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

Université M'Hamad Bougara de Boumerdes
Faculté de Technologie
Département D'Ingénierie des Systèmes Electriques

Polycopié de cours

SECURITE INFORMATIQUE

COURS ET EXERCICES CORRIGES

(Unité Fondamentale-- Domaine Sciences et Technologie — Master LMD)

Elaboré par :

Dr. RIAHLA Mohamed Amine

Maitre de conférences A, Université M'hamed BOUGARA de BOUMERDES

Année Universitaire : 2021/2022

Avant-propos

Ce polycopié est un support de cours contenant des notions essentielles en sécurité informatique et à certaines attaques et vulnérabilités actuelles, il est adressé aux étudiants en Master informatique et télécommunication. Le document contient l'essentiel à maitriser dans ce domaine, ainsi que plusieurs illustrations sous formes d'exercices, et tests de compréhension. Le cours et les exercices sont réalisés conformément aux programmes de certifications internationales comme PECB et aux normes ISO 27001, ISO 27005.

Le polycopié fait partie d'une série de mes manuscrits relatifs aux domaines des réseaux de télécommunication, sécurité informatique et Technologies d'information et communication (TIC) en général.

Certains Cours, Exercices et Travaux Pratiques de ces manuscrits sont inspirés de problématiques réelles que j'ai vécues moi-même durant mes activités pédagogiques et de consulting. Tout ça est dans le but de casser cette barrière entre « le monde universitaire académique » et « le monde professionnel entreprise», c'est-à-dire faire de nos jeunes étudiants des cadres professionnels avec une pré-expérience, donc prêts à être recrutés.

RIAHLA Mohamed amine
Docteur de l'université de LIMOGES
Expert consultant en TIC et Maitre de Conférences A à l'université de Boumerdes

But du document

- Un bon support de cours du module sécurité informatique pour les étudiants de Master
- Connaissances générales pour les non spécialistes
- Une bonne base pour les futurs spécialistes de la Sécurité informatique
- Apprendre les métiers de la sécurité informatique
- Maitriser les malwares
- Parler le jargon de la sécurité informatique
- Apprendre les notions essentielles en cryptographie

Prérequis

- Les cours de License en réseaux et système de télécommunication
- Avoir les notions de base en informatique et télécommunication
- La lecture de mon précédent polycopié portant sur les réseaux et les systèmes de télécommunications.
- Suivre mes cours vidéo en ligne dans le domaine des réseaux et sécurité de l'information
- Mes supports de cours en réseaux informatiques et Routage IP

Table des matières

Partie I : Les éléments de base de la sécurité Informatique 11

I.1. Introduction (historique) 12

I.1.1. L'époque Kevin mitnick 12

I.1.2. L'évènement de Février 2000 12

I.2. Système d'information, Système informatique et sécurité informatique : 12

I.2.1. Systèmes d'information 12

I.2.2. Les Systèmes Informatiques et la sécurité informatique au service des Systèmes d'information 13

I.3. Définition de la sécurité informatique 13

I.4. Vocabulaire 13

I.4.1. Actif 13

I.4.2. Vulnérabilité 14

I.4.3. Incident de sécurité 15

I.4.4. Menace 16

I.4.5. Risque 16

I.4.6. Attaque 17

I.4.7. Contre-mesures 17

I.5. Exigences fondamentales et objectifs de la sécurité informatique 18

I.5.1. La confidentialité 18

I.5.2. L'intégrité 19

I.5.3. Disponibilité 20

I.5.4. Non répudiation 20

I.5.5. Authentification 21

I.5.6. Respect de la vie privée (informatique et liberté) 23

I.5.6. Autres principes/objectifs et modèles de sécurité 23

I.6. Les métiers de la sécurité informatique 23

I.6.1. Débuter en sécurité de l'information 23

I.6.2. Responsable de la sécurité des systèmes d'information 23

I.6.3. Consultant en cyber sécurité 24

I.6.4. Autres métiers 24

I.7. Processus de sécurisation d'un système d'information 25

I.7.1. Analyse de la situation 25

I.7.2. Analyse des risques 25

I.7.2.1. Processus d'analyse de risques 26
I.7.3. Politique de sécurité 26
I.7.3.1. Structuration de la politique de sécurité 27
I.7.4. Mesures de sécurité 29
I.7.5. Implémentation 30
I.7.6. Validation 30
I.8. Principaux défauts de sécurité 30
TD1. Travaux dirigés du chapitre I 31
TD1.1. Questions QCM 31
TD1.1. Exercices 32
Exercice 1 « Méthode d'analyse de risque » 32
Exercice 2 « questions sur la sécurité des systèmes d'information» 32
Exercice 3 « Etapes de sécurisation des systèmes d'information » 32
Exercice 4 « Objectifs de sécurité » 33
Partie II : Terminologie des attaques 34
II.1. Menaces accidentelles vs menaces intentionnelles 35
II.2. Attaques actives vs attaques passives 35
II.3. Attaque par Interruption, Interception, Modification et Fabrication 35
II.3.1. Attaque par Interruption 35
II.3.2. Attaque par Interception 36
II.3.3. Attaque par modification 36
II.3.4. Attaque par Fabrication 36
II.4. L'origine des attaques 36
II.4.1. Les hackers vs cracker 36
II.4.2. Les concurrents industriels 36
II.4.3. Les espions 37
II.5. Objectifs des attaques 37
II.6. Motivations des attaques 37
II.7. Cible des pirates 38
II.8. Nœud malicieux 38
II.9. Attaquant actif-n-m 38
II.10. Attaque externe 38
II.11. Attaque interne 38
II.12. Les états d'insécurité 38
II.12.1. L'état actif d'insécurité 38

II.12.2. L'état passif d'insécurité 38
TD2. Travaux dirigés du chapitre II 39
Exercice 1 : « QCM rapide » 39
Exercice 2 : « Questions de compréhension » 39
Partie III : Les malwares 40
III.1. Virus 41
III.1. 1. Virus de boot 41
III.1. 2. Virus dissimulé dans les exécutables 41
III.1.3. Virus furtifs 41
III.1. 4. Virus polymorphes 42
III.2. Vers 42
III.2.1. Les familles de vers 43
III.2.1.1. Les Vers poste à poste (P2P) 43
III.2.1.2. Les vers de la messagerie électronique 43
III.2.1.3. Les vers des messageries instantanées 43
III.2.1.4. Les vers se propageant à travers les supports de stockage 43
III.3. Cheval de Troie, troyen, trojan horse, trojan 43
III.4. Porte dérobée 44
III.5. Rootkit 45
III.6. Spyware 46
III.7. Hoax 46
III.8. Bombes logiques 46
III.9. Ransomware 47
III.10. Adware 47
III.11. Autres malwares 48
III.12. Effet des malwares modernes 48
TD3. Travaux dirigés du chapitre III 49
TD3.1. « Questions QCM » 49
TD3.2. « Questions de compréhension de la partie III » 50
TD3.2. « Exercice de reflexion » 50
Partie IV : Cryptographie 51
IV.1. Introduction et historique 52
IV.2. Principe de base 53
IV.3. Terminologie 54
IV.3.1. Stéganographie VS Cryptographie 54

IV.3.2. Cryptographie par transposition 55
IV.3.3. Cryptographie par substitution 55
IV.3.4. Définitions rapides 55
IV.3.4.1. Message clair 55
IV.3.4.2. Chiffrement 55
IV.3.4.3. Déchiffrement 56
IV.3.4.4. Clé de cryptographie 56
IV.3.5. Cryptographie VS cryptanalyse 56
IV.3.6. Cryptologie 57
IV.3.7. Cryptosystème 57
IV.3.8. Algorithme secret VS Algorithme robuste 57
IV.3.9. Principe de Kerckhof 57
IV.4. Cryptographie classique 58
IV.4.1. Chiffrement mono alphabétiques 58
IV.4.1.1. Chiffrement de César 58
IV.4.2.2. Substitution aléatoire 60
IV.4.2.3. Homophones 61
IV.4.3.4. Chiffre affine 61
IV.4.2. Chiffrement polygraphique (ou polygrammiques) 62
IV.4.2.1. digramme et trigramme 62
IV.4.2.2. Le chiffre de Playfair 63
IV.4.2.3. Le chiffre de Hill 64
IV.4.3. Chiffrement poly alphabétiques 64
IV.4.3.1. Chiffrement de Vigenère 65
IV.4.3.2. Chiffrement de vername 65
IV.4.4. Transposition 66
IV.5. Cryptographie moderne 67
IV.5. 1. Cryptographie symétrique 67
IV.5. 1.1. Avantages de la cryptographie symétrique 68
IV.5. 1.2. Inconvénients de la cryptographie symétrique 68
IV.5. 2. Cryptographie asymétrique 71
IV.5. 2.1. Avantages de la cryptographie asymétrique 72
IV.5. 2.2. Inconvénients de la cryptographie asymétrique 73
IV.5. 3. Cryptographie symétrique VS Cryptographie asymétrique 73
IV.5. 4. La cryptographie hybride 73
IV.5. Comment assurer les autres objectifs de sécurité 74

IV.5.1. Signature numérique 74
IV.5.1.1. Signature numérique utilisant la cryptographie asymétrique 75
IV.5.1.2. Signature numérique utilisant les fonctions de hachage 76
IV.6. Un dernier problème à résoudre avec les certificats numériques 77
IV.6.1. Nouvelle communication avec les certificats numériques 79
IV.6.2. PKI (Public Key Infrastructure) Infrastructure à clefs publiques 80
IV.7. Un simple et efficace résumé 80
IV.8. Autres systèmes de chiffrement 80
IV.9. Protocoles cryptographiques 81
IV.10. Exemples d'applications et Communications sécurisées 81
IV.10.1 Communications sécurisées 81
IV.10.1.1. Le protocole SSH (Secure Shell) 81
IV.10.1.2. Le protocole SSL/TLS (Secure Socket Layer) 82
IV.10.1.3. Le réseau VPN (réseau privé virtuel) 83
IV.10.2 Applications sécurisées 83
IV.10.2.1. PGP 83
IV.10.2.2. KERBEROS 83
..... 84
IV.10.2.3. Les cartes à puce 84
TD4. Exercices de la partie IV 86
TD4.1. Exercices en QCM 86
Solution du TD4.1. Exercices en QCM 87
TD4.2. Exercices d'application extraits d'examens 89
Exercice 1 : « questions de compréhension » 89
Solution de quelques questions de l'exercice 1 89
Exercice 2 : « Cryptographie en pratique » 90
Solution exercice 2 : « Cryptographie en pratique » 90
Exercice 3 : 90
Solution d'exercice 3 91
Exercice 4 91
Solution de l'exercice 4 92
Exercice 5 92
Exercice 6 92
Exercice 7 93
TD4.3. Exercices d'application extraits d'une série de TD 93
Exercice 1 93

Exercice 2 94
Exercice 3 94
Exercice 4 94
Exercice 5 95
Solutions des exercices des parties 1, 2 et 3 96
Solution du TD1. Travaux dirigés du chapitre I 97
TD1.1. Questions QCM 97
TD1.2. Exercices 98
Exercice 1 « Méthode d'analyse de risque » 98
Exercice 2 « questions sur la sécurité des systèmes d'information» 98
Exercice 3 « Etapes de sécurisation des systèmes d'information » 99
Exercice 4 « Objectifs de sécurité » 99
Solution du TD2. Travaux dirigés du chapitre II 101
TD3. Travaux dirigés du chapitre III 103
TD3.1. « Questions QCM » 103
TD3.2. « Questions de compréhension de la partie III » 104
TD3.2. « Exercice de reflexion » 105
Echantillion d'examen 106
Solutions de l'echantillion d'examen 110

Partie I : Les éléments de base de la sécurité Informatique

I.1. Introduction (historique)

I.1.1. L'époque Kevin mitnick

Kevin Mitnick est l'un des pirates informatiques de référence. Il a commencé à hacker des réseaux téléphoniques puis a attaqué les machines de tsutomu shimomura qui est un expert en sécurité informatique. Il a pénétré dans les serveurs du WELL (Whole Earth Lectronic Link) et a accédé au courrier de markoff (qui est un journaliste). En 1995, Il a été arrêté avec l'aide du shimomura et de la société WELL. Kevin a servi cinq années en prison et interdit d'utiliser des ordinateurs pour deux années de suite.

Il est aujourd'hui Consultant en sécurité informatique depuis 2000. Il a publié plusieurs livres touchant des domaines sensibles de la sécurité informatique dont : l'ingénierie sociale, les systèmes de détection d'intrusion,…

I.1.2. L'évènement de Février 2000

Un adolescent de 15 a causé en février 2000, l'arrêt de plusieurs sites web majeurs dont ebay, cnn, amazon, Yahoo... pour quelques heures. Il a inondé ces serveurs par un flux énorme de Traffic (allant jusqu'à 1 Gbps) provenant de plusieurs adresses différentes. C'était la première attaque DDoS (Déni de servie Distribué) médiatisée dans la presse grand public. Il fut arrêté le 15 avril de la même année, puis condamné à 8 mois dans un centre de détention puisqu'il est mineur !

Grace à un programme automatique, il était capable d'exploiter une faille dans les serveurs ftp de 75 machines, ce qui lui a permis d'installer un programme d'attaque distribué (d'où le nom de DDOS).

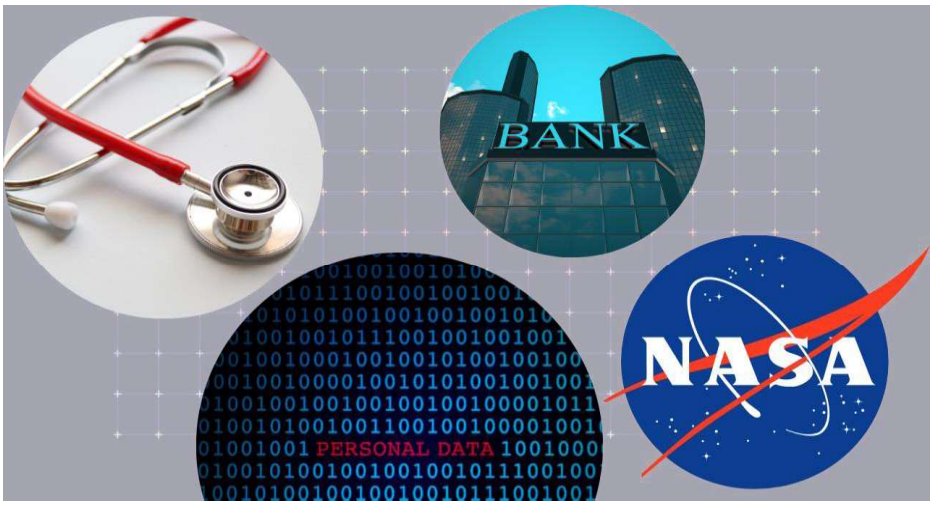
Aujourd'hui, le nombre d'attaques informatiques augmente de façon exponentielle, surtout que les cybercriminels travaillent en groupe aujourd'hui et s'organisent comme de vraies entreprises.

I.2. Système d'information, Système informatique et sécurité informatique :

I.2.1. Systèmes d'information

Un système d'information peut être définit comme étant l'ensemble des ressources matérielles et logicielles permettant de collecter, acquérir, stocker, transformer, diffuser, exploiter, gérer et traiter les informations nécessaires au bon fonctionnement d'une organisation.

Ces informations constituent donc les biens des personnes et des entreprises, et peuvent être très « convoitées ». Ainsi, les entreprises ont besoin aujourd'hui de dispositifs plus puissants pour gérer et sécuriser de très grandes quantités d'informations de nature hétérogène (financières, techniques, médicales…etc), d'où l'utilisation des systèmes informatiques.



La diversité des types de données

I.2.2. Les Systèmes Informatiques et la sécurité informatique au service des Systèmes d'information

Un système informatique est l'un des moyens techniques permettant de faire fonctionner un système d'information. C'est pour cette raison que ces systèmes informatiques sont devenus la cible de ceux qui convoitent l'information.

En conclusion, assurer la sécurité de l'information revient à assurer la sécurité des systèmes informatiques. Voilà pourquoi on parle de la sécurité informatique.

I.3. Définition de la sécurité informatique

La sécurité informatique est donc l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. Dans ce qui suit, nous allons définir les termes les plus utilisés dans le jargon de la sécurité informatique :

I.4. Vocabulaire

Afin de faciliter la compréhension des termes les plus utilisés dans le domaine de la sécurité informatique, nous allons prendre un exemple inspiré des joueurs de football, on considère donc notre entreprise est un club de foot professionnel.

I.4.1. Actif

Ou assets en anglais, il s'agit de n'importe quel élément qui a de la valeur pour l'entreprise. Un actif pour une entreprise peut être :

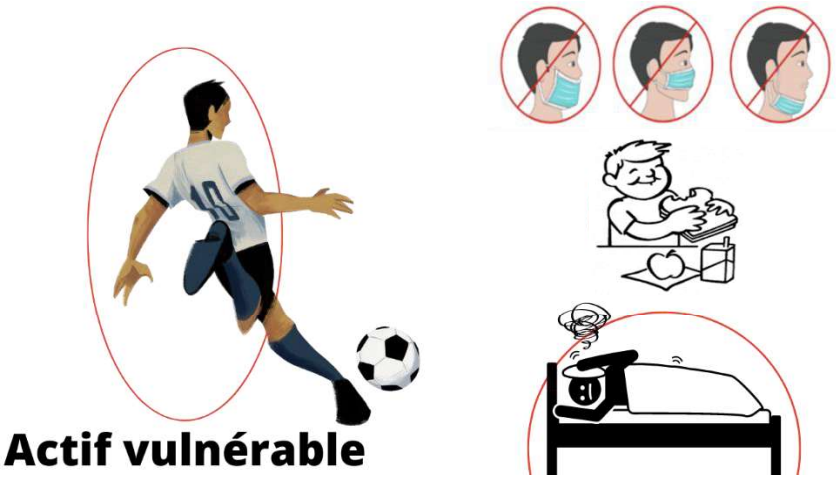
- Du Matériel
- Des Logiciels
- Des personnes
- De l'infrastructure système et réseau
- Des données
- Des Services et protocoles réseau …

Le but pour toute entreprise est donc de protéger ses actifs.

I.4.2. Vulnérabilité

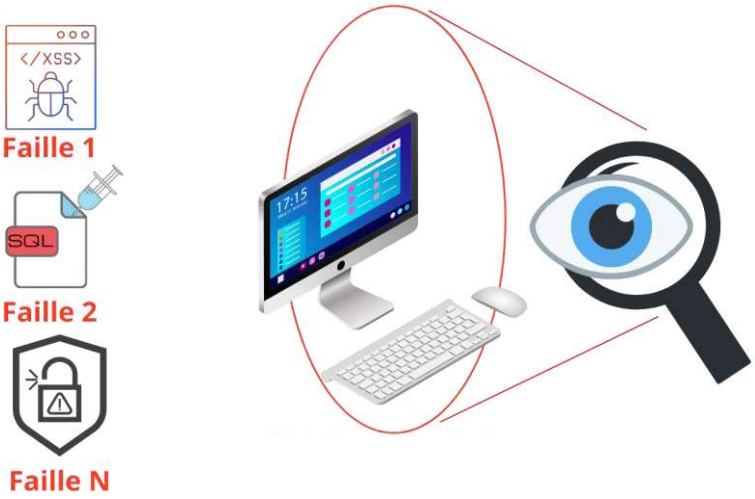
C'est une faiblesse au niveau d'un actif, c'est comme une maison avec des fissures

Prenons l'exemple suivant : notre actif est un joueur de football, on dit que notre joueur est vulnérable s'il ne se protège pas des virus, s'il ne mange pas bio et/ou il ne dort pas assez.



Par analogie, en sécurité informatique, un ordinateur est vulnérable s'il n'est pas sécurisé par un mot de passe ou s'il ne contient pas d'antivirus

On parle aujourd'hui du domaine de test de vulnérabilité (pentest en anglais) qui consiste à détecter, identifier et analyser les vulnérabilités d'un actif

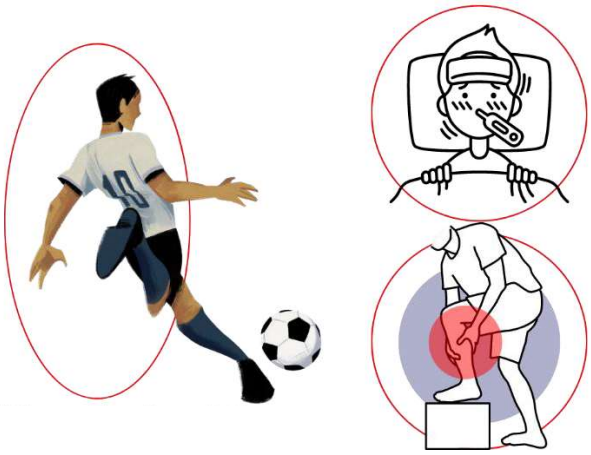


Le domaine du pentest

I.4.3. Incident de sécurité

C'est un dysfonctionnement au niveau d'un actif signalé par un utilisateur. Les exemples ci-dessous illustrent la définition d'un incident de sécurité :

Exemple d'incident 1 : notre joueur est malade ou est blessé !



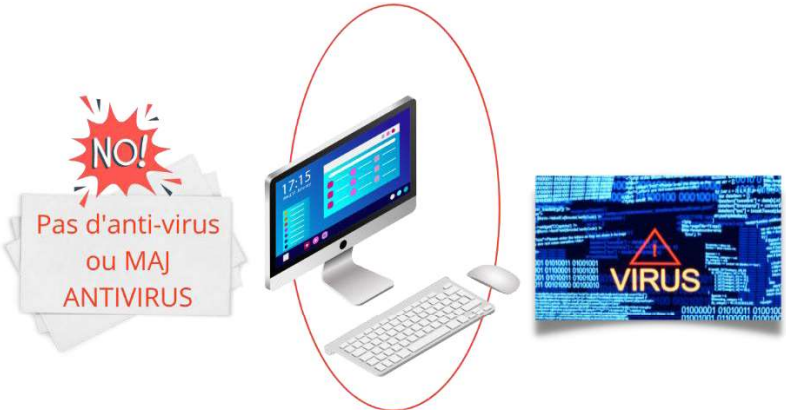
Exemple d'incident 2 : Notre ordinateur est piraté et/ou infecté par un virus

I.4.4. Menace

Une menace est une cause potentielle d'un ou plusieurs incidents, c'est tout ce qui peut exploiter une vulnérabilité sur un actif pour enfreindre la sécurité. La menace pourrait entrainer des dommages sur un actif **si elle se concrétisait.**

Notre joueur est sous la menace de blessure car il ne mange pas BIO

Notre ordinateur est sous la menace d'une infection par virus parce qu'il ne contient pas d'antivirus mis à jour.



I.4.5. Risque

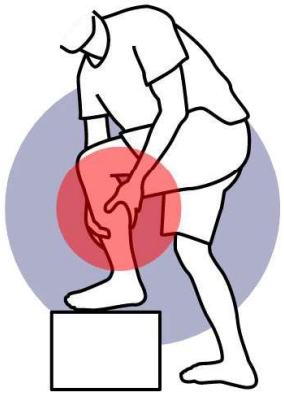
On appelle « risque de sécurité informatique », la Probabilité de voir une menace **informatique** se transformer en événement réel entraînant, par conséquence une perte.

