République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université A. MIRA de Béjaia
Faculté des Sciences Exactes
Département de Recherche Opérationnelle

Mémoire de fin de cycle
en vue de l'obtention du diplôme de Master
en Mathématiques appliquées
Option : Modélisation mathématique et évaluation des performances des réseaux

Thème :

Quelques aspects de la sécurité informatique : Cas du commerce électronique

Présenté par :

AITBOUZID Naima
IOUKNANE Soraya

Soutenu devant le jury composé de :

BENOUARET Zina	Université de Béjaia	Présidente
BOULFEKHAR Samra	Université de Béjaia	Examinatrice
ZIANE Yasmina	Université de Béjaia	Examinatrice
DJABRI Rabah	Université de Béjaia	Promoteur

Juillet 2022

Table des matières

Introduction générale **6**

1 Premières notions de la sécurité informatique **8**
1.1 Généralités sur la sécurité informatique 8
1.1.1 Définition de la sécurité informatique (SI) 8
1.1.2 Services fondamentaux de la sécurité 9
1.2 Attaques informatiques 10
1.2.1 Types attaques 10
1.2.2 Techniques d'attaques 12
1.2.3 Logiciels malveillants 12
1.3 Gestion des risques de la sécurité informatique 13
1.3.1 Types des risques 14
1.3.2 Traitements des risques 15
1.4 Normes de sécurité 16
1.5 Système de management de la sécurité de l'information (SMSI) 17

2 E-commerce **19**
2.1 E-commerce 19
2.1.1 Comparaison entre le commerce traditionnel et l'e-commerce 20
2.1.2 Différents types d'échange du commerce électronique . 20
2.1.3 Différents modes de paiement électronique 21
2.2 Mécanismes du e-commerce 22
2.3 Attaques et risques dans l'e-commerce 23
2.4 Statistiques 24
2.5 Réglementation algérienne sur le commerce électronique 26

3 Cryptographie **29**
3.1 Cryptographie . . . 29
3.1.1 Cryptanalyse . . . 30
3.1.2 Cryptologie . . . 30
3.1.3 Chiffrement . . . 30
3.1.4 Déchiffrement . . . 31
3.1.5 Crpyptosystème . . . 31
3.2 Cryptographie classique . . . 32
3.2.1 Chiffrement par substitution . . . 32
3.2.2 Chiffrement par permutation . . . 33
3.3 Cryptographie moderne . . . 33
3.3.1 Cryptographie symétrique . . . 34
3.3.2 Cryptographie asymétrique . . . 35
3.4 Primitives cryptographiques . . . 36
3.4.1 Fonctions à sens unique . . . 36
3.4.2 Fonctions de hachage . . . 36
3.4.3 Signature numérique . . . 37
3.4.4 Génération de nombres aléatoires . . . 37
3.5 Objectifs de la cryptographie . . . 38
3.6 Attaques sur les Systèmes cryptographiques . . . 38
3.7 Quel cryptosystèmes choisir ? . . . 39
3.8 Protocoles de sécurité SSL/TLS . . . 40
3.8.1 Définition . . . 40
3.8.2 Principe de fonctionnement . . . 41
3.8.3 Service de sécurité du protocole SSL . . . 41

4 Cryptosystème RSA **43**
4.1 Description de RSA . . . 44
4.1.1 Génération des clés . . . 44
4.1.2 Chiffrement et déchiffrement des messages . . . 44
4.1.3 Signature RSA . . . 45
4.2 Algorithme RSA . . . 45
4.3 Déroulement de RSA avec exemple . . . 47
4.4 Démonstration mathématique . . . 50
4.4.1 Outils mathématiques utilisés . . . 50
4.4.2 Démonstration . . . 50
4.5 Attaques mathématiques sur RSA . . . 51
4.6 Efficacité de RSA . . . 52

Conclusion et perspectives **54**

5 Annexe 1 **56**
5.1 Résumé des principales normes de sécurité de l'information . . 56
5.2 Arithmétique 58
5.2.1 Algorithme d'Euclide 58
5.2.2 Algorithme d'Euclide étendu 59

Table des figures

1.1 Attaque directe 11
1.2 Attaque indirecte 11
1.3 Logiciels malveillants 13
1.4 Représentation du risque 14
1.5 Roue de Deming (PDCA) 17

2.1 Sites de vente en ligne les plus visités dans le monde en 2020. . 25
2.2 Top 10 des pays par chiffre de vente e-commerce 2020/2021. . 26

3.1 Principe de la cryptographie 30
3.2 Cryptosystème 31
3.3 Système de chiffrement 32
3.4 Cryptographie symétrique 34
3.5 Cryptographie asymétrique 35

Liste des tableaux

2.2 Comparaison entre le commerce traditionnel et l'e-commerce . 20
2.4 Différents types d'échange du commerce électronique 21

5.2 Résumé des principales normes de sécurité de l'information . . 57

Introduction générale

Au cours de ces dernières années, les technologies de l'information ont complètement révolutionné notre société et ont même envahi notre vie privée. C'est une raison suffisante pour affirmer que la sécurité du système d'information est devenu le défi du siècle pour le monde.

Le besoin d'être en mesure d'envoyer un message de façon sécurisée préoccupe l'homme depuis le début de la civilisation. D'un point de vue historique, c'est lors des conflits entre nations que ce besoin a été le plus vif.

Le commerce électronique ne cesse de se développer dans le monde entier et cela grâce aux systèmes de sécurité attribués aux sites de ventes qui protège la vie privée des clients et les données sensibles des vendeurs. c'est l'une des disciplines qui prend appui sur la sécurité informatique. C'est un processus d'achat, de vente ou d'échange de biens et de services par l'intermédiaire d'un réseau de communication tel que l'Internet.

La cryptologie est aujourd'hui au coeur du développement des nouvelles technologies de l'information et de la communication. En effet, dans notre vie quotidienne, le nombre d'activités où l'utilisateur demande une forte sécurité est en pleine croissance notamment dans le domaine du commerce électronique. La principale contrainte de sécurité est la confidentialité de données sensibles telles que les transactions monétaire électroniques. Le but est de garantir que les données protégées ne soient lisibles que par les personnes autorisées, pour toute autre personne, elles doivent demeurer inaccessibles ou inintelligibles. Ce besoin d'échange de données confidentielles entre deux entités pose le problème de l'authenticité des données ou de leur provenance réelle.

La cryptographie reste encore le moyen le plus sérieux d'assurer la sécurité des correspondances et de transactions électroniques. Étroitement liée à l'effort de guerre, elle n'a pas cessé de se développer depuis ses origines antiques. Elle a connu une rapide évolution à notre époque. Du fait de deux domaines

essentiels : mathématiques et l'informatique, de plus le développement des moyens de télécommunication, qui ont eu pour effet de multiplier les activités où intervient la cryptographie.

Dans ce mémoire, on a partagé le travail en quatre chapitres :

Le premier résume les notions de base de la sécurité informatique, ensuite, on enchaine avec le deuxième sur le e-commerce en général et en Algérie en particulier.

Le troisième chapitre porte essentiellement sur les notions de la cryptographie classique et moderne.

On fini notre travail par le quatrième chapitre où on étudie le cryptosystème RSA.

Chapitre 1

Premières notions de la sécurité informatique

Introduction

Avec le développement de l'utilisation d'Internet, de plus en plus d'entreprises ouvrent leur système d'information à leurs partenaires ou leurs fournisseurs, il est donc essentiel de connaître les ressources de l'entreprise à protéger et de maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information. Il en va de même lors de l'ouverture de l'accès de l'entreprise sur internet.

Dans ce chapitre, on va définir en première partie les concepts fondamentaux de la sécurité informatique, ensuite, on définit les attaques et les risques liés à la sécurité informatique, après on va citer quelques normes de sécurité, et on termine par une conclusion.

1.1 Généralités sur la sécurité informatique

1.1.1 Définition de la sécurité informatique (SI)

La sécurité informatique est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, rétablir, et garantir la sécurité des systèmes informatiques. Elle est in-

trinsèquement liée à la sécurité de l'information et des systèmes d'information.

La sécurité est l'ensemble des mesures permettant d'assurer la protection des biens [1].

1.1.2 Services fondamentaux de la sécurité

Il est important d'identifier les exigences fondamentales en sécurité informatique, qui caractérisent ce à quoi s'attendent les utilisateurs de systèmes informatiques au regard de la sécurité :

L'intégrité

Il faut garantir à chaque instant que les données qui circulent sont bien celles que l'on croit, qu'il n'y a pas eu d'altération (volontaire ou non) au cours de la communication. L'intégrité des données doit valider l'intégralité des données, leur précision, l'authenticité et la validité.

La confidentialité

Seules les personnes autorisées ont accès aux informations qui leur sont destinées. Tout accès indésirable doit être empêché, les données doivent être cryptées, seuls les acteurs de la transaction possèdent la clé de compréhension.

La disponibilité

Le système doit fonctionner sans faille durant les phases d'utilisation prévues, garantir l'accès aux services et ressources installées avec le temps de réponse attendu.

La disponibilité d'un équipement se mesure en divisant la durée durant laquelle cet équipement est opérationnel par la durée durant laquelle il aurait dû être opérationnel.

La non-répudiation et l'imputation

Aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées, et aucun autre ne doit pouvoir s'attribuer les actions d'un autre utilisateur.

La non-répudiation de l'origine et de la réception des données prouve que les données ont bien été reçues. Cela se fait par le biais de certificats numériques grâce à une clé privée.

L'authentification

L'identification des utilisateurs est fondamentale pour gérer les accès aux espaces de travail pertinents et maintenir la confiance dans les relations d'échange.

La traçabilité

Cette notion c'est l'assurance que les éléments considérés sont tracés et que ces traces sont conservées pour leur exploitation par les personnes autorisées.

1.2 Attaques informatiques

Par définition, une attaque est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système et généralement préjudiciables.

Les motivations des attaques sont de différentes sortes [2] :

— obtenir un accès au système ;
— voler des informations, tels que des secrets industriels ou des propriétés intellectuelles ;
— glaner des informations personnelles sur un utilisateur ;
— récupérer des données bancaires ;
— s'informer sur l'organisation (entreprise de l'utilisateur, etc.) ;
— troubler le bon fonctionnement d'un service ;
— utiliser le système de l'utilisateur comme *rebond* pour une attaque ;
— utiliser les ressources du système de l'utilisateur, notamment lorsque le réseau sur lequel il est situé possède une bande passante élevée.

1.2.1 Types attaques

Il existe de nombreuses familles d'attaques dans le réseau Internet.

— **Attaques directes**

C'est une attaque très simple, le hacker attaque directement sa victime à partir de son ordinateur.
En effet, les programmes de hacker qu'ils utilisent ne sont que faiblement paramétrables, et un grand nombre de ces logiciels envoie directement les packets à la victime.

