aux besoins des clients [84].
- **D'une équipe de sensibilisation (**ELIT Security Awareness**) :** qui est chargée d'inculquer les bonnes pratiques de la sécurité des données au personnel.

A la production d'un incident, le client signale cet incident, dans les meilleurs délais en fournissant les informations nécessaires à l'équipe de CSIRT. Cette dernier le transmet à:

- L'équipe Helpdesk qui procède au début à une première analyse et classification de l'incident. Ensuite, elle vérifie qu'il s'agit bien un incident de sécurité en restant en contact avec le client pour identifier les informations nécessaires à l'investigation. Une fois la solution trouvée, l'équipe de réponse aux incidents de sécurité rétablie le service (résoudre le problème) puis le teste. A la fin, le service Helpdesk informe de la clôture de l'incident.
- L'équipe de veille pour traiter les incidents récurrents.
- L'équipe de SOC pour traiter les vulnérabilités.
- L'équipe de sensibilisation pour prendre en compte cet incident dans l'inculcation des bonnes pratiques de la sécurité.

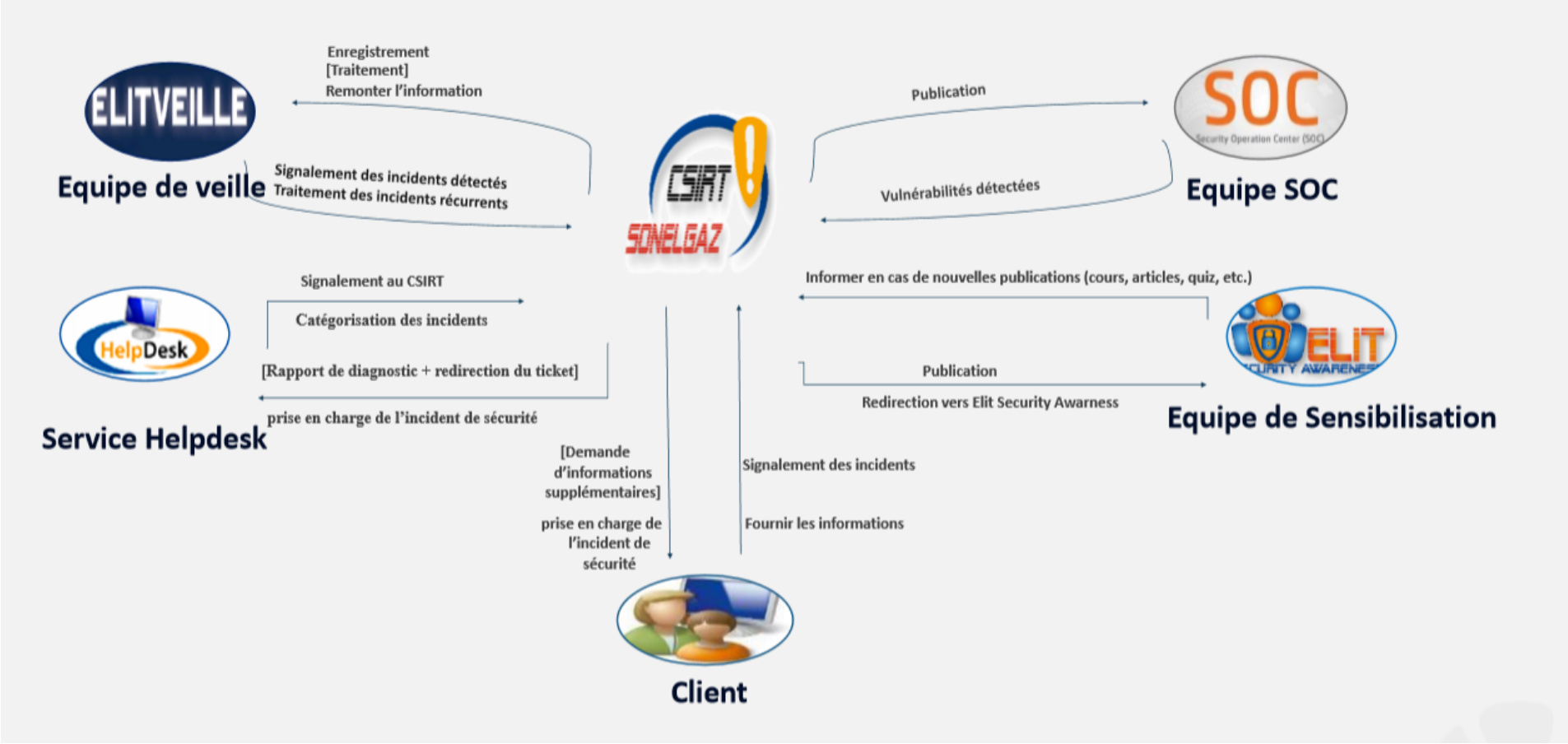


Figure 6 : Organisation du CSIRT ELIT [28].

II.6.4 Processus de réponse aux incidents

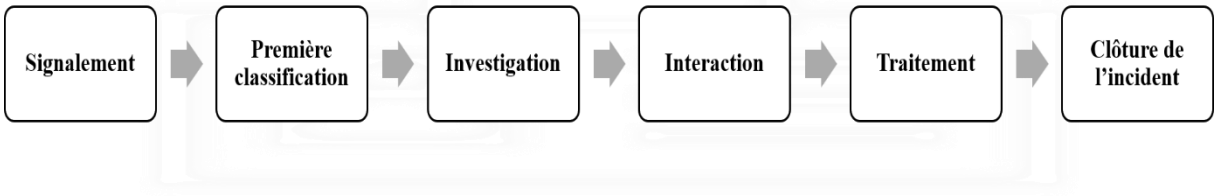


Figure 7 : Processus de réponse aux incidents CSIRT ELIT [28].

Comme illustré par la figure 7, le processus de réponse aux incidents passe par les étapes suivantes [28] :

1. **Signalement :** signaler l'incident, dans les meilleurs délais, au service Helpdesk.
2. **Première classification :** le service Helpdesk procède à une première analyse et classification de l'incident.
3. **Investigation :** l'équipe CSIRT vérifie qu'il s'agit bien d'un incident de sécurité et procède à l'investigation.
4. **Interaction :** le CSIRT reste en contact avec ses clients pour identifier les informations nécessaires à l'investigation.
5. **Traitement :** une fois la solution trouvée, le CSIRT rétablie le service puis le teste.
6. **Clôture de l'incident :** le service Helpdesk informe le client signalant l'incident, de la clôture de l'incident.

II.6.5 Limites du CSIRT ELITs

L'une des principales fonctions de cette équipe est la coopération et l'échange d'informations qui est nécessaire pour parvenir à répondre aux incidents. Néanmoins, ces échanges se font en clair sans aucune sécurisation bien que les informations contenant les déclarations des incidents soient classées très critiques. Ce qui entraine des problèmes de confidentialités d'intégrité et des données. Au fait, si les échanges se font en clair alors les données peuvent être volée, le contenu peut être altérer et les données peuvent être interceptées sans que les deux parties ne puissent s'en apercevoir.

Pour remédier à ces problèmes, il convient de veiller à ce que la diffusion de l'information doit être sécurisée et les données relatives à un incident sensible devraient toujours être envoyées sous forme cryptée**.** Aucun message ne doit passer en clair.

De plus, le CSIRT ELIT est en cours d'addition au FIRST[11], et l'une des exigences de l'adhésion au FIRST est la sécurité des échanges entre les CSIRTs afin de contribuer à la résolution rapide et efficace des incidents. Ainsi, le CSIRT ELIT doit disposer tout d'abord d'un système cryptographique pour sécuriser ses communications.

II.8 Conclusion

Dans la première partie de ce chapitre, nous avons essayé de répondre, entre autres, aux questions suivantes : C'est quoi un CSIRT ? Pour quels raisons les entreprises pensent à mettre en place un CSIRT (avantages et objectifs) ? Comment un CSIRT doit être organisé ? et Quels sont les services offerts par le CSIRT ? Dans la deuxième partie, nous nous sommes intéressés à notre cas d'étude « le CSIRT ELIT » en représentant ses objectifs, ses avantages, son organisation et son fonctionnement. Comme déjà mentionné, les échanges entre les entités du CSIRT ELIT doivent être sécurisées pour assurer au mieux la sécurité et l'intégrité des données. Une des solutions à ce problème est de disposer d'un système cryptographique pour sécuriser les échanges que ce soit en interne et ou externe. Dans le chapitre suivant, nous allons détailler le concept des systèmes cryptographiques

[11] FIRST (**F**orum of **I**ncident **R**esponse and **S**ecurity **T**eams) qui est une organisation mondiale qui regroupe 286 CSIRT et CERT. Comme TF-CSIRT, il s'agit avant tout d'un **cercle de confiance** dans lequel les différentes équipes de réponse à incident peuvent partager de l'information et des bonnes pratiques. Le FIRST organise également une sconférence annuelle internationale [76].

CHAPITRE III : SYSTEMES CRYPTOGRAPHIQUES

III.1 Introduction

À cause des nombreux d'attaques et pirates de nos jours, la sécurité des données d'information est devenue l'intérêt de tous les établissements et les sociétés, et puisque chaque action a une réaction on trouve des milliers de mécanismes de sécurité. Dans notre travail, nous nous intéressons à la cryptographie qui est une science permettant de préserver la confidentialité des échanges et 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.

Dans ce chapitre, nous allons étudier les systèmes cryptographiques, en commençant par les définir et citer leurs différentes classes. Puis, nous détaillons chaque classe (symétrique, asymétrique et hybride) pouvoir à la fin montrer et justifier notre choix du système cryptographie et des algorithmes de cryptage.

III.2 Définitions

Le mot « **Cryptographie** » est composé de deux mots grecs CRYPTO (caché) et GRAPHY (écrire).C'est donc l'art de l'écriture secrète. Plus formellement, la cryptographie peut être définie comme : « l'étude des méthodes donnant la possibilité d'envoyer des données de manière confidentielle sur un support donné » ou comme « une science permettant de préserver la confidentialité des échanges en utilisant les mathématiques pour le cryptage et le décryptage de données ». Elle permet ainsi de stocker des informations confidentielles ou de les transmettre sur des réseaux non sécurisés (tels que l'Internet), afin qu'aucune personne autre que le destinataire ne puisse les lire. La cryptographie consiste à sécuriser les données [31].

Dans ce qui suit, la définition d'autres concepts liés à la cryptographie :

- Le **cryptage** consiste à transformer une donnée (texte, message, ...) afin de la rendre incompréhensible par une personne autre que celui qui a créé le message et celui qui en est le destinataire. La fonction permettant de retrouver le texte clair à partir du texte crypté porte le nom de **décryptage** [32].
- Le **texte crypté (ou chiffré),** appelé également cryptogramme est le résultat de l'application d'un cryptage à un texte clair [32].
- La **clé** s'agit du paramètre impliqué et autorisant des opérations de cryptage et/ou décryptage [32].

III.3 Classification des systèmes cryptographiques

De nombreuses méthodes de cryptage ont été imaginées pour se protéger de la curiosité et de la malveillance des ennemis depuis de nombreux siècles. On peut classer ces méthodes comme le montre la figure suivante [33] :

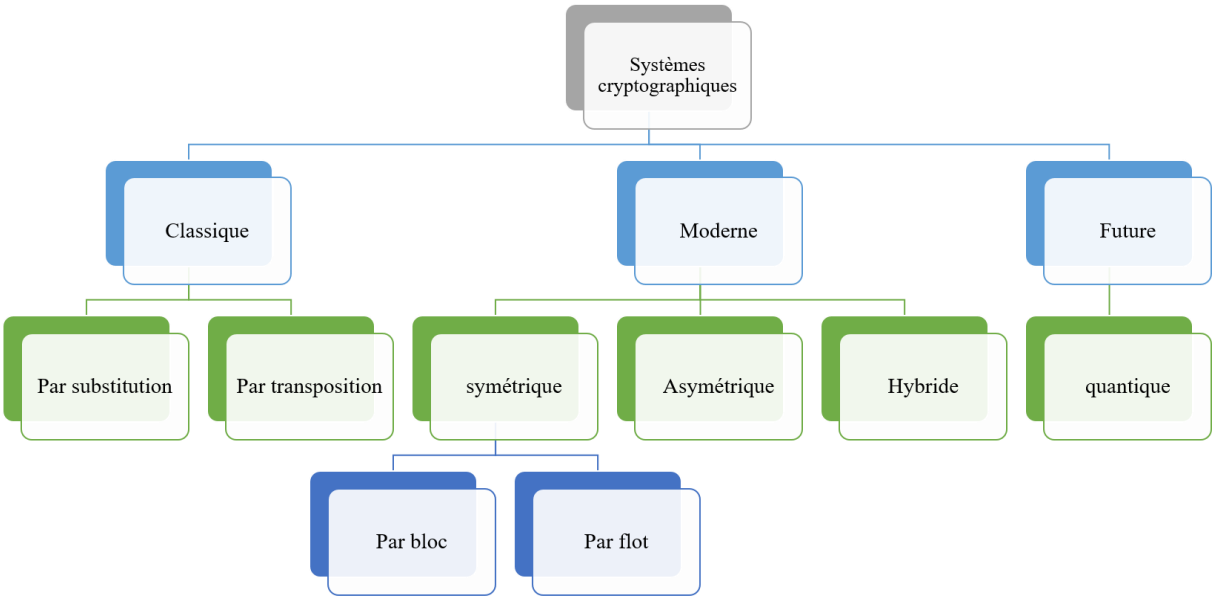


Figure 8 : Classification des systèmes cryptographiques [33].

Le tableau suivant résume la description de chaque classe des systèmes cryptographique :

Système cryptographique	**Description**	**Exemples**
Par substitution [32] [34] [35]	Le cryptage par substitution consiste à remplacer dans un message une ou plusieurs entités (généralement des lettres) par une ou plusieurs autres entités. On distingue deux types de systèmes cryptographiques par substitution : **Substitution mono-alphabétique** : consiste à remplacer chaque lettre par une autre lettre ou symbole. **Substitution poly-alphabétique :** Consiste à utiliser une suite de chiffres mono-alphabétique réutilisée périodiquement.	**Exemple de cryptage par Substitution mono-alphabétique :** le chiffre de César, le chiffre affine, ou encore les chiffres désordonnés. **Exemple de cryptage par Substitution poly-alphabétique :** le Chiffre de Vigenère, Chiffre de Vernam.
Par transposition [32]	Les transpositions 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.	La méthode de la grille.
Symétrique [37]	En raison de sa rapidité, le cryptage symétrique est largement utilisé pour protéger les informations dans de nombreux systèmes informatiques modernes.	AES (Advanced Encryption Standard), DES (Le Data Encryption Standard) …
Asymétrique [38]	La cryptographie à clé publique, également appelée cryptographie asymétrique est un domaine de la cryptographie qui utilise à la fois une clé privée et une clé publique, par opposition à la clé unique utilisée dans la cryptographie symétrique.	RSA (Rivest - Shamir – Adleman), El Gamal, **ECC (**Elliptic Curve Cryptography).
Hybride [39]	Dans les systèmes cryptographiques hybrides une clé aléatoire est générée pour l'algorithme symétrique. L'algorithme de cryptage symétrique est ensuite utilisé	PGP ((Pretty Good Privacy), SSL, GnuPG (GNU Privacy Guard) ...

	pour crypter le message. La clé aléatoire quant à elle, se voit cryptée grâce à la clé publique du destinataire. Il suffit ensuite d'envoyer le message crypté avec l'algorithme symétrique. Le destinataire décrypte la clé symétrique avec sa clé privée et via un décryptage symétrique retrouve le message.	
Quantique [40] [41]	La cryptographie quantique garantit une confidentialité absolue de l'information échangée au sein d'une fibre optique. Le secret de cette prouesse tient à la possibilité de véhiculer l'information par l'intermédiaire du constituant élémentaire de la lumière : le photon.	L'Algorithme de Deutsch-Josza, L'Algorithme de Simon, et l'Algorithme de recherche quantique (Grover)....

Tableau 5 : La description des classes des systèmes cryptographiques.

III.4 Systèmes cryptographiques modernes

Dans notre travail, nous nous intéressons aux systèmes cryptographiques modernes (symétrique, asymétrique et hybride) qui font l'objet de cette section.

III.4. 1 Système cryptographique symétrique

Dans la cryptographie symétrique (figure 9), une même clé est partagée entre l'émetteur et le récepteur. Cette clé dite symétrique est utilisée par l'émetteur pour crypter le message et par le récepteur pour le décrypter en utilisant un algorithme de décryptage symétrique [32]. Pour communiquer, il faut au préalable échanger la clé entre les deux protagonistes

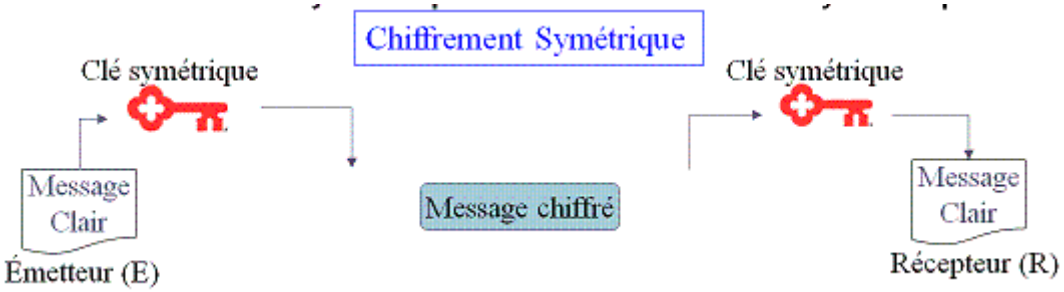


Figure 9 : cryptage symétrique [31].

III.4.1.1 Les types

Le cryptage symétrique peut être réalisé par bloc, ou par flux. [42].

Dans le cryptage par bloc, l'opération de cryptage s'effectue sur des blocs de texte clair [32], donc il est dédié aux transferts des fichiers et caractérisé par la réutilisation des clés [43].
On distingue trois catégories de chiffrement par bloc [32] :

- **Par substitution :** les substitutions consistent à remplacer des symboles ou des groupes de symboles par d'autres symboles ou groupes de symboles dans le but de créer de la confusion.
- **Par transposition :** les transpositions consistent à mélanger les symboles ou les groupes de symboles d'un message clair suivant des règles prédéfinies pour créer de la diffusion. Ces règles sont déterminées par la clé de chiffrement. Une suite de transpositions forme une permutation.
- **Par produit :** C'est la combinaison des deux. Le chiffrement par substitution ou par transposition ne fournit pas un haut niveau de sécurité, mais en combinant ces deux transformations, on peut obtenir un chiffrement plus robuste. La plupart des algorithmes à clés symétriques utilisent le chiffrement par produit.

Par ailleurs, le principe de cryptage par flux consiste à générer un flux pseudo aléatoire et de le combiner avec l'information bit à bit par l'opération XOR (eXclusive OR)[12]. A la réception, on applique le même mécanisme, et on restitue l'information. Ce type de cryptage est beaucoup plus rapide que n'importe quel algorithme de cryptage par bloc. De plus, au niveau des données cryptées en sortie, le cryptage par flux ne donnera pas forcément le même résultat en sortie alors que pour un bloc donné un cryptage par bloc aura toujours le même résultat. Ce mode de cryptage est souvent utilisé pour les communications en temps réel telles que le WI-FI, malgré qu'il permette deux utilisations d'une même clé en facilitant ainsi la cryptanalyse [43].

[12] La méthode XOR, appelée plus généralement fonction OU Exclusif est un opérateur logique. Le principe repose sur 2 opérandes qui peuvent avoir comme valeur VRAI (1) ou FAUX (0), le résultat prendra lui aussi comme valeur VRAI ou FAUX, VRAI dans le cas ou seulement l'un des deux est VRAI.)

III.4.1.2 Exemples sur les algorithmes

Dans le tableau suivant, nous citons les principaux algorithmes de la cryptographie symétrique :

Nom	**Type**	**Description**	**Avantages**	**Inconvénients**
DES [32]	Par bloc	Algorithme de cryptage par blocs de 64 bits. Il découpe virtuellement le texte clair en blocs de 64 bits qu'il code séparément, puis qu'il concatène.	• Il est complètement spécifié et facile à comprendre. • Il est facile à implémenter. • Il est rendu disponible à Tous, par le fait qu'il est public. • Il est adaptable à diverses applications (logicielles et matérielles). • Il est rapide et exportable. • Il repose sur une clé relativement petite, qui sert à la fois au chiffrement et au déchiffrement.	Les méthodes d'attaques sur le DES tel que la cryptanalyse différentielle et la recherche exhaustive de la clé avec le développement de technologie ont réussis à casser le DES. C'est pour cela la NSA perd sa confiance en DES et décide en 1987 de ne pas reconduire ce standard. La même chose, pour le 2 octobre 2000 le NIST qui en 2000 a choisi l'algorithme AES pour remplacer DES.
AES	Par bloc	Algorithme de cryptage par bloc de 128 bits permettant de crypter un texte en clair constitué de 128 bits de données à l'aide d'une clef secrète constituée de 128, 192 ou 256 bits [47].	• Grande sécurité. • Résistance à toutes les attaques connues. • Large portabilité : carte à puces, processeurs dédiés, … • Rapidité. • Lecture facile de l'algorithme. • Blocs de 128 bits et clés de	Le code et les tables sont différents pour le cryptage et le décryptage. Le décryptage est plus difficile à implanter en "Smart Card". Dans une réalisation matérielle, il y a peu de réutilisation des circuits de cryptage pour effectuer le décryptage [32].