La formule suivante permet de calculer le risque :

Risque = Menace x Vulnérabilité x Actif

I.4.6. Attaque

Il s'agit d'une action volontaire et malveillante visant à causer un dommage aux actifs. C'est la **concrétisation d'une menace**, et nécessite **l'exploitation d'une vulnérabilité.**



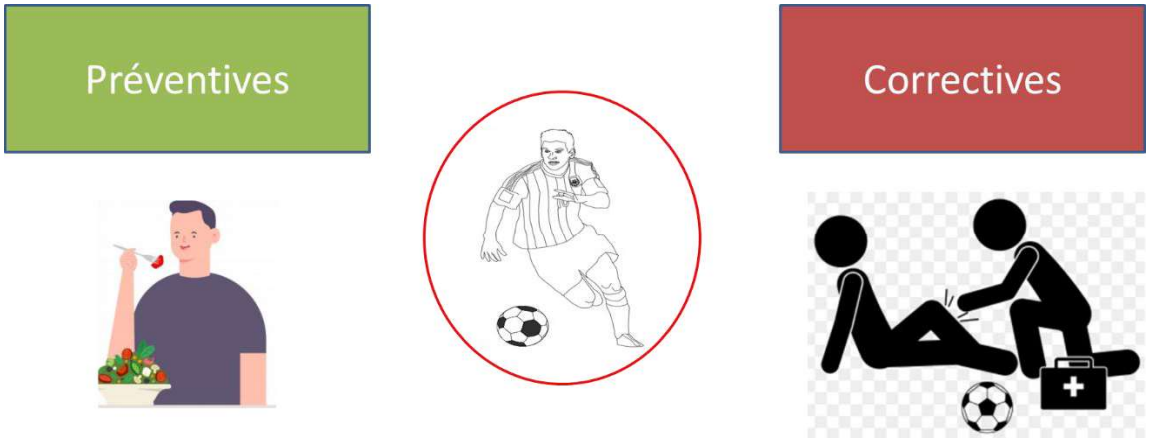
Notre joueur est blessé

Notre PC est infecté

I.4.7. Contre-mesures

Il s'agit d'un ensemble de mesures de sécurité informatique défensives prenant la forme d'une technique, d'un dispositif, d'une procédure, et dont le but est de s'opposer à un incident, de contrer une attaque pouvant porter atteinte aux actifs d'une entreprise.

On distingue deux types de contre mesure : Préventives et correctives. Les deux schémas illustrent la différence entre les deux types :



Inciter notre joueur à manger BIO est une mesure préventive, alors que le soigner après blessure est une mesure corrective.

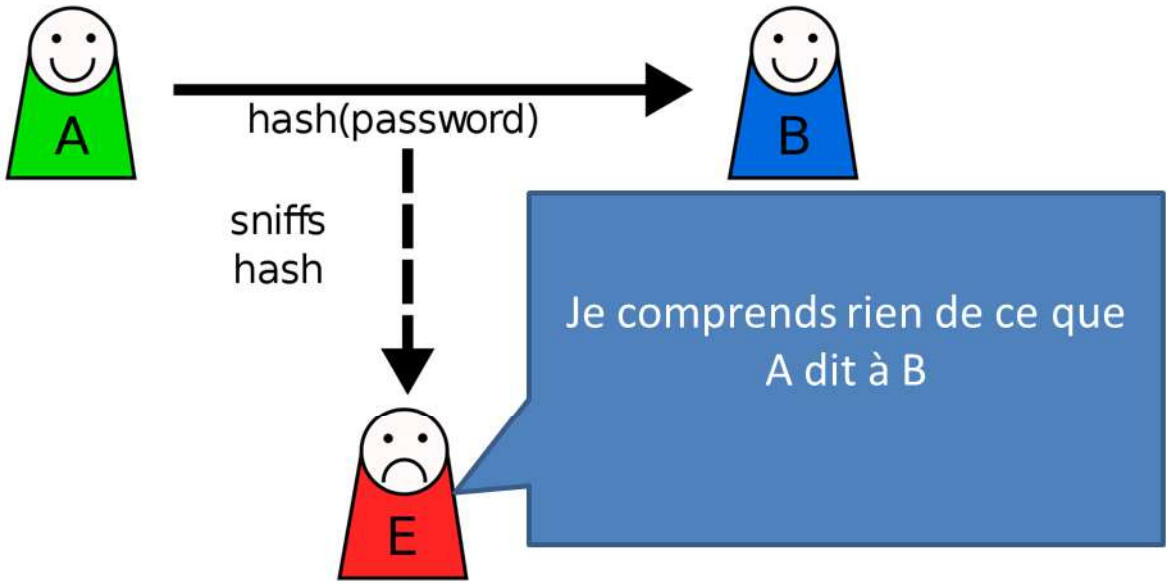
De la même façon, mettre à jour un antivirus sur un pc avant incident est une mesure préventive, alors que rétablir l'état normal d'un PC après l'avoir piraté est une mesure corrective.

I.5. Exigences fondamentales et objectifs de la sécurité informatique

L'objectif de cette section est de montrer à quoi s'attendent les utilisateurs des systèmes informatiques quant à la sécurité.

I.5.1. La confidentialité

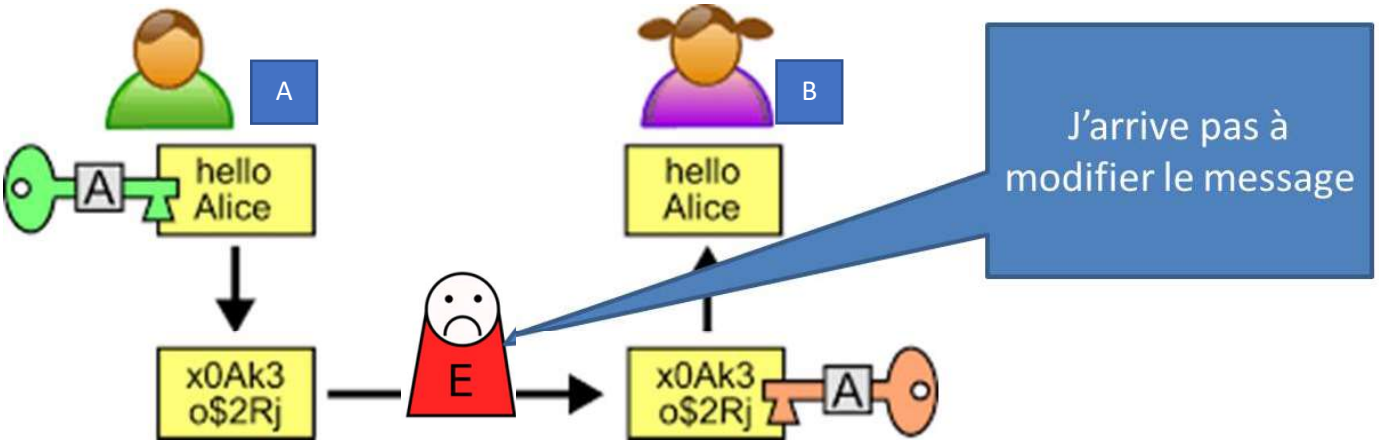
Il est question d'assurer que seules les personnes autorisées aient accès aux ressources (actifs) échangées.



Dans l'exemple du schéma, l'entité A envoie une information à l'entité B on dit que l'information est confidentielle, si cette dernière est lisible uniquement par les entités ayant les autorisations de lecture (le cas de l'entité B). L'utilisateur E ne pourra pas lire l'information confidentielle puisqu'elle ne dispose pas des autorisations nécessaires. En sécurité informatique, les techniques de cryptographie symétriques et asymétriques permettent d'assurer la confidentialité des données.

I.5.2. L'intégrité

Le but est de garantir que les données sont bien celles que l'on croit être. L'information ne doit pas être modifiée entre sa création et son traitement (ou transfert)

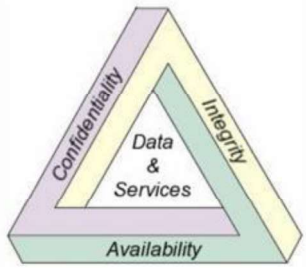


Dans cet exemple du schéma, si l'entité A envoie le message 'hello alice' à l'entité B, le message reçu par B doit être le même sans modification au cours de son transfert. De même, une information stockée dans une base de données ne doit être modifiée que par les utilisateurs ayant le privilège de modification. L'intégrité est assurée entre autres par les signatures numériques.

I.5.3. Disponibilité

Assurer le principe de disponibilité signifie que l'information doit toujours être accessible et ne peut être bloquée/perdue quel que soit les circonstances (piratage, incident naturel, panne matériel...). Cela permet de maintenir le bon fonctionnement du système d'information. Un serveur web d'une entreprise doit toujours être accessible même s'il est victime d'une attaque informatique, il faut donc prévoir des systèmes de duplication, de redondance et/ou déployer des serveurs miroirs.

Les trois premiers principes représentent les objectifs de base de la sécurité informatique, ils sont appelés le triangle CIA pour Confidentiality, Integrity et Availability. Le modèle CIA a été proposé en 1987, La plupart des autres modèles utilisent cette représentation en tant que base.



I.5.4. Non répudiation

Il faut garantir qu'une transaction ne peut être niée, c'est-à-dire mettre en place des systèmes de traçabilité permettant d'associer une action a son propriétaire.

Après avoir retiré de l'argent à la banque, le client de la banque du schéma ne doit pas pouvoir nier cette action. La banque doit pouvoir prouver que cet utilisateur (et pas un autre) a effectivement retiré la somme d'argent.

I.5.5. Authentification

De manière générale, l'authentification consiste à assurer que seules les personnes autorisées aient accès aux ressources. Pour mieux définir ce principe/objectif de sécurité, nous allons aborder cette section par étapes :

Pour permettre l'accès à une ressource ou un actif (une information, une porte sécurisée, une base de données, …), la personne souhaitant avoir accès à notre ressource doit répondre aux exigences suivantes par ordre de priorité :

1. **Qui êtes-vous** ? On appelle ça **l'identification,** c'est comme saisir un nom d'utilisateur au niveau d'un formulaire.
2. **Prouvez-le** ! c'est ce qu'on appelle l'**authentification** (exemple : saisir un mot de passe)
3. **Avez-vous les droits pour accéder à cette ressource** ? ce qu'on appelle avoir l'autorisation ou le privilège.

En poste accès à la ressource, ces trois définitions peuvent être complétées par l'audit, ce qui revient à répondre à la question : **Qu'avez-vous fait** ?

L'authentification permet donc en partie de prouver que c'est la bonne personne qui interagit avec notre actif. Prouver l'identité d'une personne peut se faire de multiples façons :

Par ce que sais la personne et ne connaissent pas les autres : mot de passe, code PIN, etc.

Par ce que possède la personne et ne possèdent pas les autres : carte magnétique.

Par ce qu'est la personne et ne sont pas les autres : empreintes digitales, réseau rétinien, reconnaissance faciale, etc.

On parle d'une authentification forte quand on combine deux de ces trois facteurs.

I.5.6. Respect de la vie privée (informatique et liberté)

Appelé aussi la liberté d'expression ou la protection des données personnelles, toute personne a droit au respect de sa vie privée, on peut voir cet objectif de sécurité (qui concerne surtout les personnes) sous différents formes :

- **La protection du droit à l'image** : exemple : ne pas diffuser les photos d'une personne sans son autorisation
- **Le secret professionnel et médical** : exemple : ne pas divulguer le dossier patient sans son accord
- **La protection du domicile**
- **La protection de l'intimité**

I.5.6. Autres principes/objectifs et modèles de sécurité

D'autres objectifs de sécurité plus avancés comme 'Admissibilité', 'Utilité' et d'autres modèles de sécurité informatique seront abordés dans le prochain polycopié, traitant principalement des attaques ainsi que la protection des systèmes informatiques

I.6. Les métiers de la sécurité informatique

On distingue principalement trois profils professionnels en sécurité informatique :

I.6.1. Débuter en sécurité de l'information

Il travaille comme assistant d'un responsable de la sécurité des systèmes d'information, son salaire est autours de 32 000 euros par an, l'équivalent de 3000 euros par mois

I.6.2. Responsable de la sécurité des systèmes d'information

ou RSSI Il propose une politique de sécurité de l'information de son entreprise. Il est responsable de la protection de sa société contre les risques relatifs aux cyberattaques. Il touche environs 70 000 euros par an, donc 6000 euros/mois.

I.6.3. Consultant en cyber sécurité

Etant expérimenté et ayant des certifications internationales dans le domaine, il pourra créer sa propre société et sera solliciter par plusieurs entreprise pour leur proposer des solutions de sécurité de leurs systèmes d'informations. Il peut faire des bénéfices de 600 € la journée, ou 18000/mois, voir plus !

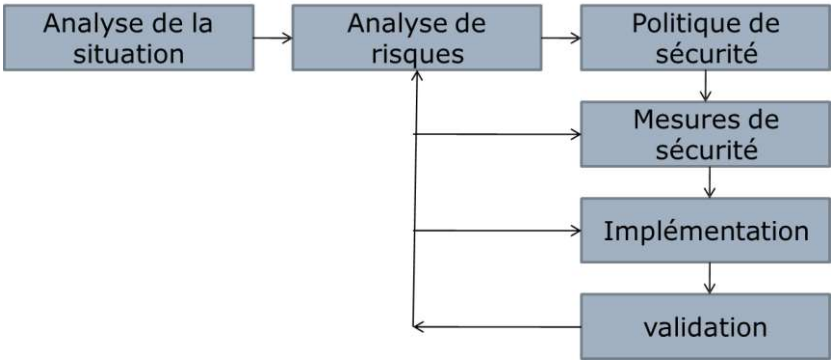
I.6.4. Autres métiers

Selon le besoin et la dimension des entreprises, on peut avoir d'autres profils relatifs au domaine de la sécurité informatique comme :

- Directeur de sécurité informatique
- Chef de projet de sécurité
- Architecte de sécurité
- Cryptologue
- Auditeur de sécurité
- Administrateur de solutions de sécurité
- Formateur en cybersécurité
- Développeur de solutions de sécurité
- Intégrateur de solutions de sécurité
- Chercheur en sécurité des systèmes d'information
- Gestionnaire de crise de sécurité informatique
- Analyste de menace et risque de sécurité informatique
- …

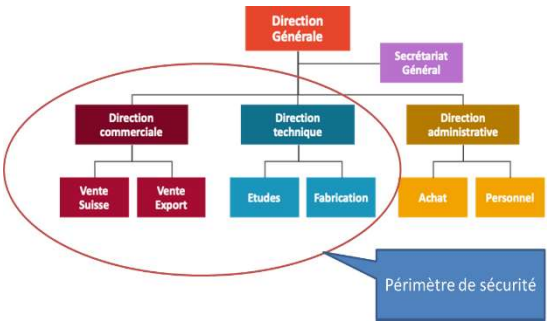
I.7. Processus de sécurisation d'un système d'information

Tout consultant ou responsable de la sécurité d'un système d'information (RSSI) doit suivre et apprendre par cœur les étapes du schéma suivant :



I.7.1. Analyse de la situation

Le responsable de la sécurité informatique (RSSI) commence par identifier le contexte, ou le périmètre du système à sécuriser. Le RSSI doit définir la frontière du système d'information qu'il doit protéger et que, au-delà, il n'est pas responsable de ce qui se passerait en dehors de son périmètre.



Cette étape ressemble au ruban utilisé par la police pour encercler une scène de crime.

I.7.2. Analyse des risques

Cette étape est la plus importante dans le processus, elle consiste à identifier les problèmes potentiels avec les solutions et les coûts associés. Le but étant d'obtenir la liste de ce qui doit être protégé (les actifs). Avant de se lancer dans la phase d'analyse de risques, il faut tenir en comptes les challenges suivants :

- L'augmentation du nombre d'utilisateurs sur Internet.
- L'augmentation, la diversité et l'apparition de nouvelles attaques.
- Les failles des technologies.
- Les failles des configurations et les problèmes des mauvaises installations des logiciels.
- Les failles des politiques de sécurité elles-mêmes.
- Le changement fréquent des profils des pirates.

Le responsable de sécurité doit faire le tour de l'entreprise et essaye d'avoir des réponses à certaines questions dont :

- Quelle est la valeur des équipements, des programmes et particulièrement des données à protéger ?
- Quel est le prix et le temps de leur remplacement ?
- Quel est l'impact sur la clientèle d'une intrusion sur les machines du périmètre de sécurité de la société ? quelle sont les conséquences d'une attaque sur le système d'information des clients suite à des attaques réussites sur la société.

Bien sûr il faut faire une analyse de vulnérabilité sur les équipements en réseau (programmes, données, analyse des paquets, logs…). Il faut cependant ne pas négliger les risques suivants :

- Un câble arraché
- Une coupure du secteur
- Le crash d'un disque de stockage

I.7.2.1. Processus d'analyse de risques

L'une des méthodes d'analyse des risques propose les étapes suivantes :

- Faire un inventaire des actifs
- Faire un inventaire des menaces (incidents) possibles sur ces actifs
- Estimer la probabilité/fréquence que ces menaces se concrétisent
- Estimer les couts relatifs à chaque incident

Il s'agit de remplir le tableau suivant :

	Cout cher	Cout faible
Incidents fréquent	Incident Incident Incident …	Incident Incident Incident …
Incidents rare	Incident Incident Incident …	Incident Incident Incident …

I.7.3. Politique de sécurité

La sécurité informatique est comme une chaîne, son niveau de protection est égale son maillon le plus faible.

Ainsi, une porte blindée d'une maison est inutile si les fenêtres sont ouvertes sur la rue. Une politique de sécurité vise donc à définir « **de façon cohérente** » les méthodes de protection à mettre en œuvre.

Après l'étape d'analyse **des risques** et avant de mettre en place des **mécanismes de protection**, il faut préparer une politique à l'égard de la sécurité.il faut proposer un ensemble des solutions qui doit être organisé sous forme d'une politique de sécurité cohérente, en fonction du seuil de tolérance au risque.

Rappelez-vous du tableau précédent d'analyse de risque, il est question maintenant de le remplir comme suit :

	Incident à cout cher	Incident à cout faible
Incident fréquent	**Mettre en place des mécanismes de sécurité** **Mesures techniques** • FireWall, • Antivirus, • IDS,... **Mesures Organisationnelles** • Procédure de secours, • Nomination responsable sécurité, • Formation des utilisateurs,…	Assurer la disponibilité des services : (déployer des serveurs miroirs. Duplication des données, etc)
Incident rare	S'assurer que les incidents sont toujours rares en faisant des vérifications périodiques	Accepter les risques

Le risque « **zéro** » n'existe pas, dont la case « Accepter les risques », il est question de définir le risque résiduel que l'on est prêt à accepter, le risque à accepter doit avoir des conséquences minimes et une fréquence d'apparition très rare.

En résumé, Après avoir identifié les risques et leurs conséquences, la politique de sécurité consiste à :

- Déterminer des règles et des procédures à mettre en place pour les risques identifiés.
- Vigilance et veille technologique sur les vulnérabilités découvertes.
- Actions à entamer et individus à contacter en cas d'incident détecté.

I.7.3.1. Structuration de la politique de sécurité

La politique de sécurité peut être structurée en plusieurs dossiers dont :

Formation et sensibilisation permanente des utilisateurs du système d'information pour éviter l'erreur humaine

Défaillance matérielle (vieillissement des équipements, défauts…)

Défaillance logicielle (bugs, problèmes de mises à jour…)

Accidents (pannes, incendies, inondations…)

Contrôle d'accès aux ressources : Vol via des supports de stockage physiques

Programmes malveillants dans les disques

Piratage (c'est le plus difficile à cerner)

I.7.4. Mesures de sécurité

Cette partie consiste à définir l'ensemble des mesures « techniques » et/ou « organisationnelles » qui vont permettre d'appliquer la politique de sécurité.

I.7.5. Implémentation

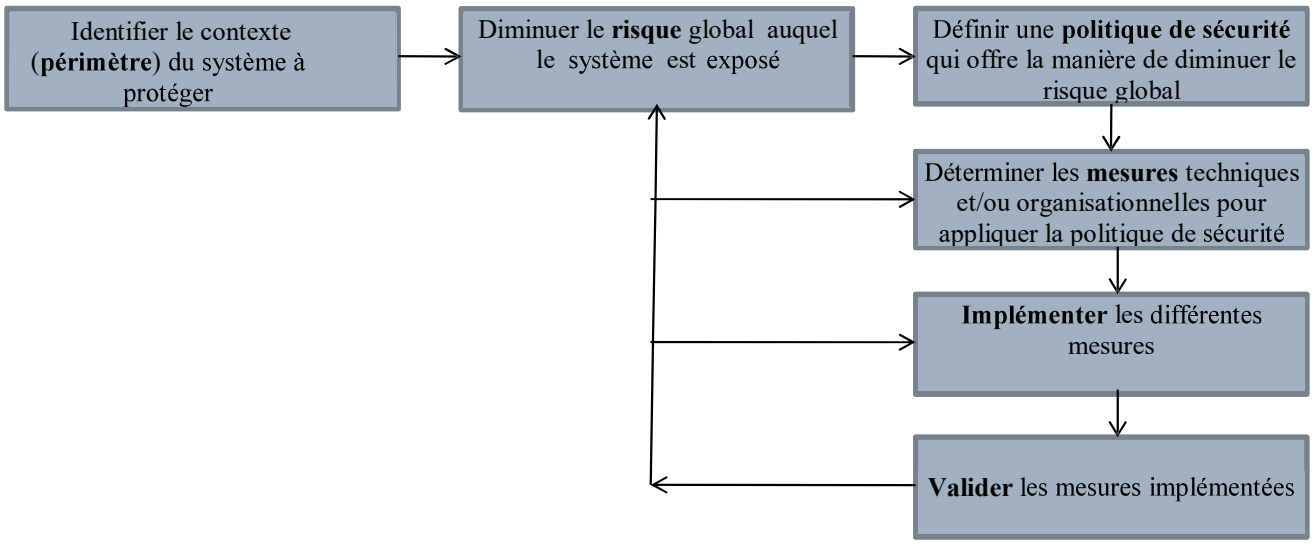
L'installation et l'implémentation des différentes mesures se fait durant cette phase. Pour les mesures techniques, il faut avoir les compétences techniques nécessaires

I.7.6. Validation

C'est l'étape de validation des mesures déployées dans le but de vérifier qu'elles offrent la protection voulue (scans de vulnérabilité, tests d'intrusion, etc…). C'est la phase d'audit, le but étant de vérifier que chaque règle de la politique de sécurité est bien appliquée et que l'ensemble des mesures prises forme un tout cohérent.

Si l'entreprise ne dispose pas des compétences nécessaires, elle peut s'appuyer sur une entité tierce de confiance (entreprise spécialisée en sécurité informatique) pour valider les méthodes de protection mises en œuvre, au regard de la politique de sécurité.