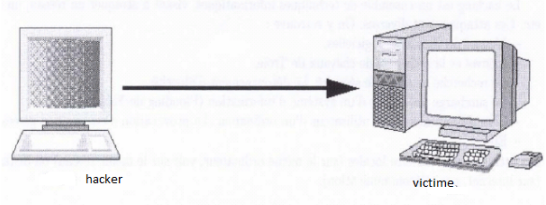

FIGURE 1.1 – Attaque directe

— **Les attaques indirectes par rebond**

Lors d'une attaque, le pirate garde toujours à l'esprit le risque de se faire repérer, c'est la raison pour laquelle les pirates privilégient habituellement les attaques par rebond (par opposition aux attaques directes), consistant à attaquer une machine par l'intermédiaire d'une autre machine, afin de masquer les traces permettant de remonter à lui (telle que son adresse IP) et dans le but d'utiliser les ressources de la machine servant de rebond.

Cela montre l'intérêt de protéger son réseau ou son ordinateur personnel, il est possible de se retrouver *complice* d'une attaque et en cas de plainte de la victime, la première personne interrogée sera le propriétaire de la machine ayant servi de rebond.

FIGURE 1.2 – Attaque indirecte

1.2.2 Techniques d'attaques

Lors de la connexion à un système informatique, celui-ci demande la plupart du temps un identifiant (en anglais login ou username) et un mot de passe (en anglais password) pour y accéder. Ce couple identifiant/mot de passe forme ainsi la clé permettant d'obtenir un accès au système.

On peut citer donc plusieurs attaques dans ce sens :

1. Attaque par force brute (brute force cracking) : le cassage d'un mot de passe en testant tous les mots de passe possibles.
2. Attaque par dictionnaire : est une méthode utilisée pour pénétrer par effraction dans un ordinateur ou un serveur protégé par un mot de passe, en essayant systématiquement tous les mots d'un dictionnaire donné.
3. Attaque hybride : Il s'agit d'une combinaison d'attaque par force brute et d'attaque par dictionnaire. utilisée principalement pour les mots de passe composés par un mot suivi d'un chiffre ou d'une lettre.

1.2.3 Logiciels malveillants

Un logiciel malveillant ou maliciel, aussi dénommé logiciel nuisible ou programme malveillant ou pourriciel (*malware* en anglais), est un programme développé dans le but de nuire à un système informatique, sans le consentement de l'utilisateur dont l'ordinateur est infecté.
En effet, les maliciels englobent les virus, les vers, les chevaux de Troie, ainsi que d'autres menaces[7].

Les logiciels malveillants peuvent être classés en fonction des trois mécanismes suivants :

— **Mécanisme de propagation**
Par exemple, un ver se propage sur un réseau informatique en exploitant une faille applicative ou humaine.
— **Mécanisme de déclenchement**
Par exemple, la bombe logique comme la bombe logique surnommée vendredi 13 se déclenche lorsqu'un évènement survient
— **Charge utile**
Par exemple, le virus Tchernobyl tente de supprimer des parties importantes du BIOS, ce qui bloque le démarrage de l'ordinateur infecté

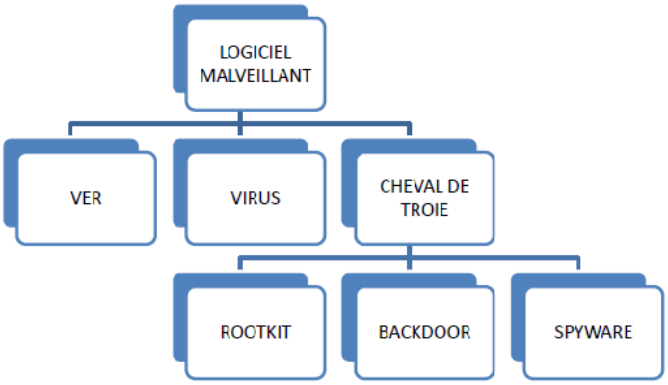

FIGURE 1.3 – Logiciels malveillants

1.3 Gestion des risques de la sécurité informatique

Les coûts d'un problème informatique peuvent être élevés ainsi que ceux de la sécurité. Il est nécessaire de réaliser une analyse de risque en prenant soin d'identifier les problèmes potentiels avec les solutions avec les coûts associés. L'ensemble des solutions retenues doit être organisé sous forme d'une politique de sécurité cohérente, fonction du niveau de tolérance au risque [7]. Le risque peut être quantifié en tenant compte des trois éléments : la menace, la vulnérabilité et l'impact.

— **La menace :** est la cause potentielle d'incident, qui peut résulter en un dommage au système ou à l'organisation [8] , elle exploite une vulnérabilité pour déclencher un événement d'attaque entraînant un risque.
— **La vulnérabilité :** est une faiblesse du système.
— **L'impact :** est la conséquence directe ou indirecte de l'insatisfaction des besoins de sécurité sur l'organisme et/ou sur son environnement [9].

Alors les trois concepts cités peuvent modifier les critères de sécurité qu'on avait défini auparavant :

— **L'intégrité**
— **La confidentialité**
— **La disponibilité**
— **La traçabilité**

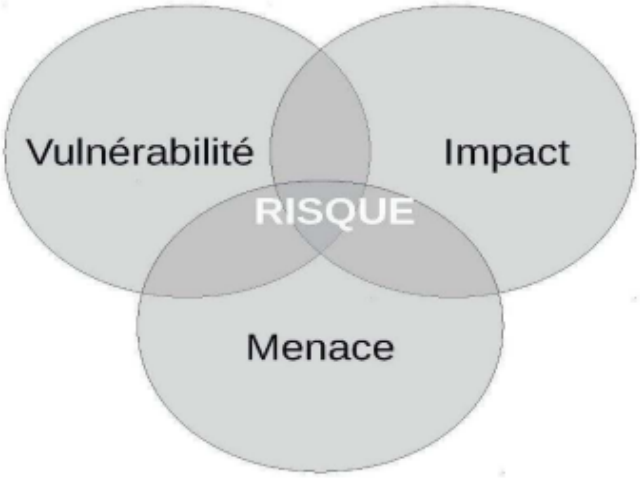

FIGURE 1.4 – Représentation du risque

La formule suivante représente le poids d'un risque [7]

$$Risque = \frac{Menace * Vulnérabilité}{Contremesure} \tag{1.1}$$

Où :

— **Risque :** C'est la probabilité qu'une menace exploite une vulnérabilité. Autrement dit, c'est une possibilité qu'un fait dommageable se produise.
— **Contre-mesure :** c'est un moyen permettant de réduire le risque dans une organisation.

On peut remarquer que :

— Le risque est d'autant plus réduit que les contre-mesures sont nombreuses
— Le risque est plus important si les vulnérabilités sont nombreuses.

1.3.1 Types des risques

En sécurité informatique, il existe deux types de risques : les risques humains et les risques matériels [7].

Risques Humains

Ils concernent les utilisateurs mais également les informaticiens eux mêmes. On peut citer :

— **Maladresse :** commettre des erreurs ou exécuter de traitement non souhaité, ou effacer involontairement de données ou des programmes ; etc.
— **L'inconscience et l'ignorance :** introduire des programmes malveillants sans le savoir (par exemple lors de la réception du courrier).
— **La malveillance :** Certains utilisateurs peuvent volontairement mettre en péril le système d'informations, en y introduisant en connaissance de cause de virus ou en introduisant volontairement des mauvaises informations dans une base des données. On parle même de la *cybercriminalité*.
— **L'ingénierie social :** une méthode pour obtenir d'une personne des informations confidentielles, en vue de les exploiter à d'autres fins.
— **L'espionnage :** emploie des moyens pour obtenir des informations sur des activités concurrentes, etc.

Risques matériels

Ils sont lies aux défauts et pannes inévitables que connaissent tous les systèmes matériels et logiciels. On peut citer :

— **Les incidents liés au matériel :** La plupart des composants électroniques modernes produits en grandes séries, peuvent comporter des défauts de fabrication.
— **Les incidents liés au logiciels :** Ce sont les plus fréquents. Les systèmes d'exploitation et les programmes sont de plus en plus complexes car ils font de plus en plus de choses. Ils nécessitent l'effort de plusieurs développeurs. Ces derniers peuvent faire des erreurs de manière individuelle ou collective que les meilleures méthodes de travail et les meilleurs outils de contrôle ou de test ne peuvent pas éliminer en totalité.
— **Les incidents liés à l'environnement** : Les machines électroniques, les réseaux de communication sont sensibles aux variations de températures ou de l'humidité ainsi qu'aux champs électromagnétiques. Dès lors, il est possible qu'un ordinateur tombe en panne.

1.3.2 Traitements des risques

Le traitement du risque est un processus de sélection et de mise en oeuvre des mesures de sécurité visant à modifier le risque. Il suffit :

Imposer des règles de sécurité adéquates

Ceci consiste en la définition de procédures internes à l'entreprise basées sur[7] :

— **Des règles administratives :** Suivre des standards de sécurité (normes ISO) ;
— **Des règles physiques :** Gardes, caméras, alarmes, verrous et Accès aux locaux sécurisés par biométrie.
— **Des règles techniques** : Utiliser la cryptographie pour le traitement et le stockage de l'information ; Mettre en place un firewall matériel et/ou logiciel, ...

1.4 Normes de sécurité

En règle générale, les normes sont des accords documentés et acceptés communément par des pays ou à l'échelle mondial. Ces accords internationaux sont essentiellement des spécifications précises destinées à une application répétitive et à une utilisation de façon systématique comme des lignes directrices,

La famille des normes internationales ainsi que les rapports techniques ISO 2700x sont dédiés, dans leur majorité, au domaine de la sécurité de l'information et du management des risques.

Le tableau de l'annexe 1 résume les principales normes de sécurité de l'information ou on peut distinguer quatre grands axe [10] :

— Normes avec vue générale et vocabulaire (ISO guide 73, ISO/CEI 27000)
— Normes qui proposent des exigences de sécurité de matière générale (ISO/CEI 15408, ISO/CEI 27001, ISO/CEI 27006)
— Normes qui proposent des orientations générales en matière de sécurité (ISO/CEI 27001 au 7, ISO/CEI 27013, ISO/CEI 27031,27035, ISO 31000)
— Normes destinées à des secteurs spécialisés (ISO/CEI 27011, ISO/CEI 27799)

Dans notre travail on va s'intéresser à la norme **ISO/IEC27001** qui nous permet de démontrer l'intégrité de nos données ainsi que l'engagement en matière de sécurité de l'information, elle peut aussi nous conduire à des opportunité commerciales surtout si on est considéré comme des clients soucieux de la sécurité.

La mise en œuvre des normes de cette famille par tout type d'organisation facilite le management de la sécurité d'actifs sensibles tels que les données financières, les documents de propriété intellectuelle, les données relatives au personnel ou les informations confiées par des tiers.

1.5 Système de management de la sécurité de l'information (SMSI)

Un système de management peut être interprété comme un ensemble de mesures organisationnelles et techniques ciblant un objectif.