			128/192/256 bits. • Durée de vie de 20 à 30 ans [46].	
RC4	Par flot	RC4 est un générateur de bits pseudo-aléatoires dont le résultat est combiné avec le texte en clair via une opération XOR [85].	• La vitesse de cryptage est élevée. • Il est très simple. • Le message clair a la même taille que le crypté. • Il existe une version allégée du cryptage RC4, portant le nom de ARC4 (Alleged RC4), utilisable légalement [32]	• RC4 vulnérable à plusieurs attaques comme l'attaque de Klein, attaque Royal Holloway, attaque Bar-mitsva
RC5 (Rivest's Cipher)	Par bloc	RC5 possède une taille variable de bloc 32, 64 ou 128 bits), une clef allant de 0 à 2048 bits et un nombre de tour de 0 à 255. Le chiffrement original suggère un choix de paramètres avec une taille de bloc de 64 bits, une clef de 128-bit et 12 tours [86].	• Utilisable en solution matérielle ou logicielle. • Rapide et simple. • Nombre de round variable. • Longueur de clé variable. • Nécessite peu de mémoire. • Haute sécurité. • Rotation dépendante des données [46].	• Vulnérable à l'attaque cryptanalyse Mod n[13]
Twofish	Par bloc	Algorithme de cryptage par blocs de 128 bits sur 16 rondes avec une clé	• Bonne marge de sécurité.	• Modérément rapide en implantation matérielle.

[13] Une forme d'attaque de partitionnement efficace contre les chiffrements qui reposent sur l'addition modulaire et la rotation des bits [48].

		de longueur variable (128, 192 ou 256 bits) [53].	• Rapide pour le cryptage/décryptage en implantation logicielle [46].	• Configuration lente de la clé en implantation logicielle. • Flexibilité modérée [46].
Blowfish	Par bloc	Algorithme de cryptage par bloc de 64 bits et la clé de longueur variable peut aller de 32 à 448 bits [46]. Blowfish est basé sur un réseau de feistel, utilisant itérativement une fonction de chiffrement 16 fois [52].	• Très rapide et économique en mémoire [46].	Avec des touches faibles en 4 tours, il est exposé des attaques différentielles[14] avec de grandes touches faibles [32].

Tableau 6 : Exemples des algorithmes de cryptographies symétriques.

[14] Il s'agit d'une attaque à clairs choisis, on utilise cela pour déterminer la clé inconnue k à partir de plusieurs messages x et de leurs chiffrés x' obtenus par E [91].

III.4. 2 Systèmes cryptographiques asymétrique

Dans un système asymétrique, le récepteur génère une paire de clés asymétrique : une clé publique qui est diffusée à tout le monde et une clé privée maintenue secrète chez le récepteur. La particularité de cette paire de clé est que tout message cryptée avec la clé publique ne peut être décrypté qu'avec la clé privée correspondante, d'où la confidentialité des messages crypté avec la clé publique d'un récepteur. Bien évidemment, la clé privée correspondante ne peut être calculée à partir de la clé publique correspondante [31]. La figure suivante illustre ce système :

Figure 10 : Un système de cryptage asymétrique [31].

Le problème majeur qu'affronte les systèmes de cryptage asymétriques est le partage des clefs car il faut garantir qu'une clé publique correspond bien à l'entité avec qui on communique et qu'elle ne peut pas être interceptée [54] comme le montre la figure suivante :

Figure 11 : Interception de la clé publique [54].

A l'heure actuelle, la solution à ce problème consiste à utiliser une infrastructure appelé infrastructure à clé publique ou PKI (Public Key Infrastructures) permettant, entre autres, de gérer les clés et d'assurer ainsi la confidentialité des utilisateurs [55]. Cette infrastructure fait l'objet de la section suivante.

III.4.2.1 Infrastructure à clé publique

Une infrastructure à clé publique PKI (Public Key Infrastructures), appelée aussi IGC (Infrastructure de Gestion de Clés) est un ensemble de moyens (techniques et organisationnels) permettant de mettre en œuvre des services de sécurité tels que l'authentification, l'intégrité, la confidentialité et la non-répudiation des échanges électroniques [57]. Ceci est rendu possible, d'une part par l'utilisation de clés et de certificats électroniques, et d'autre part par une organisation garantissant la délivrance et la gestion de ces éléments [56].

Une infrastructure PKI fournit donc quatre services principaux [55] :

- Fabrication de bi-clés.
- Certification de clé publique et publication de certificats.
- Révocation de certificats.
- Gestion la fonction de certification.

Ces services sont offerts en utilisant un de ces deux modèles de PKI [78] :

- **Ouvert** : ce sont les AC (Autorité de Certification, ou Emetteurs de Certificats) qui vendent des certificats et en assurent une certaine gestion.
- **Logiciel** : proposé par quelques éditeurs spécialisés en sécurité et par quelques solutions Open Source, consiste en une application que l'on installe au centre du réseau d'une communauté d'utilisateurs.

Dans notre travail, nous optons pour le premier modèle « ouvert » le plus connu et répandu. Ce modèle est généralement composé des entités suivantes (Figure12) :

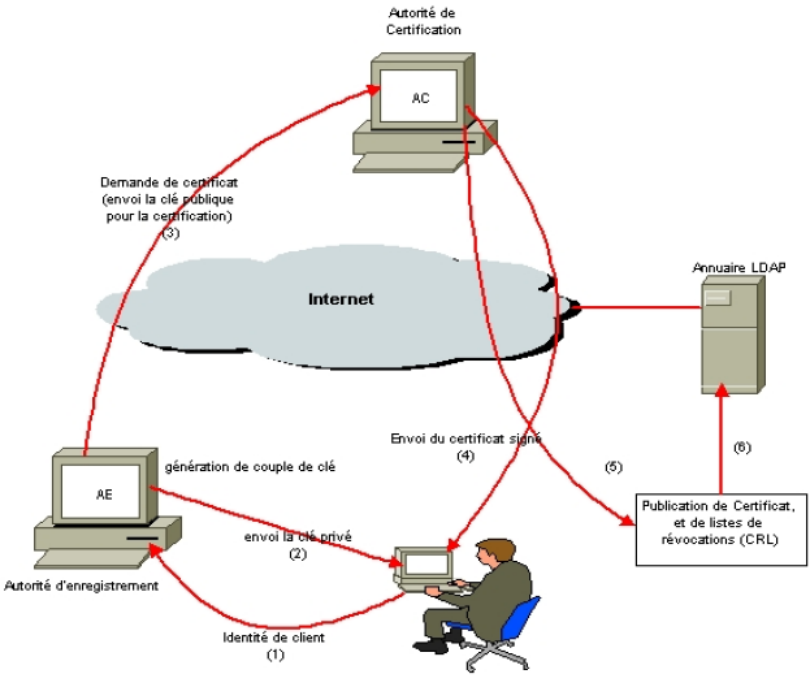


Figure 12 : Architecture de modèles ouverts d'un PKI [55].

1. **Autorité de certification (AC) :** Une autorité de certification est toute entité chargée de délivrer et gérer les certificats. En effet, elle génère des certificats à clés publiques et assure l'intégrité et l'authenticité des informations contenues en les signant avec sa clé privée. Pour émettre des certificats, elle doit recevoir, au préalable, les requêtes de certification contenant la clé publique de l'entité qui le sollicite. On peut dire que c'est le composant le plus important de l'infrastructure PKI du fait de son rôle central dans les différentes cinématiques d'échanges à l'intérieur d'une PKI [58]. Un AC possède lui-même un certificat (auto signé ou délivré par un autre AC) et utilise sa clé privée pour créer les certificats qu'il délivre. La figure suivante représente un certificat numérique signé et l'autre auto-signé [54].

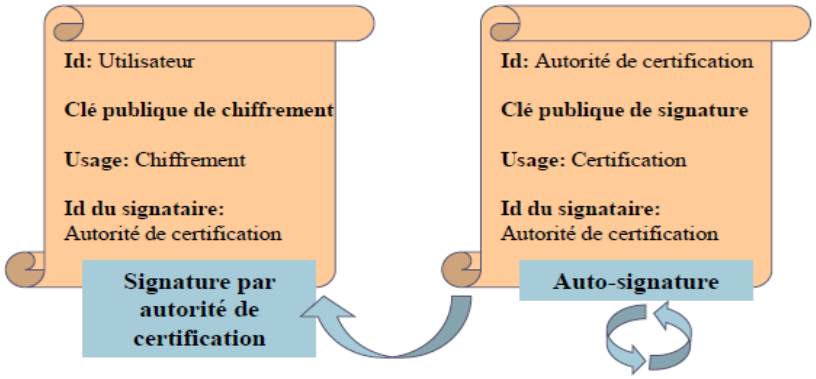


Figure 13 : Certificats numériques [54].

2. **Autorité d'enregistrement (AR) :** Elle joue le rôle d'intermédiaire entre l'utilisateur et la AC et dépend de cette dernière. Elle a comme responsabilité de vérifier tout ce qui concerne l'utilisateur, son identité, la concordance entre clés privées/publiques, de certifier et d'assurer qu'il possède les droits nécessaires pour demander des certificats. En résumé, cette autorité a pour tâche de gérer les requêtes de certificat qu'elle reçoit des différentes entités et de concevoir les paires de clés qui leur sont spécifiques. [55]
3. **Les certificats :** Le certificat est une structure de donnée signé numériquement qui atteste sur l'identité du processeur de la clef privé correspondante à une clef publique. Donc, c'est un document électronique [54] qui garantit la confidentialité et la sécurité des informations sur internet à l'échange, en s'appuyant sur l'infrastructure à clé publique PKI où il est émis par une agence officielle de confiance [55]. Les certificats servent principalement dans trois types de contextes [59] :

    - **Le certificat client** : Il est stocké sur le poste de travail de l'utilisateur ou embarqué dans un conteneur tel qu'une carte à puce, permettant d'identifier un utilisateur et de lui associer des droits. Dans la plupart des scénarios, il est transmis au serveur lors d'une connexion, qui affecte des droits en fonction de l'accréditation de l'utilisateur. Il s'agit

d'une véritable carte d'identité numérique utilisant une paire de clé asymétrique d'une longueur de 512 à 1024 bits.

- **Le certificat serveur :** Ce type de certificat est installé sur un serveur web permet d'assurer le lien entre le service et le propriétaire du service. Dans le cas d'un site web, il permet de garantir que l'URL (Uniform Resource Locator) et en particulier le domaine de la page web appartiennent bien à telle ou telle entreprise. Par ailleurs, il permet de sécuriser les transactions avec les utilisateurs grâce au protocole SSL**.**
- **Le certificat VPN :** est un type de certificat installé dans les équipements réseaux, permettant de chiffrer les flux de communication de bout en bout entre deux points (par exemple deux sites d'une entreprise). Dans ce type de scénario, les utilisateurs possèdent un certificat client, les serveurs mettent en œuvre un certificat serveur et les équipements de communication utilisent un certificat particulier (généralement un certificat IPSec).

4. Les services d'archivage et de publication : L'archivage est un service qui permet le stockage des paires de clés pour une restitution en cas de perte de la clé privée. En effet, il a pour mission de stocker en toute sécurité les clés de cryptage émis au sein de l'infrastructure. La publication est un service qui répertorie les différents certificats à clés publiques émis par la AC afin de les rendre disponibles aux éventuels futurs utilisateurs, c'est pourquoi on se réfère communément à lui par le terme de dépôt qui peut être mis en place par un annuaire peut être utilisé (LDAP[15] (**L**ightweight **D**irectory **A**ccess **P**rotocol) ou X500 par exemple), un serveur Web ou encore un outil de messagerie, etc. Ce service est contraint par plusieurs exigences telles que, par exemple, le délai de mise à jour des listes de révocation ou la disponibilité de ces listes. Le dépôt est également responsable de la publication de la CRL (Liste de Révocation de Certificat) [58].

5. Les utilisateurs : Ce sont les personnes ou entités organisationnelles ayant émis ou émettant des demandes de certificat, ou souhaitant simplement vérifier la validité et les informations sur l'identité d'un certificat préalablement reçu [55].

[15] (LDAP) est un protocole de communication avec les annuaires**.**

III.4.2.2 Exemple des algorithmes : Dans le tableau suivant, nous citons les principaux algorithmes de la cryptographie asymétrique

Nom	Description	Avantages	Inconvénients
ElGamal	Algorithme de cryptage est basé sur la difficulté de calculer des logarithmes discrets [32].	• Possibilité de techniques d'exponentiation rapide. • Cryptage randomisé nativement • Meilleure sécurité basique [62].	• Augmentation de la taille du texte crypté. • Deux fois plus lent que RSA [62].
Cryptographie sur les courbes elliptiques	Les courbes elliptiques sont bien adaptées à la cryptographie à clé publique. Elles permettent de remplacer les calculs sur des entiers, ou dans les groupes Z/nZ,par des calculs dans les groupes associés à une courbe elliptique [61].	• La taille des clés croît moins vite que le RSA si on souhaite une meilleure sécurité. • Utilisation pour systèmes embarqués. • Calculs moins lourds que l'exponentiation d'ElGamal. • Utilisation mémoire moindre. • Cryptanalyse par algorithme exponentiel [32].	• Complexe. • Peu de développement sur des systèmes à grande échelle (mais tend à changer). • Travaux d'optimisation essentiellement destinés aux systèmes mobile [32].
RSA	Algorithme de cryptage est basé sur le calcul exponentiel [32] et repose en partie sur le problème de la factorisation [60].	• Système cryptographie largement répandu. • Nombreuses études au sujet de sa sécurité [32].	• Opérations de dé/cryptage très inégales en termes de temps de calcul. • Cryptanalyse par algorithme sous exponentiel[16] [32].

Tableau 7 : Exemple sur les algorithmes de la cryptographie asymétrique

[16] Un algorithme est sous-exponentiel si le logarithme du temps d'exécution croît asymptotiquement moins vite que tout polynôme donné. Le niveau de sécurité d'une clé est en directe correspondance avec sa taille. Ainsi, pour une même résistance [45].

III.4.3 La cryptographie hybride :

La cryptographie hybride permet de combiner les avantages des deux systèmes cryptographiques : asymétrique et symétrique tout en minimisant leurs inconvénients [63] comme le montre le tableau suivant :

Systèmes Cryptographiques	**Avantages**	**Inconvénients**
Symétriques	• Le cryptage/décryptage est très rapide. • Les algorithmes de chiffrement symétrique sont généralement beaucoup moins complexes que les algorithmes de chiffrement asymétrique. • Ils sont adaptés aux grands flux de données à crypter [65].	• Ils n'assurent que la confidentialité des données, contrairement au chiffrement asymétrique qui permet d'assurer des principes de sécurité supplémentaire (l'authenticité de l'expéditeur). • Une clé symétrique correspond à un échange entre 2 personnes, pour communiquer avec d'autres personnes, il faudra une autre clé symétrique [44]. • L'utilisation d'une clé unique présente un problème lors de l'échange de clé [2].
Asymétriques	• Ils offrent multiples services (confidentialité, signature) [65]. • Ils renforcent la sécurité, par exemple, même en interceptant le message, impossible de le décrypter sans la clé privée [2].	• Ils nécessitent une consommation importante en ressources CPU (**C**entral **P**rocessing **U**nit). • Ils ne sont pas adaptés pour le cryptage de flots de données importants [59]. • Le cryptage/décryptage est lent en raison de ses algorithmes complexes [2].

Hybrides	Un système cryptographie hybride consiste à utiliser les avantages des cryptages symétrique et asymétrique tels que : • La rapidité d'un système symétrique. • La possibilité de transmettre la clé secrète par un système cryptographique asymétrique. • Assurer l'intégrité des données échangées grâce à des fonctions de hachage cryptographiques qui permettent de générer des empreintes numériques des données envoyées et reçues afin de les comparer [39]. • Ainsi, ils sont plus performants et Plus sécurisés [68].	• Ils nécessitent l'échange de deux informations (clé symétrique chiffré et message crypté) [68]. • Ils sont complexes à mettre en place que les systèmes symétriques et asymétriques

Tableau 8 : Comparaison entre les systèmes cryptographiques.

Ainsi, la cryptographie hybride utilise une paire de clés : privée et publique (comme dans la cryptographie asymétrique) avec un cryptage du texte rapide (comme dans la cryptographie symétrique) [63]. Le processus de cryptage/décryptage est détaillé dans la section suivante.

III.4.3.1 Cryptage/Décryptage

En général, la plupart des systèmes hybrides procèdent de la manière suivante : une clé secrète est générée pour l'algorithme symétrique (3DES, IDEA (International Data Encryption Algorithm), AES et bien d'autres encore), cette clef fait généralement entre 128 et 512 bits selon les algorithmes. L'algorithme de cryptage symétrique est ensuite utilisé pour crypter le message. La clef aléatoire quant à elle, se voit cryptée grâce à la clef publique du destinataire, c'est ici qu'intervient la cryptographie asymétrique (RSA ou Diffie-Hellman). Comme la clef est courte, ce cryptage prend peu de temps. Cependant, le cryptage de l'ensemble du message avec un algorithme asymétrique serait bien plus lourd, c'est pourquoi on passe par un algorithme symétrique.

Il suffit ensuite d'envoyer le message crypté avec l'algorithme symétrique et l'accompagner de la clef cryptée correspondante, comme montre la figure suivante [63] :

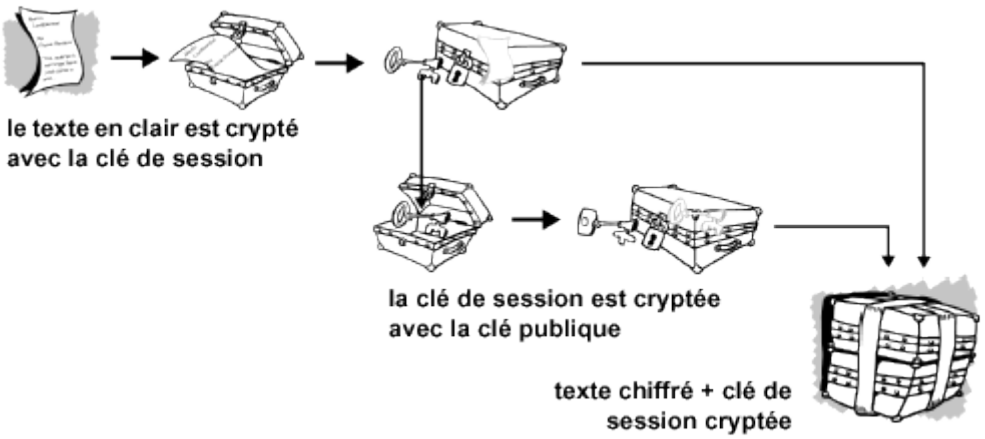


Figure 14 : Fonctionnement du cryptage hybride [64].

Le destinataire décrypte la clef symétrique avec sa clef privée et via un décryptage symétrique, il trouve le message [63].

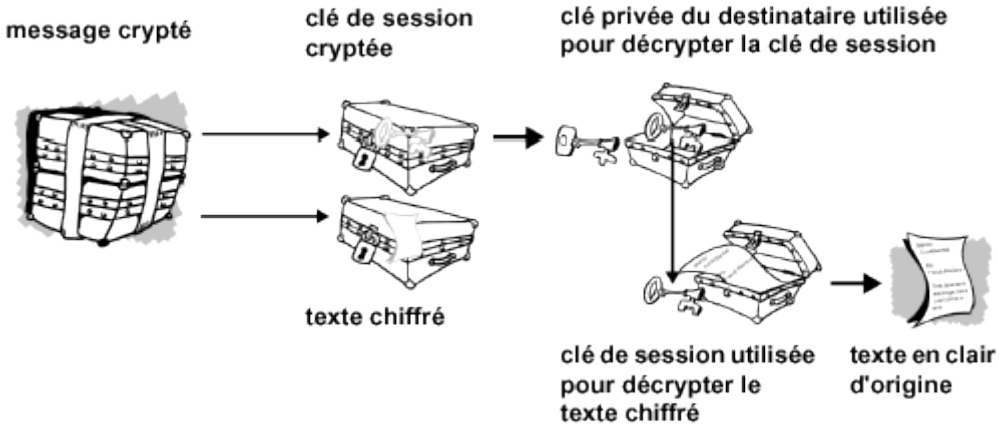


Figure 15 : Fonctionnement du décryptage hybride [64].

III.4.3.2 Exemples de la cryptographie hybride les plus connus :

Dans le tableau suivant, nous citons les principaux exemples de la cryptographie hybride :

Nom	Description	Avantages	Inconvénients
PGP	Le PGP de Phil Zimmermann utilise deux algorithmes distincts pour crypter et décrypter les données dans un réseau de téléinformatique, l'un est à clé publique (RSA) et l'autre à clé secrète (IDEA). [65].	• Très rapide, très sûr et inattaquable (du moins inattaquée jusqu'à présent). • Ils peuvent aussi signer les clés des autres, en ajoutant ainsi un niveau de confiance dans le système [65].	• Un processus complexe pour de nombreuses personnes. • PGP est une rue à deux voies : si un émetteur envoie un email crypté par PGP à un récepteur qui n'utilise pas PGP, le récepteur ne peut pas ouvrir le fichier pour le voir. [87].
GnuPG	GnuPG comme PGP, qui fonctionnent de la même façon et sont compatibles servent à échanger des messages/fichiers chiffrés et signés, il utilise des algorithmes à clé publique (RSA ou un système basé sur les courbes elliptiques) et des algorithmes à clé discrète (AES 128 ou encore 3DES). Il utilise aussi des fonctions de hachage comme SHA-256 ou SHA-1 pour les signatures [66].	• Assurer l'authenticité, l'intégrité et la confidentialité des données. • Signature des clefs.	• GPGShell est un programme dont la source n'est pas disponible, en conséquence on ne sait pas ce qu'il fait réellement [88].