Après avoir expliqué chaque étape, notre schéma deviendra comme suit :



I.8. Principaux défauts de sécurité

Il faut noter que les principaux défauts de sécurité restent :

- L'installation par défaut des logiciels et des équipements.
- L'absence de stratégie de mise à jour des logiciels et des équipements.
- L'utilisation de mots de passe par défaut ou complètement inexistants (Authentification faible), surtout pour accéder à des services critiques tels que la télémaintenance
- Laisser fonctionnels des services inutiles.
- La non prise en considération par l'administrateur réseau des fichiers journaux (fichiers logs)
- Le déploiement de politiques de sécurité obsolètes.

TD1. Travaux dirigés du chapitre I

TD1.1. Questions QCM

Cocher une, aucune ou plusieurs bonnes réponses

1. L'analyse de la situation lors de l'analyse de risque permet de :
   - Définir un périmètre de sécurité
   - Définir le contexte de la politique de sécurité
   - Définir les éléments du système à protéger
   - Faire un audit de sécurité

2. L'analyse de risque permet de :
   - Mesurer la fréquence d'apparition des incidents
   - Installer des systèmes contre les risques identifiés
   - Préparer une politique de sécurité
   - Faire des audits de sécurité.

3. Le respect de la vie privée permet de :
   - Assurer l'anonymat des utilisateurs
   - Assurer l'authentification des utilisateurs
   - Assurer la confidentialité des informations des utilisateurs
   - Assurer la non répudiation

4. Le rôle de la sécurité en entreprise est :
   - Réduire le risque à un niveau acceptable
   - Prévenir tout risque
   - Empêcher les employés de travailler correctement
   - Surveiller le bon fonctionnement des systèmes

5. La politique de sécurité permet de :
   - De répondre aux incidents de sécurité selon leur fréquence et cout
   - Installer des systèmes contre les risques identifiés
   - Préparer une analyse de situation
   - Faire des audits de sécurité.

6. La non répudiation :
   - Permet de garder la trace de qui a fait quoi
   - Permet d'assurer la vie privée des personnes
   - A besoin des signatures numériques
   - Est un objectif de sécurité

7. La politique de sécurité permet de :
   - Préparer des mécanismes de sécurité
   - Définir le contexte de la politique de sécurité
   - Définir les incidents possibles sur le système à protéger
   - Faire un audit de sécurité
   - Répondre aux incidents de sécurité selon leur fréquence et cout

8. Quand on a un risque à cout faible mais à haute fréquence :
   - On installe des serveurs miroirs
   - On accepte le risque
   - On installe des mécanismes de sécurité
   - On tente d'assurer la disponibilité des données et des services

TD1.1. Exercices

Exercice 1 « Méthode d'analyse de risque »

La banque WDZ subit chaque année six infections par des malwares (virus, vers….) et quatre déformations de son site internet. La restauration du bon état des machines âpres une infection requiert deux jours de travail à l'administrateur, avec un cout de 200 000 DZD. Le design du site internet peut être réparé en 06 heures, avec un cout de 100 000 DZD.

Une société tierce de sécurité informatique propose le déploiement et la maintenance d'un antivirus et d'un outil de protection du site internet avec un cout annuel de 2 500 000 DZD.

1. Calculer le risque annuel

2. Est-il bénéfique pour l'entreprise WDZ d'acheter la solution proposée par la société tierce ? Pourquoi ?

Exercice 2 « questions sur la sécurité des systèmes d'information»

1. Pourquoi le niveau réel de sécurité d'un système d'information est toujours inferieur au niveau estimé par un RSSI ?

2. Décrire le genre de mesures à prendre pour éviter une baisse du niveau de sécurité.

3. Les systèmes d'information des entreprises sont plus exposés aux attaques informatiques aujourd'hui, donner quelques raisons ?

4. On souhaite sécuriser l'accès des personnes à une entreprise, donnez les différentes méthodes à utiliser pour avoir des systèmes d'authentification efficaces.

5. Expliquez l'impact des réseaux sociaux (Facebook, twitter, etc.) sur la sécurité des systèmes d'information des entreprises.

Exercice 3 « Etapes de sécurisation des systèmes d'information »

Remplir le tableau ci-dessous par les actions suivantes

Analyse de la situation	Analyse de risque	Politique de sécurité	Mesures de sécurité	Implémentation	Validation

1. Essayer de pirate ma propre politique de sécurité.
2. Le serveur Web tombe fréquemment en panne il faut prévoir une redondance
3. Recruter un ingénieur en sécurité informatique
4. Installer un système de détection d'intrusion
5. Déterminer le périmètre du système à protéger
6. Le serveur web tourne sur une vielle machine avec une alimentation faible
7. Recruter un administrateur réseau compètent
8. Installer un antivirus
9. Le serveur web tourne sur une vielle machine
10. Tester les vulnérabilités du système de sécurité mis en place.
11. Le serveur ftp tombe fréquemment en panne il faut prévoir une redondance

Exercice 4 « Objectifs de sécurité »

2. Pour chaque risque ci-dessous, fournissez les vulnérabilités et montrez s'il s'agit d'un problème de confidentialité (**C**), d'intégrité (**I**) ou de disponibilité (**D**)

Risque	Vulnérabilité	C	I	D
Certains employés se connectent à internet avec leurs smartphone via le réseau de l'entreprise				
Le vice-président de la comptabilité est recruté par un concurrent				
L'entreprise envoie des données sans signatures numériques				
L'administrateur réseau de l'entreprise travail comme consultant chez un concurrent				
Certains utilisateurs utilisent leurs PCs portable personnels dans l'entreprise				
Certains utilisateurs insèrent leurs clés USB non scannées dans les PCs de l'entreprise				
L'entreprise utilise un mot de passe par défaut pour accéder à ses applications de gestion.				

Partie II : Terminologie des attaques

Cette partie du manuscrit décrit un ensemble de termes utilisés dans le jargon des attaques informatiques, ceci est un passage obligatoire pour comprendre le reste du document.

II.1. Menaces accidentelles vs menaces intentionnelles

Les attaques accidentelles ne supposent aucune préméditation. Il s'agit de défaillances "incontrôlables" survenues au sein d'une organisation.

Exemple :

- Les Bugs logiciels et
- Les pannes matérielles suite à des incidents naturels ou vieillissement des actifs

Par contre, les attaques intentionnelles reposent sur l'action d'une entité tierce désirant s'introduire merveilleusement et relever des informations sensibles de notre périmètre de sécurité.

Exemple :

- Accéder à une base de données sans autorisation
- Bloquer le fonctionnement d'un serveur web d'une entreprise

II.2. Attaques actives vs attaques passives

Dans une attaque passive, l'entité malveillante va essayer de détourner les données par audit. L'entité ne modifie pas les données, ni n'altère les systèmes : Écoute des lignes de communication, Analyse de trafic réseaux,…etc, ce qui rend sa détection relativement délicate. Les attaques passives sont plus faciles avec les réseaux sans fil. Pour contrer ce type d'attaques, il faut assurer la confidentialité des informations stockées et circulant au sein d'un système de communication.

Une attaque passive est généralement une préparation d'une attaque active.

Dans ce type d'attaques, l'intrus modifie volontairement les données et/ou le système en place pour s'en emparer, l'attaquant pourra :

- **Détruire** des messages
- **Injecter** des messages erronés
- **Modifier** des messages et **usurper l'identité** d'un équipement ou utilisateur.

La détection d'une attaque active est facilitée, cependant, il peut être déjà trop tard lorsque l'attaque a lieu.

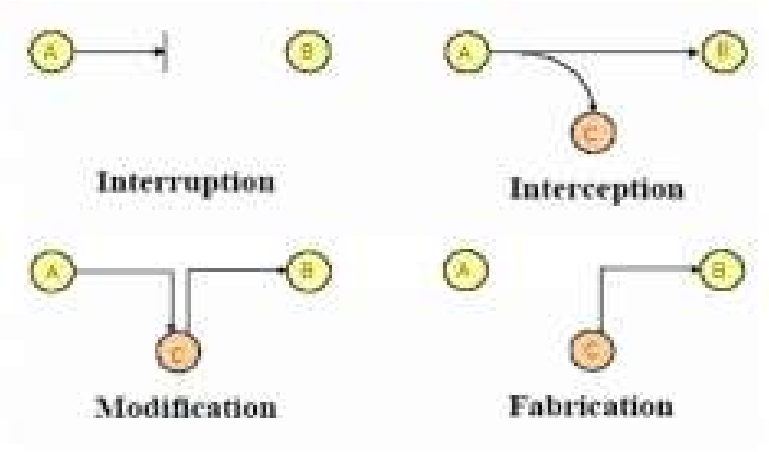
En plus de la confidentialité, pour contrer ce type d'attaques, il faut assurer les autres objectifs de sécurité tels que la disponibilité, l'intégrité, l'authentification et la non répudiation.

II.3. Attaque par Interruption, Interception, Modification et Fabrication

Se sont toutes des attaques actives, c'est l'objectif de l'attaquant qui est différent.

II.3.1. Attaque par Interruption

Cette attaque vise à bloquer la cible (serveur, service, routeur, switch,…), elle engendre des problèmes liés à la disponibilité des données.



II.3.2. Attaque par Interception

La partie malveillante s'attaque à la confidentialité des données, en essayant d'avoir accès à des informations sans posséder les autorisations nécessaires.

II.3.3. Attaque par modification

Dans cette partie, c'est l'intégrité des données qui est menacée, l'utilisateur malveillant tente de modifier des données de façon illégale.

II.3.4. Attaque par Fabrication

Un attaquant C peut fabriquer un message de données et l'envoyé à A au nom de B, c'est un problème lié à l'authenticité des données.

II.4. L'origine des attaques

La diversité des origines des attaques rend le travail des responsables de sécurité des systèmes d'information plus difficile. Ci-dessous les principales origines des attaques actuelles :

II.4.1. Les hackers vs cracker

Il est important de faire la distinction entre ces deux appellations : un hacker fait partie d'une communauté de programmeurs expérimentés et des experts en réseaux et système. Ces personnes sont généralement discrètes, anti-autoritaristes, motivés par la curiosité et il participe même au renforcement de la sécurité des systèmes d'information.

Par contre, le cracker sont des personnes qui s'autoproclament des "hackers", mais qui s'introduisant à distance dans les systèmes informatiques sans avoir les privilèges nécessaires. Les crackers utilisent des outils écrits par d'autres personnes (trouvés sur Internet) pour s'introduire illégalement dans des systèmes informatiques cibles.

II.4.2. Les concurrents industriels

Les entreprises concurrentes pour augmenter leurs chiffres d'affaires peuvent procéder au vol d'informations concernant la stratégie de l'entreprise cible ou sa conception des projets. Comme nous allons le développer par la suite dans le prochain manuscrit, certaines entreprises louent des spammeur qui utilisent des réseaux de botnets pour faire mal à leurs concurrents.

II.4.3. Les espions

La presse est le premier suspect d'un espionnage électronique, le but est de récolter des informations confidentielles, puis de faire le buzz en étant le premier à divulguer de telles informations.

II.5. Objectifs des attaques

La connaissance de l'objectif d'un attaquant est très importante pour proposer la bonne politique de sécurité, ci-dessous quelques-uns :

- **Diffuser de fausses informations**

Par exemple un attaquant peut diffuser de fausses mauvaises informations sur un candidat à des élections pour favoriser son adversaire

- **Éviter l'accès à une ressource**

L'attaquant bloque l'accès à un actif (serveur, routeur, switch, données,…) pour faire du chantage à la victime ou bien favoriser le concurrent de la victime. Ces attaque sont appelées déni de service « DOS »

- **Contrôler illégalement une ressource à distance**

Là aussi le pirate peut prendre le contrôle d'une machine à distance puis bénéficier de tous les privilèges accordés à cette machine.

- **Récupérer des données confidentielles présentes sur un système**

Ces données peuvent être financières ou militaires

- **Utiliser des machines infectées pour en attaquer d'autres**

Le pirate à travers cet objectif, pourra prendre le contrôle de plusieurs machines sur internet sans exécuter d'attaques actives sur ces victimes. Il va utiliser ces machines cependant pour construire ce qu'on appelle un réseau de « botnets » ou réseau de zombies. Ce réseau informatique spécial est constitué de plusieurs machines compromises et contrôlées pas un attaquant, il utilisera ces machines en même temps pour s'attaquer à des ressources critiques sur internet. Le pirate pourra, par conséquence, construire un super ordinateur qui décryptera des données chiffrées avec des algorithmes solides, ou effectuer des attaques de Déni de service distribué (DDOS). Les détails techniques des réseaux de botnets et des attaques DDOS seront développés dans le prochain manuscrit.

II.6. Motivations des attaques

Les pirate informatiques sont motivés par l'un ou plusieurs des objectifs ci-dessous :

- Vol de données (vol d'un mot de passe d'un réseau wifi par exemple)
- Modifications illégale de données (augmenter illégalement le montant de son compte bancaire)
- Vengeance/rancune
- Politique/religion
- Défis intellectuels
- …etc

II.7. Cible des pirates

Parmi les cibles des pirates aujourd'hui, on trouve :

- Les états
- Les Serveurs militaires
- Les Banques
- Les Universités

Sinon tout le monde peut être une cible d'attaques que le pirate utilise pour en faire des botnets

II.8. Nœud malicieux

Dans un réseau de communication, un nœud malicieux est une entité malicieuse qui commence par exécuter une attaque passive puis lance une attaque active.

II.9. Attaquant actif-n-m

Un attaquant actif-n-m est un nœud malicieux qui possède m nœuds au sein d'un réseau de communication avec lesquels il va compromettre n autres nœuds victimes

II.10. Attaque externe

C'est une attaque lancée de l'extérieur du périmètre de sécurité. Le nœud malicieux n'appartient pas au réseau ou bien qu'il n'est pas autorisé à y accéder.

II.11. Attaque interne

C'est des attaques lancées de l'intérieur du périmètre de sécurité. Le nœud malicieux peut être dans le périmètre ou contrôle une machine à distance qui se trouve à l'intérieur. C'est le type de menaces le plus délicat par ce que les systèmes de protection proposés pour contrer les attaques externes sont inefficaces devant ce type d'attaques.

II.12. Les états d'insécurité

II.12.1. L'état actif d'insécurité

C'est un état dans lequel l'utilisateur ne connaît pas les fonctionnalités de son système, donc il risque de ne pas désactiver des services réseaux non nécessaires et suspects,

Exemple : l'administrateur ne désactive pas les protocoles P2P dans son entreprise.

II.12.2. L'état passif d'insécurité

C'est un état dans lequel l'utilisateur ne connait pas les moyens de sécurité à sa disposition,

Exemple : L'administrateur ne connaît pas l'existence d'un pare-feu réseau au sein de son entreprise.

TD2. Travaux dirigés du chapitre II

Exercice 1 : « QCM rapide »

1. Une attaque passive :
   - Consiste à briser l'intégrité des messages
   - Consiste à effectuer une attaque DOS
   - Consiste à effectuer une attaque d'espionnage
   - Consiste à effectuer une attaque visant la confidentialité

2. Une attaque de déni de service consiste à :
   - Refuser l'accès d'un client à un serveur en se faisant passer par ce dernier
   - Empêcher les utilisations légitimes d'avoir accès à un système
   - Casser la clé de chiffrement d'un échange de données
   - Utiliser une erreur de programmation dans un système donné pour le compromettre

3. Quels sont les problèmes de sécurité relatifs à une attaque par interruption
   - Déni de service
   - Fabriquer de faux message d'erreur
   - Modifier illégalement la clé du réseau wifi
   - Vol de mot de passe

Exercice 2 : « Questions de compréhension »

1. Donnez la définition, avec un exemple d'attaque en réalité de chaque catégorie : Interruption, interception, modification et fabrication.

3. Donnez et expliquez deux exemples d'attaques passives et actives.

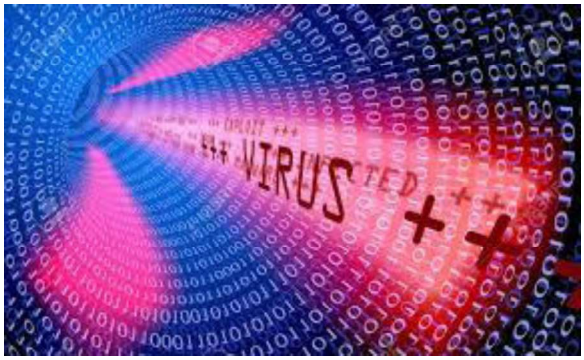
4. Comment assurer le principe de la disponibilité ?

5. Donner deux exemples d'attaques par interruption

Partie III : Les malwares

Par analogie aux virus ciblant les humains et détruisent son système immunitaire petit à petit, les malwares informatiques adoptent la même stratégie et peuvent causer des dégâts irréparables sur les équipements et les données des victimes. Dans cette partie, nous allons développer les différents types de malwares face à qui on doit protéger nos systèmes d'informations et nos données personnelles

III.1. Virus



Un virus est une portion de code inoffensive ou destructrice qui se reproduit et se propage grâce à d'autres programmes. Ces malwares se propagent de plusieurs manières :

- Échange de supports de stockage : clés USB, disques,…etc.
- Pièces jointes au courrier électronique
- Exécutables récupérés sur Internet
- …

On distingue aussi plusieurs types de virus

III.1. 1. Virus de boot

C'est des virus cachés dans la partition de démarrage d'une machine, ce qui rend leur détection très difficile par l'antivirus installé sur des systèmes d'exploitation ; d'où la recommandation de désinfecter ces machines par un antivirus de démarrage.

III.1. 2. Virus dissimulé dans les exécutables

C'est des virus cachés dans le jeu d'instructions de certains exécutables.

III.1.3. Virus furtifs

Ce malware modifie la routine du système d'exploitation pour la lecture des fichiers. Il montre une image du système exactement similaire à ce qu'il était avant l'infection. Les fichiers infectés se présentent comme sains. Il est conçu de sorte à échapper à l'antivirus installé sur le système d'exploitation (lui-même infecté). Dans certaines de ses versions, il se sépare temporairement du fichier infecté, se copie sur un autre espace de stockage et se remplace par un fichier sain. Ce malware passe aussi inaperçu par ce qu'il cache la taille réelle du fichier qu'il a infecté.

La détection d'un virus furtif se fait en démarrant la machine à partir d'un disque de démarrage contenant un antivirus (sans passer par le système d'exploitation de la machine puisque lui-même est infecté par ce malware) puis scanner la machine.

On appelle charge utile d'un malware, sa partie active qui a comme rôle d'accomplir les tâches assignées à ce malware

III.1. 4. Virus polymorphes

C'est un virus qui change son code source et la manière de changer son code après chaque infection, ils prennent donc une autre forme chaque fois qu'ils infectent. Ce malware se crypte de différentes façons pour rester indétectables. Son corps est composé de deux portions : une qui change d'apparence à chaque fois et qui est chiffré avec une routine de chiffrement variable qui se modifie à chaque duplication et une pour les déchiffrements.

En résumé les algorithmes du virus polymorphes ne sont pas modifiés, mais leur traduction en code-machine l'est.

Ce malware contient un moteur de cryptage et de décryptage pour faire varier son code. Ce moteur est un point faible d'un virus polymorphes puisque il représente une zone de code qui ne varie pas, donc utilisée par certain antivirus comme signature. Pour cela, les concepteurs des nouveaux virus utilisent une nouvelle catégorie spécifique appelée virus métamorphes dans laquelle tout le jeu d'instruction du virus est modifiable. Le virus métamorphes modifie sa structure interne et les instructions qui le composent ; il ne dispose pas de moteur de decryptage ni d'un code source viral constant, cependant il est capable de créer de nouvelles générations de lui-même différentes à chaque réplication en évitant qu'une génération soit trop semblable avec celle qui la précède.

Les virus polymorphes et les virus furtifs sont appelés parfois 'virus indétectables'

III.2. Vers

Contrairement aux virus, les vers sont des programmes malveillants autonomes. Leurs points forts et leur capacité à se déplacer librement à travers les réseaux de communication, sans être

collés à un programme exécutable sain (ou un fichier "support"). Un ver se duplique une fois qu'il a été exécuté, il peut causer les incidents suivants :

- Espionner et/ou supprimer des données utiles sur la machine de la victime dans laquelle il s'est exécuté ;
- Saturer un serveur web en lui envoyant des requêtes répétées
- Supprimer des données utiles sur la machine de la victime
- Créer un accès distant caché à la machine de la victime

Ainsi, les vers peuvent avoir les formes suivantes

- **Scripts** : intégrés dans un système de messagerie, une page html, …etc.
- **Des programmes** : C, C++, assembleur, etc.

III.2.1. Les familles de vers

On distingue plusieurs types de vers :

III.2.1.1. Les Vers poste à poste (P2P)

Ils se propagent via les dossiers partagés ou à travers les protocoles P2P, sous forme d'un fichier .torrent par exemple.

III.2.1.2. Les vers de la messagerie électronique

Il se propage soit comme des pièces jointes ou des liens hypertexte vers ce malware.

III.2.1.3. Les vers des messageries instantanées

Ce type de vers utilisent les logiciels de messagerie instantanée comme Skype, Messenger,… pour se propager, la victime reçoit un lien vers un serveur web contenant un ver, une fois exécuter sur la machine de la victime, une copie du ver est envoyée à tous les contacts de la victime

III.2.1.4. Les vers se propageant à travers les supports de stockage

Les clés USB, les disques durs externes sont tous un support de transmission efficace de ce malware, il profite aussi du démarrage automatique de ces outils de stockage mobiles pour s'exécuter automatiquement sur la machine victime ayant inséré ces supports de stockage.

III.3. Cheval de Troie, troyen, trojan horse, trojan

C'est un programme avec une apparence légitime, mais qui cache des instructions malveillante. Dans la plupart des cas, le cheval de Troie fait pénétrer un intrus sur la machine de la victime ayant installé le programme. Il faut se fier du live streaming illégal et les logiciels crackés qui hébergent souvent ce type de malwares. Certaines institutions juridiques utilisent les cheveux de trois de manière légale dans le cadre d'enquêtes. Un cheval de Troie est donc uniquement le véhicule d'un programme malveillant qui peut être :

- Virus,
- Keylogger (espion du clavier)
- Screenlogger (espion d'ecran)
- logiciel espion en générale
- Un logiciel de publicité illégale

III.4. Porte dérobée

La réussite d'un cheval de Troie cause souvent la création d'une porte dérobée sur l'ordinateur de la victime. Une porte dérobée est un accès caché à l'ordinateur de la victime, cette machine deviendra accessible illégalement à distance. La taille de ce malware est un paramètre important de sa réussite : plus il est petit, plus il est facile à installer et difficile à détecter. Techniquement, il s'agit d'un port ouvert et en attente sur TCP ou UDP prédéfini. Le malware est introduit parfois volontairement par le développeur d'un programme.