Le fonctionnement du système de management se fait selon le modèle PDCA de l'anglais Plan, Do, Check, Act : en français planifier, faire, contrôler et corriger. Ces quatre phases sont illustrées dans la figure 4 ci-dessous :

FIGURE 1.5 – Roue de Deming (PDCA)

Avec :

1. **Plan :**
   Planifier et préparer le travail à effectuer. Établir les objectifs définir les tâches à exécuter. Spécifier les missions et les responsabilités. On n'oubliera surtout pas de préciser les critères de performance.
2. **Do :**
   Faire, réaliser, exécuter les tâches prévues.
3. **Check :**
   Vérifier les résultats, mesurer et comparer avec les prévisions.
4. **Plan :**
   Agir, corriger, prendre les décisions qui s'imposent.

Conclusion

Dans ce chapitre nous avons abordé essentiellement les premières notions de la sécurité informatique, qui seront des notions de base pour les chapitres à suivre.

Les chapitres suivants sur l'e-commerce, la cryptographie et le plus célèbre algorithme de chiffrement à clé publique, le RSA, sur lequel est basé notre travail.

Chapitre 2

E-commerce

Introduction

Le commerce électronique est une nouvelle façon de faire le commerce dans le monde.

Son principal avantage est sa capacité à servir tous les participants dans le monde entier sans restriction géographique ou présence physique.

Notre objectif dans ce chapitre est d'apporter une lumière sur cette nouvelle tendance du e-commerce en générale et surtout en Algérie.

2.1 E-commerce

Le commerce est un mécanisme qui permet à deux parties, le vendeur et le client, de mener des activités de vente, d'achat et/ou d'échange de produits (biens, services ou informations), sur la base de la théorie de l'offre et la demande.

L'arrivée d'Internet et son développement assez rapide, à mener l'apparition des entreprise en ligne. Dans ce contexte virtuel, les deux entités peuvent ne jamais se rencontrer et/ou reconnaître avoir effectué des transactions électroniques. Après l'achat, la livraison peut être physique ou électronique, tout dépend du bien ou du service acheté.

2.1.1 Comparaison entre le commerce traditionnel et l'e-commerce

Les transactions en ligne offrent de nombreux avantages que le commerce traditionnel ne permet pas, notamment la rapidité, la réduction importante du cycle de vente et la réduction des coûts.

Le tableau suivant nous illustre la différence entre le commerce traditionnel et l'e-commerce.

Le commerce traditionnel	**L'e-commerce**
Rencontre des acteurs sur un lieu physique : le marché	Lieu du commerce =marché virtuel
Rencontre physique entre les acheteurs et les vendeurs	Réalisation des transactions sans contact direct à travers des liens informatiques.
Paiement par monnaie dans la majorité des cas.	Règlement par transactions numérique de compte à compte.
Utilisation des liens postaux ou de transports de tout type, avec des contraintes de délai.	Livraison instantanée par télécommunications.

TABLE 2.2 – Comparaison entre le commerce traditionnel et l'e-commerce

2.1.2 Différents types d'échange du commerce électronique

Selon l'organisation mondiale du commerce, (OMC), les transactions de l'e-commerce peuvent avoir lieu entre les entreprises, les ménages, les individus, les gouvernements et autres organisations publiques ou privées.

Le tableau suivant met en avance les différentes transactions possibles entre les différents acteurs de l'e-commerce[19].

Acronyme	Nom	Description
B2B	Business to Business	Transactions entre les compagnies
B2C/ C2B	Business to Consumer/ Consumer to Businessx	Les entreprises effectuant des transactions et le consommateur final
C2C	Consumer to consumer	Transactions entre les consommateurs finaux.
G2C/C2G	Government to consumer/ consumer to government	Transactions entre le gouvernement et le consommateur final.
B2G/G2B	Business to government/ government to business	Transactions entre le gouvernement et les entreprises.
G2G	Government to Government	Transactions entre les services gouvernementaux.

TABLE 2.4 – Différents types d'échange du commerce électronique

2.1.3 Différents modes de paiement électronique

Dans le monde :

Le paiement en ligne est un échange d'argent réalisé à travers un système numérique.

Le paiement en ligne concerne au premier chef les transactions réalisées sur Internet ou via des réseaux de télécommunications, qu'elles soient engagées à partir d'un ordinateur ou d'un smartphone

— Les cartes bancaires : les cartes de crédit se présentent aujourd'hui comme le moyen le plus privilégié sur Internet pour tous les commerces à distance, plus de 85 % des acheteurs l'utilise. Elles sont les seuls à offrir des garanties de paiement aux commerçants du monde entier.

— Le portefeuille en ligne : Ce dernier est un système permettant de stocker de l'argent et d'effectuer des paiements, le tout sans même avoir de compte en banque. Cela est ainsi rendu possible grâce à des cartes prépayées

telles que Moneo ou Veritas. Les portes monnaie les plus connu et les plus utilisés dans le monde sont : Paypal, Paylib, Paybox, Olkypay,
— Le virement bancaire Le virement bancaire est très fréquemment utilisé lorsque la cible est une cliente le professionnel c'est-à-dire entre les entreprises (B to B). Le virement bancaire s'effectue suite à l'acceptation d'un devis.

En Algérie

Les différents moyens de paiements existant en Algérie pour effectuer l'achat en ligne : le mondât ccp, le paiement par chèque de banque, le paiement à la livraison (cash : le plus utilisé) et le paiement par portefeuille électronique en euro. En effet chaque mode a une spécificité par exemple le paiement par le mandat CCP s'effectue à la poste et dans toutes les postes algérienne,

La loi publiée dans le numéro 28 du journal officiel[6] énonce 2 modes de paiement : le paiement à distance (e-paiement) par carte(CIB ou edhahabia d'Algérie poste) ou à la livraison du produit (cash). Pour l'e-paiement, le texte exige que les plateformes de paiement soient exploitées exclusivement par les banques de la place ou Algérie poste et connectées aux terminaux de paiement via le réseau d'Algérie télécom, et pour la sécurité il est exigé des web marchands de connecter leurs sites web à une plateforme de paiement électronique sécurisée « par un système de certification électronique ».

2.2 Mécanismes du e-commerce

Une pratique efficace du commerce électronique suppose la mise sur pied d'un certain nombre de fonctionnalités :
— **Mécanismes de ventes :** On peut citer les bons de commande, les paniers d'achats ou de commande, les réservations, ...
— **Mécanismes d'achats :** L'application qui gère les achats est généralement stockée dans un serveur sécurisé [2] .
— **Mécanisme de paiement :** (cité en détail précédemment)
— **Mécanisme de sécurité :** Plusieurs protocoles sont mis a disposition de ce genre, on étudiera les détails dans les chapitres suivants.

— **Mécanisme de connexion :** La connexion est indispensable pour que l'environnement du e-commerce soit fonctionnel, les clients utilisent plusieurs moyens tels que les ordinateurs fixes et portables, les tablettes, les téléphones ..
— **Mécanisme de législation**

2.3 Attaques et risques dans l'e-commerce

Nous allons voir les questions liées à la sécurité au niveau du client, du vendeur et des deux parties prises simultanément, dans un contexte de commerce électronique.

Le client doit être rassuré, par exemple, que le site web commercial appartient bien à une compagnie légitime ; que la page web qu'il a devant lui n'a pas un contenu dangereux ; que le site web commercial ne va pas distribuer les informations qu'il s'engage à entrer à une tierce partie sans permission.

Le vendeur quant à lui doit s'assurer que le client n'a pas pour objectif d'accéder à son serveur pour modifier le contenu de ses pages et de son site web, de rendre simplement indisponible son serveur.

De manière générale, les sites web commerciaux sont exposés à divers types d'attaques.On distingue généralement [12] :

— Les attaques issues des failles liées aux systèmes d'exploitation, aux serveurs Web et de bases de données.
— Les attaques faites à travers le frontal (l'interface) du site de vente : le frontal peut révéler des bogues du système ou du logiciel ou même de mauvaises configurations.
— Les attaques de dénis de service distribuées ou DDoS (Distributed Deniat of Service) qui visent essentiellement la saturation de toute la bande passante du site Web du vendeur. Cette catégorie inclut aussi les attaques de saturation de la mémoire le malfaiteur envoie un gros volume de données au serveur pour occuper toute sa mémoire.
— Les attaques par des données non valides entrées généralement sur la ligne contenant l'URL (Uniform Resource Locator). Ces attaques exploitent d'éventuelles failles issues du développement des scripts CGI (Common Gateway Inteiface) ou ASP (Active Server Pages), en vue de l'obtention du code source du script considéré et/ou du fichier des mots de passe.

— Les attaques dites de l'oreille indiscrète, à travers un canal de communication entre deux ordinateurs connectés ou non à Internet.
— L'attaque Person-in-the-middle, dans laquelle une entité C s'interpose entre deux entités A et B lors d'une transaction électronique.
— L'ingénierie sociale est une technique qui consiste à obtenir un bien ou une information en exploitant la confiance.
— Les attaques par des maliciels : virus, vers, chevaux de Troie ect.

2.4 Statistiques

— **Au niveau mondiale :**

Le secteur du e-commerce connaît une croissance considérable depuis plusieurs années, notamment durant la crise sanitaire qui a marqué un tournant dans le développement du e-commerce en France comme dans le monde suite aux nouveaux modes de consommation. Les périodes de confinement national et la mise en place d'un couvre-feu ont fortement réduit les achats en canal de vente direct.

Sites de vente en ligne les plus visités dans le monde en 2020, par trafic mensuel moyen [18].

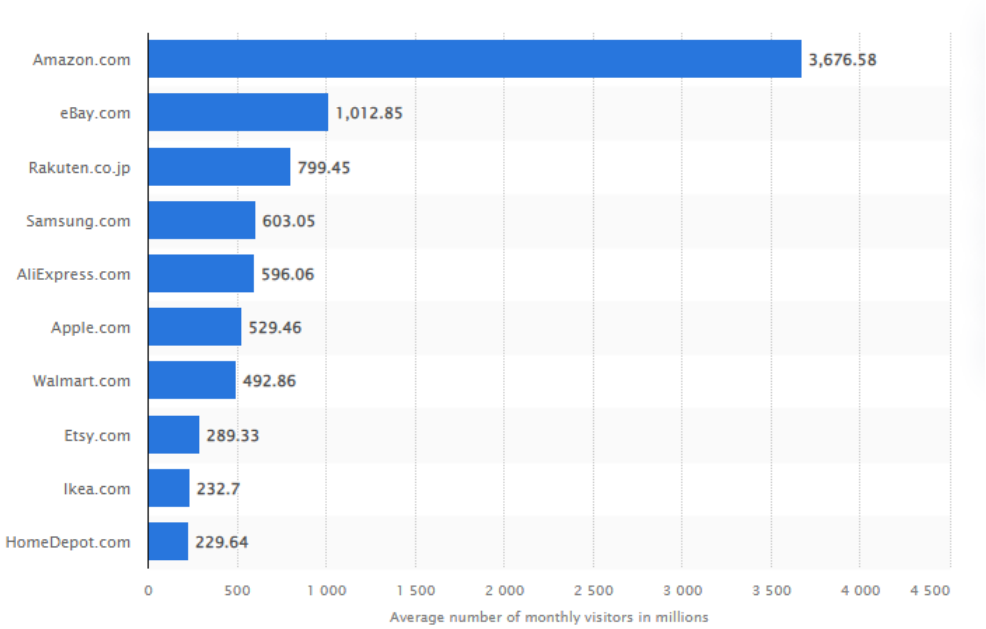

FIGURE 2.1 – Sites de vente en ligne les plus visités dans le monde en 2020.