SSL	Est un protocole de couche de transport sécurisé ayant pour but de sécuriser les transactions effectuées sur Internet. Ce système repose à la fois sur les algorithmes à clef publique (RSA, Diffie-Hellman), et l'algorithme à clef secrète (AES) et sur les certificats électroniques afin de garantir au maximum la sécurité de la transmission de données avec un tel site [67].	L'utilisation de SSL est donc assez simple. Le protocole SSL prend en charge les principes de sécurité suivants : l'authentification, l'intégrité et la confidentialité des données.	Quand un certificat expire, l'utilisateur reçoit un message et doit obtenir manuellement un nouveau certificat [89].

Tableau 9 : Exemples de la cryptographie hybride les plus connus.

III.4.3 Choix des algorithmes de cryptographie

A partir des comparaisons précédentes entre les systèmes cryptographiques symétriques, asymétriques et hybrides, nous optons pour un système hybride. En effet, Il combine la vitesse de cryptage/ décryptage symétrique du texte/message avec la sécurité fournie à l'échange de la clé secrète en utilisant la paire de clés publique-privée. Donc, il est considéré comme un système hautement sécurisé [15]. La question qui se pose maintenant quels sont les algorithmes de cryptage/décryptage que nous allons utiliser.

Etant donné que les protocoles hybrides déjà cités (PGP, GnuPG et SSL) ne sont pas des solutions open-sources pour pouvoir les utiliser directement, alors nous avons décidé dans notre travail, de mettre en œuvre notre propre protocole en suivant leur principe de fonctionnement. Ainsi :

- Pour le choix des algorithmes symétrique, d'après le tableau 6, nous constatons que l'algorithme AES est également un candidat particulièrement approprié pour notre travail.
- De même pour l'algorithme asymétrique, et selon le tableau 7, nous privilégions l'algorithme le plus simple, le plus connu et le plus utilisé RSA.

Ces deux algorithmes (AES et RSA) sont détaillés dans les sections suivantes.

III.5 Algorithme AES

En janvier 1997, le NIST (National Institute of Standard and Technology) a lancé un appel d'offre pour l'élaboration d'un nouveau système cryptographique pour remplacer DES [69]. Cela est suite à la faiblesse du DES vis-à-vis de la cryptanalyse qui est dû principalement à la longueur relativement faible de la clef secrète et à l'augmentation des puissances de calcul, permettant ainsi de lancer des recherches exhaustives de la clé secrète. L'algorithme AES a été choisi en octobre 2000 parmi les 15 systèmes proposés en réponse à l'appel d'offre de NIST [42]. Cet algorithme a été officiellement approuvé comme standard le 6 décembre 2001 [47].

L'AES est un algorithme de cryptage par bloc capable d'utiliser des clés cryptographiques de 128, 192 et 256 bits pour crypter et décrypter des données dans des blocs de 128 bits [70]. Il se compose principalement d'un module « round » ou « ronde » qui sera itéré 10, 12 ou 14 fois suivant la taille de la clé secrète utilisée. Trois étapes sont distinguées (Figure 16) :

1. **Ronde initiale :** qui ne compte qu'une seule opération : AddKey [53]. Cette opération se résumé à un « ou-exclusif » entre le texte en clair et la clé secrète K (si chiffrement) ou le texte chiffré et la clé de ronde PK10 (si déchiffrement) [69].
2. **N ronde :** où N est le nombre d'itérations. Ce nombre varie en fonction de la taille de la clef utilisée (128 bits, N=9 ; 192 bits, N=1 1 ; 256 bits, N=13) [53]. Cette deuxième étape est composée d'un ensemble de 9 rondes chacune réalisant 4 opérations. Dans le cas du chiffrement les opérations sont SubBytes, ShiftRows, MixColumns et AddRoundKey et

dans le cas du déchiffrement, l'inverse de l'ensemble des 4 opérations précédentes interviennent MixColumns-1, ShiftRows-1, SubBytes-1 et AddRoundKey [69].

3. **Dernière ronde** : est quasiment identique à l'une des N itérations de la deuxième étape. La seule différence est qu'elle ne comporte pas l'opération mixColumns ou MixColumns-1 [53].

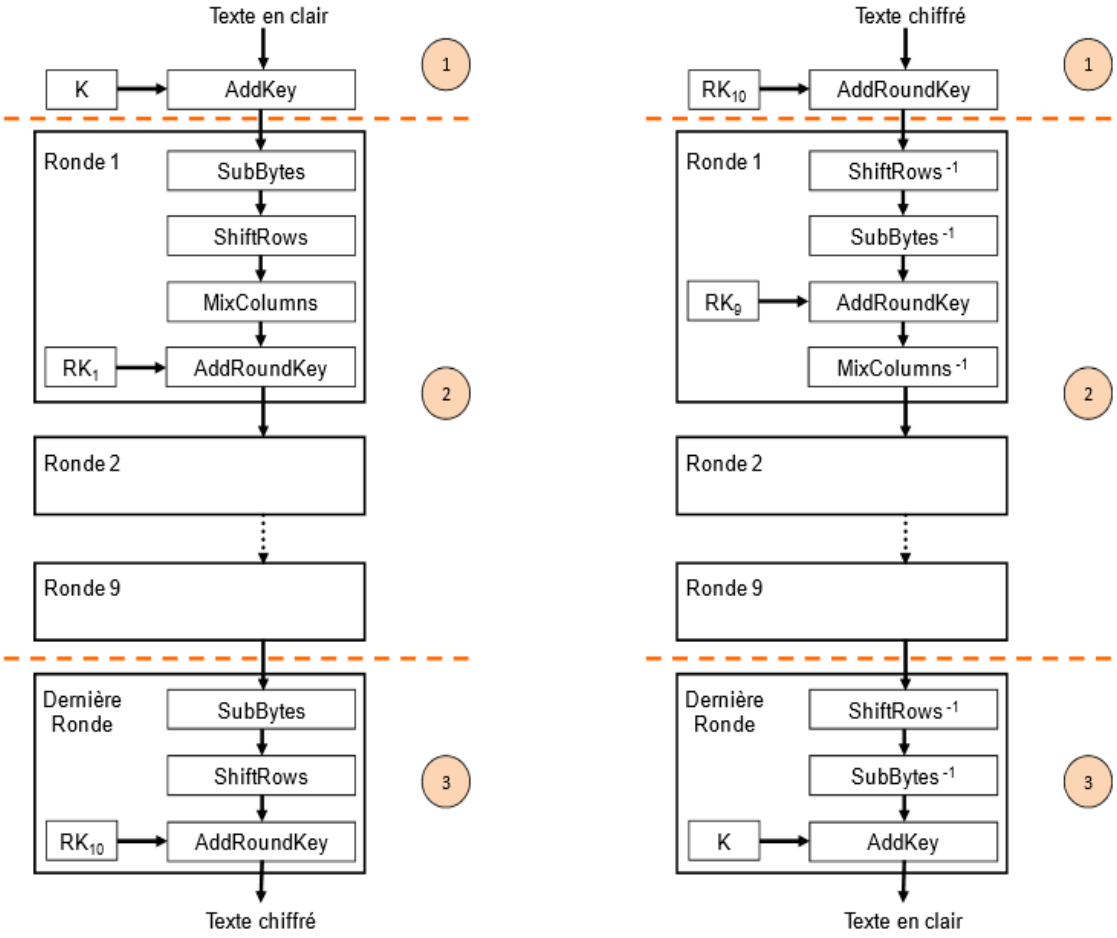


Figure 16 : Cryptage et Décryptage AES [53].

Comme déjà mentionné, une ronde d'AES est constituée de 4 opérations :

a) L'opération SubBytes : opération de substitution non linéaire lors de laquelle chaque octet est remplacé par un autre octet choisi dans une table particulière « S-box » [42]. Par exemple, dans la figure 17, on explique l'effet de cette opération sur des blocs de données de 128 bits organisés sous forme de matrice d'octet 4×4. Chaque octet S_{1c} (lc pour ligne-colonne) est représenté par deux nombres de 4 bits x et y. Les octets (notés sous forme hexadécimale) contenus dans la table sont les octets de remplacement S'_{lc}. L'intersection de la ligne x avec la colonne y représente la valeur de remplacement de l'octet xy (exemple : si l'octet de départ vaut B8, x = B et y = 8, l'octet de remplacement vaut 6C) [69].

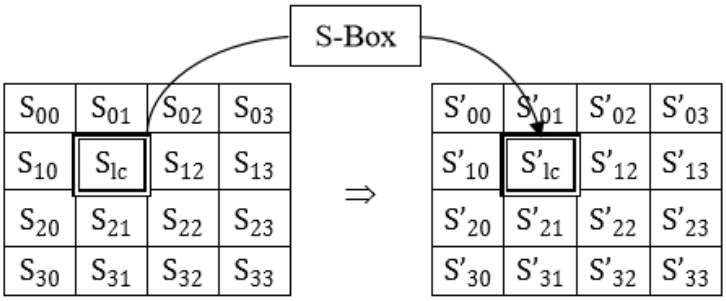


Figure 17 : Principe de l'opération SubBytes [69].

x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
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

Figure 18 : S-BOX : Table de substitution [69].

b) L'opération ShiftRows : est un décalage circulaire des lignes de données de la matrice. La première ligne ne subit pas de décalage, la seconde, la troisième et la quatrième se décalent de façon circulaire vers la gauche respectivement d'un, deux et trois octet [47].

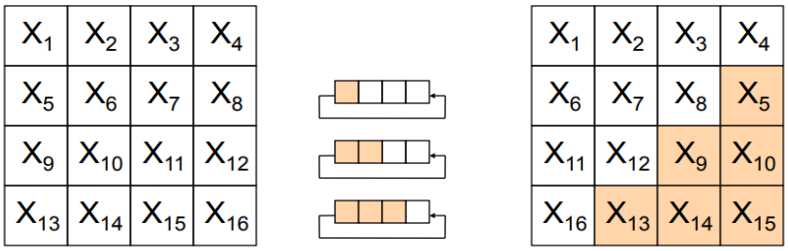


Figure 19 : Principe de l'opération ShiftRow [71].

c) L'opération MixColumns : est une opération de multiplication entre une matrice d'éléments connus et la matrice de données résultant de l'opération ShiftRows [47].

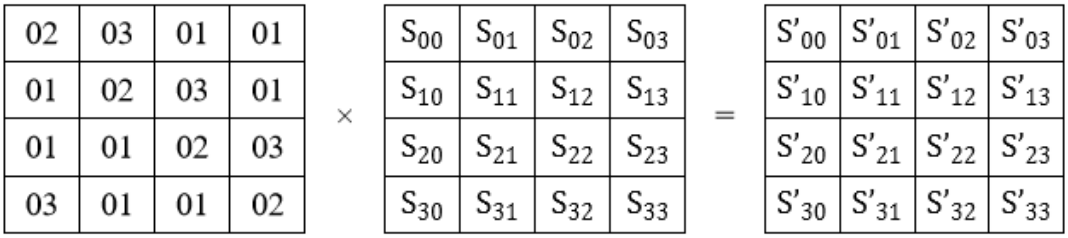


Figure 20 : Principe de l'opération MixColumn [69].

d) L'opération AddRoundKey : est une opération de ou-exclusif entre la matrice de données et la clef de ronde [47].

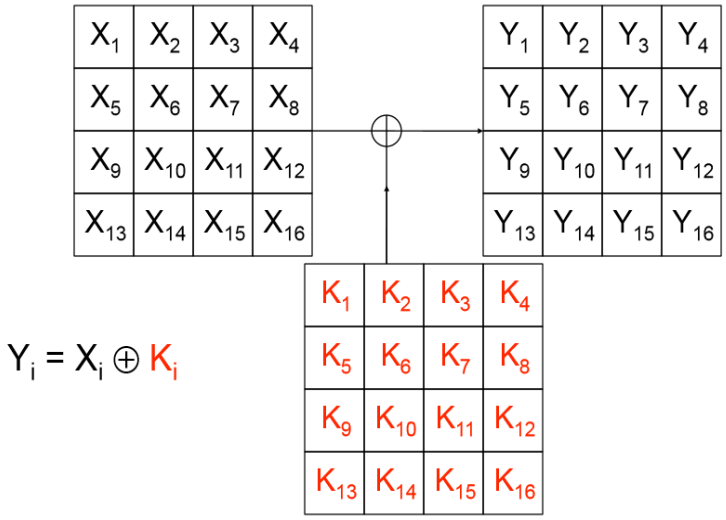


Figure 21 : Principe de l'opération AddRoundKey [71].

Toutes les opérations de cryptage sont inversibles. Ainsi pour décrypter un texte, les opérations inverses sont appliquées. La procédure de génération des clés de rondes est identique en cryptage et décryptage. La différence majeure au niveau des clefs de rondes par rapport au cryptage est que celles-ci sont utilisées dans l'ordre inverse. Ainsi la première clef utilisée dans le processus de décryptage est la clef de ronde numéro dix (RK10) [69].

III.6 Algorithme de RSA

RSA a été présenté par Ron Rivest, Adi Shamir et Leonard Adleman. C'est un algorithme asymétrique le plus connu et le plus utilisé. Il peut tout aussi bien fournir du cryptage que des signatures [72].

Le RSA est basé sur la théorie des nombres premiers, et sa robustesse tient du fait qu'il n'existe aucun algorithme de décomposition d'un nombre en facteurs premiers. Alors qu'il est facile de multiplier deux nombres premiers, il est très difficile de retrouver ces deux entiers si l'on en connaît le produit [73].

Le RSA est un algorithme de chiffrement à clé publique, ce qui signifie que l'algorithme de calcul n'est pas caché, ni la clé de chiffrement (appelé de ce fait clé publique). La connaissance permet à tous les émetteurs de chiffrer des messages qui ne pourront être déchiffrés que par le destinataire, grâce à sa clé secrète [39].

L'algorithme se décrit ainsi (figure 22) :

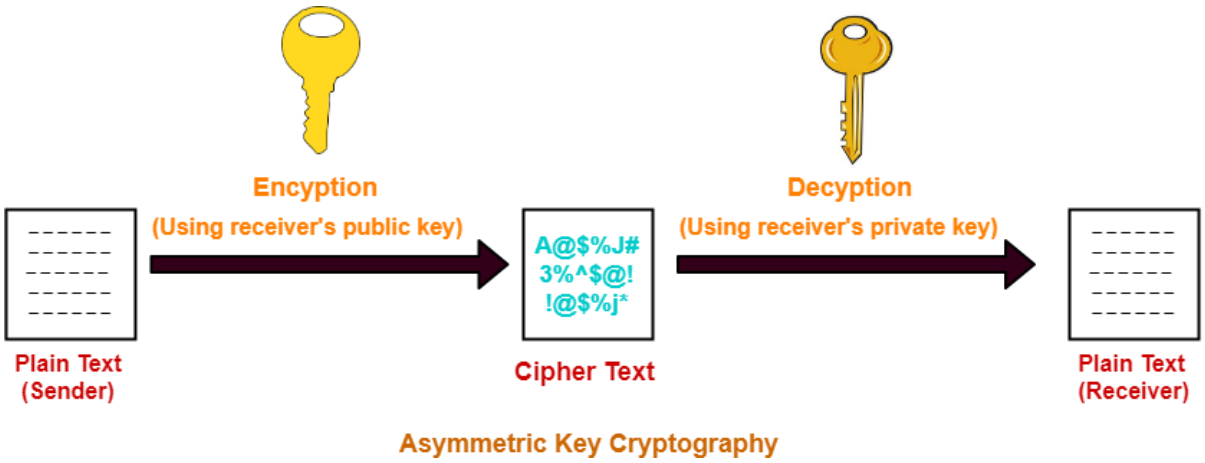


Figure 22 : Principe d'algorithme RSA [90].

a. Génération des clés

Le RSA fonctionne à partir de deux nombres premiers, que l'on appellera p et q. Ces deux nombres doivent être très grands, car ils sont la clé de voûte de cryptage. Aujourd'hui, on utilise des clés de 128 à 1024 bits, ce qui représente des nombres décimaux allant de 38 à 308 chiffres [73] !

La génération de la paire de clé (publique, secrète) citées dans le principe de fonctionnement se fait en suivant les étapes ci-dessous [39] :

a. Générer deux nombres premiers p et q.
b. Calculer $N = pq$ et $\varphi(N) = (p-1)(q-1)$.
c. Choisir un entier e, $1 < e < \phi(N)$ tel que le Plus Grand Commun Diviseur entre e et $\varphi(N)$ soit égal à 1, i.e. $(PGCD(e,\phi(N)) = 1$.
d. Utiliser l'algorithme d'Euclide étendu pour calculer d tel que $e * d \equiv 1 \bmod \phi(N)$.
e. Alors : (N, e) est la clé publique et d est la clé privée est : (d) [72].

b. Exponentiation modulaire :

Pour implémenter le RSA, on a besoin d'un algorithme l'exponentiation modulaire rapide pour calculer $\boldsymbol{a^b \bmod n}$. On présente ci-dessous un algorithme qui permet de réaliser cette tâche [39].

1. Diviser b en puissances de 2 en l'écrivant en binaire.

2. Commencer du chiffre le plus à droite, soit k=0 pour chaque chiffre :

- Si le chiffre est 1, nous gardons le terme 2^k, sinon nous ne le gardons pas.

- Incrémenter k, et on analyse le chiffre suivant.

3. On calcule le modulo n des puissances de deux ≤b. 4. Utiliser les propriétés de multiplication modulaire pour combiner les valeurs calculées du modulo n.

c. Cryptage :

Le cryptage d'un message M se fait comme suit [39] :

a. Le message original doit être décomposé en une série d'entiers M_i de valeurs comprises entre 0 et n-1.

b. Pour chaque entier M_i il suffit alors de calculer $C_i$le message chiffré avec : $= M^e \ \boldsymbol{mod\ n}$, en utilisant la méthode d'exponentiation modulaire introduite en haut.

Le message crypté est alors la concaténation des entiers Ci.

3. Décryptage :

Conformément à la manière dont il a été crypté, le message reçu doit être composé d'une succession d'entiers de valeurs comprises entre 0 et n-1. Pour chaque entier C il faut calculer $\boldsymbol{M} = C^d \boldsymbol{mod\ n}$.

Le message original peut alors être reconstitué à partir de la série d'entiers M [39].

III.7 Conclusion

Au niveau de ce troisième chapitre, nous avons comparé entre les différents systèmes et algorithmes de la cryptographie. De cette étude comparative, nous avons constaté qu'un système hybride semble être une solution prometteuse car il combine entre les avantages des deux systèmes (symétrique et asymétrique). En s'inspirant des algorithmes hybrides existants (PGP, GnuPG et SSL), nous avons choisi d'implémenter notre propre algorithme qui combine l'algorithme symétrique AES et l'algorithme asymétrique RSA. Le chapitre suivant est consacré à la conception de notre solution qui consiste à implémenter un système cryptographie hybride pour un portail de déclaration des incidents de sécurité.

PARTIE 2 : CONCEPTION ET DEVELOPPEMENT

CHAPITRE IV : CONCEPTION D'UN SYSTEME CRYPTOGRAPHIQUE POUR LE CSIRT ELIT

IV.1 Introduction

Afin de réaliser les trois principes fondamentaux de la sécurité des informations (Confidentialité, Intégrité et Disponibilité), de contrôler les menaces, les vulnérabilités dans l'organisation, et d'avoir un véritable processus de gestion et de réponse aux incidents qui est piloté et mis en œuvre par le CSIRT ELIT, nous allons développer un système cryptographique pour un portail de signalement des incidents de sécurité. La conception de cette solution est décrite dans ce chapitre.

IV.2 Processus de développement 2TUP

Le processus 2TUP (Two Track Unified Process) est un processus unifié. Il gère la complexité technologique en donnant part à la technologie dans son processus de développement (Franck,2004)
.Le 2TUP propose un cycle de développement qui sépare les aspects techniques des aspects fonctionnels et propose une étude parallèle des deux branches : fonctionnelle (étude de l'application) et la technique (étude de l'implémentation) [94].

IV.3 L'étude préliminaire

IV.3.1 Identification de besoin

Un CSIRT permet de répondre aux incidents mais également de servir de relais vers l'intérieur de l'organisation (pour prévenir les menaces par information et par sensibilisation) et surtout vers l'extérieur à destination des autres CSIRTs et de la communauté sécurité en général (pour se coopérer). Dans ce contexte, le CSIRT ELIT a alors un rôle « d'alerte et de cyber pompier », prêt à intervenir pour aider et conseiller l'ensemble du groupe, ses filiales en cas d'incident de sécurité. Cependant, toutes les informations échangées se font en clair, et les informations contenant les déclarations des incidents de sécurité sont classées très critiques. C'est pourquoi, la partie déclaration doit être sécurisée. Aucun message ne doit passer en clair.

IV.3.2 Description de la Solution

Pour que la communication en interne et à l'externe soit sécurisée, l'existence d'un système cryptographique pour CSIRT ELIT est indispensable. Pour cela, notre solution consiste à concevoir et développer un système cryptographique hybride qui permet :

- La génération des clés secrètes (symétriques) de manière aléatoire.
- La génération des paires de clés (publiques et privées) et des certificats des clés avec l'autorité de certification.
- Le cryptage/décryptage des messages, formulaire ou des fichiers en utilisant l'algorithme AES.
- Le cryptage/décryptage des clés secrètes avec l'algorithme RSA.

- L'utilisation du protocole SSH pour sécuriser la communication entre l'autorité de certification et la machine cliente.