Parmi les objectifs de ce malware, on cite :

- La surveillance des activités de l'utilisateur victime

- La suppression des informations d'authentification de la victime : mots de passes, clés secrètes, …
- La prise de contrôle à distance de l'appareil de la victime pour en faire une base d'attaque, cette base sera utilisée pour :
    - Envoyer des spam à d'autres victimes à partir de la machine contrôlée
    - Injecter des virus
    - Effectuer des dénis de services

Si le pirate arrive à contrôler plusieurs machines à distance, il pourra créer son propre réseau de botnets, avec lequel il effectuera sur internet les attaques suivantes entre autres :

- Empêcher le fonctionnement de machines et/ou équipements réseaux
- Truquer des statistiques d'accès à un site internet
- Faire du marketing illégale

III.5. Rootkit

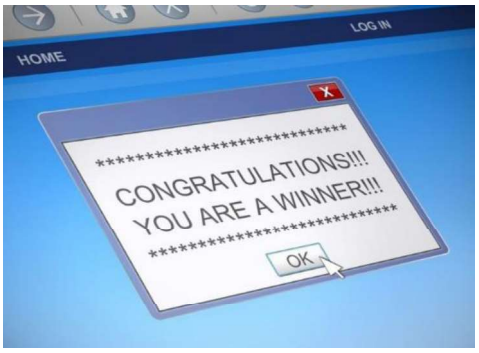
C'est un logiciel malveillant qui masque la présence d'un intrus au sein d'un périmètre de sécurité. Le pirate efface sa trace en supprimant son existence dans les fichiers logs (journaux) des serveurs. Il peut aussi implémenter des scripts pour ne pas appeler les fonctions standards du système d'exploitation qui écrivent dans les fichiers logs.

Avec ce malware, il est question de dissimuler des « processus » et/ou des « fichiers » permettant de cacher l'activité du rootkit. Sous Windows, le pirate manipule la base de registre ; alors que sous Unix, le pirate remplace « par exemple » la commande d'affichage « **ls** » de telle sorte à ne pas afficher certains fichiers du rootkit. Après son installation, ce malware supprime ses propres fichiers d'installation pour éviter d'être détecté.

III.6. Spyware

C'est un programme informatique qui transmet illégalement des données privées de la victime, Il peut modifier le comportement des navigateurs web pour exécuter cette tache malveillante. Le pirate collecte et transfère des données sur l'environnement dans lequel il s'est installé pour des raisons de statistique et/ou de détections de vulnérabilités.

III.7. Hoax



Appelé aussi canular informatique est une rumeur produite par un utilisateur puis divulgué le plus rapidement possible à d'autres personnes via lien hypertexte ou courrier électronique. Le but est d'augmenter le nombre de personnes influencées par la rumeur.

III.8. Bombes logiques

Les bombes logiques sont des malwares qui s'exécutent à un moment déterminé en exploitant principalement la date du système. Un employé avec préavis de licenciement peut programmer

des bombes logiques dans le programme qu'il a développé pour son entreprise. Le logiciel est intentionnellement conçu pour Buger après le licenciement de l'employé.

III.9. Ransomware

Un utilisateur malveillant développe un malware appelé ransomware pour chiffrer les documents confidentiels d'une entreprise (portefeuille client par exemple), puis fait du chantage en demandant à la société victime de payer une rançon en échange de la clé qui permettra de déchiffrer ces documents

La payement de la rançon peut se faire de plusieurs manières :

- Virement bancaire
- SMS surtaxés
- Bitcoin
- Via les sites de paiement en ligne

III.10. Adware

Ce malware se présente comme un programme qui affiche de la publicité à chaque fois qu'il est exécuté. Un adware est constitué de deux portions de codes

- Une portion utile (jeux, lecteur vidéo,…) qui pousse un utilisateur à l'installer sur sa machine
- Une partie qui affiche la publicité.

III.11. Autres malwares

On distingue aussi d'autres programmes malveillants dont :

Dialers : La victime paie des frais téléphoniques sans le savoir

Downloader : La victime télécharge des fichiers exécutables malveillants en arrière-plan

Droppers : Lancer un malware au démarrage de la machine, ou à l'ouverture d'un navigateur Internet

Maldocs : des documents informatiques malveillants (exemple fichiers PDF ou autres fichiers de suite bureautique)

III.12. Effet des malwares modernes

Les malwares utilisent aujourd'hui Internet pour se propager plus rapidement, Ils peuvent contaminer toutes la planète en quelques heures, voir quelques minutes. Ces programmes informatiques malveillants peuvent avoir des conséquences dramatiques dont :

- Perte de données sensibles des personnes ou des entreprises
- Perte d'image de marque d'une entreprise
- Perte de fonctionnalité (serveurs ou systèmes bloqués)
- Intrusion et/ou vol d'informations
- Perte de temps de travail
- Perte de confidentialité

TD3. Travaux dirigés du chapitre III

TD3.1. « Questions QCM »

1. Un screenlogger est :
   - Une préparation d'une attaque passive
   - Un cheval de Troie
   - Une préparation d'une porte dérobée
   - Logiciel Espion

2. Un mail de ma banque m'avertit que mon compte a été débité de 78 DZD par erreur. Pour me faire rembourser, je suis invité à cliquer sur le lien dans le message afin de confirmer mes coordonnées de compte. Quel est le piège à éviter ?
   - Je clique sur le lien et je tombe sur le site de ma banque avec les cases à remplir. Je les remplis, c'est très simple.
   - Je vais sur le site de ma banque en utilisant mes favoris dans mon navigateur pour voir ce qu'il en est.
   - Je détruis le mail sans me soucier de la mise à jour de mes données bancaires.
   - Je téléphone à ma banque et je traite cela par téléphone.

3. Mon petit frère a téléchargé un petit jeu sympa sur Internet que j'amènerais bien au bureau pour montrer aux collègues. Quelle est la meilleure attitude à adopter ?
   - Je l'amène au bureau sur une clé USB que j'ai passée à l'anti-virus à la maison.
   - Je l'amène au bureau sur une clé USB que j'ai passée à l'anti-virus au bureau.
   - Je l'amène au bureau sur une clé USB que j'ai passée à l'anti-virus à la maison ET au bureau.
   - Je ne l'amène pas au bureau.

4. Je trouve une clé USB dans ma boîte à lettres. Quelle est la meilleure action ?
   - Je la connecte à mon ordinateur pour en voir le contenu.
   - Je l'analyse avec un anti-virus, on ne sait jamais.
   - Je la jette, une clé peut contenir un virus.

5. Un virus de démarrage est :
   - Un virus qui se cache derrière le secteur MBR
   - Un virus qui se cache dans la FAT
   - Un virus qui modifie son code est la façon de changer son code
   - Une bombe logique

6. Je reçois un mail m'annonçant que je peux gagner une voiture. Il suffit d'envoyer un mail à l'adresse qui apparaît dans le message : winner@tombola.com. Quelle sont les menaces possibles ?
   - Je serai victime d'un cheval de Troie
   - Le pirate tentera de de m'envoyer un ver en réponse à mon émail
   - Je serai victime d'un hoax

7. Un pirate installe un ransomware pour :
   - Préparer une porte dérobée
   - Chiffrer illégalement les données confidentielles d'une entreprise victime
   - Faire du chantage à une victime
   - Exécuter un rootkit

TD3.2. « Questions de compréhension de la partie III »

1. Quelle est la différence entre un virus et un ver
2. Dans quel cas les vers deviennent plus dangereux que les virus

3. Certains vers circulant sur internet ne cause pas de dommages sur les machines victimes, c'est quoi le danger ?

4. Certains concepteurs d'antivirus recommandent de scaner une machine avec un antivirus de démarrage se trouvant sur supports de stockage externe, pourquoi ?

5. Donnez les étapes d'installation d'une porte dérobée

6. Donnez les étapes d'installation d'un cheval de troie

7. Donner deux méthodes implémentées dans certains virus pour les rendre indétectables par les antivirus

TD3.2. « Exercice de reflexion »

1. Donnez quelques conséquences des vers :

2. Donnez les étapes adoptées par un pirate pour mettre en place une porte dérobée (Backdoor)

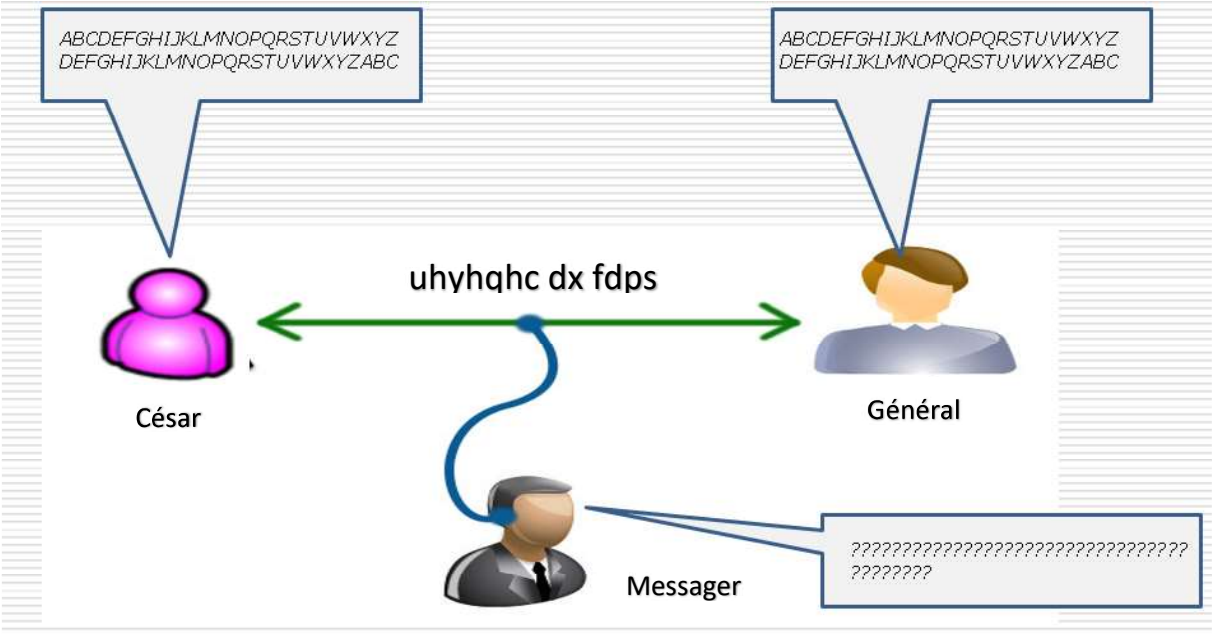
Partie IV : Cryptographie

IV.1. Introduction et historique

Le concept de cryptographie remonte à l'époque de jules césar. Par manque de confiance envers ses messagers, jules envoyait des messages modifiés (brouillés) à ses généraux. Cette modification est faite en décalant de 3 l'ordre des lettres en alphabet, comme montré ci-après :

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

Par exemple, comme illustré à la figure suivante, quand jules souhaite envoyer le message « ***revenez au camp*** », il va plutôt envoyer « ***uhyhqhc dx fdps*** » via ses messagers. Ces derniers ne comprendront jamais le message s'ils ne connaissent pas le secret qui est : ***le décalage à 3.***



A partir de cette époque, l'histoire de la cryptographie a commencé !

Aujourd'hui on trouve la cryptographie partout :

- Les systèmes militaires.
- Les banques
- Le paiement en ligne sur internet
- Les communications téléphoniques mobiles.
- La télévision payante
- La carte d'identité numérique.
- Le vote numérique.
- Et beaucoup d'autres domaines

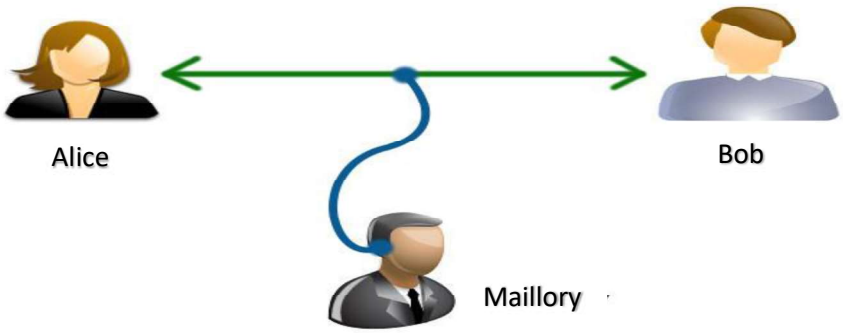
La cryptographie d'aujourd'hui fait appel à plusieurs domaines

- Informatique
- Mathématiques
- Electronique
- Biologie
- Physique
- …

IV.2. Principe de base

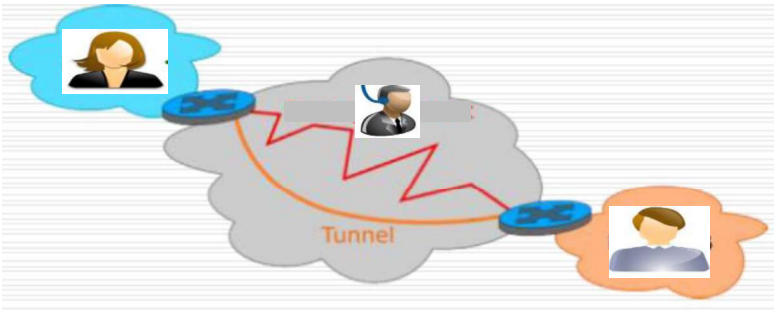
Deux utilisateur Alice et Bob veulent s'échanger des informations. Cependant l'utilisateur Maillory qui s'oppose à cette communication, il va donc essayer de :

- Espionner Alice et Bob
- Prendre l'identité de l'un des deux utilisateurs et parler à l'autre au nom du premier
- Modifier les messages échangés



Le but utilisant la cryptographie est de d'offrir aux utilisateurs Alice et Bob la possibilité de communiquer à travers un canal de communication non sûr (internet par exemple), en leurs garantissant les objectifs suivants :

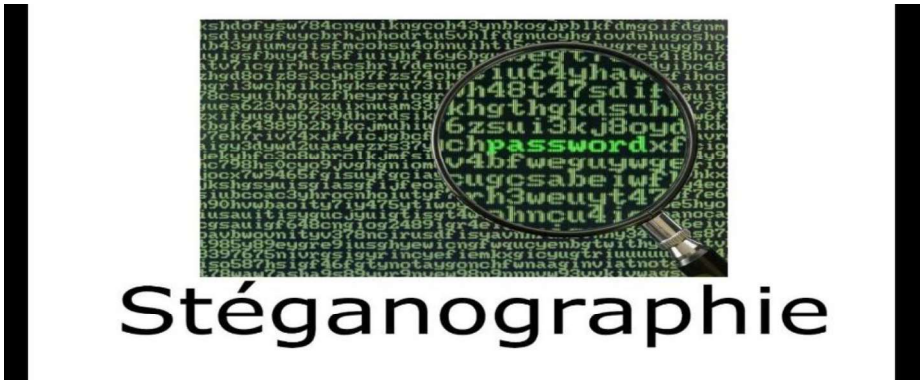
- Confidentialité des échanges
- Authentification des utilisateurs et des messages
- Intégrité des messages
- Non répudiation



IV.3. Terminologie

IV.3.1. Stéganographie VS Cryptographie

La stéganographie consiste à cacher une donnée sensible « ***d1*** » dans une autre donnée « ***d2*** » pour la rendre « invisible ».



Par contre, la cryptographie propose de modifier l'information selon des règles et procédures afin de la rendre « incompréhensible »

Dans ce document, on s'intéresse à la cryptographie.

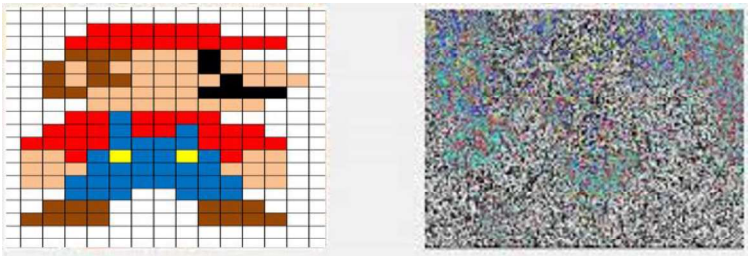
Deux grandes familles de systèmes de cryptographie existent : La transposition et la substitution

IV.3.2. Cryptographie par transposition

Le but est de changer l'ordre des éléments d'une donnée, ces éléments peuvent être des caractères d'une langue, des pixels d'une image,…le chiffrement de césar est un exemple de ce type de cryptographie.

IV.3.3. Cryptographie par substitution

Ça consiste à remplacer les éléments d'une donnée par d'autres selon une procédure



Les algorithmes de cryptographie actuels utilisent des successions de substitutions et de transpositions. Certains algorithmes seront étudiés dans ce manuscrit.

IV.3.4. Définitions rapides

IV.3.4.1. Message clair

Un message 'M'est dit clair lorsqu'il n'a pas encore été transformé par les méthodes de cryptographie, c'est l'information dans son état initial qu'il faut protéger, cette information peut être textuelle, image, vidéo,…etc.

IV.3.4.2. Chiffrement

C'est le processus de transformation d'un message clair en un message chiffré compréhensible uniquement par les entités autorisées. Il s'agit d'une fonction mathématique E appliquée à un message clair M pour donner le message chiffré C, ce message chiffré est appelé aussi cryptogramme.

$$C = E(M)$$

IV.3.4.3. Déchiffrement

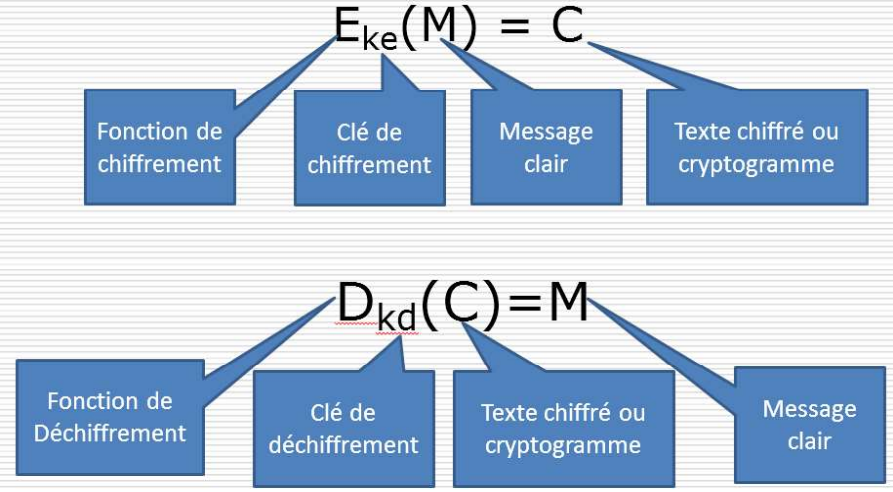
C'est le processus inverse du chiffrement, il s'agit de retrouver le message clair à partir du cryptogramme. A ce niveau, on utilise une fonction de déchiffrement D tel que :

$$D(C) = D(E(M)) = M$$

IV.3.4.4. Clé de cryptographie

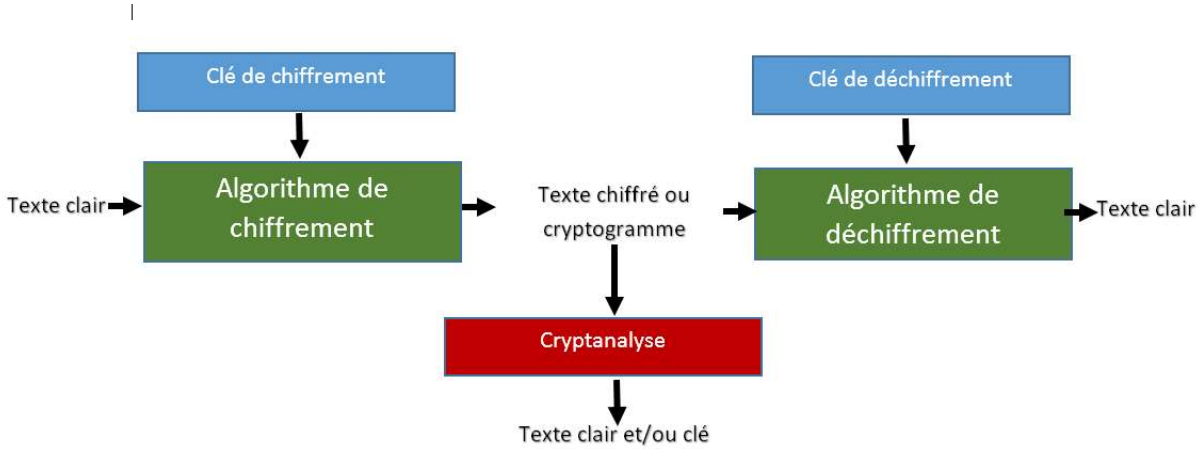
C'est une succession de bits permettant de chiffrer et/ou déchiffrer un message. Les fonctions E et D sont paramétrées par des clés K_e et K_d :

$$E_{ke}(M) = C$$
$$D_{kd}(C)=M$$



IV.3.5. Cryptographie VS cryptanalyse

Comme expliqué précédemment dans ce manuscrit, la cryptographie est le domaine qui assure le chiffrement et le déchiffrement des données. La cryptanalyse est le domaine qui analyse les messages chiffrés (cryptogrammes) pour retrouver le message clair sans connaitre les clés de déchiffrement.



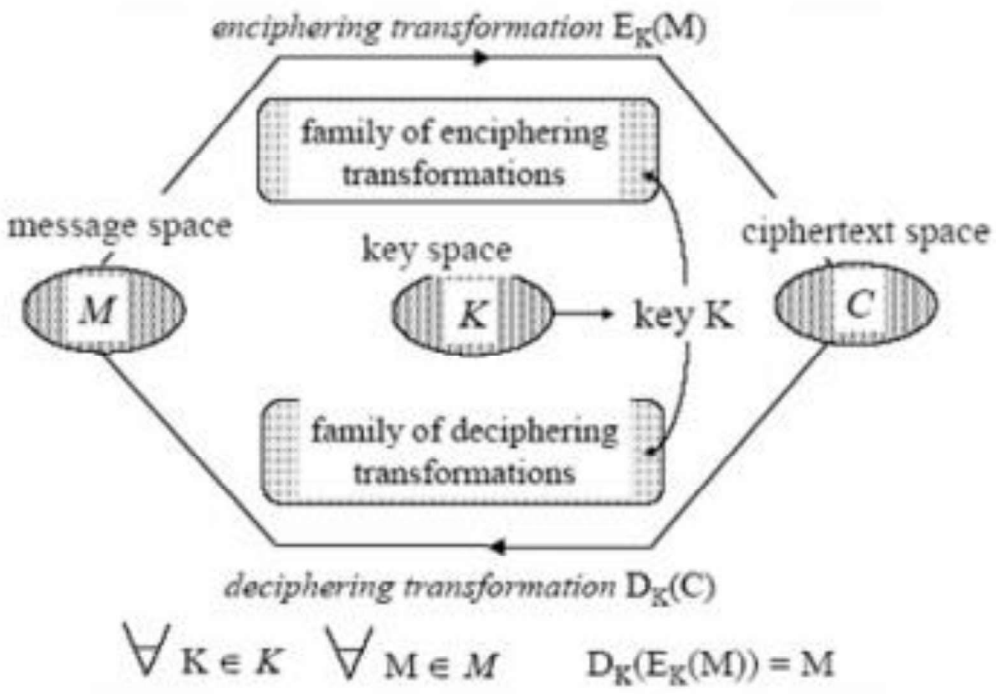
IV.3.6. Cryptologie

La cryptologie est la science qui regroupe la cryptographie et la cryptanalyse

IV.3.7. Cryptosystème

Tout cryptosystème doit regrouper les éléments suivants :

- L'ensemble de toutes les **clés** (espace de clés)
- L'ensemble de tous les **messages clairs** (espace de messages)
- L'ensemble de tous **cryptogrammes** (espace de cryptogrammes)
- L'ensemble de tous **les algorithmes qui sont :**
  - Algorithmes générateurs des clés
  - Algorithmes de chiffrement
  - Algorithmes de déchiffrement



IV.3.8. Algorithme secret VS Algorithme robuste

Un algorithme de chiffrement/déchiffrement est dit secret si les instructions qui le composent sont gardées confidentielles.