Les plus gros marchés mondiaux e-commerce[18].

Ce tableau montre le classement des meilleurs pays dans le monde en termes de chiffre de vente réalisé en 2020/2021 dans le domaine du e-Commerce en milliards d'euro, et en pourcentage d'évolution.

Aujourd'hui, les chiffres ont bien évolué et les usages se modifient.

Les tendances du e-commerce global sont formelles : le mobile va devenir le levier principal pour les transactions sur Internet.

Top 10 des pays par chiffres de ventes ecommerce 2020 & 2021

en milliards et en % d'évolution

	2020	2021	% change
1. China*	$2,296.95	$2,779.31	21.0%
2. US	$794.50	$843.15	6.1%
3. UK	$180.39	$169.02	-6.3%
4. Japan	$141.26	$144.08	2.0%
5. South Korea	$110.60	$120.56	9.0%
6. Germany	$96.86	$101.51	4.8%
7. France	$73.80	$80.00	8.4%
8. India	$55.35	$67.53	22.0%
9. Canada	$39.22	$44.12	12.5%
10. Spain	$36.40	$37.12	2.0%

Note : incluant les produits et services commandés sur Internet, sans différenciation de moyen de paiement ; sont exclus : voyages, billetterie, paiements de factures, de taxes et les transferts d'argent, les services alimentaires et de boisson, les jeux d'argent et autres ; *excluant Hong Kong

Source : eMarketer, Décembre 2020

261835 eMarketer | InsiderIntelligence.com

Traduit de l'anglais par WiziShop

FIGURE 2.2 – Top 10 des pays par chiffre de vente e-commerce 2020/2021.

— **En Algérie :**
En 2019 l'Algérie occupe la 107e position sur 152 pays.
L'Algérie gagne 4 place par rapport a la 111e place occupait en 2018. Le chiffre d'affaire de l'e-commerce en Algérie ne peut être calculé du fait que le marché informel prend l'ampleur mais le chiffre d'affaire est en croissance du fait que le nombre de commande augmente d'une année à une autre selon Jumia Algérie.
Les sites de vente en ligne en Algérie se sont multipliés ces dernières années notamment depuis le lancement de la 3G en 2014 et la 4G en 2016 et par la promulgation d'un texte de loi encadrant ce marché.
Les leaders de l' e-commerce algérien : jumia.dz, Yassir, Batolis, Ouedknisse, Guiddini, et plusieurs d'autres.

2.5 Réglementation algérienne sur le commerce électronique

La loi qui fixe les règles générales du commerce électronique a vu le jour le 16 mai 2018. Elle est publiée dans le numéro 28 du journal officiel [6].

Cette loi a pour but l'organisation des opérations du commerce

électronique en Algérie et expliquer ses apparences après qu'elle a été sans loi pour l'organiser. Tous ceux qui souhaitent se lancer en e-Commerce en Algérie doivent donc prendre en considération cette loi qui porte principalement sur :

1. **Les produits**

   Dans les premiers articles, cette loi évoque les produits et les services interdits pour les ventes via l'e-Commerce, et cela d'une manière incontestable vu leur sensibilité et la nature de la société algérienne. Elles viennent donc comme suit :

   — Les jeux de hasard, paris et loteries ;
   — Les boissons alcoolisées et tabac ;
   — Les produits pharmaceutiques ;
   — Les produits portant atteinte aux droits de propriété intellectuelle, industrielle ou commerciale c'est-à-dire que je n'ai pas le droit de créer une boutique en ligne portant le nom d'une marque sauf avec leur autorisation ;
   — Tout bien ou service prohibé par la législation en vigueur c'est-à-dire que tous ce qui est interdit en commerce traditionnel et aussi interdit pour le commerce en ligne ou électronique ;
   — Tout bien ou service qui requiert un acte authentique.

   Les conditions de la pratique de l'e-Commerce sont très strictes et nécessitent plusieurs étapes pour obtenir la certification pour la pratique de cette activité officiellement.

2. **Les devoirs des e-fournisseurs**

   Suite a l'envoie du contrat électronique au client et de sa ratification, l'étape suivante est donc le fait que le e-fournisseur devient responsable sur l'arrivée de ses produits dans les délais précisés, c'est pour cela que la loi a mis en place des devoirs qui doivent être respectées.

   — Les spécifications détaillées des biens ou des services ;
   — Les conditions et modalités de livraison ;
   — Les conditions de garantie et de service après vente ;
   — Les conditions de résiliation du contrat électronique ;
   — Les conditions et modalités de paiement ;
   — Les conditions et modalités de retour de produit ;
   — Les modalités de traitement des réclamations ;
   — Les conditions et modalités particulières liées à la vente a essaie, le cas échéant ;

— La durée du contrat selon le cas.

3. **Le paiement électronique**

   Le paiement électronique est le frein majeur pour le développement du commerce électronique en Algérie. Jusqu'à présent on n'a pas mis en places les algorithmes nécessaires pour le paiement électronique, à l'exception d'une minorité des grandes sociétés.

   De plus, la plupart des sites web algériens restent non sécurisés.

Conclusion

Nous pouvons conclure que le commerce électronique n'est pas très développé en Algérie car pour le pratiquer il faut respecter certains paramètres pour assurer le bon fonctionnement des transactions en ligne.

La méfiance des consommateurs aux transactions sur internet par manque de sécurité, ce qui freine les opérations d'achats et de ventes sur internet.

Chapitre 3

Cryptographie

Introduction

L'origine de la cryptologie mot réside dans la Grèce antique. La cryptologie est un mot composé de deux éléments : *cryptos* , qui signifie caché et *logos* qui signifie mot.

La cryptologie est aussi vieille que l'écriture elle-même, et a été utilisé depuis des milliers d'années pour assurer les communications militaires et diplomatiques. par exemple, le célèbre empereur romain Jule César utilisait un algorithme de chiffrement pour protéger les messages à ses troupes. Dans le domaine de l'un de cryptologie peut voir deux visions : la cryptographie et la cryptanalyse, le cryptographe cherche des méthodes pour assurer la sûreté et la sécurité des conversations alors que le Cryptoanalyse tente de défaire le travail ancien en brisant ses systèmes.

3.1 Cryptographie

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

La cryptographie est l'art de chiffrer, coder les messages est devenue aujourd'hui une science à part entière. Au croisement des mathématiques, de

l'informatique, et parfois même de la physique, elle permet ce dont les civilisations ont besoin depuis qu'elles existent : le maintien du secret. Pour éviter une guerre, protéger un peuple, il est parfois nécessaire de cacher des choses.

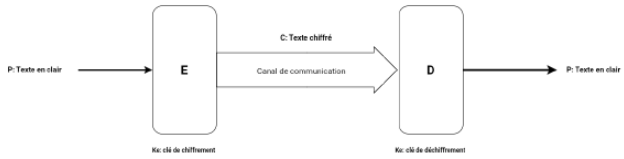

FIGURE 3.1 – Principe de la cryptographie

3.1.1 Cryptanalyse

La cryptanalyse, à l'inverse, est l'étude des procédés cryptographiques dans le but de trouver des faiblesses, en particulier, de pouvoir décrypter des messages chiffrés. Le décryptement est l'action consistant à trouver le message en clair sans connaître la clef de déchiffrement.

3.1.2 Cryptologie

Etymologiquement *la science du secret* , ne peut être vraiment considérée comme une science que depuis peu de temps. Cette science englobe la cryptographie (l'écriture secrète) et la cryptanalyse (l'analyse de la cryptographie).

3.1.3 Chiffrement

Le chiffrement est une méthode permettant d'assurer la confidentialité en rendant un message inintelligible afin de le transférer à un destinataire de telle sorte que s'il est intercepté il ne puisse être lu. Le destinataire possède, quant à lui, un moyen de retrouver le message originel.

Un exemple simple est le chiffrement de César où l'on décale simplement les lettres de l'alphabet, il suffit alors à l'interlocuteur de connaître le nombre de lettres à décaler pour retrouver le message originel. Le problème de cette méthode est qu'une personne interceptant le message et connaissant la méthode utilisée n'a que 25 décalages non triviaux à tester pour retrouver le message.

De nombreuses méthodes plus complexes ont vu le jour et à présent on considère qu'un attaquant doit faire face à au moins 2^{80} possibilités pour considérer le chiffrement comme sûr. Cette limite va certainement passer à 2^{100} à cause de l'augmentation des capacités calculatoires des ordinateurs.

3.1.4 Déchiffrement

Est le processus inverse du chiffrement, consiste à retrouver le texte original du message chiffré dont on possède la clé de déchiffrement.

3.1.5 Crpyptosystème

La cryptographie est l'ensemble des procédures qui permettent de transformer un message intelligible ou texte clair, en un texte chiffré incompréhensible ou cryptogramme, à travers des algorithmes préalablement convenus entre l'émetteur et le destinataire du message. Ces algorithmes sont au nombre de trois d'abord, l'algorithme de chiffrement, qui permet de transformer le texte en clair en un texte chiffré et, d'autre part, l'algorithme de déchiffrement, qui permet de retrouver le texte en clair à partir du texte chiffré. Par ailleurs, le chiffrement et le déchiffrement utilisent une information additionnelle appelée clé, produite par le biais de l'algorithme de génération de clé. Les trois algorithmes forment ce qu'on appelle système cryptographique ou cryptosystème.

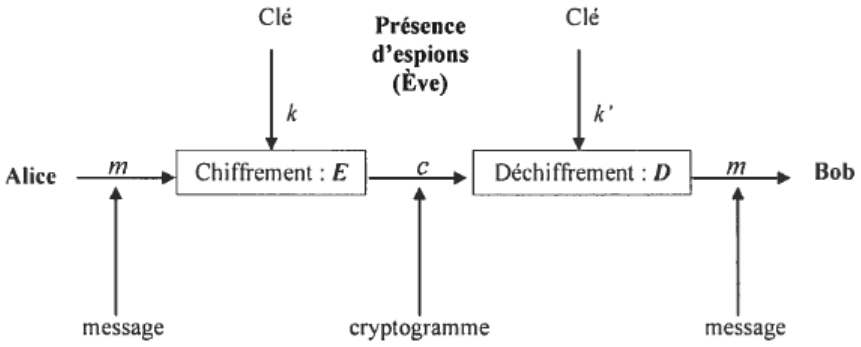

FIGURE 3.2 – Cryptosystème

De nombreuse méthodes de chiffrement différentes ont été imaginées pour se protéger depuis de nombreux siècles, on peut les classer comme suit :

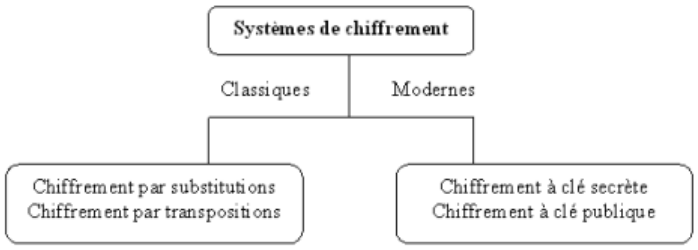

FIGURE 3.3 – Système de chiffrement

3.2 Cryptographie classique

La cryptographie classique repose sur deux principes essentiels, la substitution et la permutation : [14]

3.2.1 Chiffrement par substitution

Chaque symbole ou ensemble de symboles est remplacé par un autre symbole ou un ensemble de symboles pour obtenir le texte chiffré.