IV.3.3 Hypothèses du travail

Pour mettre en place et tester ce système de cryptographique, il faut l'intégrer dans le site du CSIRT ELIT. Cela n'est pas possible aux raisons des failles pouvant être engendrées durant la mise en œuvre. Pour cela, nous avons pensé à mettre en œuvre un simple portail web permettant le signalement des incidents par les parties prenantes et le traitement de ces incidents par les experts de sécurité. Ainsi, le fonctionnement de processus de gestion des incidents est simplifié comme suit :

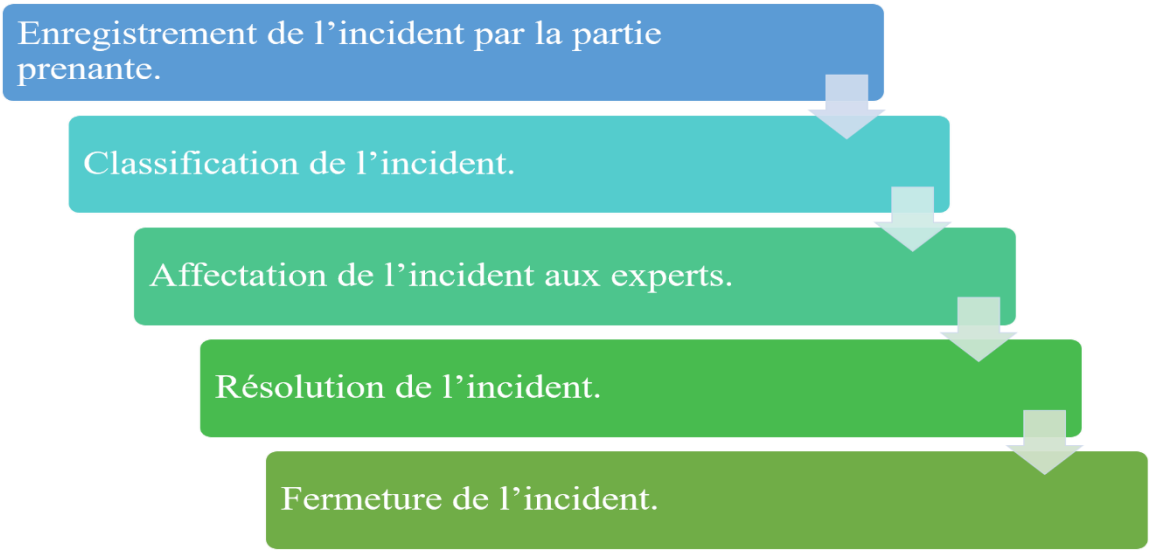


Figure 23 : Organigramme simplifié de gestion des incidents aux experts de sécurité.

IV.3.4 Recueil des besoins fonctionnels

Nous avons effectué plusieurs recherches pour identifier au mieux les besoins de l'application, et ceci afin de répondre aux attentes des utilisateurs. Nous sommes allés chercher les informations au sein de l'administration de **ELIT** -**El** Djazïar **I**nformation **T**echnology. Mais, cette recherche n'était pas vraiment suffisante à cause de la situation actuelle relative au confinement causé par le Covid-19. Pour cela on a beaucoup plus se basé sur la recherche des travaux connexes, dont on a conclu que l'existence d'un système cryptographique pour CSIRT ELIT est indispensable, pour que la communication en interne et à l'externe soit sécurisée.

IV.3.5 Recueil des besoins techniques

La capture des besoins techniques, qui recense toutes les contraintes et les choix dimensionnant la conception du système, les outils et le matériel sélectionnés ainsi que la prise en compte des contraintes d'intégration avec l'existant (pris requis d'architecture technique). Les choix techniques adoptés pour le projet sont comme suit :

- La modélisation du système avec UML et l'outil StartUML.

- Notre application se fonctionne sous forme client/serveur et est implémentée en utilisant les langages suivants (Tableau 14) : HTML, CSS, PHP.
- Les machines utilisées : une machine physique et une machine virtuelle.
- L'algorithme AES pour le cryptage/décryptage symétrique des messages, formulaire ou des fichiers.
- L'algorithme RSA pour le cryptage/décryptage asymétrique des clés secrètes.
- PKCS pour les standards de cryptographie à clé publique.
- Utilisé la librairie OpenSSL pour le cryptage symétrique AES et pour la configuration des composants PKI.
- Utilisé le package Crypt_RSA de la bibliothèque phpseclib - (PHP Secure Communications Library) 17 pour le cryptage asymétrique RSA.
- Configuré le protocole SSH sur les deux machines.

IV.3.6 Architecture générale du système cryptographique

Suivant les hypothèses décrites ci-dessus, la figure suivante montre l'architecture générale de notre système cryptographique qui est composé des entités suivantes : émetteurs/récepteurs (partie prenante ou expert en sécurité) et l'infrastructure à clé publique ou PKI (AC, serveur de publication, serveur d'archivage).

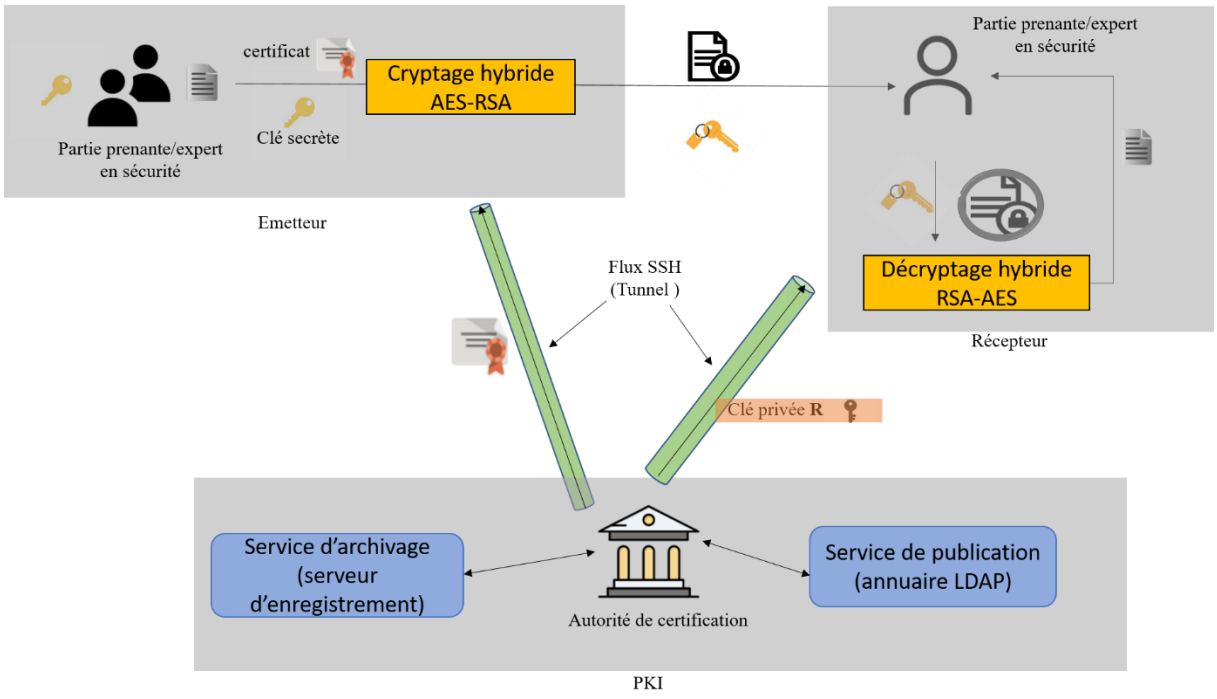


Figure 24 : Architecture de notre système cryptographique.

Chaque composant possède un rôle ben précis dans le système :

- **Emetteurs et récepteurs (partie prenante ou expert de sécurité) :** ce sont des entités qui communiquent entre eux en tout sécurité lorsqu'un incident de sécurité survient. Noter ici que les experts de sécurité peuvent être tout membre du CSIRT ELIT : les

membres du service helpdesk, de l'équipe SOC, de l'équipe sensibilisation et de l'équipe de veille.

- **PKI** : C'est une entité qui génère les paire clés (la clé publique et la clé privée) pour l'algorithme asymétrique RSA qui sont utilisées par la suite pour le cryptage et le décryptage de la clé secrète de l'algorithme symétrique AES. Ainsi, l'AC est chargé de créer et signer les certificats pour certifier l'identité du porteur de clé publique. Ces certificats numériques permettant d'effectuer des opérations de cryptographie. Ils sont stockés dans un serveur d'archivage et publier sur un serveur de publication.

Dans la cryptographie hybride, une clé aléatoire est générée pour l'algorithme symétrique (AES) afin de crypter le message. La clé aléatoire quant à elle, se voit cryptée grâce à la clé publique du destinataire, c'est ici qu'intervient la cryptographie asymétrique (RSA). Pour son bon fonctionnement, l'algorithme RSA a besoin de ces éléments : une paire de clés (publique et privée) ainsi qu'un certificat de sécurité. Ces éléments, générées et gérés par le KPI, sont partagés à travers une connexion SSH entre deux machines.

En résumé, notre solution comprend deux mécanismes de sécurité : l'algorithme hybride de cryptage\décryptage et le protocole SSH, que nous allons expliquer par la suite.

IV.3.6.1 Algorithme Hybride de Cryptage/Décryptage

Comme présenté dans la figure suivante, le fonctionnement de notre système cryptographique hybride se déroule comme suit.

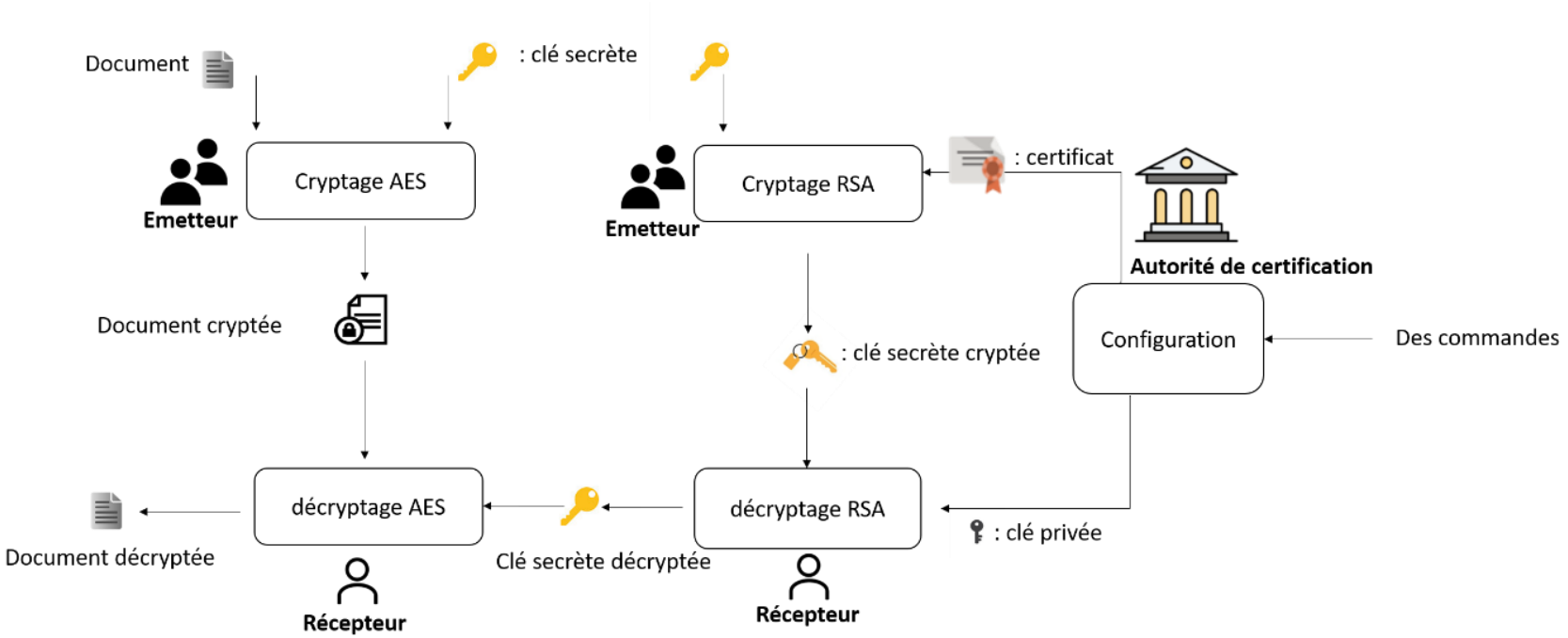


Figure 25 : Fonctionnement de notre algorithme hybride (cryptage/décryptage).

Nous distinguons deux types de clé :

- **La clé symétrique (ou secrète) :** est générée de manière aléatoire par notre système.
- **Les clés asymétriques (une paire de clés : publique et privée)** : sont générées par l'AC qui certifie la clé publique pour garantir l'identité de l'utilisateur.

Quand l'émetteur envoie un document. En arrière-plan, ce document va être crypté comme suit :

- La clé secrète est générée de manière aléatoire par le système.
- Le contenu est chiffré en utilisant l'algorithme AES et la clé secrète.
- La clé secrète est ensuite cryptée en utilisant l'algorithme RSA et la clé publique récupérée à partir de l'AC.
- Le contenu chiffré de document ainsi que la clé secrète cryptée sont envoyés au récepteur.

Quand le récepteur reçoit le document :

- La clé secrète va être décryptée en utilisant l'algorithme RSA avec sa clé privée déjà envoyée par l'AC,
- Ensuite, le contenu de document est décrypté en utilisant l'algorithme AES et la clé secrète décryptée.

IV.3.6.2 Protocole SSH

Pour une communication sécurisée entre l'autorité de certification et les utilisateurs de notre CSIRT (parties prenantes ou experts de sécurité), nous utilisons le protocole SSH (Protocole Secure Shell) qui est un protocole permettant de faciliter les connexions sécurisées entre deux systèmes à l'aide d'une architecture client/serveur [79]. En effet,

- Les données circulantes entre le client et le serveur sont chiffrés, ce qui garantit leur confidentialité (personne d'autre que le serveur ou le client ne peut lire les informations transitant sur le réseau) [80].
- Le client et le serveur s'authentifient mutuellement afin d'assurer que les deux machines qui communiquent sont bien celles que chacune des parties croit être. Il n'est donc plus possible pour un pirate d'usurper l'identité du client ou du serveur [80].

L'établissement d'une connexion SSH se fait en deux étapes [80] (Figure 26) :

- Dans un premier temps, le serveur (PKI) et le client (partie prenante ou expert en sécurité) s'identifient mutuellement afin de mettre en place un canal sécurisé (couche de transport sécurisée).
- Dans un second temps, le client s'authentifie auprès du serveur pour obtenir une session.

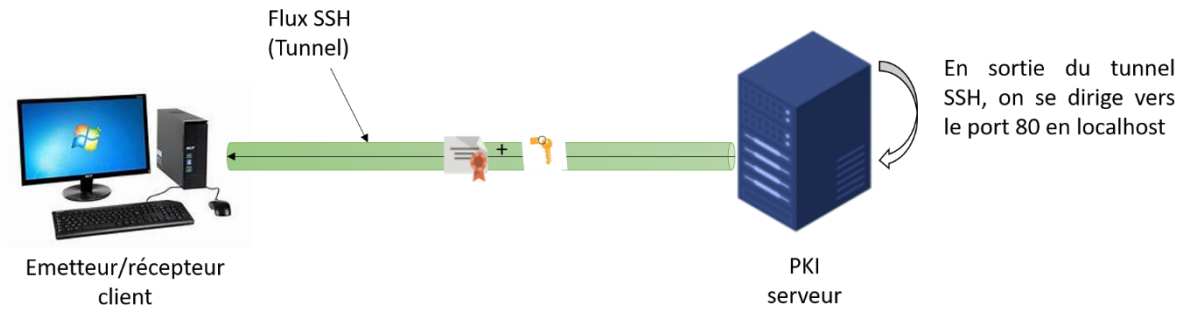


Figure 26 : Le fonctionnement de protocole SSH.

IV.3.7 Etude conceptuelle de notre application

Pour mettre en place notre système cryptographique proposé pour CSIRT ELIT, il fallait implémenter tout d'abord un portail web qui permet de communiquer entre les experts de sécurité du CSRIT ELIT et ses parties prenantes (voir les hypothèses de travail). La conception de notre application est décrite avec les diagrammes UML suivants :

IV.3.7.1 Diagramme de cas d'utilisation

Un diagramme de cas d'utilisation indique le comportement attendu du système [77]. Dans notre solution, nous distinguons quatre acteurs :

1. **Administrateur :** personne qui a pour rôle principale de gérer et administrer toutes les opérations du système.
2. **Partie prenante (Client)** : désigne la base de clientèle d'un CSIRT.
3. **Expert en sécurité** : ayant pour mission principale de répondre aux incidents en proposant les services nécessaires au traitement des attaques et en aidant leurs parties prenantes à restaurer les systèmes qui en ont fait l'objet.

La figure suivante illustre les différentes fonctionnalités de notre système :

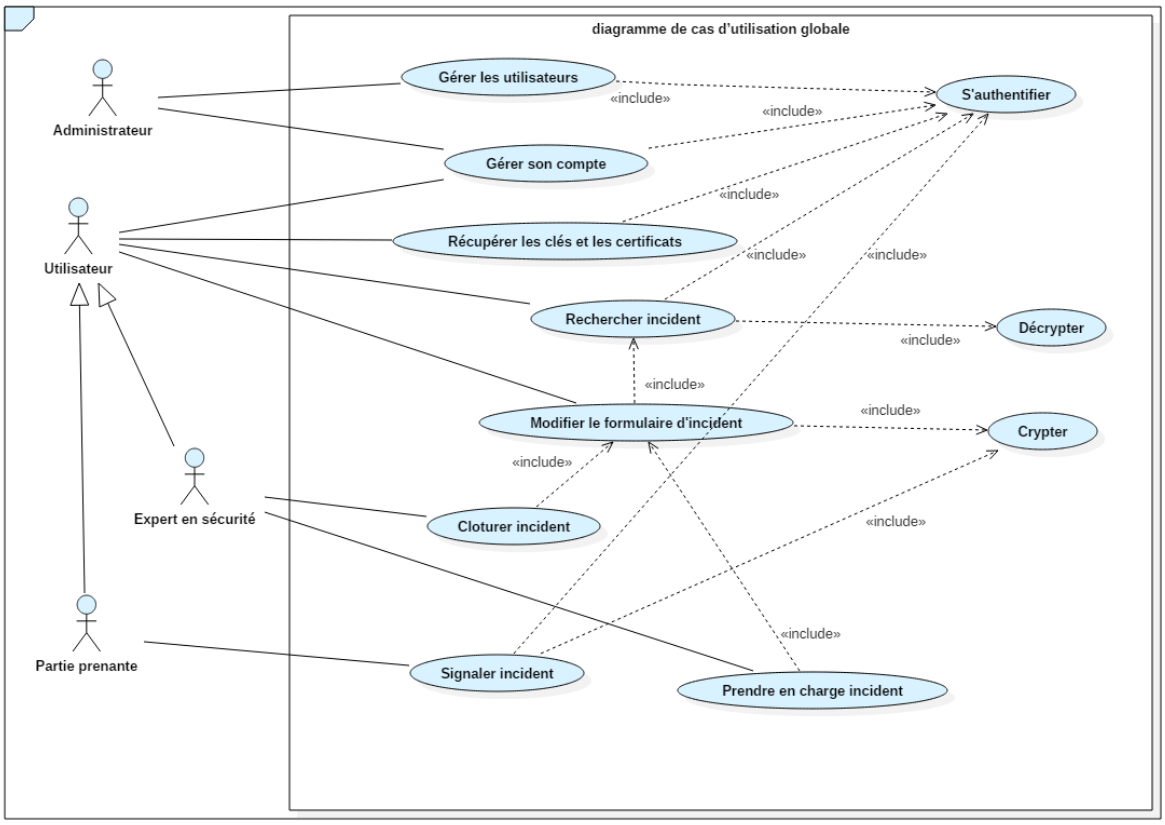


Figure 27 : Diagramme de cas d’utilisation global.

Cas d'utilisation	**Acteurs**	**Description**
S'authentifier	Administrateur, Partie prenante, Expert en sécurité	L'administrateur, les parties prenantes, doivent s'authentifier pour pouvoir accéder à leur espace.
Gérer les utilisateurs	Administrateur	L'administrateur peut ajouter, rechercher, supprimer ou modifier un utilisateur (partie prenante ou expert de sécurité)
Gérer le compte	Partie prenante, Administrateur, Expert en sécurité	L'administrateur, les parties prenantes ainsi l'expert en sécurité peuvent modifier leur profil, modifier le mot de passe, et se déconnecter.
Gérer les incidents	Partie prenante, Expert en sécurité	Les parties prenantes peuvent rechercher incident, modifier le formulaire d'incident, signaler un 'incident, et l'expert en sécurité peut prendre en charge incident, clôturer incident, rechercher incident, et modifier le formulaire d'incident aussi.
Récupérer les clés et les certificats	Partie prenante, Expert en sécurité	Dès que le certificat expire les parties prenantes, et les experts en sécurité demandent à l'administrateur de les renouveler.
Rechercher incident	Partie prenante, Expert en sécurité	Rechercher des informations d'un incident. Le résultat de recherche doit être décrypté pour l'affichage.
Modifier le formulaire d'incident	Partie prenante, Expert en sécurité	Modifier les informations d'un incident. Le formulaire doit être décrypté pour l'affichage et crypté après modification.

Signaler incident	Partie prenante	Signaler tous événements liés à la sécurité de l'information indésirables ou inattendus en remplissant un formulaire d’incident. Ce formulaire doit être crypté avant l’envoi.
Prendre en charge incident	Expert en sécurité	Prendre en charge incident. Le formulaire doit être crypté après modification.
Clôturer incident	Expert en sécurité	Une fois la solution trouvée, l’expert en sécurité informe de la clôture de l’incident. Le formulaire doit être crypté après modification.

Tableau 10 : Descriptions des cas d'utilisation du diagramme globale.