L'algorithme est dit robuste s'il résiste face aux différentes attaques de cryptanalyse

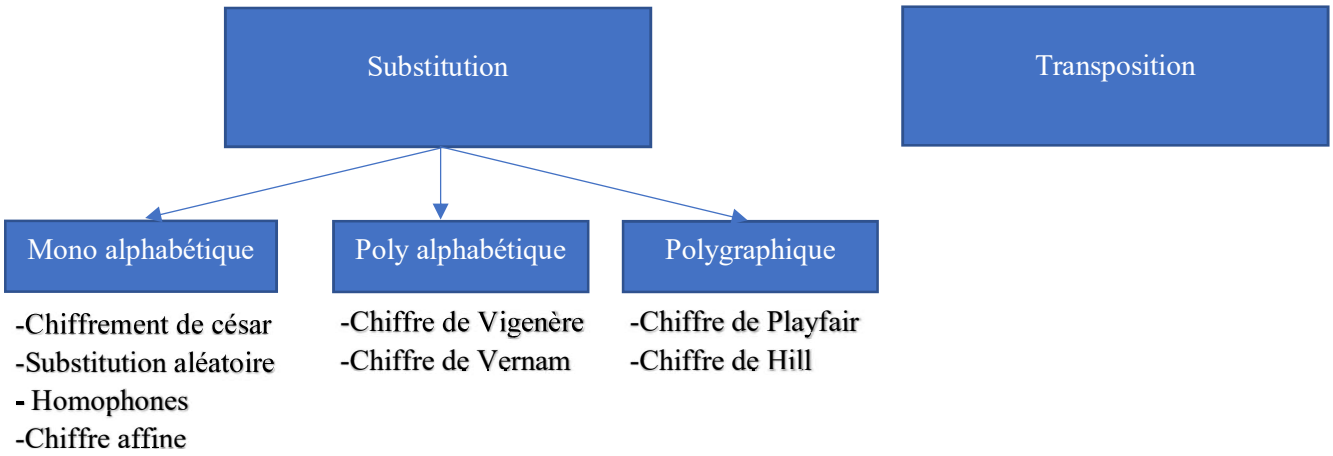
IV.3.9. Principe de Kerckhof

La sécurité du chiffre ne doit pas dépendre de ce qui ne peut pas être facilement changé

Au début, le secret étaient les algorithmes de chiffrement/déchiffrement eux-mêmes (on parlait d'algorithmes secrets). Cependant, garder confidentiel ces algorithmes était une tache très fastidieuse. C'est pour cela qu'aujourd'hui, les algorithmes sont publics et c'est plutôt les clés qu'il faut gardé confidentielles. D'où le principe de Kerckhof.

IV.4. Cryptographie classique

Cette section abordera les principaux systèmes de cryptographie classique, mais qui ont permis d'avoir aujourd'hui des communications avec un haut degré de sécurité. Nous structurons les différents schémas de cryptographie classique comme illustré dans la figure ci-après :



Les chiffrements par substitution et transposition sont expliqués précédemment dans ce document (sections IV.3.2. et IV.3.3.), Il nous reste donc à définir les systèmes de chiffrement mono alphabétiques, poly alphabétiques et polygraphique :

IV.4.1. Chiffrement mono alphabétiques

Le chiffrement mono alphabétique consiste à remplacer un caractère par un autre caractère ou symbole. A l'époque, ce système de chiffrement était utilisé dans les énigmes, il souffre de la cryptanalyse par analyse de fréquence qui sera développée plus loin dans ce document. Le chiffrement de césar et le chiffre affine sont des exemples types de cette catégorie de cryptographie. A noter qu'un caractère d'un message clair est toujours remplacé par le même autre caractère ou symbole durant le processus de chiffrement.

IV.4.1.1. Chiffrement de César

C'est le premier système de chiffrement qui a été le plus populaire, son principe de fonctionnement est très simple, il consiste à effectuer des décalages des lettres d'alphabet comme suit :

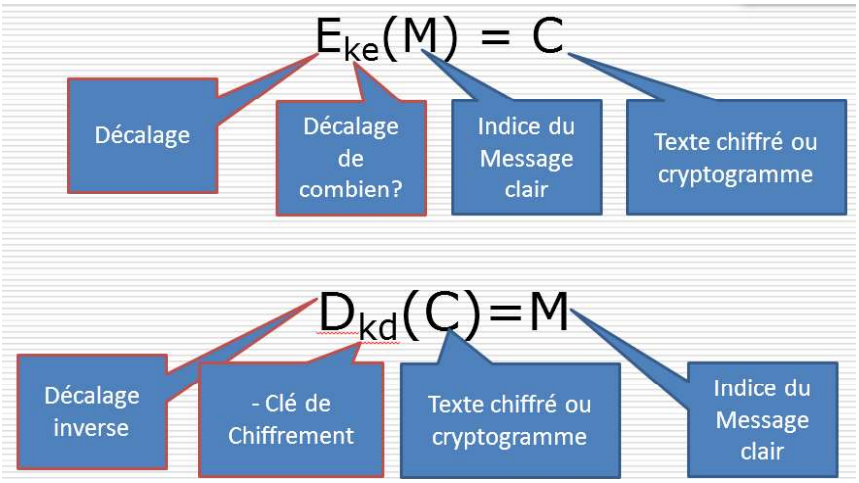
$$E(i)= (i+k) \bmod 26 = C$$

La fonction E est la fonction de chiffrement, i est l'indice de la lettre à chiffrer et k est la clé de chiffrement qui traduit le nombre de décalage à effectuer.

Pour le déchiffrement du cryptogramme C, on utilise la fonction **D(C)** suivante :

$$i = D(C) = (C - k) \bmod 26$$

Par analogie avec notre schéma de la section IV.3.4. (Définitions rapides), on obtient la figure ci-après :

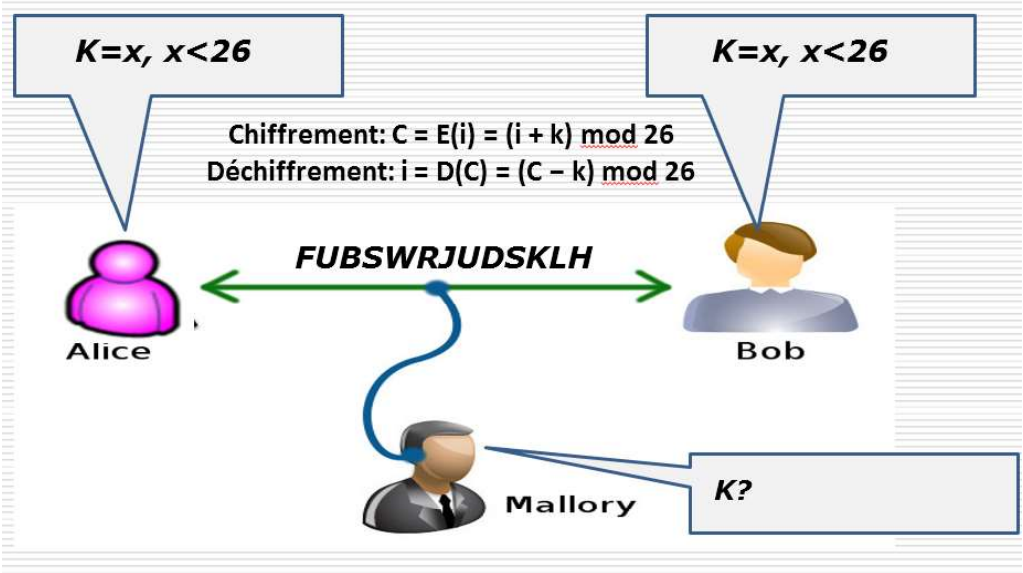


Par exemple, si on souhaite crypter le message '***CRYPTOGRAPHIE***' avec k=3, la table de correspondance de l'alphabet sera comme suit :

ABCDEFGHIJKLMNOPQRSTUVWXYZ

DEFGHIJKLMNOPQRSTUVWXYZABC

Le mot '**CRYPTOGRAPHIE'** deviendra donc '**FUBSWRJUDSKLH'**



Cryptanalyse du chiffrement de césar

Un pirate ayant connaissance des fonctions E(M) et D(C) de césar utilisera une attaque appelée force brute pour casser l'algorithme de césar, il suffit d'essayer les cas possibles de décalage de l'alphabet (25 pour les lettres de la langue française) pour retrouver le message clair.

Exercice :

- Chiffrez 'Cryptographie et sécurité réseaux' avec k=8,

Travail Demandé :

- Développer l'algorithme de chiffrement de César en C ainsi que sa cryptanalyse

IV.4.2.2. Substitution aléatoire

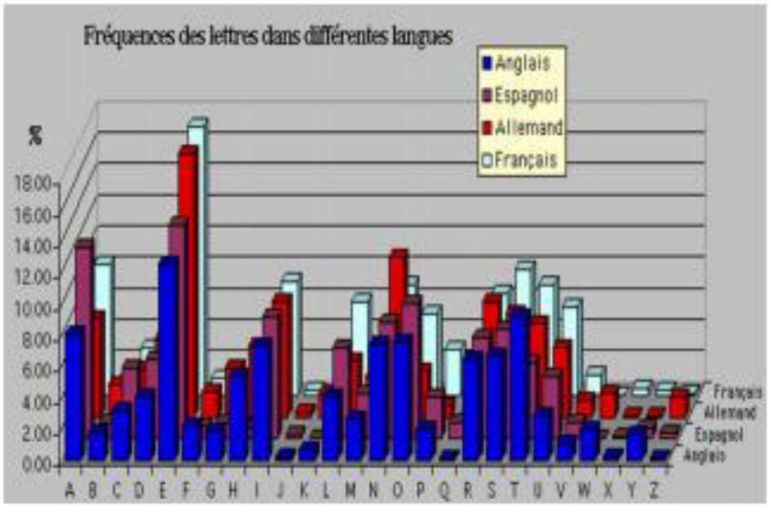
Pour éviter l'attaque par force brute, la substitution aléatoire évite le décalage des lettres de l'alphabet et remplace plutôt aléatoirement des lettres par d'autres.

Exemple

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

Cryptanalyse de la substitution aléatoire

L'attaque par force brute n'est pas techniquement réalisable, un ordinateur puissant aujourd'hui passera des années à tester tous les cas possibles de clés de chiffrement. Pour cela, la cryptanalyse utilisée contre ce type de chiffrement est appelée analyse de fréquence d'apparition des lettres de l'alphabet.



Cette cryptanalyse fonctionne comme suit :

1. Dans plusieurs langues du monde, la fréquence d'apparition des lettres de cette langue (français par exemple) est stable, il faut donc définir la table de fréquence de la langue du texte chiffré (cryptogramme).
2. Déterminer la fréquence d'apparition de chaque lettre du cryptogramme
3. Comparer la table de fréquence du cryptogramme avec celle de la langue française
4. Deviner l'alphabet chiffré

Rang	Caractère	Nombre d'occurrences	Pourcentage
1	e	115 024 205	12,10
2	a	67 563 628	7,11
3	i	62 672 992	6,59
4	s	61 882 785	6,51
5	n	60 728 196	6,39
6	r	57 656 209	6,07
7	t	56 267 109	5,92
8	o	47 724 400	5,02
9	l	47 171 247	4,96
10	u	42 698 875	4,49
11	d	34 914 685	3,67
12	c	30 219 574	3,18
13	m	24 894 034	2,62
14	p	23 647 179	2,49
15	é	18 451 937	1,94
17	g	11 684 140	1,23
18	b	10 817 171	1,14
19	v	10 590 858	1,11
20	h	10 583 562	1,11
21	f	10 579 192	1,11
28	q	6 140 307	0,65

Statistique selon la langue française

Rang	Caractère	Nombre d'occurrences	Pourcentage
1	h	115 024 205	12,10
2	j	67 563 628	7,11
3	e	62 672 992	6,59
4	k	61 882 785	6,51
5	u	60 728 196	6,39
6	p	57 656 209	6,07
7	w	56 267 109	5,92
8	x	47 724 400	5,02
9	r	47 171 247	4,96
10	v	42 698 875	4,49
11	d	34 914 685	3,67
12	c	30 219 574	3,18
13	m	24 894 034	2,62
14	p	23 647 179	2,49
15	é	18 451 937	1,94
17	g	11 684 140	1,23
18	b	10 817 171	1,14
19	v	10 590 858	1,11
20	h	10 583 562	1,11
21	f	10 579 192	1,11
28	q	6 140 307	0,65

Statistique du texte chiffré

Travail Demandé

Ecrire un programme en C traduisant la substitution aléatoire avec sa cryptanalyse

IV.4.2.3. Homophones

Certaines améliorations de la substitution aléatoire utilisent des homophones, c'est-à-dire remplacer une lettre du message clair par un symbole parmi plusieurs choisi aléatoirement.

Le nombre de symboles chiffrant la lettre du message clair doit être proportionnel à la fréquence d'apparition de cette lettre dans la langue en question. De cette manière, ce système de cryptographie évite l'attaque par analyse de fréquence des lettres en équilibrant les pourcentages

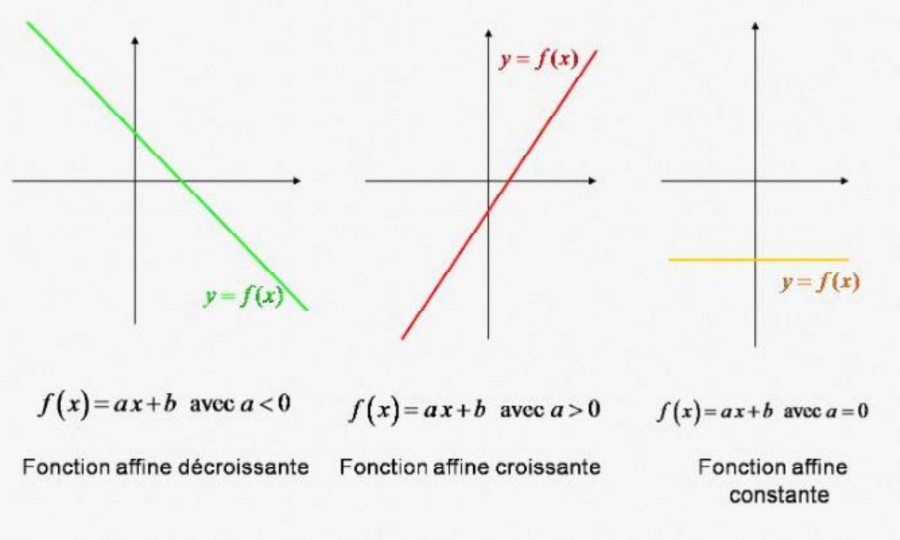
Lettre	%	Chiffre
A	9	09 12 33 47 48 53 67 78 92
B	1	81
C	3	13 41 62
D	3	01 03 45
E	16	06 10 14 16 23 24 44 46 54 55 57 74 79 82 87 98
F	1	31
G	1	25
H	1	39
I	8	32 50 56 70 73 83 88 93
J	1	15
K	0	04
L	5	26 37 51 65 84
M	3	22 27 68

Lettre	%	Chiffre
N	7	18 58 59 66 71 91 99
O	5	00 05 07 54 72
P	3	38 90 95
Q	1	94
R	6	29 35 40 42 77 80
S	8	11 19 21 36 76 86 96 97
T	7	17 20 30 43 49 69 75
U	6	02 08 61 63 85 90
V	2	34 52
W	0	60
X	0	28
Y	0	24
Z	0	01

IV.4.3.4. Chiffre affine

Une fonction affine s'écrit comme suit : **y→ a ∗ x + b (**polynôme de premier degré). Le processus de chiffrement est donc une fonction affine **mod 26,** a et b sont des constantes tandis que x et y sont les indices des lettres de l'alphabet

Quand a = 1, on retrouve le chiffrement de César où b est le décalage (le k du chiffre de César).



Algorithme du chiffre affine

la clé **k** est un couple **(k_1, k_2)** tel que $k_1, k_2 \in [0, 25]$ et **pgcd(k_1, 26) = 1**.

Le processus de chiffrement est le suivant :

$$c_i = E(m_i) = k_1 * m_i + k_2 \bmod 26.$$

Ainsi, la fonction de déchiffrement est :

$$m_i = D(c_i) = f^{-1}(c_i) = k_1^{-1} * (c_i - k_2) \bmod 26.$$

Cryptanalyse

Le nombre de lettres en alphabet de la langue française par exemple est 26, il existe donc uniquement 12 nombres entiers entre 0 et 26, et, premier avec 26 qui sont : 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23 et 25. Cela donnera uniquement 312 clés possibles (12*26). Donc ici la cryptanalyse par force brute fera l'affaire de casser l'algorithme des chiffres affines. A noter aussi que même l'analyse de fréquence d'apparition des lettres réussira comme cryptanalyse.

IV.4.2. Chiffrement polygraphique (ou polygrammiques)

Au lieu de chiffrer une lettre par une autre comme le cas de la mono substitution, ce schéma de chiffrement propose de crypter p lettres par p autres lettres et/ou symboles. Dans cette section, nous allons développer les méthodes de chiffrements suivantes faisant partie de cette famille :

- Le digramme et le trigramme
- Le chiffre de Playfair
- Le chiffre de Hill

IV.4.2.1. digramme et trigramme

Afin d'éviter la cryptanalyse par analyse de fréquence d'apparition des lettres d'un alphabet, certaines solutions proposent de crypter par :

Di-gramme qui consiste à remplacer les deux lettres successives les plus fréquentes d'une langue par deux autres lettres ou symboles

Tri-gramme qui consiste à remplacer les trois lettres successives les plus fréquentes d'une langue par trois autres lettres ou symboles

Les 20 bigrammes les plus fréquents

Bigrammes	ES	DE	LE	EN	RE	NT	ON	ER	TE	EL	AN	SE	ET	LA	AI	IT	ME	OU	EM	IE
Nombres	3318	2409	2366	2121	1885	1694	1646	1514	1484	1382	1378	1377	1307	1270	1255	1243	1099	1086	1056	1030

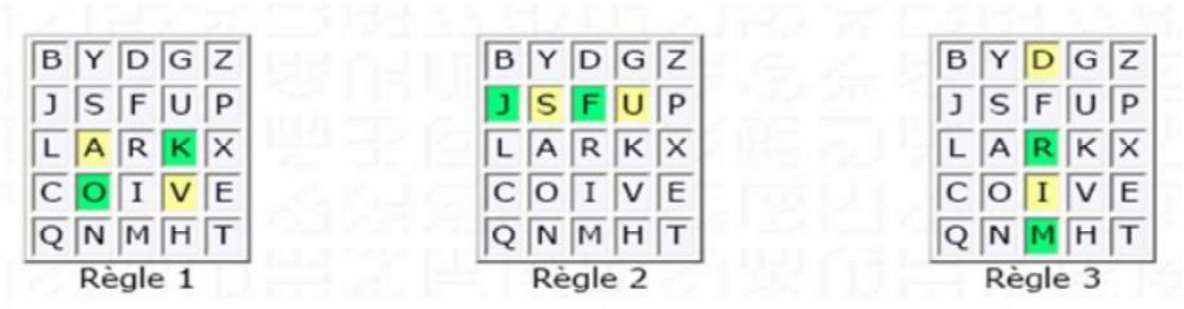
Les 20 trigrammes les plus fréquents

Trigrammes	ENT	LES	EDE	DES	QUE	AIT	LLE	SDE	ION	EME	ELA	RES	MEN	ESE	DEL	ANT	TIO	PAR	ESD	TDE
Nombres	900	801	630	609	607	542	509	508	477	472	437	432	425	416	404	397	383	360	351	350

IV.4.2.2. Le chiffre de Playfair

Toujours dans la même logique de chiffrer deux lettres avec deux autres, le chiffre de playfair procède de même que le digramme. L'algorithme est le suivant :

1. Répartir les lettres de l'alphabet dans une matrice de 5*5 qui représente la clé k



2. On prend deux lettres du message clair à chiffrer :
   - Si les deux lettres sont sur des "coins", les lettres chiffrées résultantes sont celles se trouvant aux 2 autres coins (règle 1 du schéma)
   - Si les deux lettres sont sur la même ligne, on les remplace par les deux lettres à leur droite (règle 2 du schéma)
   - Si les deux lettres sont sur la même colonne, on les remplace par les deux lettres en dessous (règle 3 du schéma)
   - Si les deux lettres sont identiques, on insère un X entre elles

Cryptanalyse

Si on dispose de suffisamment de textes clairs avec les textes chiffrés correspondants, on peut deviner la clé. Cette cryptanalyse est appelée attaque à texte clair connu

IV.4.2.3. Le chiffre de Hill

Le chiffrement de Hill utilise des matrices pour ses différents calculs. Dans un premier temps, les lettres de l'alphabet seront remplacées par leur rang (a=1, b=2, etc.).

$$\begin{pmatrix} C_k \\ C_{k+1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} P_k \\ P_{k+1} \end{pmatrix} (\mathrm{mod} 26)$$

P_k et P_{k+1} sont les deux rangs des lettres du message clair et C_k , C_{k+1} sont les cryptogrammes correspondants. Les éléments des matrices sont des entiers positifs et la matrice de chiffrement doit être inversible dans Z_{26}

$$C_k = a*p_k + b*P_{k+1}$$

$$C_{k+1} = c*p_k + d*P_{k+1}$$

La dimension de la matrice représentant la clé (a, b, c, d du schéma) peut varier selon le nombre de lettre qu'on souhaite chiffrer simultanément.

Exercice

Cryptez le message clair 'bienvenu chez hill' avec la clé suivante :

$$\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$$

Pour le processus de déchiffrement on utilise la fonction suivante :

$$\begin{pmatrix} P_1 \\ P_2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} C_1 \\ C_2 \end{pmatrix} (\mathrm{mod} 26)$$

Exercice

Décryptez le cryptogramme 'FGXGEDSPGV' avec l'inverse de clé précédente

IV.4.3. Chiffrement poly alphabétiques

La substitution poly alphabétiques présente des similitudes avec la mono alphabétique, sauf qu'ici, une lettre chiffrée n'est pas toujours la même pour une lettre du message clair, la méthode de chiffrement utilise une clé pour chiffrer des messages, le chiffrement de Vigenère est un exemple type de cette famille de cryptographie.