On distingue trois types de substitution qui sont :

Substitution mono-alphabétique

Elle consiste à remplacer chaque symbole du texte en clair, par un autre symbole pour obtenir le texte chiffré.

On peut citer :

— **Code de César** : consiste à décaler les lettres de l'alphabet d'un nombre K qui représente la clé.

Substitution polyalphabétiques

Elle consiste à utiliser une suite de chiffres mono-alphabétiques réutilisée périodiquement. Un même symbole peut être remplacé par plusieurs symboles.

On peut citer :

— **Chiffrement de Vigenère :** C'est un chiffrement symétrique de substitution poly-alphabétique et une amélioration du code de César, il utilise un mot de passe dont chaque lettre indique le décalage alphabétique à appliquer sur chaque lettre du texte en clair.

Substitution polygrammiques

Consiste à substituer un groupe de n symboles dans le texte en clair par un autre groupe de n symboles.

On peut citer :

— **Chiffrement de Hill :** le chiffrement consiste à :

- Remplacer chaque lettre par son ordre dans l'alphabet, $A = 0$, $B = 1$, ..., $Z = 25$. - Regrouper les nombres ainsi obtenus en bloc de m. - Pour chaque bloc de m nombres à coder, calculer le texte codé en effectuant des combinaisons linéaires avec une clé K de la forme d'une matrice carrée d'ordre m. - Le déchiffrement peut être effectué en utilisant la matrice inverse K^{-1} dans $Z26$.

3.2.2 Chiffrement par permutation

Le chiffrement par permutation se contente de changer l'ordre des lettres du message. C'est une technique dans laquelle le texte en clair est réécrit comme une séquence de lignes, puis réordonnée comme une séquence de colonnes. L'ordre des colonnes ainsi que leur nombre constitue la clé de cryptage. La position de chaque symbole du texte en clair est échangée ou permutée avec la position d'un autre symbole pour obtenir le texte chiffré.

3.3 Cryptographie moderne

La cryptographie moderne se divise en deux parties différentes : [19]

— **La cryptographie symétrique ou à clé privée** : elle utilise la meme clé pour le chiffrement et le déchiffrement.

— **La cryptographie asymétrique ou à clé publique** : elle utilise une clé publique pour le chiffrement et une clé privée pour le déchiffrement.

3.3.1 Cryptographie symétrique

Les algorithmes de la cryptographie symétrique (ou à clé privée) sont ceux pour lesquels l'émetteur et le destinataire partagent une même clé. L'emploi de ce genre d'algorithme lors d'une communication nécessite donc l'échange préalable de la clé entre les deux interlocuteurs à travers un canal sécurisé ou au moyen d'autres techniques cryptographiques. L'avantage principal de ce mode de chiffrement est sa rapidité. Cependant un paramètre essentiel pour la sécurité d'un système à clé privée est la taille de la clé. En effet, il est possible de retrouver la clé en menant une attaque dite l'attaque exhaustive, cette attaque consiste simplement à énumérer toutes les clés possibles du système et à essayer d'utiliser chacune d'entre elles pour décrypter un message chiffré. Si la taille de la clé est de k bits, le nombre de tentatives d'attaque exhaustive en vue de décrypter le message chiffré est égal à 2^k. Donc, pour pénaliser une telle attaque, il faut que la taille de la clé soit suffisamment grande.

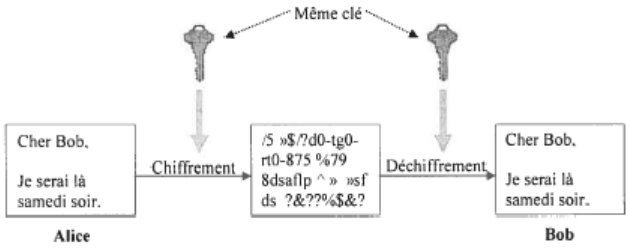

FIGURE 3.4 – Cryptographie symétrique

Il existe de nombreux systèmes symétriques. Ils se subdivisent en deux groupes selon qu'ils utilisent le chiffrement par blocs (block ciphers) ou le chiffrement par flots (stream ciphers).

Dans le chiffrement par blocs, le texte est découpé en blocs, puis chiffré bloc après bloc. Les principaux algorithmes de ce groupe sont :

— **DES** (Data Encryption Standard)

— **AES** (Advanced Encryption Standard)

Les chiffrements par flot (on parle aussi de chiffrements en continu) agissent directement sur chaque bit du texte, on chiffre un bit/caractère à la fois, la structure d'un chiffrement par flots repose sur un générateur de clé qui produit une séquence de clés. Le principal avantage des chiffrements par flot est qu'ils permettent de chiffrer et déchiffrer un message en continu, sans avoir besoin de connaitre tout le message. Ceci justifie leur utilisation dans

les domaines où il faut du chiffrement et du déchiffrement en temps réel et simultané (communications téléphoniques, Bluetooth, etc.)

3.3.2 Cryptographie asymétrique

La cryptographie symétrique ou le chiffrement à clé publique, a été présenté pour la première fois par Whitfield Diffie et Martin Hellman dans leur article en 1976, puis publié quelques mois plus tard sans pouvoir donner un exemple d'un système à clé publique. Il a fallu attendre 1978 où la version académique du premier cryptosystème à clé publique a fait apparition. Dans le chiffrement à clé publique chaque interlocuteur dispose d'un couple de clés, une clé publique connue par tous et une clé privée gardée secrète. L'émetteur chiffre le message en utilisant la clé publique du destinataire, et le destinataire déchiffre le message en utilisant sa clé privée qu'il est le seul à connaitre.

Les algorithmes à clé publique servent à chiffrer des messages, mais aussi à calculer des signatures numériques. Une signature numérique est une valeur qui dépend du message, considéré alors sous sa forme numérisée comme un nombre, et de l'identité du signataire, qui doit être le seul à pouvoir calculer cette signature. Un message signé est composé du message en clair et de cette signature numérique. Vérifier une signature consiste, en appliquant la fonction inverse de la signature, à retrouver le message en clair.

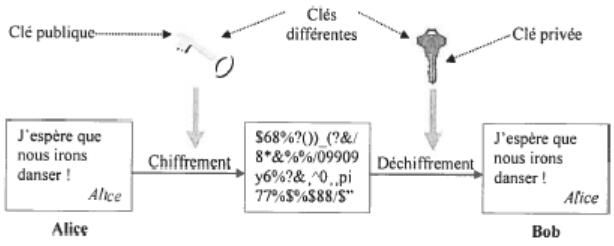

FIGURE 3.5 – Cryptographie asymétrique

Il existe de nos jours plusieurs systèmes de chiffrement asymétriques (**Rabin**, **ElGamal**, etc.), mais le plus utilisé est **RSA**.

— **Le Cryptosystème RSA** :

La sécurité du système RSA repose sur la difficulté présumée de factoriser un grand nombre, c'est-à-dire le décomposer en produit de nombres premiers.

L'opération relativement simple avec de petits nombres et particulièrement difficile avec des nombres de plus de 200 positions décimales. La clé privée dans RSA est fabriquée à partir de deux grands nombres premiers p et q alors que la clé publique ne révèle que leur produit $n = pq$.

C'est le système le plus utilisé dans les transactions en commerce électronique (Le cryptosystème **RSA** va etre présenté en détail dans le chapitre suivant) .

3.4 Primitives cryptographiques

De nombreuses primitives mathématiques jouent un rôle de premier plan dans la conception des solutions cryptographiques. Il s'agit notamment des fonctions à sens unique, des fonctions de hachage, des générateurs aléatoires et pseudo-aléatoires, etc.

3.4.1 Fonctions à sens unique

Les fonctions à sens unique sont des fonctions faciles à calculer dans un sens mais difficiles à calculer dans l'autre sens. Plus concrètement, si f est une fonction à sens unique, alors étant donné x, il est facile de calculer $y = f(x)$ mais, étant donné y, il est difficile de trouver x tel que $f(x) = y$.

Voici un exemple de fonctions conjecturées comme fonctions à sens unique :[4]

— Étant donné deux grands nombres premiers, p et q, on pense que la fonction $f(p.q) = pq$, est à sens unique car, s'il est facile de calculer $n = pq$, l'opération inverse consistant à trouver p et q à partir de n est plutôt difficile à effectuer.

3.4.2 Fonctions de hachage

C'est un algorithme symétrique par bloc. Il permet l'usage du chiffrement asymétrique sans engendrer trop de ralentissement, mais également d'assurer la provenance d'un fichier ainsi que son intégrité. Dans la majorité des cas, elles seront utilisées pour créer une signature numérique qui permet d'authentifier les expéditeurs.

On les utilise en cryptographie pour fournir un "condensé" ou "haché" ou encore "empreinte" de taille fixe. Un condensé est la caractéristique d'un

texte ou de données uniques dont l'objectif est d'être représentatif d'une donnée particulière et bien définie ce qui permet une détection simplifiée des changements dans un message.[16]

Les fonctions de hachage sont de la forme = $H(m)$ et possèdent de nombreuses propriétés :

– Il doit être facile de calculer = $H(m)$ pour n'importe quel message m.

– Elles produisent un résultat de longueur constante.

– Pour un donné, il est impossible de trouver x tel que $H(x) =$. On parle de propriété à sens unique.

– Pour un x donné, il est impossible de trouver y tel que $H(y) = H(x)$. Résistance faible de collision.

– Il est impossible de trouver x, y tels que $H(y) = H(x)$. Résistance forte de collision.

3.4.3 Signature numérique

Les signatures manuscrites ont été longtemps utilisées pour prouver l'identité de leur auteur ou du moins l'accord du signataire avec le contenu du document. Avec des documents numériques, les objectifs d'une signature sont les suivants [14] :

— Une signature est authentique. Elle convainc le destinataire que le signataire délibérément signé le document ;
— Une signature ne peut être falsifié (imitée). Elle est la preuve que le signataire a délibérément signé le document.
— Une signature n'est pas réutilisable. Elle fait partie du document et une personne mal intentionnée ne peut pas déplacer la signature sur un autre document ;
— Un document signé est inaltérable. Une fois le document signé, il ne peut plus être modifié ;
— Une signature ne peut pas être reniée. La signature et le document sont des objets physique et le signataire ne peut prétendre plus tard ne pas avoir signé le document.