IV.3.7.2 Diagrammes de séquence

La figure 29 présente le diagramme de séquence « Crypter et Décrypter » qui décrit comment les éléments du système interagissent entre eux :

Quand la partie prenante signale un incident, il doit remplir un formulaire et l'envoyer. En arrière-plan, ce formulaire va être crypté comme suit :

- Le contenu est chiffré en utilisant l'algorithme AES et la clé secrète.
- La clé secrète est ensuite cryptée en utilisant l'algorithme RSA et la clé publique récupérée à partir de service d'archivage du KPI. Au fait, génère la paire des clés et le certificat la première fois, ensuite il les enregistre dans le service d'archivage.
- Le contenu chiffré du formulaire ainsi que la clé secrète chiffrée est envoyé au destinataire qui n'est qu'un expert de sécurité

Afin de traiter à cet incident, l'expert de sécurité va consulter le formulaire envoyé. En l'ouvrant, l'opération de décryptage se déclenche :

- La clé secrète va être décryptée en utilisant l'algorithme RSA avec sa clé privée,
- Ensuite, le contenu du formulaire est décrypté en utilisant l'algorithme AES et la clé secrète déchiffrée.

Notons ici que la partie prenante puisse être émetteur (comme dans le cas de signalement d'un incident décrit ci-dessus) ou destinataire (le cas de modification/recherche d'un incident). La même chose pour l'expert de sécurité qui peut être aussi émetteur dans le cas où il modifie ou clôture un incident. :

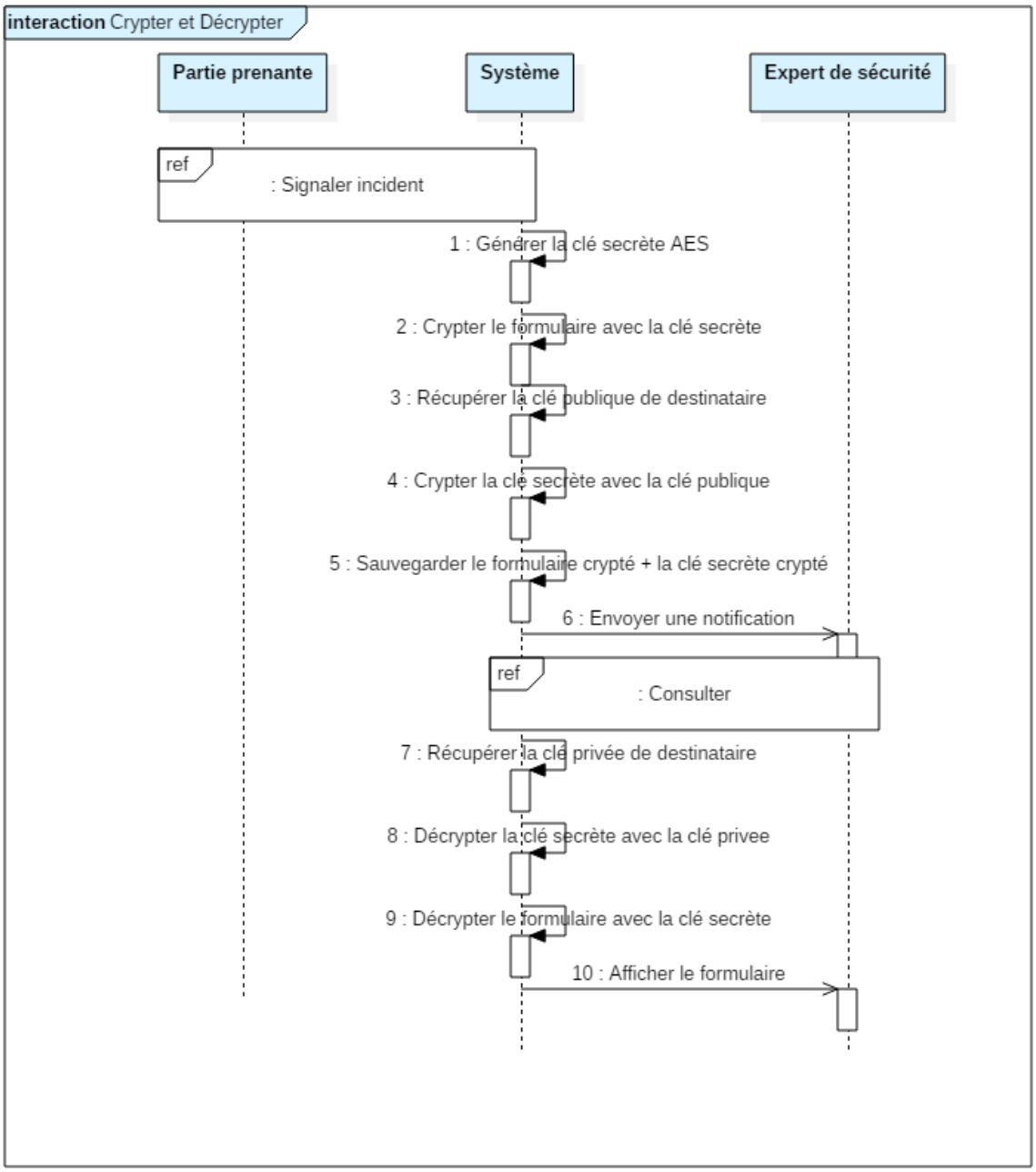


Figure 28 : Diagramme de séquence ‘’Crypter et décrypter’’.

IV.3.7.3 Diagramme de classe

Notre diagramme de classe présenté dans la figure suivante décrit la structure du système en montrant les classes intervenantes et les relations entre elles :

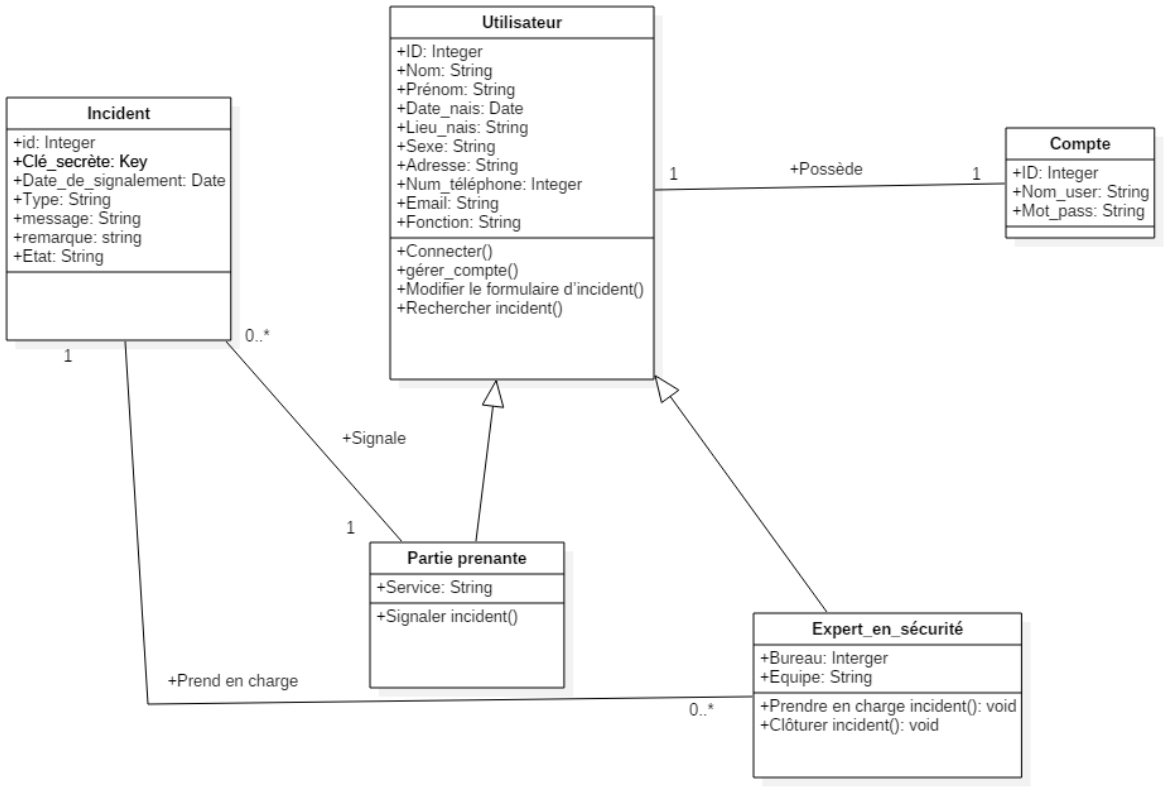


Figure 29 : Diagramme de classe.

IV.4 Conclusion

Dans ce chapitre, nous avons décrit notre solution cryptographique pour le CSIRT-ELIT qui est basé sur la cryptographie hybride, qui combine les avantages de cryptage symétrique AES et asymétrique RSA, afin d'assurer la rapidité et la sécurité du système. Dans le chapitre suivant, nous présenterons les étapes suivies dans l'implémentation et la réalisation de notre application composée d'un portail web et d'un système cryptographie.

CHAPITRE V : REALISATION

V.1 Introduction

Dans ce chapitre nous allons présenter la partie de réalisation de notre application qui a pour objectif de mettre en œuvre la solution décrite dans le chapitre précèdent. Nous allons commencer par une description de l'environnement de développement. Ensuite, nous allons décrire l'implémentation du système cryptographique utilisé. Enfin, nous allons et représenter les différentes interfaces de notre application.

V.2 Environnement de développement

Un environnement de développement est défini par une suite d'applications et d'outils que nous avons installés sur nos machines pour nous aider à développer notre application (figure 31). Nous avons utilisé deux machines : une machine physique et l'autre virtuelle en utilisant Oracle VM Virtuel Box pour mettre en œuvre notre système. Les caractéristiques des deux machines sont décrites dans le tableau 12. Notre application se fonctionne sous forme client/serveur et est implémentée en utilisant les langages suivants (Tableau 14) : HTML, CSS, PHP et java script.

Machines utilisé	Machine physique	Machine virtuelle
Système d'exploitation	Windows 10 pro	ubuntu-20.04.1
RAM	4,00 GO	1,50 GO
Processeur	Intel ® Core ™ i3-3110M CPU @ 2,40GHz	Intel ® Core ™ i3-3110M CPU @ 2,40GHz
Acteurs présentés	Administrateur, client SSH (partie prenante ou experts de sécurité)	Autorité de certification racine et intermédiate, serveur SSH
Logiciels utilisées	PhpMyAdmin 5.0.1, HTML, CSS, PHP, java script, OpenSSL, Crypt_RSA, client SSH	PKI, serveur SSH.

Tableau 11 : Caractéristiques des machines utilisées.

Langage	Description	Page officielle
HTML	Signifie « *HyperText Markup Language* » qu'on peut traduire par « langage de balises pour l'hypertexte ». Il est utilisé afin de créer et de représenter le contenu d'une page web et sa structure.	https://developer.mozilla.org/fr/docs/Web/HTML
CSS	Signifie « Feuilles de style en cascade » CSS est l'un des langages principaux du Web ouvert et a été standardisé par le W3C. Ce standard évolue sous forme de niveaux (levels), il décrit comment les éléments HTML doivent être affichés.	https://developer.mozilla.org/fr/docs/Web/CSS
PHP	PHP (officiellement, ce sigle est un acronyme récursif pour PHP Hypertext Preprocessor) est un langage de scripts généraliste et Open Source, spécialement conçu pour le développement d'applications web. Il peut être intégré facilement au HTML.	php.net/manual/fr/intro-whatis.php
Java script	**JavaScript** (qui est souvent abrégé en « JS ») est un langage de script léger, orienté objet, principalement connu comme le langage de script des pages web.	https://developer.mozilla.org/fr/docs/Web/JavaScript

Tableau 12 : Description des langages utilisés.

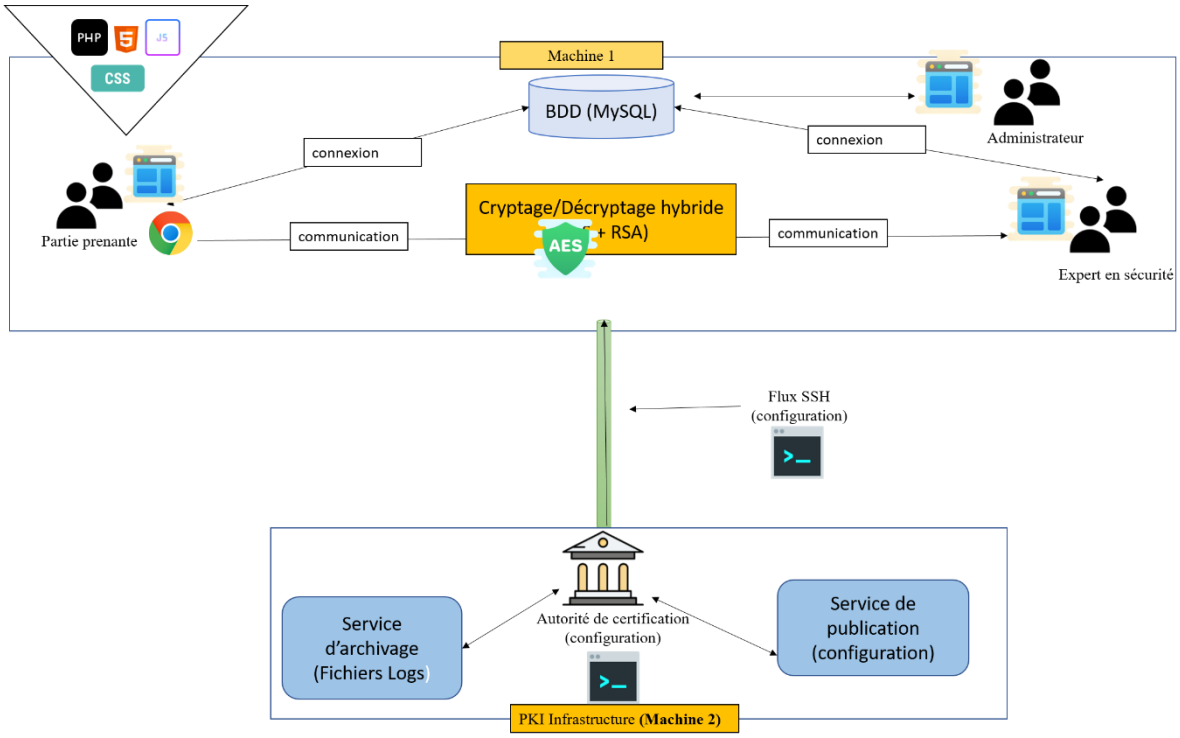


Figure 30 : L'environnement de développement de notre application.

V.3 Implémentation du système cryptographique

Pour l'implémentation de notre système cryptographique, nous avons

- Utilisé la librairie OpenSSL pour le cryptage symétrique AES et pour la configuration des composants PKI.
- Utilisé le package Crypt_RSA de la bibliothèque phpseclib - (PHP Secure Communications Library) [17] pour le cryptage asymétrique RSA.
- Configuré le protocole SSH sur les deux machines.

[17] https://sourceforge.net/projects/phpseclib/files/phpseclib1.0.19.zip/download

V.3.1 Librairie Openssl

C'est une boîte à outils robuste, de qualité commerciale et complète pour les protocoles Transport Layer Security (TLS) et Secure Sockets Layer (SSL). C'est également une bibliothèque de cryptographie à usage général [82], ainsi qu'une interface en ligne de commande. OpenSSL est disponible sur les principaux systèmes d'exploitation et dispose de nombreux wrappers[18] ce qui la rend utilisable dans une grande variété de langages informatiques [83].

Pour utiliser l'algorithme AES intégré, nous devons préciser son nom «aes-256-cbc » dans les fonctions de cryptage/décryptage comme suit:

```php
function encryptthis($data) {

$key=openssl_random_pseudo_bytes(64);
    $encryption_key = base64_decode($key);
    $iv = openssl_random_pseudo_bytes(openssl_cipher_iv_length('aes-256-cbc'));
    $encrypted = openssl_encrypt($data, 'aes-256-cbc', $encryption_key, 0, $iv);
    return base64_encode($encrypted . '::' . $iv.'::'.$key);
    }
```

Chiffre les données passées avec la méthode aes_cbc et la clé précisée.

Retourne une chaîne de caractères encodé en base64.

Fonction de cryptage aes-256-cbc

```php
function decryptthis($data)
    {

        list($encrypted_data, $iv,$key) = array_pad(explode('::', base64_decode($data), 3),3,null);
        $encryption_key = base64_decode($key);
        return openssl_decrypt($encrypted_data, 'aes-256-cbc', $encryption_key, 0, $iv);
    }
```

Fonction de décryptage aes-256-cbc

Retourner les valeurs concaténées

(le message, la clé et le vecteur d'initialisation)

[18] **Adaptateur** (ou wrapper) est un patron de conception (*design pattern*) de type structure (*structural*). Il permet de convertir l'interface d'une classe en une autre interface que le client attend.

Figure 31 : Les fonctions de cryptage/décryptage de l'algorithme AES.

V.3.2 Package Crypt_RSA :

C'est une classe de phpseclib (purement en php) qui est mieux entretenu et moins vulnérable aux problèmes de sécurité. Crypt_RSA fournit la génération de clés de type RSA, le cryptage /décryptage, la signature et la vérification de signature [81]. La figure suivante présente es fonctions de cryptage/décryptage.

Figure 32 : Les fonctions de cryptage/décryptage de l'algorithme RSA.

V.3.3 Configuration des composants PKI

Dans le tableau suivant, nous allons détailler la configuration des composants du PKI tout en donnant les commandes nécessaires [92]:

Les commandes	Description
apt-get install openssl	Installer openssl. Notons ici que la librairie Openssl est la librairie open source, quasiment élevée au rang de standard sous UNIX, pour ce qui concerne les fonctions cryptographiques et les fonctions de hachage. En particulier, elle implémente quasi-complètement le standard des PKI, i.e la norme X509 [75].
mkdir /root/ca cd /root/ca	Créer et accéder au répertoire ça dans lequel nous allons travailler.
mkdir certs crl newcerts private	Créer des dossiers qui contiennent : Certs: les certificats Crl : liste des révocations newcerts : les nouveaux certificats private : les clés privées
chmod 700 private	Aucune permission pour le dossier private
touch index.txt echo 1000 > serial	Créer un fichier vide « index.txt » Les fichiers index.txt et serial sont des fichiers de base de données plat qui serviront à conserver l'information sur les certificats signés. Numéro de série du 1er certificat : echo 1 > serial
config.cnf	Créer le fichier de configuration qui contient les paramètres de certificats par défaut.
openssl genrsa -aes256 -out private/ca.key.pem 4096 chmod 400 private/ca.key.pem	Générer de la clé privée et changer les permissions avec chmod.

openssl req -config config.cnf \-key private/ca.key.pem \-new -x509 -days 7300 -sha256 -extensions v3_ca \-out certs/ca.cert.pem chmod 444 certs/ca.cert.pem	Générer le certificat et changer les permissions.
openssl x509 -noout -text -in certs/ca.cert.pem	Vérifier le certificat
mkdir /root/ca-intermediate cd /root/ca-intermediate mkdir certs crl csr newcerts private chmod 700 private touch index.txt echo 1000 > serial	Créer l'autorité de certification intermédiaire qui sera utilisé pour faire la signature des certificats
Config_intermediate.cnf	Fichier de configuration de l'AC intermédiaire
openssl genrsa -aes256 -out private/intermediate.key.pem 4096 chmod 400 private/intermediate.key.pem	Création des clés de l'AC intermédiaire.
openssl req -config openssl.cnf -new -sha256 \-key private/intermediate.key.pem \-out csr/intermediate.csr.pem	Générer une demande de certificat.
cd /root/ca openssl ca -config config.cnf -extensions v3_intermediate_ca -days 90 -notext -md sha256 -in /root/tp/ca-intermediate/csr/intermediate.csr.pem -out /root/tp/ca-intermediate/certs/intermediate.cert.pem	Nous avons donc notre demande de certificat prête qui fut réalisé avec la clé privé de l'autorité de certification intermédiaire. Nous allons donc maintenant signer / valider / indiquer que nous trustons l'autorité intermédiaire en signant la demande de certificat.
chmod 444 /root/ca-intermediate/certs/intermediate.cert.pem	Changer les permissions
cat /root/ca/index.txt	Vérifier la data de donnée.
cd /root/ca openssl genrsa -aes256 \ -out intermediate/private/user.key.pem 2048 chmod 400 intermediate/private/user.key.pem	Nous allons aller dans le répertoire ça. Ensuite nous allons créer la clé privée et changer ces permissions avec chmod.

openssl req -config intermediate/openssl.cnf \ -key intermediate/private/user.key.pem \ -new -sha256 -out intermediate/csr/user.csr.pem	Créer la demande de certificat client
openssl ca -config intermediate/openssl.cnf \ -extensions usr_cert -days 375 -notext -md sha256 \ -in intermediate/csr/user.csr.pem \ -out intermediate/certs/user.cert.pem chmod 444 intermediate/certs/user.cert.pem	Créer le certificat client et changer ces permissions avec chmod.
openssl x509 -noout -text \ -in intermediate/certs/user.cert.pem	Verifier le certificat.

Tableau 13 : Configuration des composants PKI.