IV.4.3.1. Chiffrement de Vigenère

Ce chiffrement présente des similitudes avec César mais utilise un mot de passe pour ses différents décalages.

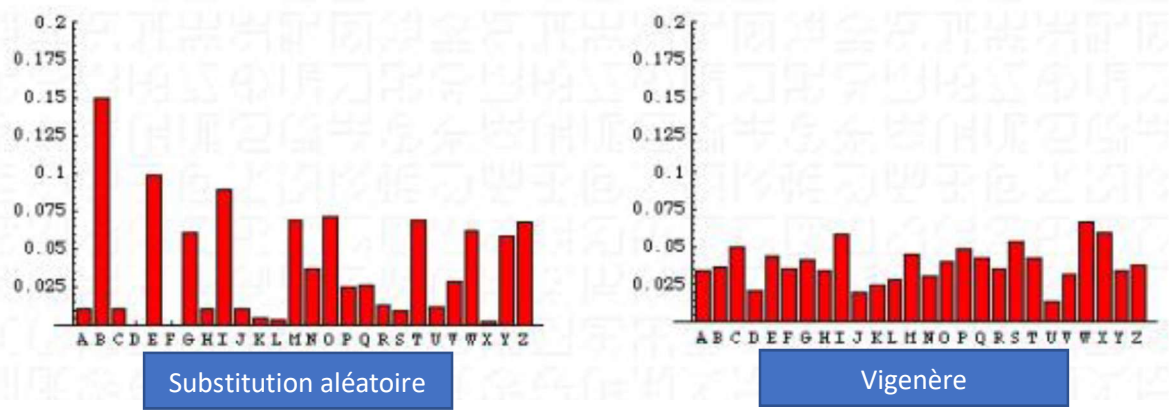
Le décalage est effectué en fonction du mot de passe, on peut donc avec une même lettre chiffrée différemment. Le décalage n'est pas fixé comme le cas de césar, par exemple, pour chiffrer le message 'cryptographie' avec la clé 'clim', on procède comme suit :

Message clair	c	r	y	p	t	o	g	r	a	p	h	i	e
Clé	c	l	i	m	c	l	i	m	c	l	i	m	c
Décalage de combien	2	11	8	7	2	11	8	7	2	11	8	7	2
cryptogramme		w						y					

On remarque ici que la première lettre 'r' du message clair coïncide avec la lettre 'l' (de rang 11), on lui effectue donc un décalage de 11 : on obtient 'w'.

Par contre, le deuxième 'r' coïncide avec 'm', donc on effectue un décalage de 7, ce qui donnera 'y'

Cela renforcera la sécurité du système et évitera la cryptanalyse par analyse de fréquence d'apparition des lettres car la table de fréquence aura la forme suivante :



IV.4.3.2. Chiffrement de vername

Ce système de chiffrement utilise la même méthode que celui de vigenere sauf qu'il possède une caractéristique particulière :

La taille de clé de chiffrement est la même que celle du message clair.

La clé est appelée ici masque jetable car elle est formée de caractères aléatoires et n'est jamais réutilisable. Ces différentes caractéristiques rendent la tache de retrouver la clé très délicate.

IV.4.4. Transposition

Comme expliqué précédemment, le cryptogramme d'un message clair M gardera les mêmes caractères que ceux de M, sauf que l'ordre est différent. Nous présentons dans cette partie, un exemple de chiffrement par transposition qui a été utilisé depuis plusieurs dizaines d'années.

Par exemple, pour chiffrer un message de 35 caractères, on aura 35 != 1040 manières différentes de réarranger ces caractères. Plus le message à chiffrer est grand, plus il est difficile à décrypté sans connaitre la règle de décalage.

La transposition rectangulaire est un exemple type de ce système de cryptographie : il est question de rédiger le message clair dans une matrice rectangulaire puis arranger les colonnes suivant un mot de passe.

Exemple :

Si on veut chiffrer le message '*RIAHLA Mohamed Amine*' avec la clé '*farine*', notre matrice aura la forme suivante :

F	A	R	I	N	E
6	1	18	9	14	5
R	I	A	H	L	A
M	O	H	A	M	E
D	A	M	I	N	E

On va réordonner les colonnes de sorte à respecter l'ordre d'apparition des lettres du mot de passe dans l'alphabet, on obtient :

A	E	F	I	N	R
1	5	6	9	14	18
I	A	R	H	L	A
O	E	M	A	M	H
A	E	D	I	N	M

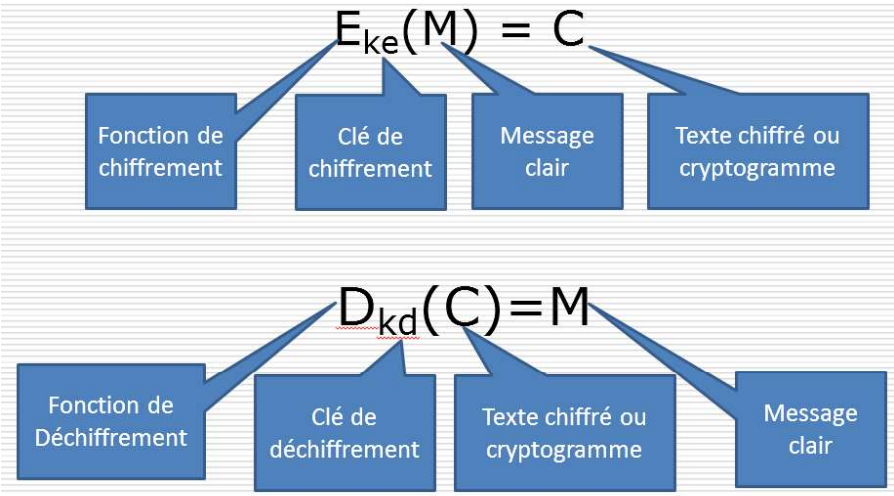
Notre cryptogramme sera :

C= IARHLAOEMAMHAEDINM

IV.5. Cryptographie moderne

Les algorithmes de cryptographie actuels font abstraction des méthodes classiques et proposent deux grands schémas de chiffrement, à savoir la cryptographie symétrique et la cryptographie asymétrique.

Rappelez-vous de notre schéma précédent définissant les principes de base de la cryptographie :

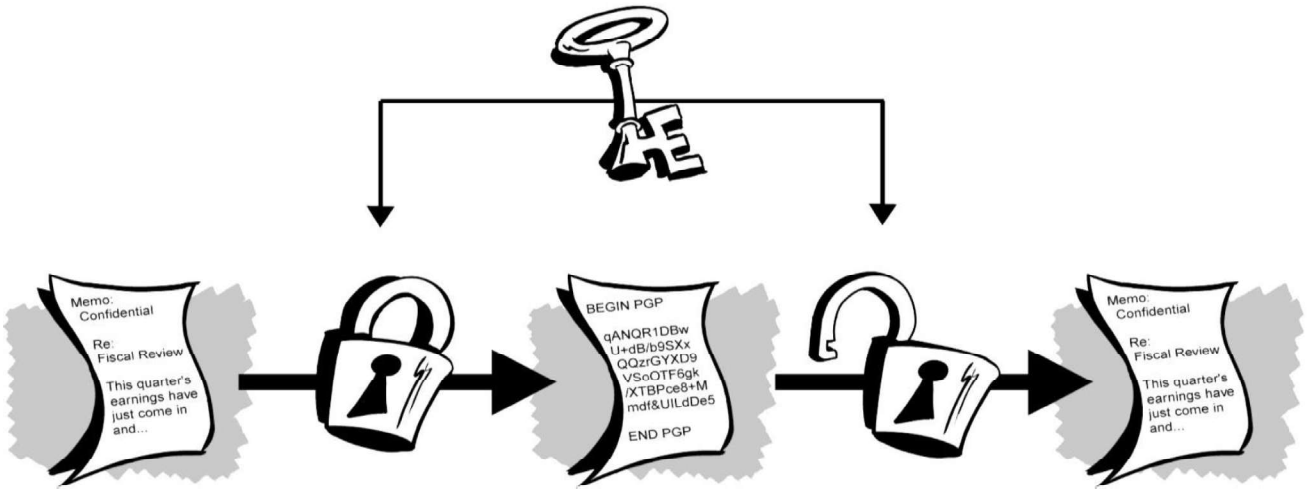


On parle de la cryptographie symétrique ou à clé privée quand ke=kd=k, c'est-à-dire quand la clé de chiffrement est elle-même la clé du déchiffrement.

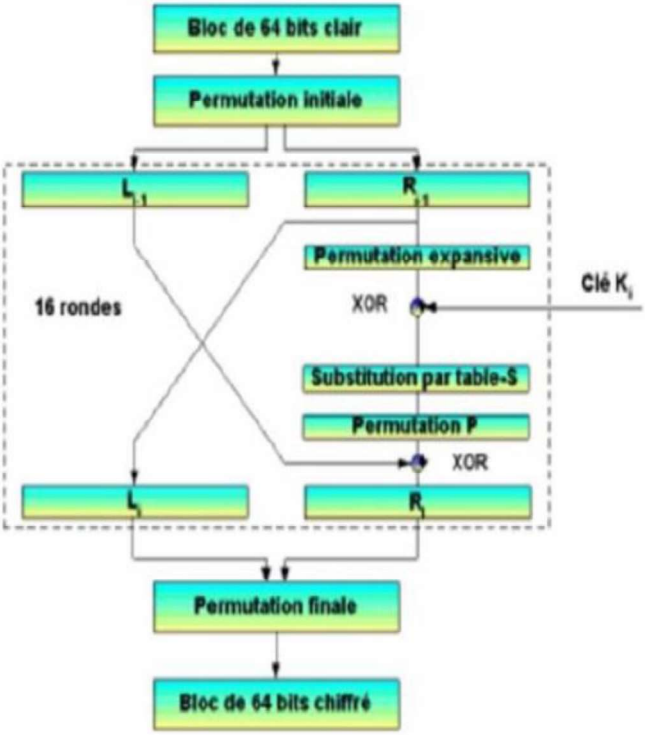
On parle de la cryptographie asymétrique ou à clé publique quand ke<>kd, c'est-à-dire quand la clé de chiffrement est différente de la clé du déchiffrement.

Dans ce qui suit, nous allons détailler les deux concepts

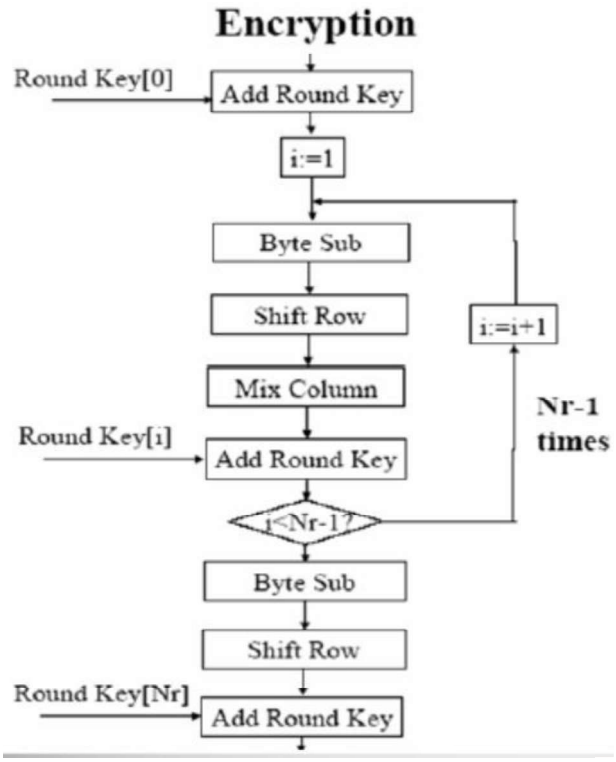
IV.5. 1. Cryptographie symétrique



Dans ce schéma de chiffrement, les deux entités communicantes doivent avoir préalablement échangé cette unique clé de chiffrement et déchiffrement. Les algorithmes les plus connus de cette catégorie sont : DES, 3DES et AES qui sont basés sur des séries de transpositions et de substitutions des bits du message clair en fonction de la clé.



DES



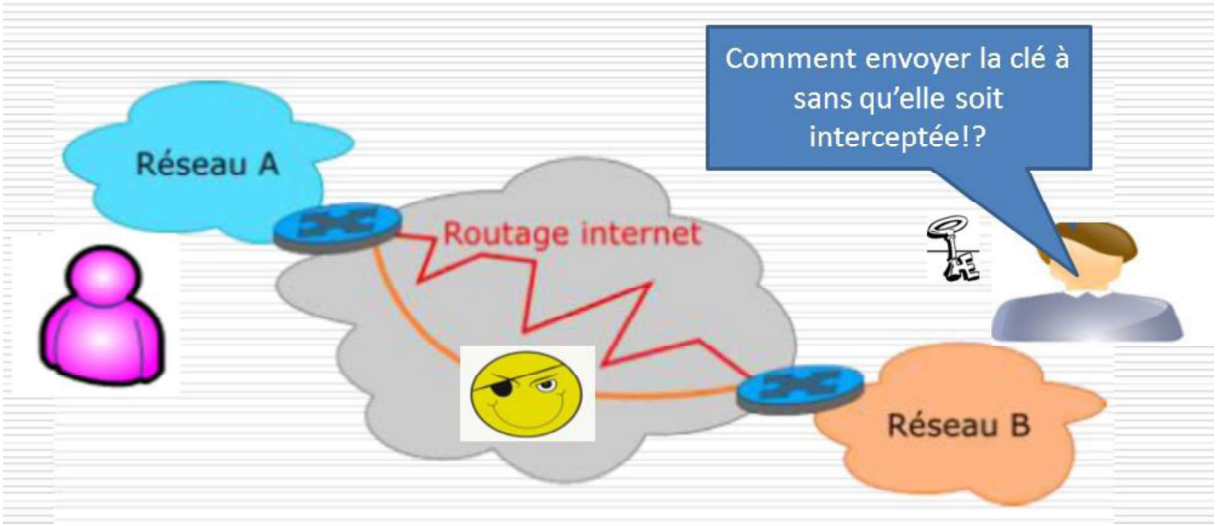
AES

IV.5. 1.1. Avantages de la cryptographie symétrique

L'avantage de ce schéma de chiffrement est qu'il est très rapide, donc bien adapté pour les faibles processeurs comme les capteurs.

IV.5. 1.2. Inconvénients de la cryptographie symétrique

Le principal inconvénient réside dans la distribution des clés, comment es ce que deux communicants distants puissent s'échanger cette clé sans qu'elle soit interceptée par un utilisateur malveillant ?



Ainsi, pour assurer une communication entre N=20 utilisateur, il faut prévoir N*(N − 1)/2 paires de clés, à savoir 192.

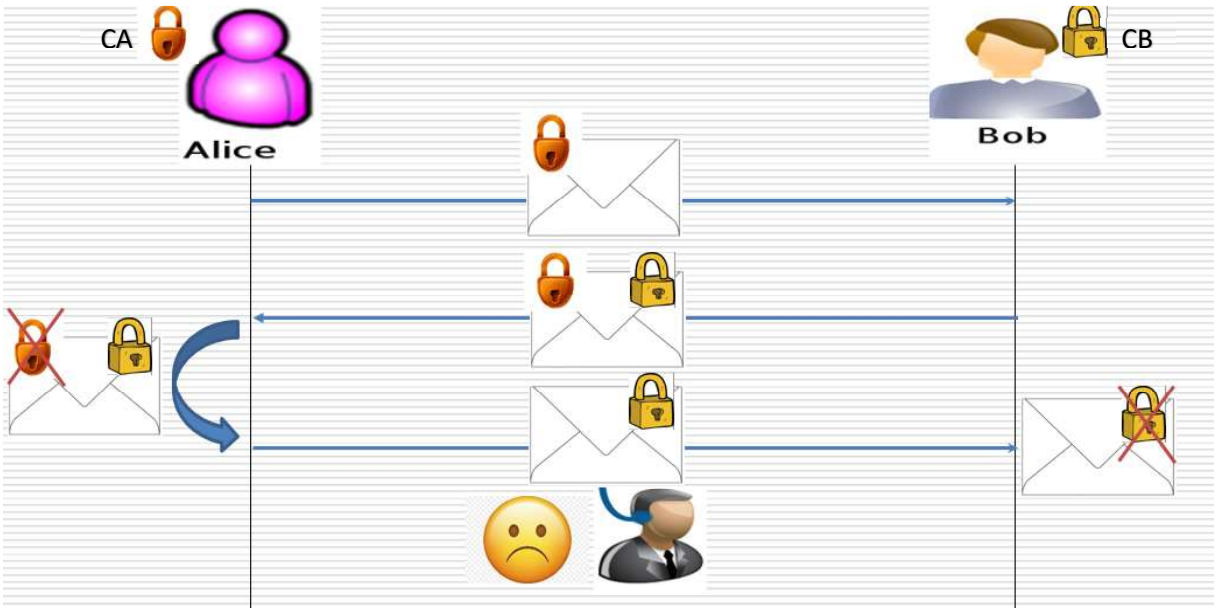
Pour résoudre le problème de l'échange de clé symétrique, il a fallu attendre 20 ans, pour trouver une solution inspiré de la figure suivante :

Admettons qu'Alice souhaite échanger un secret avec Bob, mais que leur messager Mallory n'est pas de confiance.

1. Alice chiffre son message avec sa clé CA (que bob ne connait pas) et l'envoie à Bob.
2. Bob reçoit le message, chiffre le message avec sa propre clé CB et renvoie le tout à Alice. A ce niveau le message est doublement chiffré par CA et CB.
3. Alice déchiffre le message avec CA et renvoie le message à Bob.
4. Bob peut maintenant ouvrir le message avec sa clé CB

Remarque

A aucun moment Mallory n'a pu voir le message en clair



L'algorithme a l'air de résoudre le problème d'échange de clé de chiffrement/déchiffrement, mais là encore, il y a des choses à dire :

S'il y aura erreur au niveau de l'ordre d'envoi et réception des messages, ces derniers risquent de ne jamais retrouver leurs formes claires. Ainsi, en absence de l'un des deux communicants, la communication ne peut s'effectuer

Suite à cela la cryptographie asymétrique est apparue

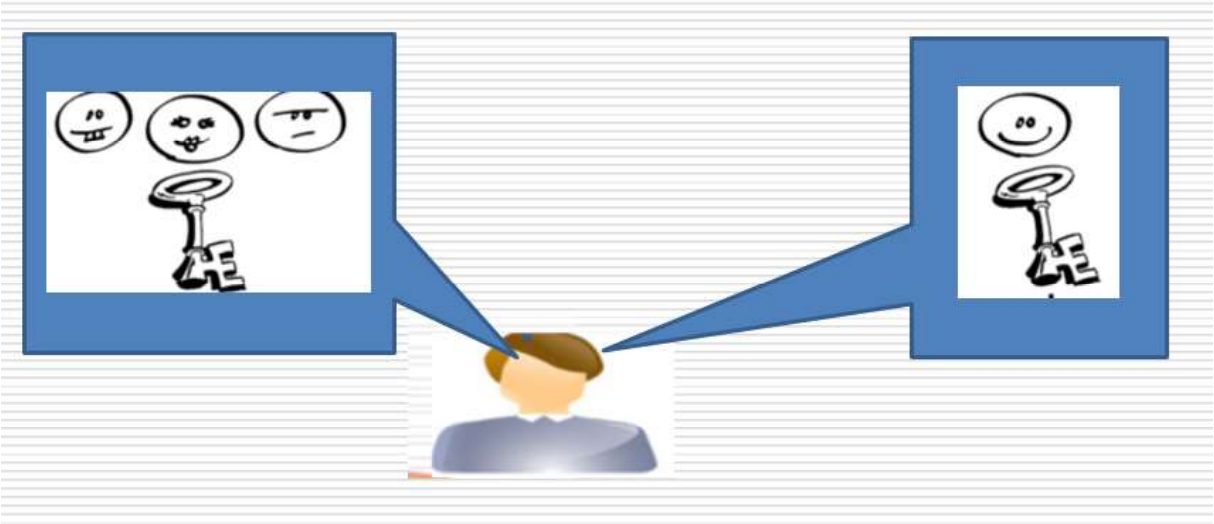
IV.5. 2. Cryptographie asymétrique

Dans ce type de chiffrement, chaque utilisateur dispose de deux clés différentes :

- **Une clé publique Pk**, connue par tout le monde et sert à crypter un message,
- **Une clé privée Sk** qui ne doit être connue que par son propriétaire, et qui sert à décrypter un message

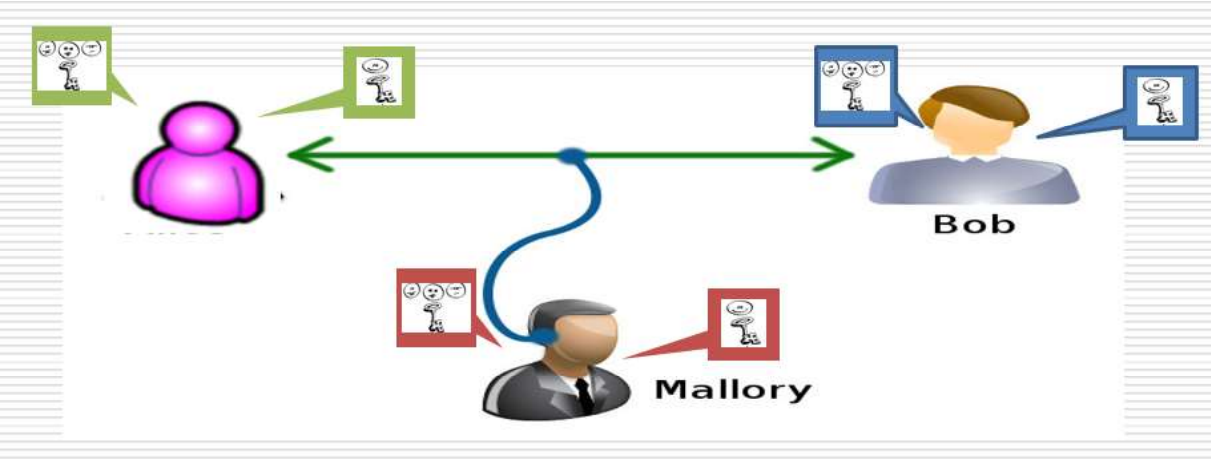
Propriété : La connaissance de P_K ne permet pas de déduire S_K,

$$D_{SK}\,(E_{PK}\,(M)) = M,$$



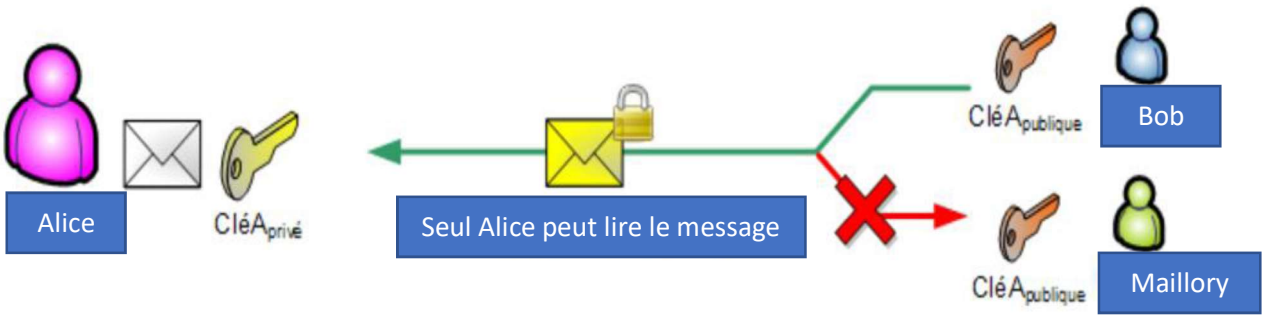
Remarque :

Une donnée cryptée avec une clé publique ne peut être décryptée qu'avec la clé privée correspondante.