3.4.4 Génération de nombres aléatoires

La génération de nombres aléatoires intervient dans la production des clés de sessions. Une clé de session peut être perçue comme un identifiant de la connexion d'un ordinateur “client” à un ordinateur “serveur”. La

génération de nombres aléatoires peut aussi être utile à la création des vecteurs d'initialisation d'un système crytographique (i1 s'agit d'un ensemble de données nécessaire au démarrage d'un processus ; si un générateur aléatoire n'est pas disponible, la valeur d'une horloge ou un simple compteur peut généralement faire l'affaire) , des secrets nécessaires à la production des signatures numériques, etc. Un générateur aléatoire est un dispositif capable de produire des nombres de façon aléatoire, imprévisible et non reproductible [17].

Les primitives ci-dessus sont généralement utilisées dans des cryptosystèmes tels que RSA (des noms de ses auteurs Rivest, Shamir et Adleman), AES (Advanced Encrvption Standard), PGP (Prett' GoodPrivacy), etc. Elles permettent aussi de développer des protocoles pour sécuriser les transactions électroniques, sujettes à divers risques et attaques.

3.5 Objectifs de la cryptographie

Le but fondamental de la cryptographie est de respecter les objectifs majeurs de la sécurité suivants [20] :

1. **Confidentialité :** Il s'agit de rendre la lecture du message intelligible à des tièrs non autorisés.
2. **Authentification :** Il s'agit de s'assurer que le correspondant connecté est bien le correspondant souhaité et de s'assurer de signataire de l'acte.
3. **Intégrité :** Il s'agit de s'assurer que le message n'a pas été modifié durant la transmission.
4. **Non répudiation :**l'expéditeur ne peut pas nier avoir envoyé le message.

3.6 Attaques sur les Systèmes cryptographiques

Différents types d'attaques peuvent être faits sur des systèmes cryptographiques [4],[20] :

— **Attaque à texte chiffré seulement :** l'adversaire essaie de trouver la clé ou les textes clairs à partir de l'observation de textes chiffrés dont les messages correspondants sont inconnus. L'adversaire suppose qu'une

même clé inconnue à été utilisée. Un système cryptographique vulnérable à cette attaque n'offre aucune sécurité.

— **Attaque à texte clair connu :** l'adversaire a des couples (texte clair, texte chiffré) à sa disposition et possiblement d'autres textes clairs. Son objectif est alors de trouver la clé secrète.
— **Attaque à texte clair choisi :** l'adversaire peut choisir un ou plusieurs textes clairs et obtenir les textes chiffrés correspondants, le but étant de retrouver la clé secrète.
— **Attaque dynamique à texte clair choisi :** il s'agit d'une attaque à texte clair choisi dans laquelle le choix du texte clair à une étape donnée peut dépendre des textes chiffrés reçus lors des étapes précédentes.
— **Attaque à texte chiffré choisi :** l'adversaire choisit un ou plusieurs textes chiffrés et obtient les textes clairs correspondants. L'objectif de cette attaque est de trouver la clé.
— **Attaque dynamique à texte chiffré choisi :** il s'agit d'une attaque à texte chiffré choisi dans laquelle le choix du texte chiffré à une étape donnée peut dépendre des textes clairs reçus lors des étapes précédentes.
— **Cryptanalyse différentielle :** Cette attaque différentielle demande actuelement 2^{47} texte clair choisis. la phase d'analyse calcule la clé à l'aide e ces données. La propriété de cette attaque est qu'il est possible de l'utiliser meme si le nombre de données disponible et petit , en fait la probabilité de succès augmente linéairement avec ce nombre.
— **Cryptanalyse linéaire :** Cette attaque utilise des approximations linéaire pour décrire les opérations conduisant au chiffré, plus le nombre d'essai augmente plus la probabilité d'obtenir la clé est forte.

3.7 Quel cryptosystèmes choisir ?

Le premier avantage de la cryptographie à clé publique est d'améliorer la sécurité elle permet d'échanger des messages de manière sécurisée sans aucun dispositif de sécurité. L'expéditeur et le destinataire n'ont plus besoin de partager des clés secrètes via une voie de transmission sécurisée. Les communications impliquent uniquement l'utilisation de clés publiques et plus aucune clé privée n'est transmise ou partagée. Avec un système à clé secrète, au contraire, il existe toujours le risque de voir la clé récupérée par une personne tierce quand elle est transmise d'un correspondant à l'autre. Toute personne interceptant la clé lors d'un transfert peut ensuite lire, modifier et falsifier

toutes les informations cryptées ou authentifiées avec cette clé. De la norme de cryptage de données DES au code secret de Jules César, la distribution des clés reste le problème majeur du cryptage conventionnel. (Autrement dit, comment faire parvenir la clé à son destinataire sans qu'aucune personne ne l'intercepte ?) les moyens à déployer pour garantir la distribution sécurisée des clés correspondants sont très onéreux, ce qui constitue un inconvénient supplémentaire. Le cryptage à clé publique représente une révolution technologique qui offert à tout citoyen la possibilité d'utiliser une cryptographie robuste.

En effet, la cryptographie conventionnelle était auparavant la seule méthode pour transmettre des informations secrètes. Les couts d'institutions disposants de moyens suffisants, telles que gouvernements et banque. Un autre avantage majeur des systèmes à clé publique est qu'ils permettent l'authentification des messages par signature électronique, ce qui peut aussi servir devant un juge, par exemple.

L'inconvénient des systèmes à clé publique est leur vitesse contrairement aux méthodes à clé secrète qui sont plus rapide. Ils sont particulièrement adaptés à la transmission de grandes quantités de données. Mais les deux méthodes peuvent être combinées de manière à obtenir le meilleur de leurs systèmes. Pour le cryptage, la meilleure solution est d'utiliser un système à clé publique pour crypter une clé secrète qui sera alors utilisée pour crypter fichiers et messages. [22]

3.8 Protocoles de sécurité SSL/TLS

3.8.1 Définition

Le système Secure Socket Layer (SSL) est un protocole de sécurisation des transactions. Ce protocole, conçu à l'origine par Netscape, et normalisé par l'Internet Engineering Task Force sous le nom de Transport Layer Security (TLS), permet de transmettre de manière sécurisée le numéro de carte bancaire sur Internet. SSL est aujourd'hui le système le plus utilisé sur Internet.

La sécurisation des connexions à l'aide du protocole SSL doit assurer que :
— La connexion assure la confidentialité des données transmises
— La connexion assure que les données transmises sont intègres
— L'identité des correspondants peut être authentifiée

— La connexion est fiable
SSL, assure donc une communication sécurisée entre le client et le serveur. Ce protocole, aujourd'hui très répandu, doit sa réussite et son utilisation massive à sa facilité d'implémentation.

3.8.2 Principe de fonctionnement

Le principe de fonctionnement de SSL se présente comme suit :

— **Authentification du serveur :** Qui permet à un utilisateur d'avoir une confirmation de l'identité du serveur. Cela est fait par les méthodes de chiffrement à clés publiques qu'utilise SSL. Cette opération est importante, car le client doit pouvoir être certain de l'identité de son interlocuteur à qui par exemple, il va communiquer son numéro de carte de crédit.

— **Authentification du client :** Selon les mêmes modalités que pour le serveur, il s'agit de s'assurer que le client est bien celui qu'il prétend être.

— **Chiffrement des données :** Toutes les données qui transitent entre l'émetteur et le destinataire, sont chiffrées par l'émetteur et déchiffrées par le destinataire, ce qui permet de garantir la confidentialité des données, ainsi que leur intégrité grâce souvent à des mécanismes également mis en place dans ce sens.

3.8.3 Service de sécurité du protocole SSL

Le protocole SSL assure plusieurs services de sécurité [21] :

— L'authentification : du serveur (obligatoirement) et du client (optionnellement) lors de l'établissement de la session ;
— la confidentialité : par négociation d'un algorithme de chiffrement et génération de clé lors de l'établissement de la session ;
— l'intégrité :par fonction de hachage .

Le protocole SSL utilise plusieurs algorithmes cryptographiques connus :

— DES pour le chiffrement symétrique ;
— RSA Pour le chiffrement asymétrique ;
— SHA et MD5 pour le hachage.

Conclusion

Dans ce chapitre nous avons présenté la cryptographie qui satisfait les objectifs de la sécurité informatique, qui sont : confidentialité, authentification, intégrité et non-répudiation, nous avons présenté aussi les fonctions à sens unique, les foncions de hachages cryptographiques, signature numérique et la générations des nombres aléatoire,et nous avons donner un petit aperçu sur la cryptanalyse et les attaques sur les systèmes cryptographiques. Nous avons présenté comment choisir un cryptosystème (comparaisons entre la crptographie à clé publique et la cryptographie à clé privée) et nous avons décrit les algorithmes cryptographiques les plus répandus.

Le chapitre suivant portera sur le premier et le plus célèbre algorithme de chiffrement à clé publique, le RSA, sur lequel est basé notre travail.

Chapitre 4

Cryptosystème RSA

Introduction

Le chiffrement RSA (nommé par les initiales de ses trois inventeurs) est un algorithme de cryptographie asymétrique, très utilisé dans le commerce électronique, et plus généralement pour échanger des données confidentielles sur Internet. Ce système, proposé par Rivest, Shamir et Adleman en 1978, est aujourd'hui le plus connu et le plus utilisé de par sa simplicité.[14], C'est à dire qu'on utilise une clé publique que tout le monde connaît qui permet de crypter le texte et une clé privée, dont seul le destinataire du message est censé la connaître afin de décrypter le message. Ce qui est important avec ce système, c'est qu'on ne peut pas retrouver la clé privée à partir de la clé publique.

Cette méthode est très utilisée de nos jours par exemple, dans les navigateurs Internet afin de garantir la sécurité de certains sites ou encore pour chiffrer des e mails. Il est aussi le standard de chiffrement du secteur bancaire de plusieurs pays [15]

Afin de crypter, nous avons besoin d'un message codé (il faut donc que le message d'origine soit transformé en nombres). Le RSA utilise l'arithmétique des congruences modulos N, c'est à dire qu'il utilise les restes des divisions. Il est alors possible, pour certains nombres, de trouver deux autres entiers qui nous permettent, par le calcul de puissance, de retomber sur le reste de départ (ainsi un premier calcul crypte et un second nous ramène sur

ce chiffre de départ, donc décrypte). Un des principaux avantages du RSA, c'est qu'il crypte par blocs de caractères, donc il ne conserve pas la fréquence d'apparition des lettres.

4.1 Description de RSA

RSA est fondé sur l'utilisation d'une paire de clés, composée d'une clé publique pour le chiffrement et d'une clé privée pour le déchiffrement. Il se base sur : la génération des clés, le chiffrement et le déchiffrement, la signature et la vérification de la signature.

4.1.1 Génération des clés

Dans le système RSA, Un utilisateur crée son couple (clé publique, clé privée) en utilisant la procédure suivante : [14]

1. choisir au hasard deux grands nombres premiers p et q. Il faut que p et q contiennent au moins 100 chiffres décimaux chacun ;
2. Calculer $N = p * q$;
3. Choisir un petit entier e qui est premier avec
   $\phi(N) = (p-1) * (q-1)$,
   C.à.d. Le $PGCD(e,(N)) = 1$;
4. Calculer d, l'inverse par la multiplication de e modulo $\phi(N)$;
5. publier la paire $K_e = (e, N)$ comme sa clé publique RSA ;
6. garder secrète la paire $K_d = (d, N)$ qui est sa clé privé RSA.