Les figures suivantes montrent un Exemple de clés et de certificat générés :

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-256-CBC,A7F42D2F6C6C78E1B40CCA59D9D547C6

7pg6xgyDFxc3HXfNAK2vxIOPKaJ0AHrZQ9Ko7BRJOG4+FjKHUhVqSpQv1gQHdGwD
0stIe3zVwJf82jIpIpbCl91m1YxPe53TnlsHjBF/FcyakhCh5bzqt+/A36sZCG3H
1jeJOJfboEaC1b/Uq00QRejmArxzPv5wa3EYl+7NM/UpQOuoRgcmL3Qy7dv1JWtW
j2QoZm5FGLSHMZegSfhUg6PU0wAJZVSphE2C30J5wCW6Eueflxd0tFeCMuErH0aF
A2AxpC2SB40wcIPtl9m8qhVSepyB7mLU/QhRcATnaZYHTZgC0O0aseNtY1LEZhcM
xdqp09OVt7vaMpFYRblaW+SAlXh3+VYt7QuH12v1xeIPoYETkb2ZEXRIGy3cHQH3
JJh8tqupTO51FGotqQMfbXa2H1uyu0pQ3dAaP8tKUVpJfLCp4IgB67zA6xi0GHah
C8SHDgSr3xx4fECvcKH4+5dSzCMbfo6QBvJmOTCwlFZcJmZJfUQ2ak4nI/y2gonM
2q2ZrKJ7NHEB3O5r0SBaCKqNSqhW46ULXnQCMzfeyd1muQ47URzPvoV8hdI/ZqPN
OsQ/MTK0y0Vd87Yn1GFAwmZU+weY0nj+5DCEPwxkTKsCo92Dndft69CtnO129F3Y
MH++UxD2CDtzgpPhA4aaXXeCzKAZKXemNHGDtBQ6bvx7NPXXph8I415S1N95r6eg
3ArVtM9O1ONnOYp3CiIKNYctATn7y1Qa6JQ80suKbGhohR1N/IabNwehyxTRhNH9
0zvp5uINOtb/0MijeYKi73WzeWFLULVZh6YR96QbqHLXHhMwgTKzgN2HgenU1sFd
KC9Sm4/FjSx8PpzCaAfOuf+1I/vYg2X1yNRmC0RN9riGxpIXscl1Jrl89voft1rz0
n/qM8dPx+aWOoiUo389ZZetO1waBztzkdbmvTARdIOY1TaNXV0JfoUZd25Iftoyp
BxNTGOyhUotPfBR7IbgufdVTc8N6Fc8gPJP8X93z5m/gR91QsEONJX4ssE/R/W1C
pH7DyWoVA+43nIabWX1qcswYC4Hz5hCeATUZ3xoh/Z7Te1JxtiFHbXFL/Ht6SQsE
pWp4a+vAsgizGz0+G2z/n592RGEbm8USnscoLdt8fu3voE/z/XgHWf1RzsN1MXje
qB07/peUJyg0Woui6B+Lw1MX02p1xUD1XqQRhpjBjSGqsRD8ewcRGAj/swGNWAgT
0+Kej5jlgabCDWsJfrnK71SzPaR0bjboOmQoDi22zsbi5aT+ZHgH9RCkT+u4UgvL
h6N4AwzQf4RA7LuBPLdo8mROrt+Dt232uj0+IyuqrsZcC1IK8tpZT33uFCpRtgEd
xPn7JqRRIgCUkj9K6vU6s1O9WQ/n4MorxzGD5J9s1n1amH26F1Lv7bywB6NHEO6X
X4XTja94IbsS1TcibGoViVSUctte0c4Jid6RrvPrPjqFyy/aiL6nRORjbY20vH97
XpqnP1MVGHxygBIz6OCSytvwAcMhM4OLrL6ycu2XJaomyriLfg5g0OW4/eq+/rRO
1tMRIaDGupf1vcz/LiZYFv/4uOmv6UYESGpdsBzsE13B1n5BfnZXjcouohMrkrhZ
-----END RSA PRIVATE KEY-----
```

Figure 33 : un exemple de la clé privée générée par AC.