L'algorithme asymétrique deviendra comme suit :

1. Alice met à disposition de tout le monde sa clé publique
2. Bob chiffre un message avec la clé publique d'Alice et lui envoie le cryptogramme
3. Alice peut facilement déchiffrer le message avec sa propre clé privée.



Les algorithmes les plus connus de cette catégorie sont :

- L'exponentiation de grands nombres premiers (RSA),
- Le problème des logarithmes discrets (ElGamal),
- Le problème du sac à dos (Merkle-Hellman).

La taille des clés varie entre 512 bits à 2048 bits.

IV.5. 2.1. Avantages de la cryptographie asymétrique

L'avantage est évidement la non nécessité de la distribution des clés comme le cas de la cryptographie symétrique, un message chiffré avec une clé publique connue par tout le monde n'est jamais déchiffrable avec cette clé publique. Mais plutôt avec sa clé privée correspondante qui n'est connue que par son propriétaire. Ainsi, seules n paires de clés sont nécessaires.

IV.5. 2.2. Inconvénients de la cryptographie asymétrique

La difficulté d'un algorithme asymétrique réside dans le fait qu'il faut trouver des fonctions mathématiques faciles à calculer dans un sens et très difficile à son inverse : une fonction unidirectionnelle à trappe, cette dernière sert à calculer l'inverse de la fonction. Par exemple dans RSA il est question de choisir deux grands nombres premiers entre eux p et q, puis calculer leur produit p*q=n : en connaissant p et q il est très aisé de connaitre n, cependant ayant n il est très difficile de trouver p et q. Les failles de ce type d'algorithme à trappe peuvent résider dans les générateurs de clés

Ainsi, les algorithmes de la cryptographie asymétrique sont très gourmands en calcul surtout quand il s'agit d'un grand message à chiffrer, il est 1000 fois plus lent que l'algorithme symétrique.

IV.5. 3. Cryptographie symétrique VS Cryptographie asymétrique

Après avoir expliqué les deux concepts de cryptographie symétrique et asymétrique, on remarque que les avantages de l'un représente l'inconvénient de l'autre :

- **La cryptographie symétrique qui est 'très rapide' souffre du problème de distribution des clés**
- **La cryptographie symétrique qui 'n'a pas de de problème de distribution des clés' est très lourd, surtout quand il s'agit de chiffrer des messages clairs de grande taille.**

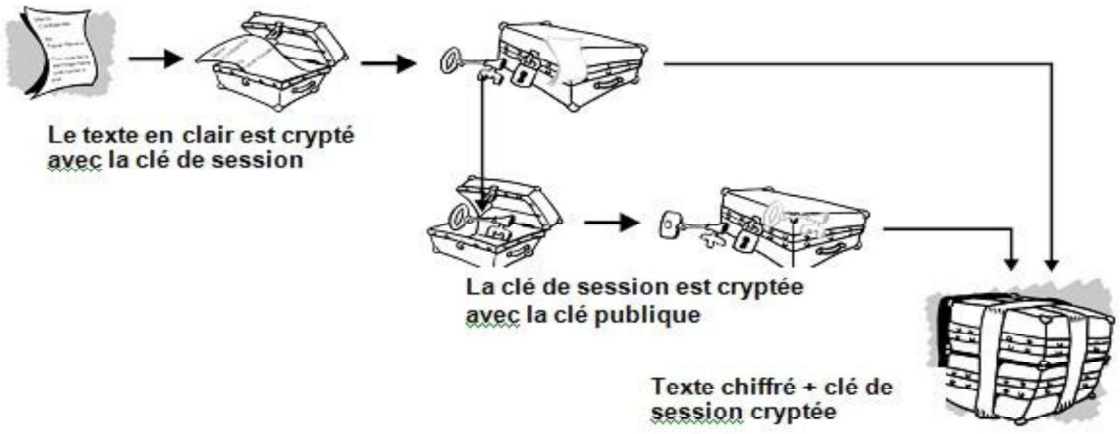
Pour cela, il a fallu proposer une alternative qui prend en considération les avantages de ces deux familles de cryptographie, d'où le nom de la cryptographie hybride.

IV.5. 4. La cryptographie hybride

La cryptographie hybride, comme son nom l'indique utilise les deux systèmes précédents en récoltant les avantages de chacun et éliminant les inconvénients, l'algorithme est comme suit :

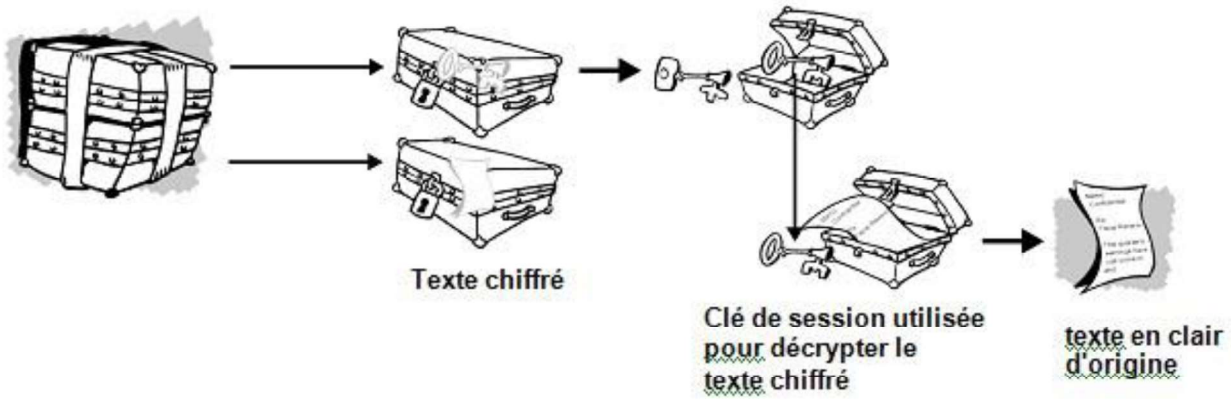
- **Le chiffrement asymétrique est utilisé pour distribuer des clés symétriques**, c'est-à-dire Alice envoie la clé symétrique *Sm* à Bob chiffrée avec la clé publique de B *PubB*, donc E_{PubB} **(Sm)**, on ne parlera pas ici du temps de calcul puisqu'il ne s'agit pas de chiffrer un grade message, mais uniquement d'une 'petite' clé symétrique.
- **Le message à chiffrer est crypté avec la clé symétrique, donc très rapide**

Donc le paquet envoyé par Alice à bob contient une clé symétrique chiffrée par la clé publique de bob ainsi qu'un message clair chiffré avec la clé symétrique que bob ne connait pas encore.



Fonctionnement du cryptage PGP

A la réception du paquet, bob déchiffre le premier message avec sa clé privé pour récupérer la clé symétrique, avec laquelle il va déchiffrer et retrouver le message clair.



Fonctionnement du décryptage PGP

IV.5. Comment assurer les autres objectifs de sécurité

Jusqu'à présent, on a traité uniquement la problématique de confidentialité, il ne faut pas négliger les autres objectifs, à savoir :

- **L'authentification**
- **L'intégrité des données**,
- **Non répudiation**

Pour atteindre ces objectifs, on utilise le concept de la signature numérique.

IV.5.1. Signature numérique

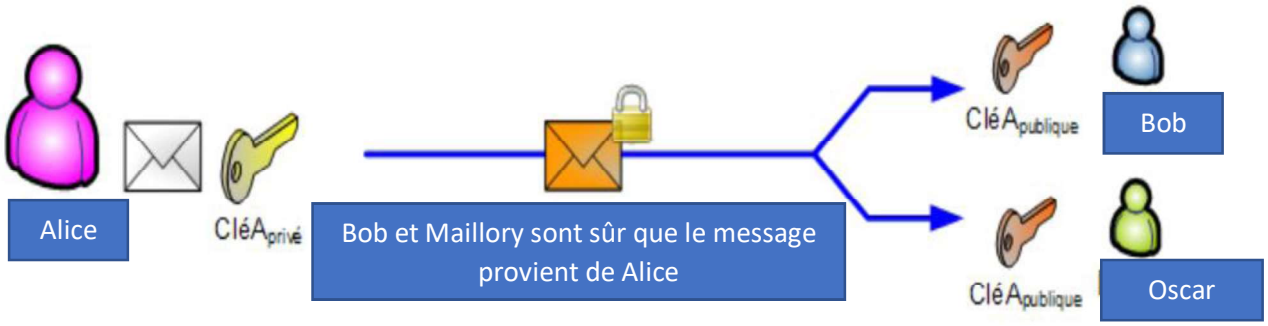
Comme dans la vie réelle, la signature numérique est utilisée pour assurer ces objectifs, une signature numérique est une série de bits qui accompagne le message clair afin de répondre aux exigences citées précédemment.

La réalisation de ces signatures numériques peut se faire de deux manières :

- En inversant la cryptographie asymétrique
- En utilisant les fonctions de hachage

Dans ce qui suit, nous allons détailler les deux méthodes

IV.5.1.1. Signature numérique utilisant la cryptographie asymétrique

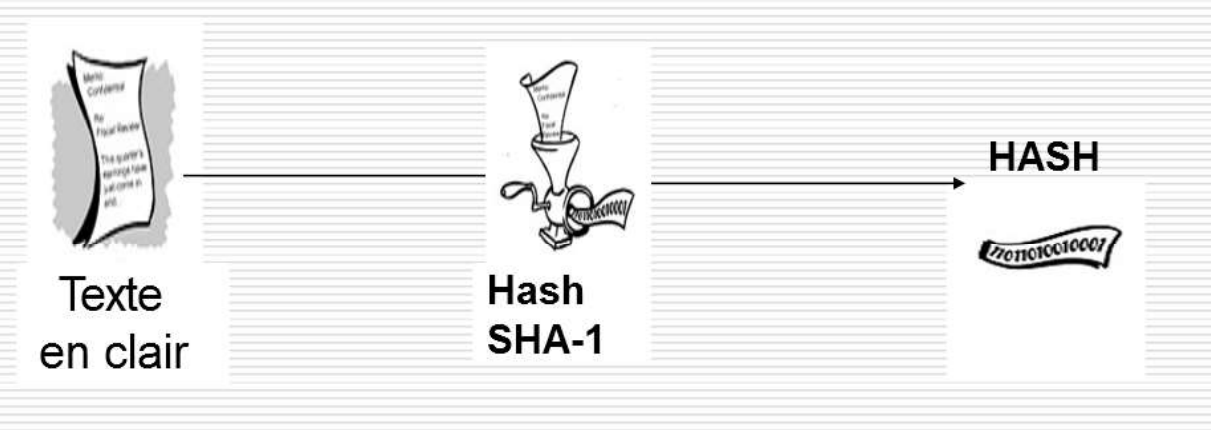


Sur le schéma, Alice envoie un message à Bob et oscar chiffré avec sa clé privée, un message chiffré avec la clé privé de Alice ne peut être déchiffrable que pas la clé publique correspondante.

- Bob et Oscar ayant pu déchiffrer le message avec la clé publique de Alice sont sûr que la source du message est bien Alice (authentification).
- Si un utilisateur malveillant parvient à modifier le message clair, Bob et Oscar vont s'en rendre compte, car en déchiffrant le message avec la clé publique d'Alice, ils vont trouver deux messages clairs différents et vont donc signaler une alerte (intégrité).
- Même Alice ne pourra pas nier d'avoir envoyé le message puisqu'il a été chiffré par sa propre clé privée que, elle seule, possède (non répudiation)

A noter ici que le principe de confidentialité n'est pas respecté car ne s'est pas notre objectif. Le problème de confidentialité a déjà été réglé avec la cryptographie hybride

IV.5.1.2. Signature numérique utilisant les fonctions de hachage



Les fonctions de hachage H (M) sont des fonctions mathématiques à sens unique, elles prennent une entrée de taille variable M et produisent des données de longueur de 160 bits généralement. En modifiant un seul bit de M, la sortie sera complètement différente (aucune similitude). Ces fonctions ont donc deux caractéristiques principales :

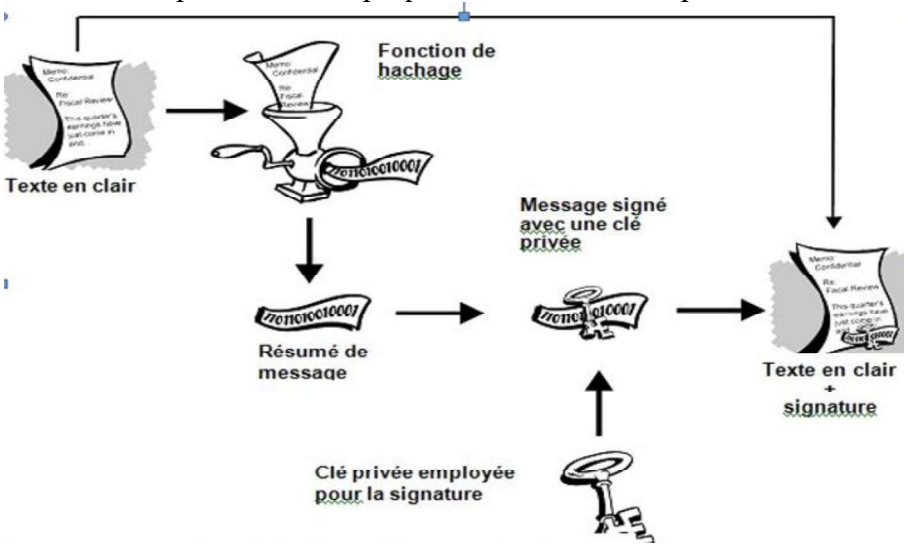
- **Unidirectionnelles :** A partir de H(M) il est impossible de retrouver M.
- **Sans collisions :** A partir de H(M) et M il est impossible de trouver M^1 <> M tel que $H(M^1) = H(M)$.

En réalité, on remplace le terme 'impossible ' par "très difficile", car il y a toujours des failles découvertes par la cryptanalyse.

Les fonctions de hachage les plus connues sont :

- **MD5** : Message Digest 5, il génère une empreinte de 128 bits.
- **SHA-1** : Sécure Hash Algorithm, il génère une empreinte de 160 bits.

Le but avec ce message haché est de l'utiliser comme empreinte digitale du message clair, donc comme signature numérique, comme expliqué sur le schéma ci-après :



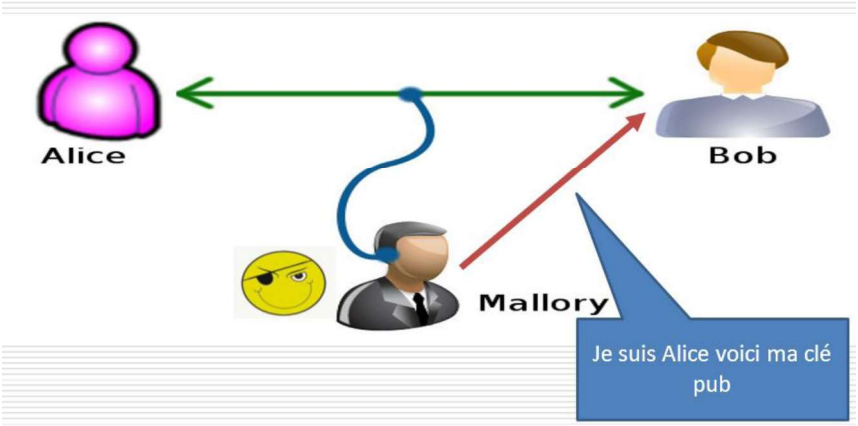
Alice prends un message clair M, hach une copie de M (qu'on appellera M') avec une fonction de hachage H(M'), puis le résultat est chiffré avec la clé privée asymétrique de Alice (k_{priva}) : $E_{kpriva}(H(M'))$. Au final Alice envoie à Bob M et $E_{kpriva}(H(M'))$. M est envoyé utilisant la cryptographie hybride.

A la réception du paquet, Bob déchiffre $E_{kpriva}(H(M'))$ avec la clé publique de Alice K_{puba} $D_{Kpuba}(E_{kpriva}(H(M')))=H(M')$, Bob récupère M envoyé par la méthode hybride puis recalcule H(M) et le compare avec H(M'), s'il trouve le même résultat donc :

- Le message M n'a pas été modifié au cours de sa route (**intégrité**)
- Bob est sûr que c'est Alice qui lui a envoyé le message, car $D_{\mathbf{Kpuba}}(E_{kpriva}(H(M')))=H(M')$ (**authentification**)
- Alice ne peut pas nier d'avoir envoyé le message toujours par ce que $D_{\mathbf{Kpuba}}(E_{kpriva}(H(M')))=H(M')$ (**non répudiation**)

De nos jours, les applications et communications sécurisées actuelles utilisent ce schéma de signature numérique

IV.6. Un dernier problème à résoudre avec les certificats numériques



Comme illustré au niveau du schéma ci-avant, Maillory peut placer une fausse clé publique Kpubm (celle de Maillory) comportant le nom et l'ID de Alice, puis il se présente à Bob au nom d'Alice. Bob, en croyant qu'il va parler avec Alice, va chiffrer son message M avec E_{Kpubm} (M), Alice, elle-même ne pourra pas déchiffrer le message, mais Maillory si !!!

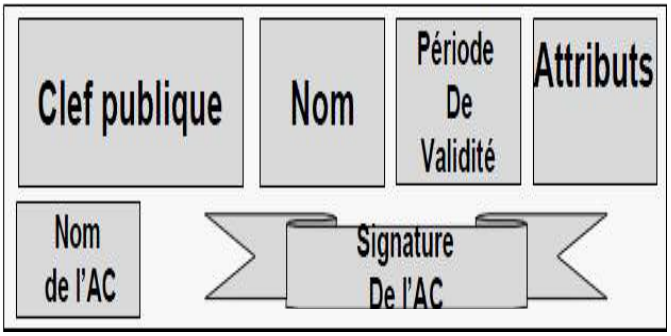
Il faut donc proposer un système permettant aux utilisateurs de vérifier qu'ils cryptent avec les bonnes clés publiques des destinataires, d'où le nom de Certificats numériques

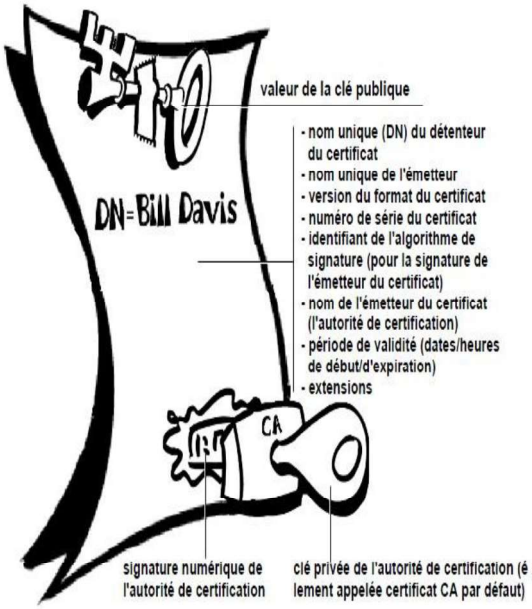
Dans la vie réelle, un certificat correspond à une référence : permis de conduire, carte d'identité certificat de naissance,…

Ce certificat est émis par une Autorité de Certification (Certificate Authority – CA) : mairie, consultat,… Les éléments du certificat contiennent des informations relatives à une personne et déclarant qu'une CA a confirmé son identité.

Un certificat numérique présente des similitudes avec un certificat physique, son rôle est de s'assurer qu'une clé publique appartient réellement à son détenteur supposé. Un certificat numérique d'une entité est composé de :

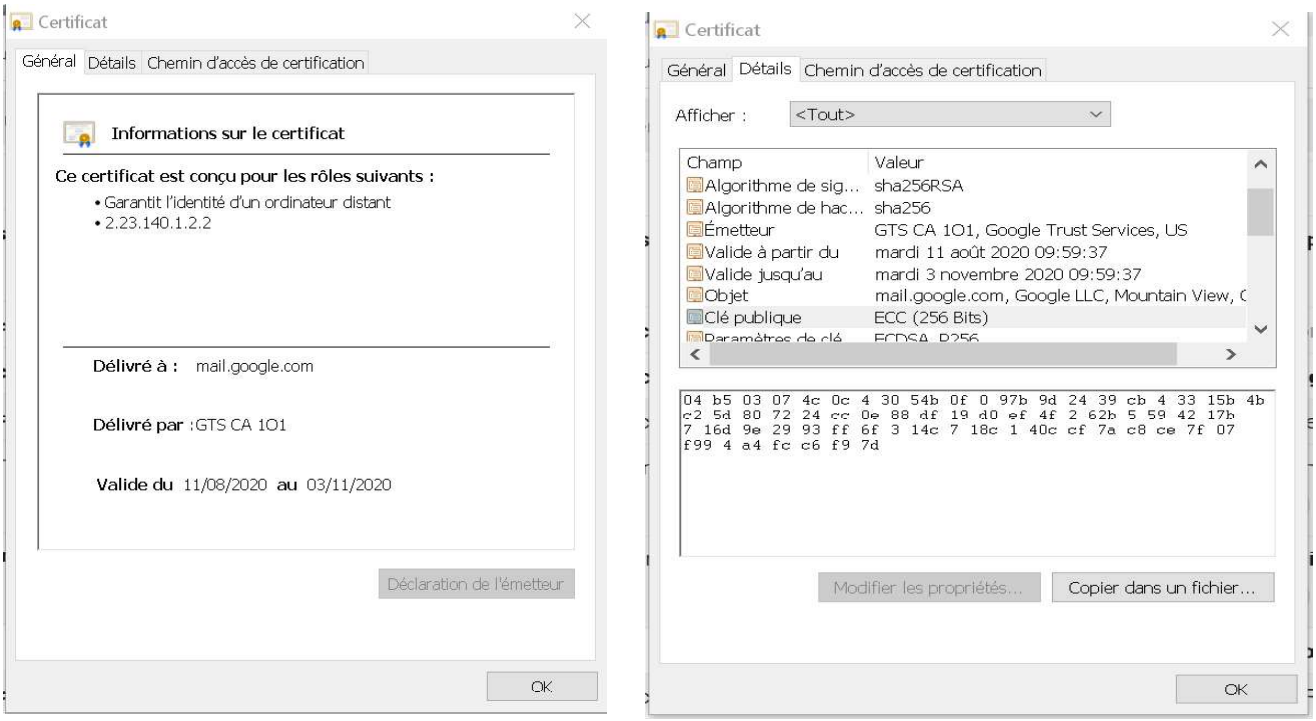
- Sa clé publique.
- Ses informations : nom, ID utilisateur, etc.
- Une ou plusieurs signatures numériques, particulièrement la signature de l'autorité de certification.
-



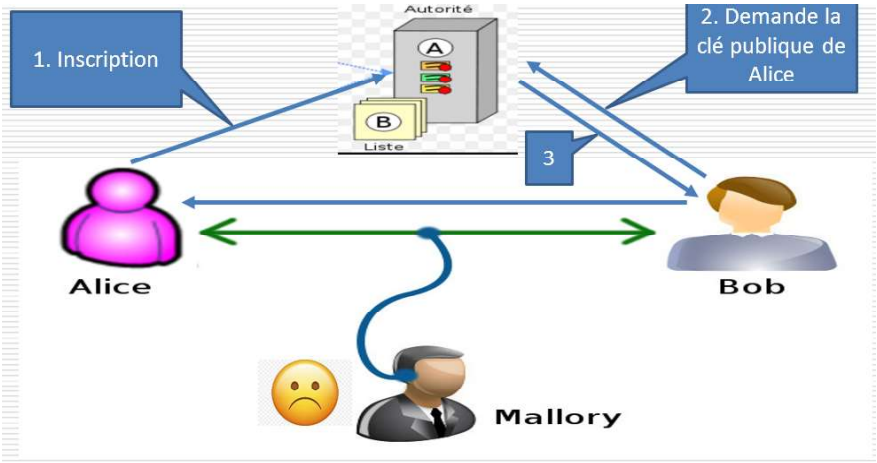


La signature numérique dans un certificat numérique permet d'attester que ces informations ont été attestées par une autorité de confiance (ou de certification).