4.1.2 Chiffrement et déchiffrement des messages

— Un message m est chiffré en

$$c = m^e \, mod \, N$$

où :
e : est l'exposant de chiffrement
c : le message chiffré

— Le déchiffrement d'un chiffré c est :

$$c^d \, mod \, N$$

Où :
d :est l'exposant de déchiffrement.

4.1.3 Signature RSA

Génération des paramètres

Alice choisit deux nombres premiers p et q et un exposant e tel que $3 \leq e < (p-1)(q-1)$ et $PGCD(e,(p-1)(q-1)) = 1$. Alice calcule $N = p * q$ et d tel que $1 < d < (p-1)(q-1)$ et $e * d = 1 \, mod \, (p-1)(q-1)$.

La clé publique de Alice est (N, e) et sa clé secrète est d.

Génération d'une signature

Un message à signer m est un élément de l'ensemble $0, ..., N-1$. La signature du document m par Alice est :

$$s = m^d \, mod \, N$$

Dans la pratique, on préfère signer une empreinte du message m plutôt que de signer directement sa valeur.Pour cela, on utilise une fonction de hachage h pour calculer l'empreinte du document à signer $h = H(m)$.

De même, le calcul de l'empreinte est aussi nécessaire pour la vérification e la signature

Vérification d'une signature

Bob reçoit de Alice le message m et sa signature s. Il récupère la clé publique (N, e) de Alice et vérifie l'identité :

$$m = s^e \, mod \, N$$

4.2 Algorithme RSA

Tout ce qu'on a vu dans la section précédente sera traduit en algorithme pour mieux comprendre la description du cryptosystème RSA. [23] :

Entrée : taille de la clé // exprimée en bits.

Sortie : la clé publique (N, e) et la clé privée (N, d).

1. Prendre deux nombres premiers ***p*** et ***q*** suffisamment grands (de taille à peu près égale),
2. Calculer N = $p * q$,
3. Calculer φ(N) = $(p-1) * (q-1)$,
4. Choisir un nombre e tel que $1 < e < \varphi(N)$ et le *pgcd* $(e, \varphi(N)) = 1$,
5. Prendre un nombre e qui n'a aucun facteur en commun avec φ(N),
6. Calculer d tel que $e*d \bmod \varphi(N)=1$,
7. **Return :** *N, e, d.*

Algorithme 1 : Génération de clés avec RSA.

Entrée : (N, e) et m // la clé publique et le texte en clair m avec $m \in [0, N-1]$.

Sortie : C // *texte chiffré.*

1. Calculer $C = m^e \bmod N$,
2. **Return :** C.

Algorithme 2 :Chiffrement avec RSA

Entrée : (d, e) et C // la clé privée et le texte Chiffré.

Sortie : m // *texte clair.*

1. Calculer $m = C^d \bmod N$
2. **Return :** m.

Algorithme 3 : Déchiffrement avec RSA.

Entrée : (*N*, *d*) et *m* // la clé privée et le texte en clair *m* avec $m \in [0, N-1]$.

Sortie : *S*, *m* *// La signature et le texte clair.*

1. Calculer $h = H(m)$, //le hachage du message m,
2. Calculer $S = h^d \ mod \ N$,
3. **Return :** *S*, *m*.

Algorithme 4 : Signature avec RSA.

Entrée : (e, N), *m*, S

Sortie : *Acceptation ou rejet de la signature* *// La signature et le texte clair.*

1. Calculer $h = H(m)$, //le hachage du message m,
2. Calculer $h' = S^e \ mod \ N$,
3. **Accepter** si $h = h'$ **rejeter** Sinon

Algorithme 5 : Vérification de la signature.

4.3 Déroulement de RSA avec exemple

Bob veut envoyer un message secret à Alice

— Alice prépare une clé publique et une clé privée.

— Bob utilise la clé publique d'Alice pour crypter son message

— Alice reçoit le message crypté et le déchiffre grâce à sa clé privée

1. **Etape 1** : *préparation des clés* :

   (a) **Choix de deux nombres premiers**

   Alice effectue les opérations suivantes

   • Choix de deux nombres premiers distincts p et q

   • Calcul de $N = p * q$

- Calcul de $\phi(N) = (p-1) * (q-1)$

Exemple

- $p = 5$ et $q = 17$
- $N = p * q = 85$
- $\phi(N) = (p-1) * (q-1) = 64$

(b) **Choix d'un exposant et calcul son inverse**

- Alice choisit un exposant e tel que le $pgcd(e, \phi(N)) = 1$
- Alice calcule l'inverse d de e modulo $\phi(N)$ par l'algorithme d'euclide étendu : $d * e \equiv 1 (mod\, \phi(N))$

Suite de l'exemple

- $e = 5$ et on a bien le $pgcd(e, \phi(N) = pgcd(5, 64) = 1$
- $5 * 13 + 64 * (-1) = 1$
- Donc $5 * 13 \equiv 1 (\, mod\, 64)$
- L'inverse de e modulo $\phi(N)$ est $d = 13$

(c) **Clé publique** La clé publique d'Alice est constituée des deux nombres N et e

(d) **Clé privée** Alice garde pour elle sa clé privée d

Suite de l'exemple

- $N = 85$ et $e = 5$
- $d = 13$

2. **Etape 2** : *Chiffrement du message*

(a) **Message**

— Bob veut envoyer un message secret à Alice
— Il transforme son message en un (ou plusieurs) entier m
— L'entier m verifie $0 \leq m < n$

Suite de l'exemple

• $m = 10$

(b) **Message chiffré**
— Bob récupère la clé publique d'Alice e et N
— Il calcule le message chiffré $C \equiv M^e (mod\, N)$
— Il transmet ce message C à Alice

Suite de l'exemple

• $m = 10$, $N = 85$ et $e = 5$
• $C \equiv m^e (mod\, N)\, C10^5 \pmod{85}$
  • $10^2 = 100 \equiv 15 \pmod{85}$
  • $10^4 = (10^2)^2 \equiv 15^2 \pmod{85} \equiv 255 \equiv 55 \pmod{85}$
  • $10^5 = (10^4) * 10 \equiv 55 * 10 \pmod{85} \equiv 550 \equiv 40 \pmod{85}$

3. **Etape 3** : *Déchiffrement du message*
   • Alice reçoit le message chiffré par Bob
   • Alice le décrypte à l'aide de sa clé privé d

- $m \equiv C^d \pmod{n}$

Suite de l'exemple

- $C = 40$, $d = 13$, $N = 85$ $\quad 40^13(mod85)$
  - $40^2 = 1600 \equiv 70 \pmod{85}$
  - $40^4 = (40^2)^2 \equiv 70^2 \pmod{85} \equiv 4900 \equiv 55 \pmod{85}$
  - $40^8 = (40^4)^2 \equiv 55^2 \pmod{85} \equiv 3025 \equiv 50 \pmod{85}$
  - $40^13 = 40^{(8+4+1)} = 40^8 * 40^4 * 40 \equiv 10 \pmod{85}$
- On retrouve bien le message $m = 10$de bob.

4.4 Démonstration mathématique

Dans cette section on fera appel aux propriétés mathématiques nécessaires ensuite on étudiera la démonstration mathématique du cryptosystème RSA.

4.4.1 Outils mathématiques utilisés

$N = p*q$ sachant que p et q sont premiers entre eux, $\phi(N) = (p-1)*(q-1)$ est appelée fonction d'Euler ou indicatrice d'Euler

Theorem 4.4.1 (Petit théorème de Fermat) *Si p est un nombre premier,*

Si a est un nombre premier avec p (c'est-à-dire que $pgcd(a,p) = 1$) alors

$$a^{p-1} \equiv 1 \pmod{p}$$

Theorem 4.4.2 (Théorème d'Euler) *Si $pgcd(a,N) = 1$ alors $a^{\phi(N)} \equiv 1 \pmod{N}$*

4.4.2 Démonstration

* d est l'inverse de e modulo $\phi(N)$

$$d * e \equiv 1 \pmod{\phi(N)}$$

Il existe $k \in Z$ tel que

$$d * e \equiv 1 + k * \phi(N)$$

* En utilisant le théorème de Fermat on aura : Si $pgcd = 1$ Alors $m^{\phi(N)} = m^{(p-1)(q-1)} \equiv 1 \pmod{N}$
* Si

$$pgcd(m, N) = 1$$

alors modulo N :
$(m^e)^d \equiv m^{1+k*\phi(N)} \equiv m * m^{k*\phi(N)}$
$(m^e)^d \equiv m * (m^{\phi(N)})^k$
$(m^e)^d \equiv m * 1^k$
$(m^e)^d \equiv m \pmod{N}$

* Si

$$pgcd(m, N) \neq 1$$

Par exemple $pgcd(m, N) = p$ et $pgcd(m, q) = 1$
Alors modulo p : $m \equiv 0$ et $(m^e)^d \equiv 0$
donc

$$(m^e)^d \equiv m \pmod{p}$$

Alors modulo q : $(m^e)^d \equiv m * (m^{\phi(N)})^k$

$$(m^e)^d \equiv m * (m^{(q-1))^{(p-1)*k}}$$

$$(m^e)^d \equiv m \pmod{q}$$

$pgcd(p, q) = 1$; donc $(m^e)^d \equiv m \pmod{p}$ CQFD

4.5 Attaques mathématiques sur RSA

Il existe plusieurs attaques mathématiques sur le système RSA qui sont des attaques qui cherchent a trouver une faille dans les fondements mathématiques même de l'algorithme. Nous présentons quelques attaques :

Factorisation du module N :

La première attaque possible contre le cryptosystème RSA consiste à tenter de factoriser le module N pour retrouver p et q. La méthode des divisions successives, consiste à déterminer les diviseurs premiers de N plus petits que $\sqrt{N}$ ensuite il suffit de diviser N successivement par tous les nombres premiers retrouvés jusqu'à atteindre p qui est le plus petit diviseur premier de N ($p \leq \sqrt{N}$). C'est une technique d'attaque par force brute.[24]

Attaque de Wiener :

Cette attaque est proposé par le cryptologue Michael J. Wiener. Elle permet de retrouver facilement la clé privée à partir de la clé publique (e, N) , lorsque les conditions :
$d < \frac{1}{3}N^{\frac{1}{4}}$ (d trop petit) et
$q < p < 2q$ (p et q trop proches)
sont remplis, il est facile de retrouver d. [25]

Attaque en connaissant quelques bits de la clé privée :

Si on connaît quelques bits de la clé privée d. D.Boneh à montré que si la taille de la clé d est de k bits alors la connaissance de $\frac{k}{4}$ bits de poids faible est largement suffisante pour récupérer la clé d. [26]

4.6 Efficacité de RSA

— Il est facile de générer des grands nombres premiers, tout au moins en acceptant un taux d'erreur, dans RSA l'erreur n'est pas grave car si l'on commet une erreur en croyant que p et q son premiers, le destinataire se rendra rapidement compte que les nombres ne sont pas premiers : soit la clé d n'est pas inversible, soit le message décrypté est incompréhensible, dans ce c cas on recalcule p et q .
— Le calcul de du couple (e, d) est facile, il suffit d'appliquer l'algorithme d'Euclide étendu.
— Le chiffrement et déchiffrement sont réalisés par exponentiation modulaire.
— La sécurité fournie par RSA repose essentiellement sur la difficulté à factoriser le nombre $N = p * q$ de la clé publique

Conclusion

Le cryptosystème RSA travaille avec les nombres premiers. Or factoriser un très grand nombre premier en deux autres prend beaucoup de temps.