```
-----BEGIN CERTIFICATE-----
MIIEKDCCAxCgAwIBAgICEAAwDQYJKoZIhvcNAQELBQAwVjELMAkGA1UEBhMCQUcx
EDAOBgNVBAgMB0FsZ2VyaWUxDTALBgNVBAoMBEVsaXQxDDAKBgNVBAsMA1NTSTEY
MBYGA1UEAwwPaW50ZXJtZWRpYXRlIENBMB4XDTIwMDYxOTIzNDgwOVoXDTIxMDYy
OTIzNDgwOVowgY8xCzAJBgNVBAYTAkFHMRAwDgYDVQQIDAdBbGdlcmllMQ4wDAYD
VQQHDAVBbGdlcjENMAsGA1UECgwERWxpdDEMMAoGA1UECwwDU1NJMRgwFgYDVQQD
DA9DSEFCTkkgQ2hhaGluZXoxJzAlBgkqhkiG9w0BCQEWGGNoYWhpbmV6Y2hhYm5p
QGdtYWlsLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOu03p/C
YYMbHPPKZmrts4WWzqGJGMyD5sVJ2K45vU82JJ5mQ/A3BgTDVxCV0ZZABJYzga4m
+ZmCJso3tupeU12UgVt/cJYPo+9RR2Pakx6rIaFNM10hp+nAvAApeKEwNzPBOqWq
zM6TTMrpxc7wRHv5LEq1HHYyGHPc/b5W9himVhKdIebksaWh5i9vt4ot/3CYr+X3
Cnw0YYv9C8RbdbDth/3acyHrf5yBSeimhjYcNeOFyHuaibZxSViOEN2Xun2Tse6t
QaqlRSr2DjRurqMQ8enKw4XReC6cl1IP1gWr/mcXwvphbPfAbzuyuAg2yZrmu3ML
MbL08wUjzDKfgtUCAwEAAaOBxTCBwjAJBgNVHRMEAjAAMBEGCWCGSAGG+EIBAQQE
AwIFoDAzBglghkgBhvhCAQ0EJhYkT3BlblNTTCBHZW5lcmF0ZWQgQ2xpZW50IENl
cnRpZmljYXRlMB0GA1UdDgQWBBTUd0FfDaRBXHzAExSiFTVxFe1rgzAfBgNVHSME
GDAWgBRUoJqVBDikcQLJW6rjE5Lij7rieDAOBgNVHQ8BAf8EBAMCBeAwHQYDVR01
BBYwFAYIKwYBBQUHAwIGCCsGAQUFBwMEMA0GCSqGSIb3DQEBCwUAA4IBAQCUiqo7
rLCQF4Enf3hvE8NTNMnKOo69PEdmr5stc/bBzwY6QBn2ARIdbfR84c8sWneHcUzR
bvHAH1DGyFAa/NU0mzO6oTEwSO6ceadqgN2t+7QY3dILMiINCiUiVjisWIu2BzUo
IrZB6Mj5oGmw+aXS8jzLDLH1R696hsj3/qar0A+avwkbD2eOysiPO0pEC4fuH2wF
GXw85QSo0MZGW4P/asoKsieGp8dMzZEvsMVUnHxLCdHs+qCGTvjm6inzsyRlQmf8
1+bONE53B+i31tdNh95ZPwjusSePIVfDXUTTrIwu4mYWaUAqq8MtjwsVGTu9C/KV
insk4Y78kMPj7lGv
-----END CERTIFICATE-----
```

Figure 34 : Un exemple de certificat généré par AC.

V.3.4 Configuration du protocole SSH

L'objectif d cette configuration est de se connecter à un serveur SSH Linux depuis un terminal Windows via une authentification par mot de passe :

- **Serveur SSH sous Linux :**

La configuration qui est décrite ci-dessous pour la partie serveur du protocole SSH [93] :

Commande	**Description**
sudo apt-get install openssh-server	Exécuter et installer l'application Open SSH.
sudo service ssh start	Démarrer le service SSH
service ssh status	Vérifier si le service SSH est activé
nano /etc/ssh/sshd_config	Ouvrir le fichier de configuration et configurer le service SSH.
systemctl restart sshd	Redémarrez le service SSH

Tableau 14 : La configuration SSH coté Linux.

- **Client SSH sous Windows**

Il faut tout d'abord tester si l'outil "OpenSSH client" est installé sur la machine. Pour se faire, on ouvre les **paramètres Windows** > **Applications** > **Fonctionnalités facultatives**. Une liste affichera les outils déjà installés - si "**OpenSSH client**" n'y est pas, on clique sur "**Ajouter une fonctionnalité**", on recherche "*OpenSSH client*" et on clique sur "Installer". Sans redémarrer le système, l'outil sera disponible instantanément après l'installation. Et pour connecter au serveur SSH via l'invite de commandes Windows, nous utilisons la commande suivante : ssh username@ipaddress [51].

V.4 Présentation de l'application

Nous avons développé un portail web (Figure 36) pour gérer les incidents de sécurité au niveau du CSIRT ELIT. Notre application offre plusieurs fonctionnalités de bases aux différents acteurs : administrateur, partie prenante et expert de sécurité. Ces acteurs doivent s'authentifier afin d'accéder à leur propre espace. L'espace de chaque acteur est présenté dans les sous sections suivantes.

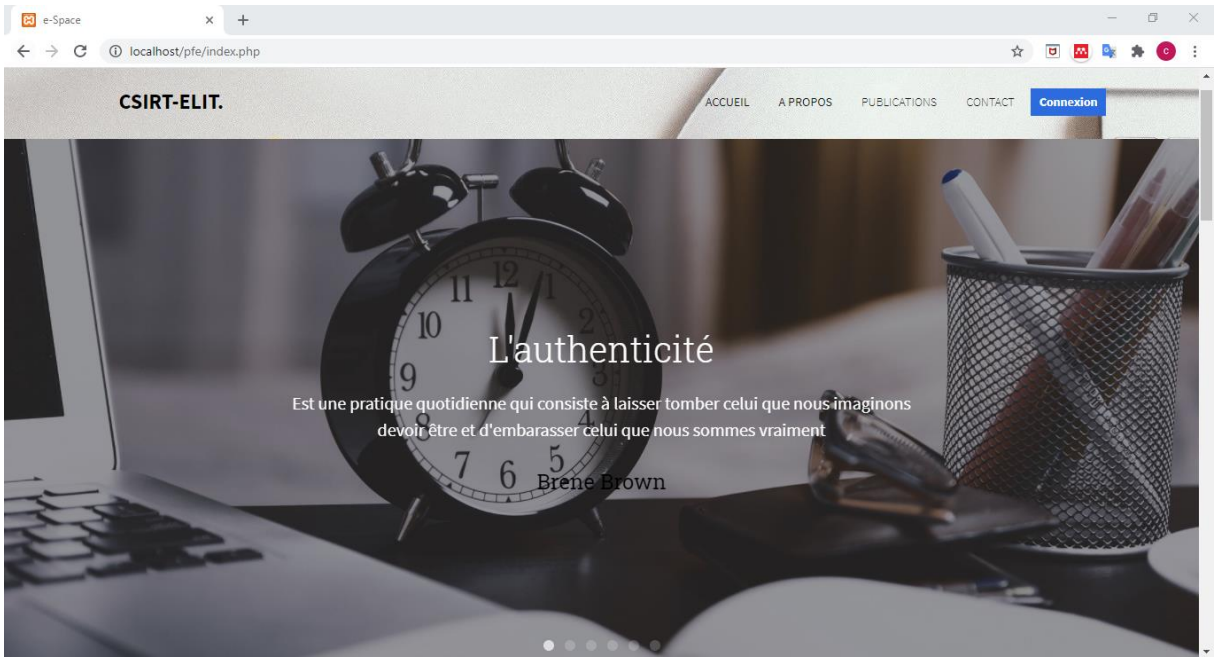
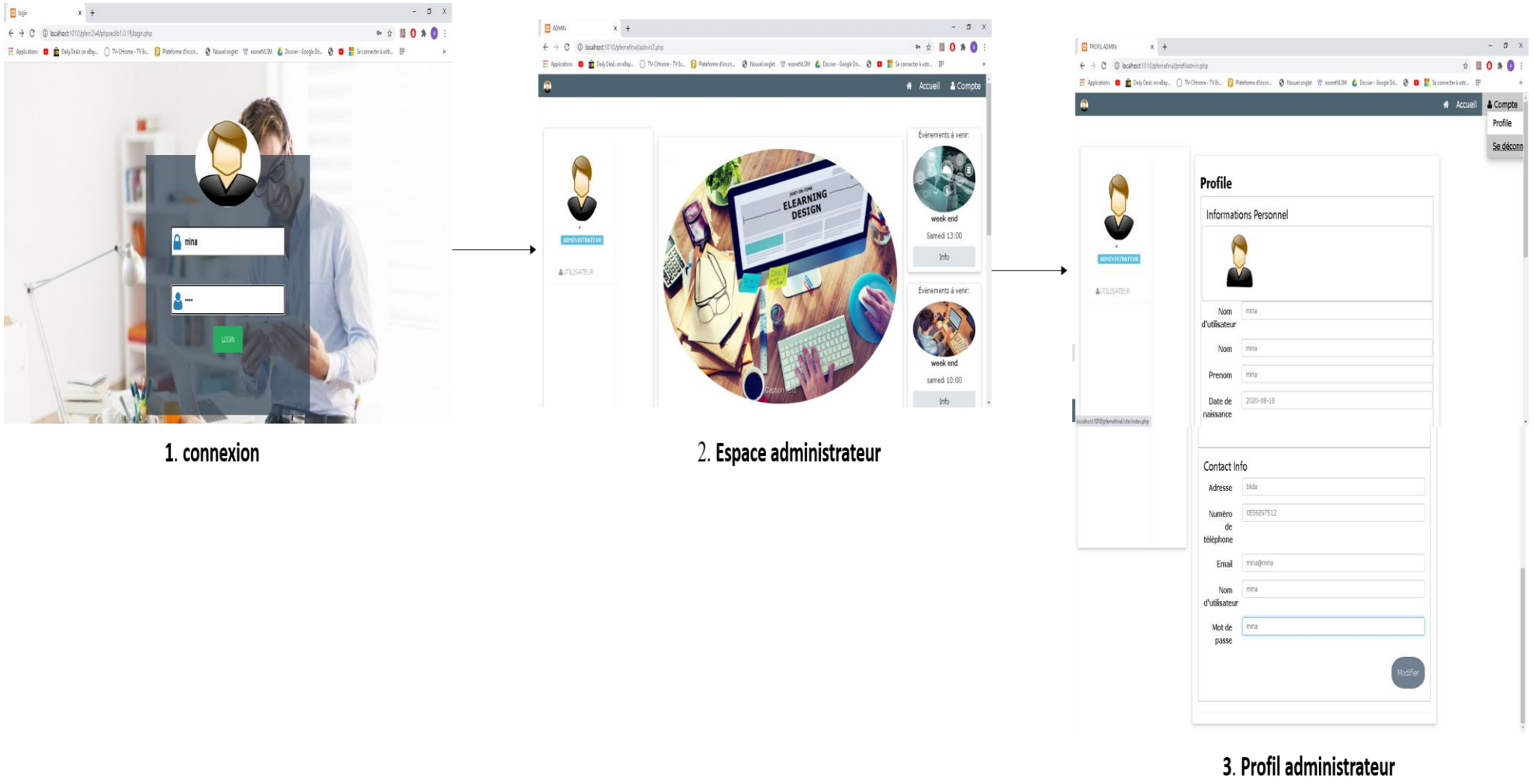


Figure 35 : La page d'accueil.

V.4.1 Espace administrateur

Chaque utilisateur possède son propre espace. L'espace de l'administrateur permet de gérer les utilisateurs ainsi que de gérer son compte comme représenté dans les figures suivantes :

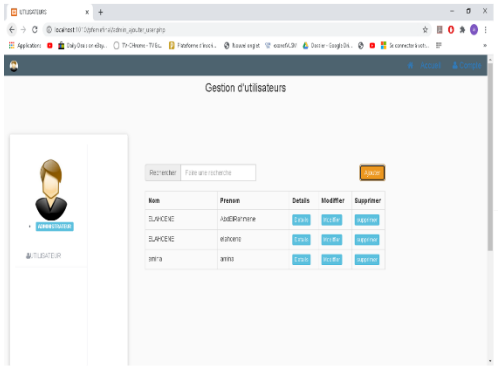


1. connexion

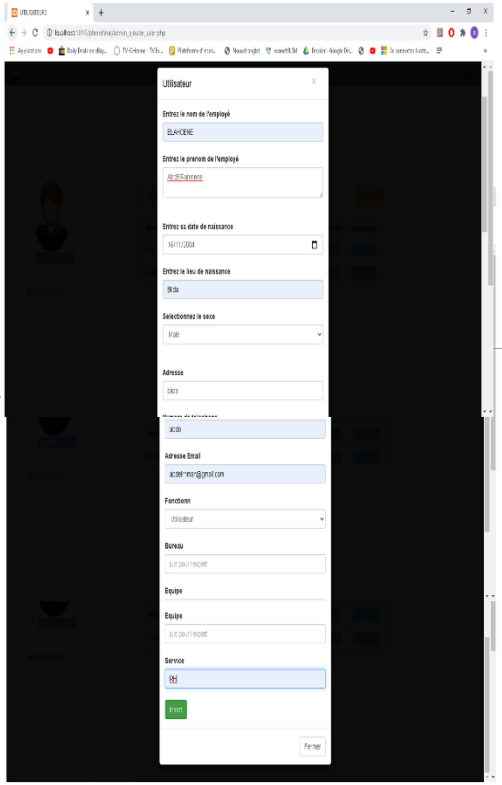
2. Espace administrateur

3. Profil administrateur

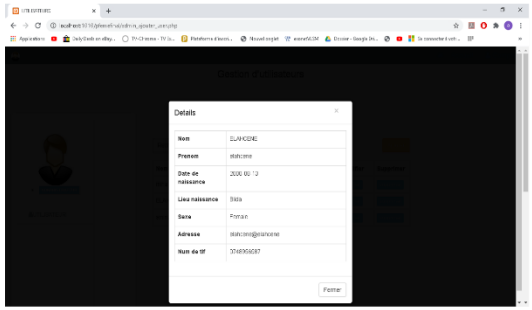
Figure 36 : Gérer le compte.



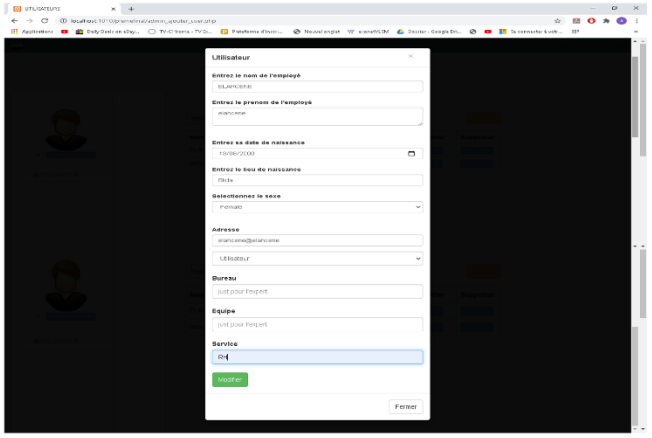
1. Gestion des utilisateur



4. Ajouter utilisateur

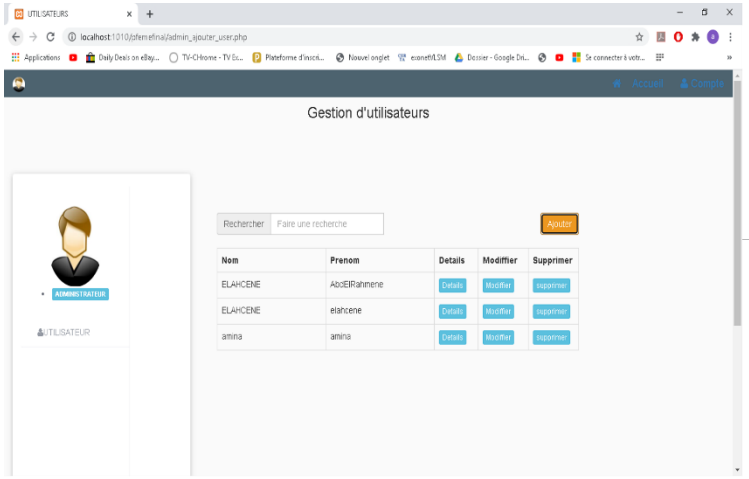


3. Détails d'un utilisateur

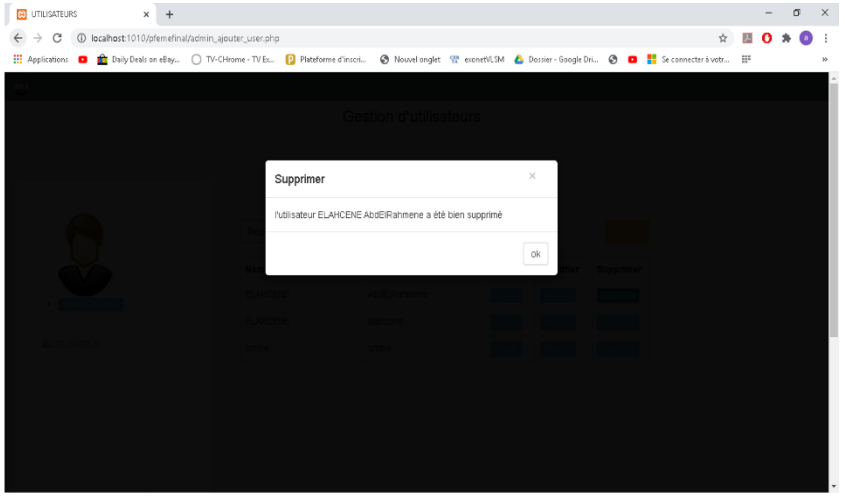


2. Modifier utilisateur

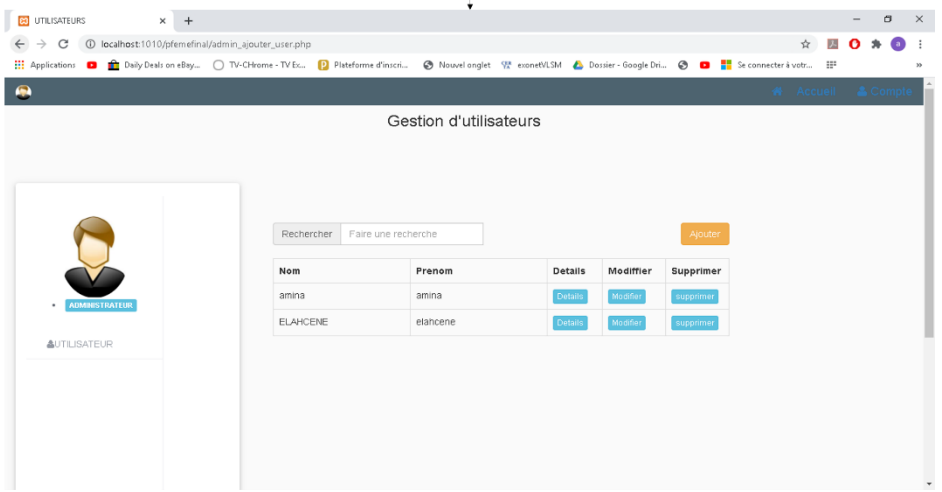
Figure 37 : Gestion d'utilisateur.



1. Supprimer un utilisateur



2. Utilisateur supprimer



3. Utilisateur supprimés de tableau

Figure 38 : Gestion d'utilisateur.

V.4.2 Espace utilisateur

Cette espace permet à l'utilisateur de gérer son compte (la même avec l'administrateur, voir la figure 37), de signaler un incident de sécurité en remplissant un formulaire bien défini (figure 40). Les parties prenantes peuvent aussi rechercher un incident, modifier le formulaire d'un incident et récupérer les certificats et les clés (la même avec l'expert de sécurité, voir la figure 45).

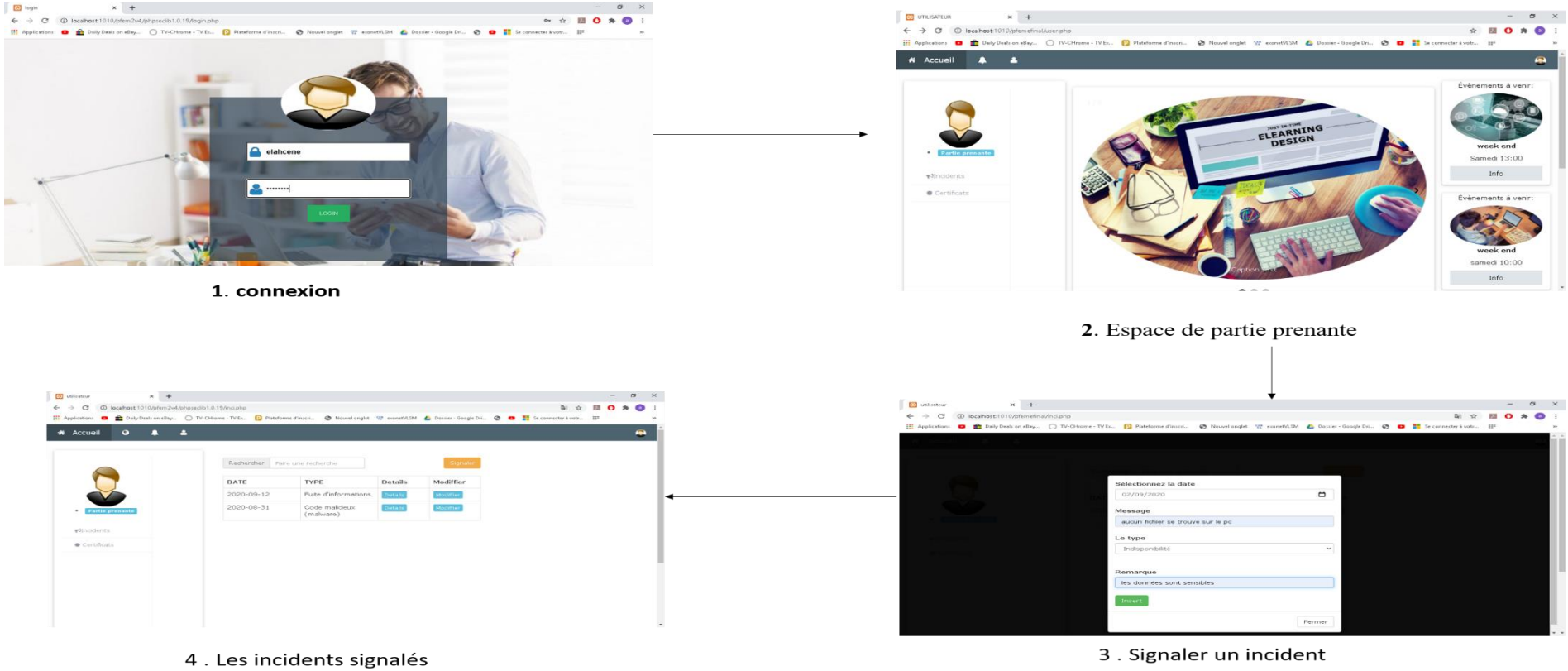


Figure 39 : Signaler incident.

Les incidents sont cryptés ensuite sauvegardés dans la base de données comme le montre la figure suivante :

id	userid	cle_secrete	date_signalement	t
27	14	Czp0Y4OZ9oPQsX9s7iTMPcyEl1yGkhbAZit/fMF/j6WWt7w+NR...	RDM5UW1kV2ZVOFVCemw4eXhRVkZwdz09OjojM2afPBo0HSaxM/...	N
28	1	Kh5ZYfJzXH8Q/8t916CfdzuplKD9y2R4X7J7ZgAgiSXNxiqMH2...	RFBZVFYwNWdTRGJuTkVvOWVxWUFFUT09OjrcsZTH7yAvSr8e6U...	N
29	14	fsy/8rZCIMU62bK1n35SazcWEf9IM7sKUlfO7+6qgNyTPgw5Fn...	Y1k2NmwzYlR3VytNRDdyNTZGZk5Fdz09OjpvEWCUli3+yfsEma...	\
30	1	OSrvJjs2dCRAEUggUT97aGwmVaAi40mw1bhFi7BkDO7R9wWHCg...	UDZkTWZnQ3pJeU5rUjU1Q3JCYUNsUT09OjrAgAUblUuluEV1zd...	\

type	message
NjhUWU1SajljdkpTSVhvZ083ME1XNk9lWGR6aGFlUHpzK21aQz...	bHpNdE04V2hpOFlOdUVjQmhsWUNrQT09OjoJkhNARljjEXxoaw...
NUUxb3FnYW1qRVdRMVlzNjZLZENoNC8xanN4R1hjOFc2aHA3NT...	R2ViYzdqaVk3VjdMTXd4VTlmZXpTUTZEVVBnNm1UYnM4Vk43a0...
Ynk1bzhkQno2ZnNxV1dvNk8wRFdJbVByalVVZVZPYWFDOFhHUX...	WXJRclJidWVpSDdGUGYzSlYwRDQ2ZzNXL0dhbDRQTER5L29QUk...
WjBDTmVRZVVKbXcvMEFwdjRDSDNTM2hOTXdDbHR0ZTd1UlhscU...	azc3VVQwQTNpQi94RURBSURkRkFyUT09Ojoc3ypNeRm0Pv5Wwq...

remarque	etat
QjVqaXJ3SnNnOGErcHRDajZTUFpZUT09OjpIx5doEwcjpPpeMu...	bnZvaCtQeEZuZlViVFNFN0JkcXVRQT09Ojqhqyu67RE+YM/lhJ...
VHBEUEZiVFVwYWN6NE1EMiszdGpuZz09OjrOBYcTalmQckksJy...	d2RKRFhMTTdpNnlKa1dWVTkweUx6dz09OjrP/8EKA7MGkq9/G8...
aFdJdDRiYnJKMFliZTF3RE91TGpUdz09Ojp9UU97w7YroNU7ps...	N20rb2J6Qnh1aEJqbk84dFhxYWRrdz09OjqEe9+DVEMkhyYyYO...
ZHBSY3FxS0R1cEpCWFlJSGE1K2xxdz09OjoyYTqu2+bCTnChOC...	TjZ2cktWdHZweEhjTW1FRVdscXFjUT09OjqNmwzFRQ5g4VTLOl...

Figure 40 : Table d'incident cryptée.

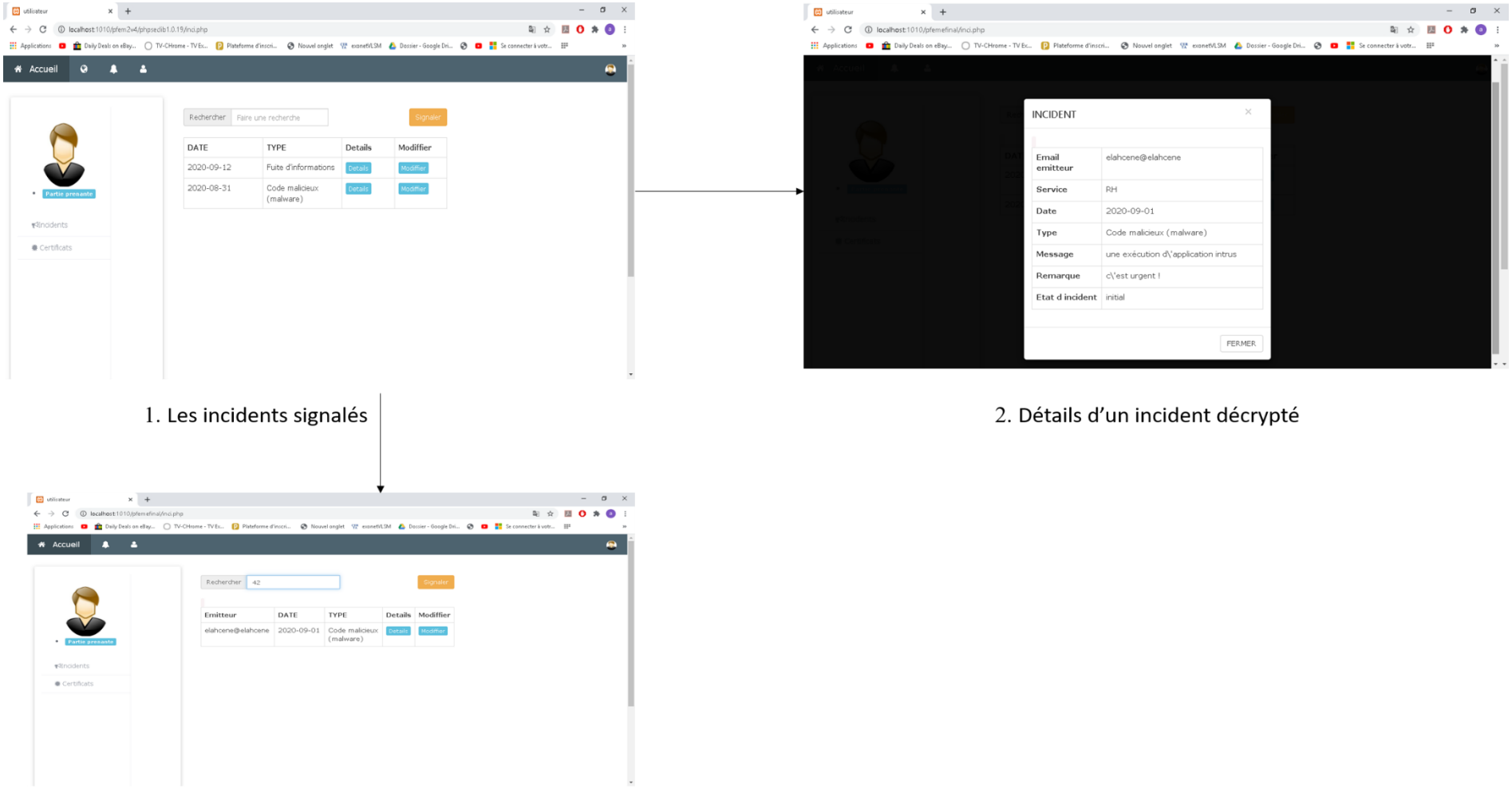


Figure 41 : Recherche et détails d'un incident.

V.4.3 Espace d'expert en sécurité :

Cet espace permet à l'expert en sécurité de gérer son compte (la même avec l'administrateur voir la figure 37), et aussi de prendre en charge un incident, clôturer un incident, rechercher un incident, et modifier le formulaire d'un incident et des récupérer les certificats et les clés, comme illustre les figures suivantes :

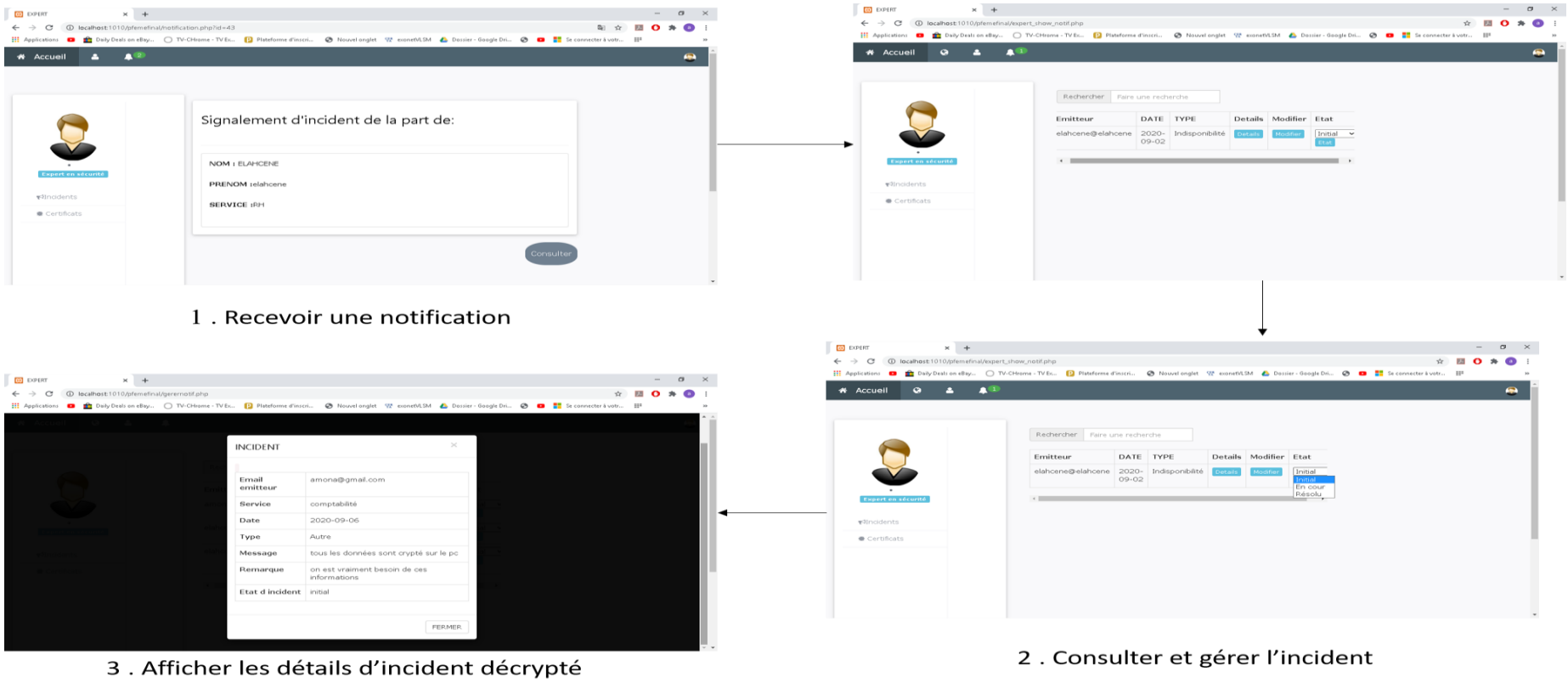


Figure 42 : La gestion d'incident.

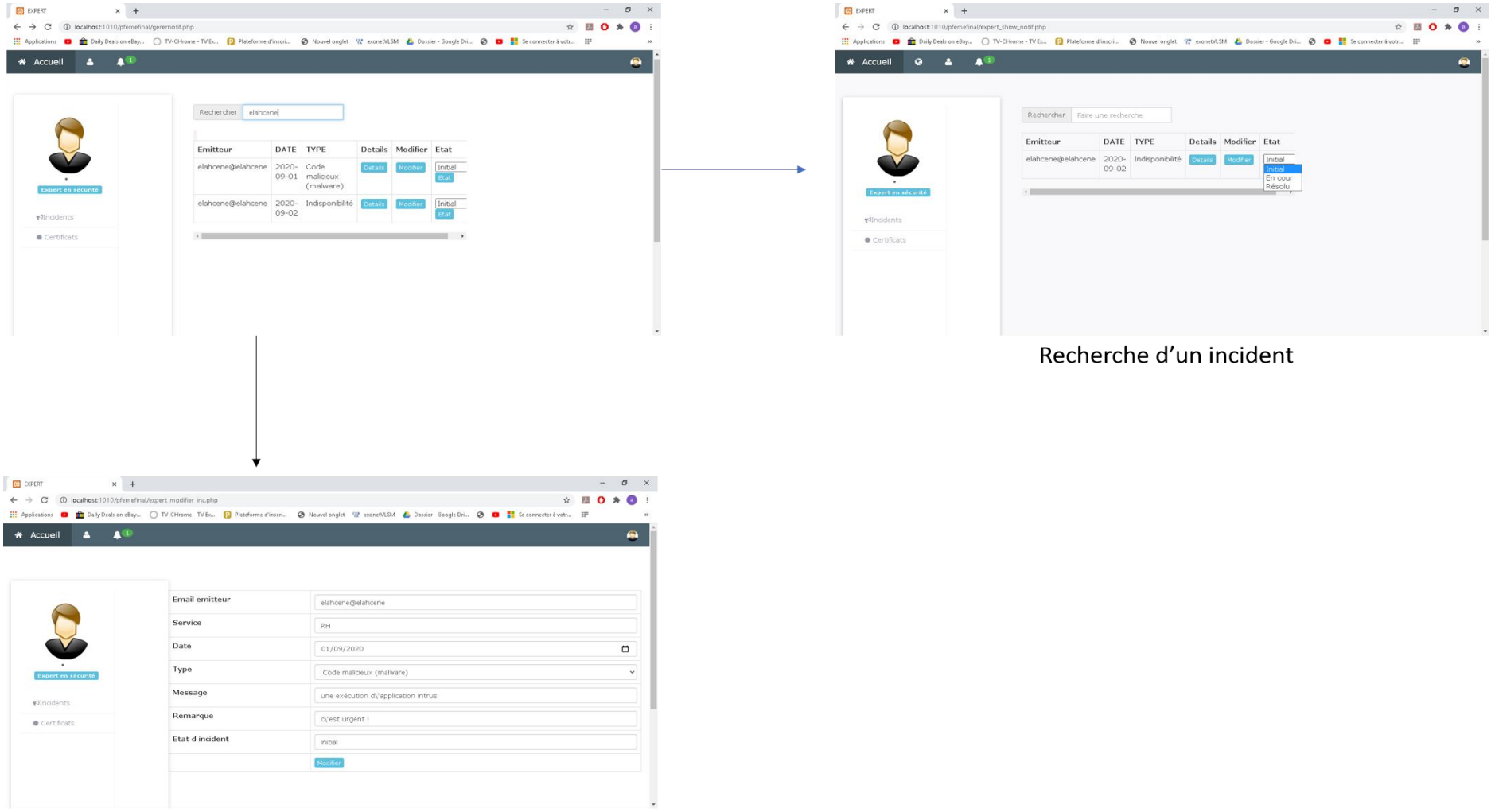
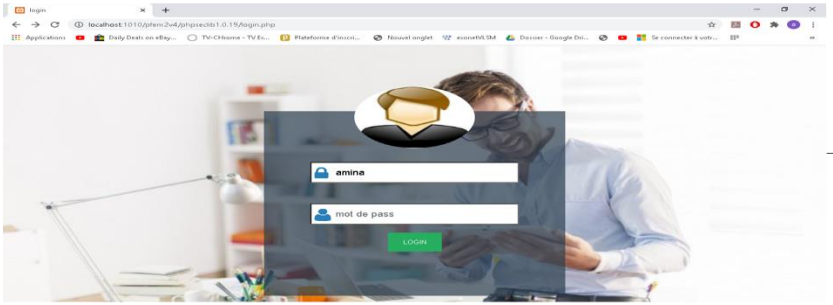
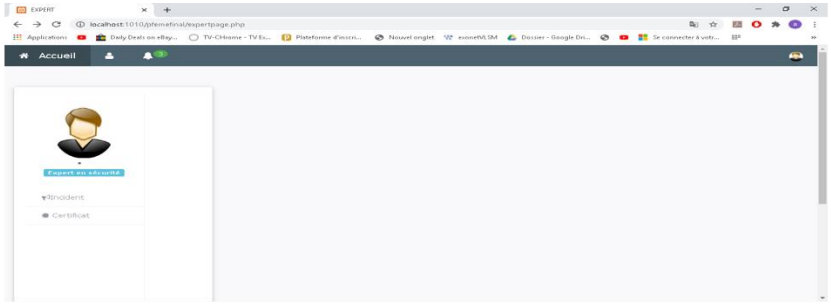


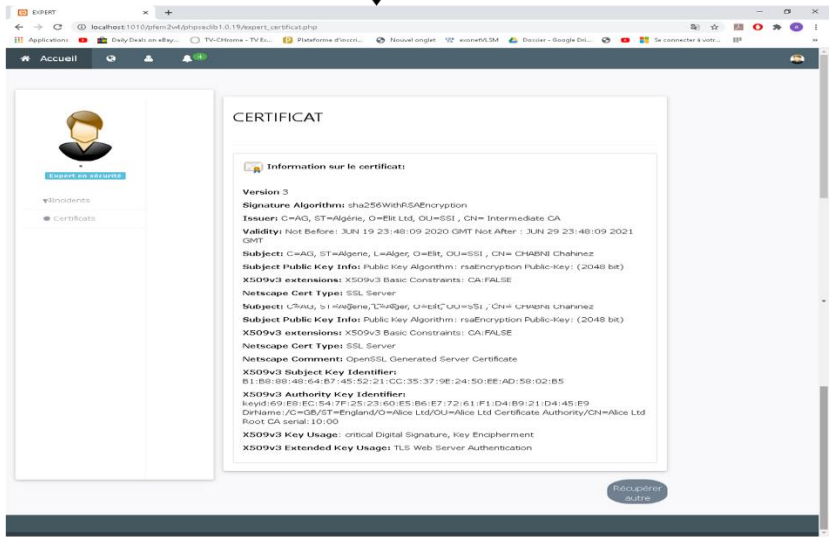
Figure 43 : la gestion d'incident.



1. connexion



2 . Espace de expert en sécurité



3. Afficher l'état de certificat

Figure 44 : Récupérer les certificats et les clés.

V.6 Conclusion

Dans ce chapitre, nous avons décrit le processus de réalisation de notre application en respectant la conception élaborée, en spécifiant les outils de développement et les fonctions de cryptage/décryptage hybride. Nous avons ensuite présenté les différents espaces de notre application à travers lesquels les utilisateurs peuvent accéder aux différentes fonctionnalités comme la gestion des utilisateurs pour l'administrateur, la gestion des incidents et la récupération des clés et certificats pour les parties prenantes et les experts de sécurité.

Conclusion Générale et Perspectives

L'objectif de notre travail est de garantir la sécurité des échanges entre l'expert en sécurité et les utilisateurs de système d'information de CSIRT ELIT, afin de pouvoir préserver la confidentialité et l'intégrité de ces données. Pour atteindre cet objectif, nous avons commencé par une étude bibliographique pour éclaircir les différentes notions liées à notre thématique qui sont : les incidents de sécurité et leur gestion (chapitre 1), les équipes de réponse aux incidents de sécurité CSIRT et notamment celle de CSIRT ELIT qui représente notre champ d'étude (chapitre 2) et enfin les systèmes cryptographiques (chapitre 3).

A partir de l'étude détaillée du fonctionnement actuelle du CSIRT ELIT, nous avons constaté que ce dernier présente un inconvénient majeur : tous les échanges internes et externes se font en texte clair sans sécurisation. Pour remédier à ce problème, nous avons opté pour un système cryptographique hybride permettant de gagner la rapidité des algorithmes symétriques et la sécurité des algorithmes asymétriques. Notre système fait appel à deux algorithmes de cryptage/décryptage : l'algorithme symétrique AES pour chiffrer/déchiffrer rapidement les échanges avec une clé secrète et l'algorithme asymétrique RSA pour chiffrer/déchiffrer le partage de la clé secrète en utilisant une paire de clé publique et privée. La conception de cette solution était décrite et détaillée dans le chapitre 4. A la fin, dans le chapitre 5, nous avons implémenté un simple portail web permettant la gestion des incidents au niveau de CSIRT ELIT de manière sécurisée. Au fait, les échanges entre les différents acteurs (parties prenantes et experts de sécurité) sont chiffrés en utilisant notre algorithme de cryptage/décryptage hybride AES-RSA. De plus, nous avons utilisé le protocole SSH pour partager les clés privées ainsi que les certificats à partir de l'autorité de certification

Enfin, comme perspectives nous suggérons :

- Concernant le portail web : d'ajouter les autres fonctionnalités/tâches offertes par le CSIRT ELIT, comme : établissement et maintenance d'une base de connaissance, coordination et échange avec les autres CSIRTs et sensibilisation.
-
- Concernant le système cryptographique :
    - D'automatiser l'utilisation des certificats avec l'annuaire LDAP et le protocole OCSP.
    - De tester d'autres algorithmes symétriques (RC4, RC5, …) et asymétriques (ECC).
    - D'implémenter les algorithmes hybrides existants (SSL).
    - D'intégrer d'autres mécanismes de sécurité (hachage comme sha)

Bibliographie

[1] Christophe.C, "Portail de la Sécurité des Systèmes d'Information", consulter le 30 juin 2020 sur https://ssi.ac-nancy-metz.fr/quest-ce-quun-incident-de-securite/.

[2] HELAL.S, « Authentification Anonyme et Contrôle d'Accès dans un Environnement Cloud : Application au Domaine e-santé », mémoire de master informatique, université Saad Dahlab Blida, pp. 12-23,2019.

[3] Savadogo.Y, « Gestion des incidents de sécurité de l'information", arcep/cirt-Burkina-Faco "centre de cybersécurité », Article, pp. 6-7, disponible sur https://www.cirt.bf/documents/gest_incidents.pdf

[4] Octopus, « Modèle de base-Incidents (pré configurations) », consulter le 1/07/2020 sur https://wiki.octopus-itsm.com/fr/articles/modele-de-base-incidents-pre-configurations.

[5] Zoho.C, « Le guide complet de gestion des incidents ITIL », consulter le 21/06/2020 sur https://www.manageengine.com/fr/service-desk/itil-incident-management-guide.html

[6] European Union Agency for Network and Information Security (enisa)," Reference Incident Classification Taxonomy Task Force Status and Way Forward", Article, pp. 6-10, Janvier 2018.

[7] Bonnefoi.P.F, « Cours de Sécurité Informatique », Livre, pp. 1-165, disponible sur https://pdfbib.com/241-cours-formation-securite-informatique.pdf

[8] Nowteam, « Tentatives d'intrusion : protégez votre système informatique », consulter le 22/06/2020 sur https://www.nowteam.net/tentatives-intrusion-protegez-systeme-informatique/

[9] Amimer.S, Hadidi.W, « Interception des attaques Réseaux avec L ' IDSSnort. », mémoire de master Electronique, université Saad Dahlab Blida, pp.18-26, 2017.

[10] Kaspersky Lab. « Qu'est-ce qu'un virus ou un ver informatique ? », consulter le 25/06/2020 sur https://www.kaspersky.fr/resource-center/threats/viruses-worms

[11] L' équipes de PCsansVirus ,« Comment se protéger contre les virus informatiques et les supprimer », consulter le 20/06/2020 sur https://www.pcsansvirus.com/pages/comment-se-proteger-contre-les-virus-informatiques-et-les-supprimer.html

[12] Kaspersky Lab. (2020) , « Qu'est-ce que le Cheval de Troie ? », consulter le 20/06/2020 sur https://www.kaspersky.fr/resource-center/threats/trojans

[13] Anubhi.K, Sanjay.K.D, « A Literature Review on Sniffing Attacks in Computer Network », Department of CSE, Amity University, Noida, India - 201303, Article, pp. 7, disponible sur https://ijaers.com/Paper-July%202014/IJAERS-JULY-2014-010.pdf.