RSA utilise une clé publique et une clé privée alors c'est un bon point étant donné que le problème de communications des clés est résolu (contrairement aux algorithmes symétriques).

Mais dans RSA il faut utiliser de grandes clés, et leur génération prend un certain temps. et le cryptage également, puisqu'on travaille avec de très grandes clés, donc il est puissant. Il existe des algorithmes pour casser RSA, mais ceux-ci sont très lents et donc la plupart des fois inefficaces .

Conclusion et perspectives

Conclusion

La science du secret a bien évolué depuis ses débuts, passant progressivement d'un art protéger l'information à une discipline visant à apporter de la confiance à des échanges numériques.

Le développement des échanges électroniques est au cœur de la dynamique économique des années à venir. Il entraîne des changements profonds dans l'organisation et le fonctionnement des entreprises.

Le e-commerce dans notre pays l'Algérie se développe mais se heurte encore à l'obstacle majeur qui est le manque de sécurité et de confiance. On estime un changement dans ce domaine et un avenir meilleur si les conditions nécessaires seront développées suivant les points :

— **Juridique** : Réformes réglementaires ayant pour objectif un cadre juridique clair, concis et transparent ;
— **Organisationnelle** : Développement institutionnel, consultations au niveau du secteur privé, et coopération entre les différentes institutions ;
— **Technologique** : Mise en place et modernisation des infrastructures pour traitement électronique et échanges de données, y compris les systèmes de TI (technologies de l'information) ;
— **Sécurité informatique** : Gagner la confiance des acheteurs par un renforcement des sites du e-commerce et les soumettre à des règles internationnale.

Dans ce mémoire, nous avons traité quelques aspects de cryptographie, cas de sécurité dans le commerce électronique, nous avons présenté le travail sous forme d'une synthèse qui consiste à décrire les éléments nécessaire au développement du commerce électronique spécialement en Algérie.

Nous avons présentés quelques cryptosystèmes les plus utilisés en commerce électronique, le protocole SSL, et TLS et en particulier, on a fait une étude sur le cryptosystème RSA , le cryptosystème le plus populaire et le plus utilisé dans le e-commerce.

Perspectives

Suite au travail fait dans ce mémoires nous suggérons :

— Réaliser une application qui permet de simuler des attaques contre le RSA , on prend par exemple l'attaque par factorisation.
— Élargir l'étude de la cryptographie en Algérie et utiliser des cryptosystèmes fiables pour bien sécuriser les sites de vente ce qui donne plus de confiance pour les utilisateurs.
— Cryptanalyse du cryptosystème RSA.

Chapitre 5

Annexe 1

5.1 Résumé des principales normes de sécurité de l'information

Nom	**Fondement**	**Objectif**
ISO/CEI Guide73	ISO 31000 :2009	Définition des termes relatifs au management du risque
ISO/CEI 15408	Orange book, IT-SEC,CTCPEC	Évaluation et certification
ISO/CEI 17799	BS7799-1	Lignes directrices et des recommandations SMSI
ISO/CEI 27000	/	Vue d'ensemble et vocabulaire
ISO/CEI 27001	BS 7799-2	Systèmes de gestion de sécurité de l'information – Exigences
ISO/CEI 27002	ISO/ CEI 27001	Code de bonne pratique pour le management de la sécurité de l'information
ISO/CEI 27003	ISO/ CEI 27001	Mise en œuvre du système d'orientation

ISO/CEI 27004	ISO/ CEI 27001	Management de la sécurité de l'information – Mesurage
ISO/CEI 27005	ISO/ CEI 13335	Gestion des risques liés à la sécurité de l'information
ISO/CEI 27006	/	Exigences pour les organismes procédant à l'audit et à la certification des SMSI
ISO/CEI 27007	ISO/ CEI 27006	Lignes directrices pour l'audit des SMSI
ISO/CEI 27011	ISO/ CEI 27001	Lignes directrices du management de la sécurité de l'information pour les organismes de télécommunications sur la base de l'ISO/CEI 27002
ISO/CEI 27013	ISO/ CEI 27001 ISO/CEI 20000	Guide sur la mise en œuvre intégrée d'ISO/CEI 27001 et ISO/CEI 20000-1
ISO/CEI 27031	ISO/CEI 27001	Lignes directrices pour l'information et la technologie des communications de préparation pour la continuité des activités
ISO/CEI 27035	ISO/CEI 27001	Gestion de l'information des incidents de sécurité
ISO/ CEI 27799	ISO/ CEI 27001	Gestion de la sécurité de l'information en matière de santé
ISO 31000	AS/NZS 4360	Management du risque, principes et lignes directrices

TABLE 5.2 – Résumé des principales normes de sécurité de l'information

5.2 Arithmétique

Deux algorithmes nécessaires dans les calculs de la cryptographie en général et en cryptosystème RSA en particulier.[21]

5.2.1 Algorithme d'Euclide

Entrée : a, b ;

Sortie : R_1=0, $R_0 = pgcd\ (a, b)$;

$R_0 := a$;

$R_1 := b$; *(b différent de 0)*

Tant que $(R_1 > 0)$ **Faire**

$R := reste\ de\ division(R_0, R_1)$;

$R_0 := R_1$;

R_1:=R

Fin TQ

Algorithme 1 : Algorithme Euclide

5.2.2 Algorithme d'Euclide étendu

Entrée : a, b ;

Sortie : u, v;

$$R_0 := a \; ; \; a \geq 0$$

$$R_1 := b \; ; \; (b > 0)$$

$$U_1 := 0 \; ; \; U_0 := 1 \; ;$$

$$V_0 := 0 \; ; \; V_1 := 1 \; ;$$

Tant que ($R_1 > 0$) **Faire**

$$Q := Quotion\_division(R_0, R_1);$$

$$R := reste\_de\_division(R_0, R_1);$$

$$U := U_0 - Q * (U_1);$$

$$V := V_0 - Q * (V_1);$$

$$R_0 := R_1 \; ;$$

$$R_1 := R \; ;$$

$$U_0 := U_1 \; ; \; U_1 := U \; ;$$

$$V_0 := V_1 \; ; \; V_1 := V \; ;$$

Fin TQ

Algorithme 2 : Algorithme Euclide étendu.

Bibliographie

[1] Didier Godart, *Sécurité informatique, risques, stratégies et solutions, échec au cyber-roi.*

[2] Jean-François Pillou, Jean-Philippe Bay, *Tout sur la sécurité informatique,2016.*

[3] Renaud Dumont, *Notes de cours provisoires*, `https://www.cours-gratuit.com/cours-divers/support-de-cours-de-cryptographie-et-securiteinformatique`, *2009 - 2010.*

[4] Flavien Serge Mani Onana, *Vie privée en commerce électronique, 2005.*

[5] *Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information - Exigences.* `https://standards.iteh.ai/catalog/standards/sist/9339502a-f914-41bf-9251-f6956d09eafa/iso-iec-27001-2013`, *2013.*

[6] *Le journal officiel*, Algérie `https://www.droit-afrique.com/uploads/Algerie-Loi-2018-05-commerce-electronique.pdf`, *2018.*

[7] Raphael Yende, *Support de cours de sécurité informatique et cryptographie.*

[8] ISO/CEI 27002.*Technologies de l'information , Techniques de sécurité , Code de bonne pratique pour le management de la sécurité de l'information, International Organisation for Standardisation*, Genève, *2013.*

[9] EBIOS, *Secrétariat Général De la Défense Nationale, 2010.* EBIOS, *Expression des Besoins et Identification des Objectifs de Sécurité.* http ://www.ssi.gouv.fr/guide/ebios-2010- expression-des-besoins-et-identification-des-objectifs-de-securite/

[10] Nabil Laoufi, *Thèse Doctorat, École Doctorale d'Informatique, Télécommunications et Electronique Centre d'étude et de recherche en informatique et communications, 2017.*

[11] Y.Asnar, P.Giorgini, *Modelling Risk and Identifying Countermeasure in Organizations.* CRITIS *2006.*

[12] ISO/CEI 17799,*Information technology - Security techniques - Code of Practice for Information Security Management, International Organisation for Standardisation*, Genève.*2005.*

[13] G. Pujolle, *Les réseaux*, Édition 2005, Eyrolles, *2004.*

[14] Touradj Ebrahimi, franck Leprévost, bertrand Warusfel, *Cryptographie et sécurité des systèmes et réseaux.*

[15] Morges-Beausobre - Vincent, *La Cryptographie et Le RSA. 2005.*

[16] Stéphane Jacob, *Thèse de doctorat de l'université Pierre et Marie Curie Spécialité Informatique, Protection cryptographique des bases de données : conception et cryptanalyse*, https ://tel.archives-ouvertes.fr, *2006.*

[17] C. Kaufman, R. Periman and M. Speciner, *Network Securitv , Private Communication in a Public World, 2nd edition, Prentice Hall, 2002.*

[18] *Site statistica*, `https://www.statista.com/statistics/274708/online-retail-and-auction-ranked-by-worldwide-audiences/`, *2022.*

[19] *International Journal of Business Administration, Vol. 8, No. 7*, `http://ijba.sciedupress.com`, *2017.*

[20] Louiza Rezallah, *Mémoire de fin d'études en recherche opérationnelle, Université Houari Boumedienne, De la cryptographie classique a la cryptographie moderne théorie et application* . http ://repository.usthb.dz, *2007*.

[21] Pierre Barthélemy, Robbert Rolland, Pascal Véron, *Cryptographie (Principes et mises en oeuvres*, Hermes science, *2005*.

[22] W. Diffie, *dix premières années de la cryptographie à clef publique*. Edition *1988*.

[23] Rebiha Hadaoui, *Thèse de doctorat, Université Mouloud MAMMERI Tizi-Ouzou,le chiffrement RSA dans les systèmes à ressources limités.2020*

[24] Alain Kraus, *Cours de cryptographie MM067 - , Méthodes de factorisation, Université Pierre et Marie Curie*, https ://www.math.univ-paris13.fr/ boyer/enseignement/crypto/Chap6.pdf, *2009*.

[25] A. Dragut,*Cours de cryptographie, Université Aix-Marseille*, http ://pageperso.lif.univ-mrs.fr/ andreea.dragut/enseignementCLAA/CryptoChap3RSA.pdf,*2012*

[26] Christophe Grenier,*Techniques de cryptanalyse de RSA*, ftp ://ftp.irisa.fr/local/caps/DEPOTS/BIBLIO2009/Grenier$_C$*hristophe.pdf*, *2009*