[14] Panda Security 2019, « Attaques informatiques : quelles sont les plus courantes ? », consulter le 10/07/2020 sur https://www.pandasecurity.com/france/mediacenter/malware/attaques-informatiques-courantes/

[15] codeflow, "Java - Exemple de cryptographie hybride", consulter le 30/06/2020 sur https://www.codeflow.site/fr/article/java__java-hybrid-cryptography-examplez

[16] Nomios, « qu'est-ce que le cryptojacking et comment s'en protéger ? », consulter le 12/06/2020 sur https://www.nomios.fr/definition-cryptojacking/.

[17] Ronny.R, North.M, « Ransomware : Evolution, Mitigation and Prevention », Article, pp 13, 2017.

[18] Xyoos, « Les cours d'informatique-VPN », consulter le 04/07/2020 sur https://cours-informatique-gratuit.fr/dictionnaire/vpn/ .

[19] cisco, « ACL – Access Control List », Article, pp. 1, disponible sur https://www.ciscomadesimple.be/wp-content/uploads/2011/06/CMSBE_F04_ACL.pdf

[20] Internet Society, « C'est quoi le cryptage ? », consulter le 06/07/2020 sur https://www.internetsociety.org/fr/encryption/what-is-encryption/.

[21] Mellef.A, « Mise en place d'un système de gestion des incidents informatiques », mémoire de master, Université Virtuelle de Tunis , pp. 1-88, 2017, disponible sur http://pf-mh.uvt.rnu.tn/917/1/systeme-gestion-incidents-informatiques.pdf

[22] « La boite à outils», Livre, Grenoble école de management, pp. 1-143, disponible sur https://indico.in2p3.fr/event/5710/contributions/35070/attachments/28170/34734/IN2P3_octobre_2012_partie_1v1.pdf

[23] freshworks, « La gestion des incidents », consulter le 26/06/2020 sur https://freshservice.com/fr/gestion-des-incidents/

[24] PG Software (2020), « Gestion des incidents – ITIL », consulter le 26/06/2020 surhttps://www.pgsoftware.fr/gestion-des-incidents-itil

[25] Jeff.p, Adrien.R.G, « Qu'est-ce que la réponse aux incidents ? Un plan en 6 étapes », consulter sur https://blog.varonis.fr/quest-ce-que-la-reponse-aux-incidents-un-plan-en-6-etapes/.

[26] European Network and information Security Agency (ENISA), « guide de création d'un csirt pas à pas » ,pp. 6-31, 2006, disponible sur https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-french/at_download/fullReport

[27] Equipe CSIRT ELIT, « Etude des CERTs », Projet : Etude, Conception et Mise en œuvre du CSIRT SONELGAZ, pp. 4-14, 2017.

[28] Equipe CSIRT ELIT, « Présentation CSIRT du Groupe Sonelgaz », pp. 4-20, 2017

[29] Elit, « Qui sommes-nous ? », consulter le 21/07/2020 sur https://www.elit.dz/639/qui-sommes-nous

[30] Elit, « Centre d'alerte et de réaction aux incidents de sécurité "CSIRT Sonelgaz"

», consulter le 31/06/2020 sur https://www.elit.dz/682/centre-dalerte-et-de-reaction-aux-incidents-de-securite

[31] Network Associates International BV. Gatwickstraat Amsterdam, « Introduction à la cryptographie », livre, pp. 2.

[32] Renaud.D, « Cryptographie Et Sécurité informatique », Livre, Université de Liège, pp. 8-91, 2010.

[33] Rezkallah.l , « de la cryptographie classique a la cryptographie moderne théorie et application “, mémoire de magister en mathématiques, université houari Boumediene, pp. 11, 2007, disponible sur http://repository.usthb.dz/bitstream/handle/123456789/3526/TH4946.pdf?sequence=3&isAllowed=y

[34] communauté d’assistance et de conseil high-tech, « Cryptographie - Chiffrement par substitution », consulter le 23/06/2020 sur https://web.maths.unsw.edu.au/~lafaye/CCM/crypto/simple.htm

[35] Pillou.J.F**,** « Le chiffrement par substitution **»,** consulter le 30/06/2020 sur https://www.commentcamarche.net/contents/213-chiffrement-par-substitution

[36] Raphael.Y, « **sécurité** informatique et crypto3 », livre, Congo-Kinshasa. 2018. cel-01965300, pp.99, 25 Dec 2018.

[37] Binance, « Cryptage symétrique vs. Cryptage asymétrique », consulter le 2020 sur https://academy.binance.com/fr/security/symmetric-vs-asymmetric-encryption

[38] Binance, « Qu'est-ce que la cryptographie à clé publique ? », consulter le 2020 sur https://academy.binance.com/fr/security/what-is-public-key-cryptography

[39] Boutora.M, Ben ami.D, « Conception, Etude et Réalisation d’un Crypto système Hybride de Transmission d’Images. », Mémoire de master Génie électrique, université mouloud Mammeri de Tizi-Ouzou, pp.46, 2015.

[40] P. Navez, G. Van Assche, “Une transmission sécurisée : la cryptographie quantique”, Article, Université Libre de Bruxelles, pp.1, Avril 2002.

[41] Haroche.S, “Les algorithmes quantiques”, Chaire de Physique quantique, Article, 26 Février 2002 disponible sur https://www.college-de-france.fr/media/serge-haroche/UPL55031_SHaroche_260202.pdf

[42] Hassan.N. « Conception et simulation des générateurs, crypto-systèmes et fonctions de hachage basés chaos performants **»**, Thèse de Doctorat Electronique, Université Nantes Angers Le Mans, pp. 11. 2012.

[43] Bir.M.A, Dahmouni.L, « Etude et implémentation d’algorithmes de chiffrement à clé secrète et à clé publique : Application au cryptage de la parole **»**, mémoire de master automatique, Université Mouloud Mammeri De Tizi-Ouzou, pp. 31, 2018, disponible sur https://dl.ummto.dz/bitstream/handle/ummto/7749/BirMohandAmokrane_DahmouniLyes.pdf?sequence=1

[44] Gonzales.L, “Chiffrement symétrique”, consulter le 16/06/2020 sur https://blog.devensys.com/chiffrement-symetrique/

[45] Youssou.F, « Algorithmes d’authentification et de cryptographie efficaces pour les réseaux de capteurs sans fil », Livre, Université de Franche-Comté, 2014. Français disponible sur https://tel.archives-ouvertes.fr/tel-01127167/document

[46] Metec.A, “Modes de chiffrement symétrique”, article, pp. 1-25, disponible sur https://fr.scribd.com/user/270518182/AliXmetec

[47] Marion.D, Marie-Lise.F, Bruno.R. « L’auto-test d’un cœur de chiffrement AES », Article, JNRDM’08 : Journées Nationales du Réseau Doctoral en Microélectronique, May 2008, France. pp.4.

[48] John.K, Bruce.S,David.W, « Mod n Cryptanalysis, with Applications Against RC5P and M6», livre, pp. 17, disponible sur https://www.schneier.com/academic/paperfiles/paper-mod3.pdf

[49] Piotrowski. J.N, « Qu’est-ce qu’un plan de réponse aux incidents de sécurité informatique ? », consulter le 02/02/2020 sur http://globbsecurity.fr/quest-ce-quun-plan-reponse-aux-incidents-securite-informatique-44333/

[50] « Qu’est-ce qu’un SOC », consulter le 02/09/2020 sur https://www.oracle.com/fr/cloud/soc-security-operations-center.html

[51] Hommet,J, « Connexion SSH par clés sur Windows vers Linux », consulter le 04/09/2020 sur https://computerz.solutions/authent-cle-ssh/

[52] Badr.D, « Qu'est-ce que l'algorithme Blowfish ? » consulter le 26/06/2020 sur https://ripfd.blogspot.com/2016/04/quest-ce-que-lalgorithme-blowfish.html.

[53] Neveu.L, « Towfish », consulter le 26/06/2020 sur https://www.futura-sciences.com/tech/definitions/tech-twofish-1827/

[54] Y. Challal, « ICP/PKI : Infrastructures à Clés Publiques », Article, Université de Technologie de Compiègne Heudiasyc, pp. 7-10, 2009.

[55] Doucene.W, « Infrastructures à Clés Publiques Basées sur la Technologie Blockchain », mémoire de master informatique, université Mohamed Boudiaf - m’sila, pp. 11-15, 2019.

[56] AZMI.S, « Gestion de certificat PKI », consulter le 13/06/2020 sur https://www.cert-devoteam.fr/tls-certificats-a-cle-publique-pki-33/.

[57] Mezhoud.k, Mokhtari.H, « Infrastructure de gestion de clés publiques avec EJBCA », mémoire de master informatique, Université A. MIRA, pp. 24,2012.

[58] Saidou.D, “une infrastructure à clés publiques (pki) pour sécuriser les messages dans un réseau v2g“, mémoire présenter à l'université du québec, pp. 10-11, Mars 2018.

[59] CCM.Benchmark, “Les certificats”, consulter le 20/07/2020 sur

https://www.commentcamarche.net/contents/198-les-certificats.

[60] Pasini.S, « Pourquoi les versions théoriques d’ElGamal et de RSA ne sont pas sûres ? », Article, école polytechnique fédérale de lausanne, pp. 6, Mars 2005.

[61] Bayart.F « Chiffrer à l'aide des courbes elliptiques », consulter le 20/07/2020 sur http://www.bibmath.net/crypto/index.php? Ek.

[62] Nitulescu.A, « Crypto systèmes : Sécurité et attaques », Article, Université Paris 13 Villetaneuse, pp. 27, 08/02/2016 disponible sur https://www.di.ens.fr/~nitulesc/files/CRYPTO13/cours6.pdf?

[63] Gherbi.N, Saadi.N, « Cryptage et décryptage d'une image fixe par l'algorithme AES avec une cleff de 128 bits », mémoire de licence Aéronautique, Université Saad Dahleb Blida, pp. 33-34, 2009.

[64] Didier.M, "PGP (Pretty Good Privacy)", consulter le 25/08/2020 sur https://www.apprendre-en-ligne.net/crypto/moderne/pgp.html?

[65] Ali-Pacha.A, Hadj-Said.N, B. Belmekki, Belgoraf.A, « Systèmes Cryptographiques à clef Mixte: PGP », Article, 3rd International Conference: Sciences of Electronic TUNISIA, pp. 2, 2005.

[66] Mickael Rigonnaux, « GnuPG – Introduction & Cheat-Sheet », consulter le 22/08/2020 sur https://net-security.fr/security/gnupg-introduction-cheat-sheet/

[67] Jonathan.B, Adrien.G, « techniques de cryptographie », Article, Licence Informatique, pp. 17, 20040

[68] Synetis.A, « Notion de cryptologie », consulter le 15/08/2020 sur https://www.synetis.com/notion-de-cryptologie-et-algorithme-de-chiffrement/

[69] Doulcier.M, "Test Integre De Circuits Cryptographiques. Micro et nanotechnologies/Microélectronique », Article, Université Montpellier II - Sciences et Techniques du Languedoc, pp. 15-17, 2008.

[70] Betka.I, "Etude et Implémentation Pipeline sur FPGA de L'algorithme de Chiffrement AES", mémoire master électronique, Université Mohamed Boudiaf - M'sila, pp. 15, 2018.

[71] Fouque.P.A, Equipe de Cryptographie, « Algorithmes de chiffrement symétrique par bloc (DES et AES) », Ecole normale supérieure, pp. 49-57.

[72] Grenier.C, « Techniques de cryptanalyse de RSA », Article, pp. 4, 28 janvier 2009.

[73] Destree.L, Marchal.M, « Mini-RSA, programme d'initiation au chiffrement RSA », Article, pp. 4-5.

[74] Pierre.G, « UML Cours 5 : Diagramme de séquences », consulter le 28/08/2020 sur https://lipn.univ-paris13.fr/~gerard/uml-s2/uml-cours05.html

[75] « OpenSSL », consulter le 04/09/2020 sur http://www.open-source-guide.com/Solutions/Developpement-et-couches-intermediaires/Pki/Openssl

[76] Nicolas.C, « Un CSIRT, à quoi ça CERT ? », consulter le 20/07/2020 sur https://www.cyber-securite.fr/2013/12/13/un-csirt-a-quoi-ca-cert/.

[77] Microsoft, « Créer un diagramme de cas d'utilisation UML », consulter le 20/08/2020 sur https://support.microsoft.com/fr-fr/office/cr%c3%a9er-un-diagramme-de-cas-d-utilisation-uml-92cc948d-fc74-466c-9457-e82d62ee1298?ui=fr-fr&rs=fr-fr&ad=fr.

[78] cryptosec, « Les PKI », consulter le 10 mai 2004 sur https://www.cryptosec.org/?Les-PKI.

[79] Hat.R, « Protocole SSH », consulter le 09/08/2020 sur http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-fr-4/ch-ssh.html

[80] Jean-François. P, « SSH - Protocole Secure Shell », consulter le mardi 19 mai 2015 à 12 :55 sur https://www.commentcamarche.net/contents/214-ssh-protocole-secure-shell.

[81] Pear, « Package Information : Crypt_RSA », consulter le 04/09/2020 sur https://pear.php.net/package/Crypt_RSA

[82] Openssl, **«** Open SSL cryptography and SSL/TLS Toolkit », consulter le 04/09/2020 sur https://www.openssl.org/

[83] **«** OpenSSL », consulter le 15/08/2020 sur https://fr.wikipedia.org/

[84] l'équipe force plus, « Qu'est-ce qu'un Help Desk ? », consulter le 28/08/2020 sur https://www.forceplus.com/quest-ce-qu-un-help-desk

[85] S. LAZAAR, « Algorithme RC4 et tests de sécurité », Livre, Université Abdelmalek Essaadi-ENSA de Tanger, Maroc, pp. 11-7, disponible sur https://lazaarsaiida.files.wordpress.com/2015/11/algorithme-rc4-slazaar2015.pdf

[86] Ron.R, « RC5 (chiffrement) », consulter le 01/09/2020 sur https://fracademic.com/dic.nsf/frwiki/1400001

[87] « Quels sont les inconvénients de PGP Encryption ? », consulter le 04/09/2020 sur https://www.saloninnovationsinc.com/Vgr1V19O/

[88] Razny.I, « GnuPG », consulter le 04/09/2020 sur https://www.generation-nt.com/reponses/gnupg-winpt-entraide-7340.html

[89] Sebastien.F, « Protocole SSL et TLS », consulter le 01/09/2020 sur https://www.frameip.com/ssl-tls/#5-8211faiblesses-et-attaques-envisageables

[90] Akshhay.S, « Public Key Cryptography/RSA Algorithm Example », consulter le 01/09/2020 sur https://www.gatevidyalay.com/public-key-cryptography-rsa-algorithm/

[91] Ferradi.H, « Chiffrement par Bloc : Cryptanalyse Linéaire/Différentielle », Article, École normale supérieure dispense à Paris, pp 1-28 ,2016, disponible sur https://www.di.ens.fr/~ferradi/Cryptanalyse.pdf

[92] Jamie,N, « OpenSSL Certificate Authority », consulter le 04/09/2020 sur https://jamielinux.com/docs/openssl-certificate-authority/create-the-root-pair.html

[93] Inzen.S, « SSH Configuration in Kali Linux », consulter le 04/09/2020 sur https://medium.com/@InzenSecure/ssh-configuration-in-kali-linux-3f7c456560a9

[94] Hachoum.I, « Processus de développement en Y (Processus 2TUP) », consulter le 24/09/2020 sur https://imilsoftware.blogspot.com/2017/01/processus-de-developpement-en-y.html