Ci-dessous, un des certificats de Google :



IV.6.1. Nouvelle communication avec les certificats numériques

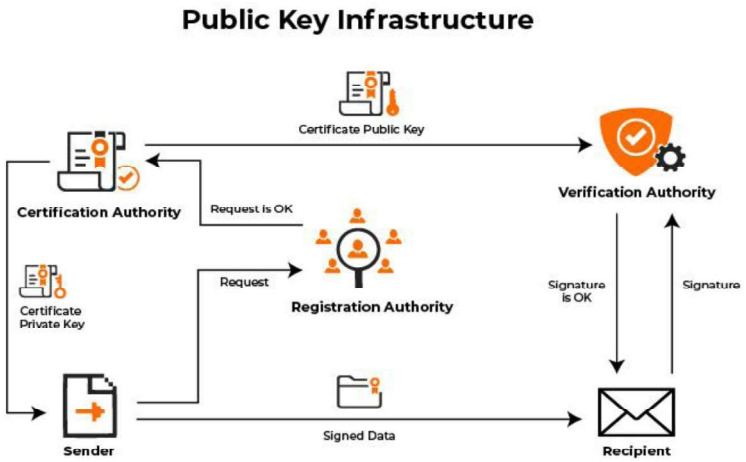


Après l'intégration des certificats numériques, la communication aura la forme suivante :

1. Alice commence par demander un certificat auprès de l'autorité de certification
2. L'autorité de certification vérifie les véracités des données du certificat de Alice, si tout est bon, le certificat sera stocké dans un annuaire.
3. Bob qui souhaite communiquer avec Alice, récupère la clé publique de Alice via l'annuaire, il va donc obtenir son certificat signé par l'autorité de certification et vérifie son intégrité grâce à la signature de la CA (étudié à la section précédente).

Dans ce nouveau schéma de communication, Maillory n'aura aucune chance d'usurper l'identité de Alice ou de Bob

IV.6.2. PKI (Public Key Infrastructure) Infrastructure à clefs publiques



Cette infrastructure contient un ensemble d'éléments, protocoles et services permettant de faire fonctionner plusieurs autorités de certifications qui délivrent des certificats. Une PKI est composée de :

- **Matériel** : PC, Salles Machines, Cloud…
- **Logiciel** : Programmes réseaux…
- **Ressource humaine** : les ingénieurs, développeurs…
- **Aspect juridique** : procédures de révocation…
- **Aspect administratif** : définir les responsabilités
- **Aspect Financier** : assurance des risques en cas d'incidents par utilisation de certificat

IV.7. Un simple et efficace résumé

- **Pour assurer la confidentialité (chiffrement hybride)** :
  - Clé (de session) Symétrique pour chiffré les messages
  - Clé Asymétrique pour chiffré la clé symétrique

- **Pour assurer l'intégrité, Authentification, Non répudiation** :
  - Fonctions de hachage pour la signature numérique
  - Certificats pour authentifier les clés publiques

IV.8. Autres systèmes de chiffrement

Dans une version plus avancée de ce manuscrit nous présenterons d'autres notions dans le domaine de la cryptographie, dont :

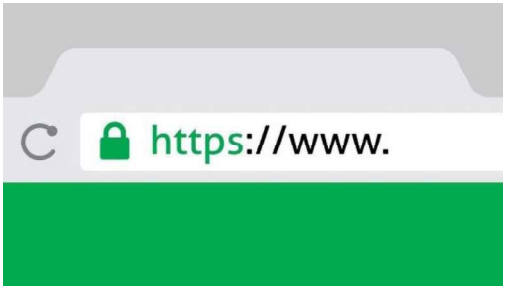
- L'échange de clés Diffie-Hellman
- Cryptographie à seuil
- Cryptographie Quantique (utiliser les propriétés de la physique quantique)
- MAC (Code d'Authentification de Message)
- ECC (La cryptographie sur les courbes elliptiques)
- TESLA
- …

En gros, ces concepts reprennent toujours les concepts utilisés dans ce document

IV.9. Protocoles cryptographiques

A partir du moment où on souhaite faire communiquer en sécurité plusieurs entités, on doit faire appel aux services de la cryptographie. En parlant 'd'échange sécurisé' on fait référence essentiellement aux trois objectifs essentiels de sécurité, à savoir la confidentialité, l'intégrité et l'authentification. La plupart des communications et applications sécurisées utilisent aujourd'hui un ou plusieurs protocoles cryptographiques.

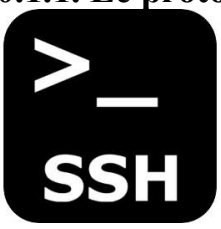
IV.10. Exemples d'applications et Communications sécurisées



Nous présentons dans cette section, quelques exemples d'applications et communications utilisant les principes de la cryptographie

IV.10.1 Communications sécurisées

IV.10.1.1. Le protocole SSH (Secure Shell)



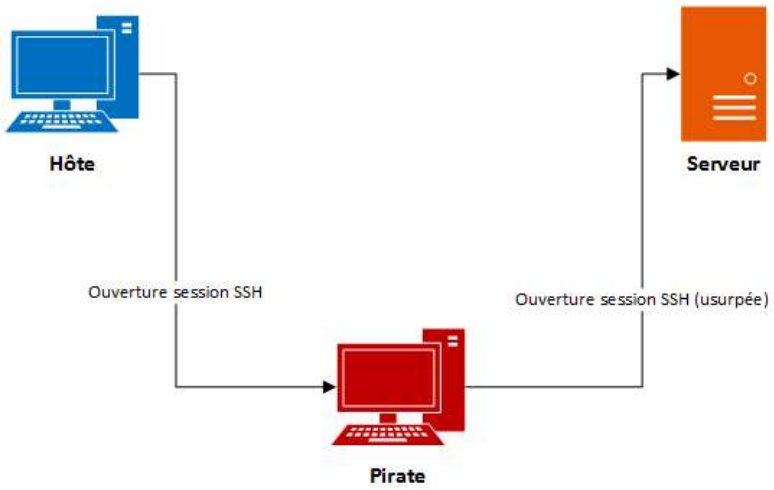
SSH est un protocole réseau d'accès distant à une machine tout comme Telnet, et rlogin. Cependant, ces derniers font circuler des messages en clair (y compris les mots de passes

d'accès à distance !), ce qui les rend très vulnérables. SSH par contre utilise un système de cryptographie hybride.
Un serveur SSH sous linux, stocke un couple de clés stocké dans son répertoire **/etc/ssh** généré lors du démarrage du service.

1. Quand un client SSH souhaite se connecter à un serveur SSH, ce dernier envoie sa clé publique au client.
2. Le client génère une clé symétrique, la chiffre avec la clé publique du serveur et envoie le cryptogramme au serveur
3. Le serveur décrypte le cryptogramme avec sa clé privée.
4. Pour montrer au client qu'il est bien le bon serveur, il chiffre une donnée standard avec la clé symétrique et l'envoie au client.
5. Si le client retrouve le message standard, alors il sera rassuré qu'il parle au bon serveur.
6. La clé symétrique est partagée, donc un canal sécurisé est établit.

Il faut noter que la clé symétrique est régénérée à chaque fois pour éviter à un pirate ayant eu accès à celle-ci d'en profiter plus longtemps en déchiffrant les échanges. C'est pour cela qu'on appelle cette clé symétrique régénérable : une clé de session.

Bien sûr, en l'absence de certificats numériques, le protocole SSH souffre du problème du Man in the middle : c'est-à-dire qu'un pirate peut remplacer la clé publique du serveur par la sienne et il se présente au client comme étant le serveur, et au serveur comme étant le client. Au final il aura une clé symétrique avec le client KPC et une autre avec le serveur KPS, qui lui permettront de lire tous les messages chiffrés et de passer transparent entre le client et le serveur



IV.10.1.2. Le protocole SSL/TLS (Secure Socket Layer)

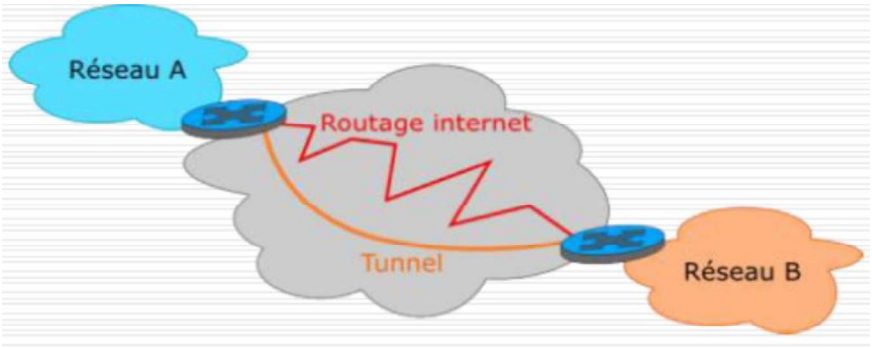
C'est un protocole réseau qui se trouve entre la couche application et la couche transport du modèle TCP/IP, c'est le célère HTTPS. Son fonctionnement se résume comme suit :

1. Le client envoie au serveur une demande de connexion http sécurisée Https.
2. Le serveur lui envoie son certificat : sa clé publique, ainsi qu'une signature numérique (de la AC) sous forme de texte chiffré.
3. Dans le cas idéal, le navigateur du client déchiffre la signature numérique de la CA et récupère la clé publique du serveur.

4. Le navigateur du client génère une clé de chiffrement symétrique, appelée clé de session, qu'il chiffre à l'aide de la clé publique contenue dans le certificat du serveur puis transmet cette clé de session au serveur.
5. Dorénavant, les requêtes et réponses http sont chiffrées via cette clé de session

IV.10.1.3. Le réseau VPN (réseau privé virtuel)

Un réseau VPN permet d'assurer des communications sécurisées en s'appuyant sur un réseau existant non sécurisé, d'où le nom de tunnel.



Dans l'une de ses versions, il utilise le protocole IPSEC contenant les protocoles suivants :

- **Le protocole AH** (Authentification Host) : pour l'authenticité des données échangées
- **Le protocole ESP** (Encapsuling Security Payload) : pour la confidentialité des données
- **Le protocole IPComp** pour compresser les paquets
- **Le protocole IKE** (Internet Key Exchange) : pour l'échange des clés des différents chiffrements.

IV.10.2 Applications sécurisées

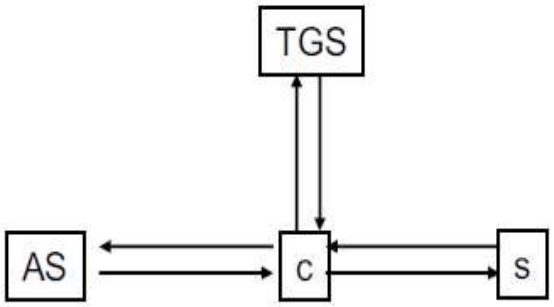
IV.10.2.1. PGP

PGP est un programme exemple type de la cryptographie hybride, les exemples de la cryptographie hybride du document sont pris de PGP. PGP utilise en plus la compression des données ainsi qu'une clé symétrique de session (clé régénérable)

IV.10.2.2. KERBEROS

C'est est un protocole d'authentification au sein d'un réseau qui utilise un système de tockets, il utilise les éléments suivants dans son protocole :

- **Le client** (C),
- **Le centre de distribution de clés** (AS: Authentication Server)
- **Le serveur de tickets** (TGS pour ticket granting server)
- **Le serveur** (S)



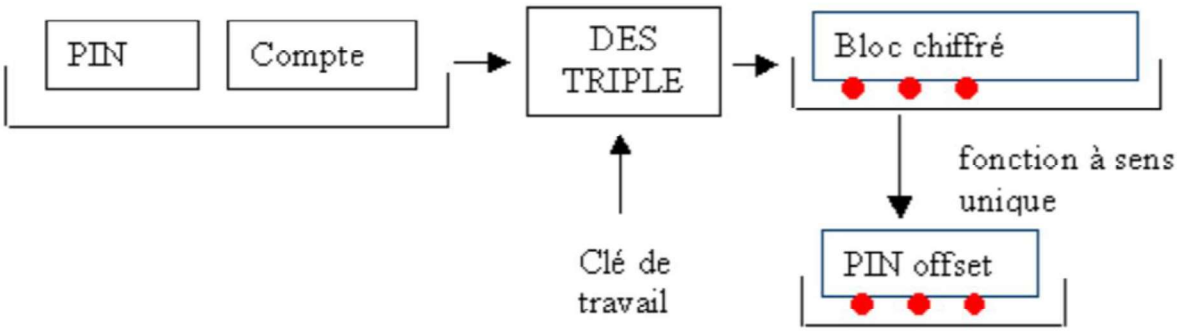
IV.10.2.3. Les cartes à puce

Généralement, les cartes à puce utilisent l'algorithme symétrique DES dans son fonctionnement. La carte contient un code PIN qui est un nombre de 4 chiffres permettant de s'assurer que seules les personnes autorisées peuvent utiliser la carte.

Lors de la fabrication de la carte :

1. Un numéro PIN sera généré aléatoirement
2. Ce PIN + numéro de compte seront chiffrés par un algorithme symétrique 3DES, en utilisant une clé appelée clé de travail
3. Une fonction à sens unique extrait certains bits du cryptogramme obtenu, ces bits sont appelés PIN offset
4. Le PIN Offset est stocké dans la mémoire de la carte, avec le numéro de compte.
5. Le PIN est posté au possesseur de la carte et effacé de la mémoire.
6. Une fois la carte émise, seul le possesseur légitime de la carte connaît le PIN

La figure suivante montre le calcul du PIN offset



Le propriétaire de la carte procèdera comme suite, après avoir inséré sa carte dans le terminal (distributeur de billets) :

1. Il tape son PIN sur le terminal
2. Le terminal chiffre le PIN et le numéro de compte par 3DES, en utilisant la clé de travail et extrait le PIN offset
3. Le PIN offset est comparé avec celui enregistré sur la carte.

TD4. Exercices de la partie IV

TD4.1. Exercices en QCM

1. Citez-le(s) principe(s) de sécurité traité(s) par un système de cryptographie symétrique
    - Authentification, intégrité, non-répudiation.
    - Disponibilité, intégrité, authentification.
    - Confidentialité, intégrité, non-répudiation.
    - Respect de vie privée, intégrité, disponibilité
2. L'inconvénient de la cryptographie symétrique est :
    - Le temps de calcul
    - L'espace de stockage des clés
    - La difficulté de partager un secret
    - La vulnérabilité aux attaques classiques
3. Le protocole SSH
    - Utilise la cryptographie hybride pour l'administration à distance des serveurs
    - Utilise le HTTPs
    - Remplace le protocole Telnet
    - Est un protocole d'administration à distance
4. Un certificat numérique permet de :
    - S'assurer qu'on parle avec la bonne personne
    - S'assurer que les messages arrivent sans modifications
    - S'assurer que le message n'a pas été lu par une personne non autorisée
    - S'assurer qu'on chiffre avec la bonne clé publique
5. Une méthode de signature numérique :
    - Permet d'envoyer la clé à son interlocuteur pour que celui-ci puisse décrypter les données
    - Permet de hacher les données en plus du chiffrement
    - Est utilisée pour assurer l'intégrité des échanges
    - Aucune bonne réponse
6. Citez-le(s) principe(s) de sécurité traité(s) par les fonctions de hachage
    - Authentification, intégrité, non-répudiation.
    - Disponibilité, intégrité, authentification.
    - Confidentialité, intégrité, non-répudiation.
    - Respect de vie privée, intégrité, disponibilité
7. Une PKI permet de résoudre :
    - Le problème de distribution de mots de passe
    - Le problème de distribution de clefs publiques
    - Le problème de la confidentialité
    - Le problème de l'authentification
8. Une méthode de chiffrement symétrique :
    - Consiste à communiquer la clé à son interlocuteur pour que celui-ci puisse décrypter les données.
    - Permet de compresser les données en plus du chiffrement.

- Est plus rapide qu'une méthode de chiffrement asymétrique
- Aucune bonne réponse

9. Une attaque par statistique pour casser une clé de chiffrement est :
   - Tester tous les cas possibles
   - Analyser la fréquence d'apparition des lettres
   - Correspondre les lettres de la langue avec celles du texte à déchiffrer
   - Aucune réponse n'est correcte
10. Une signature numérique permet de :
   - S'assurer qu'un message provient de la bonne personne
   - S'assurer que le message n'a pas été modifié durant un transfert
   - S'assurer que le message n'a pas été lu par une personne non autorisée
   - Détecter une personne qui nie avoir fait une action
11. Les fonctions de hachage sont utilisées pour
   - Les certificats numériques
   - Les signatures Numérique
   - Assurer la confidentialité des messages
   - Assurer l'intégrité des messages

12. Une Infrastructure à clés publiques :
   - Permet de hacher les données en plus du chiffrement asymétrique
   - Permet de stocker les clés symétriques des individus
   - Permet de stocker les clés publiques des individus
   - Permet de stocker des certificats numériques
13. Le protocole HTTPs
   - Utilise la cryptographie hybride
   - Utilise le DNS
   - Utilise le protocole SSL
   - Est un protocole de téléchargement de fichiers sécurisé

Solution du TD4.1. Exercices en QCM

1. Citez-le(s) principe(s) de sécurité traité(s) par un système de cryptographie symétrique
   - Authentification, intégrité, non-répudiation. **
   - Confidentialité, intégrité, non-répudiation. **

2. L'inconvénient de la cryptographie symétrique est :
   - L'espace de stockage des clés***
   - La difficulté de partager un secret***

3. Le protocole SSH
   - Utilise la cryptographie hybride pour l'administration à distance des serveurs***
   - Remplace le protocole Telnet ***
   - Est un protocole d'administration à distance***

4. Un certificat numérique permet de :
   - S'assurer qu'on parle avec la bonne personne***
   - S'assurer que le message n'a pas été lu par une personne non autorisée***
   - S'assurer qu'on chiffre avec la bonne clé publique***

5. Une méthode de signature numérique :
   - Permet de hacher les données en plus du chiffrement***
   - Est utilisée pour assurer l'intégrité des échanges***

6. Citez-le(s) principe(s) de sécurité traité(s) par les fonctions de hachage
   - Authentification, intégrité, non-répudiation. ***

7. Une PKI permet de résoudre :
   - Le problème de distribution de clefs publiques **
   - Le problème de l'authentification **

8. Une méthode de chiffrement symétrique :
   - Consiste à communiquer la clé à son interlocuteur pour que celui-ci puisse décrypter les données. ****
   - Est plus rapide qu'une méthode de chiffrement asymétrique***

9. Une attaque par statistique pour casser une clé de chiffrement est :
   - Analyser la fréquence d'apparition des lettres***
   - Correspondre les lettres de la langue avec celles du texte à déchiffrer***

10. Une signature numérique permet de :
    - S'assurer qu'un message provient de la bonne personne***
    - S'assurer que le message n'a pas été modifié durant un transfert ***
    - Détecter une personne qui nie avoir fait une action ***

11. Les fonctions de hachage sont utilisées pour
    - Les certificats numériques***
    - Les signatures Numérique **
    - Assurer l'intégrité des messages ***

12. Une Infrastructure à clés publiques :
    - Permet de stocker les clés publiques des individus***
    - Permet de stocker des certificats numériques***

13. Le protocole HTTPs
    - Utilise la cryptographie hybride ***
    - Utilise le protocole SSL***

TD4.2. Exercices d'application extraits d'examens

Exercice 1 : « questions de compréhension »

1. L'administrateur souhaite installer au niveau du réseau un système de cryptographie hybride comme PGP avec certificat numérique, donner tous les éléments nécessaires

2. L'administrateur réseau de cette entreprise veut transformer le serveur HTTP à un Serveur HTTPS. Pour cela, il doit implémenter le protocole SSL qui utilise un système de cryptographie hybride, Donnez le nouveau fonctionnement de la requête et réponse HTTPS

3. Déchiffrez le message '**cuskqxwmfwituk**' crypter avec Vigenère utilisant le mot de passe '**bgfbcdfbfdecdg'** et le mot de passe **'quauwtedbdisjg'** (a=0, b=1, etc). **(2 points)**

4. Expliquez l'intérêt des signatures et certificats numériques dans un système de communication.

5. Expliquez comment utiliser la cryptographie pour assurer les objectifs de la sécurité informatique suivants :

- L'intégrité
- La confidentialité
- La disponibilité
- La non répudiation
- L'authentification
- Disponibilité

Solution de quelques questions de l'exercice 1

1. L'administrateur souhaite installer au niveau du réseau un système de cryptographie hybride comme PGP avec certificat numérique, donner tous les éléments nécessaires
- L'ensemble des clés possibles (espace de clés) : clés pub, privées et clés de session
- Les algorithmes de chiffrement et déchiffrement : RSA, AES, SHA
- Les fonctions de hachage **et** Les certificats numériques
- L'infrastructure PKI

2. L'administrateur réseau de cette entreprise veut transformer le serveur HTTP à un Serveur HTTPS. Pour cela, il doit implémenter le protocole SSL qui utilise un système de cryptographie hybride, Donnez le nouveau fonctionnement de la requête et réponse HTTPS

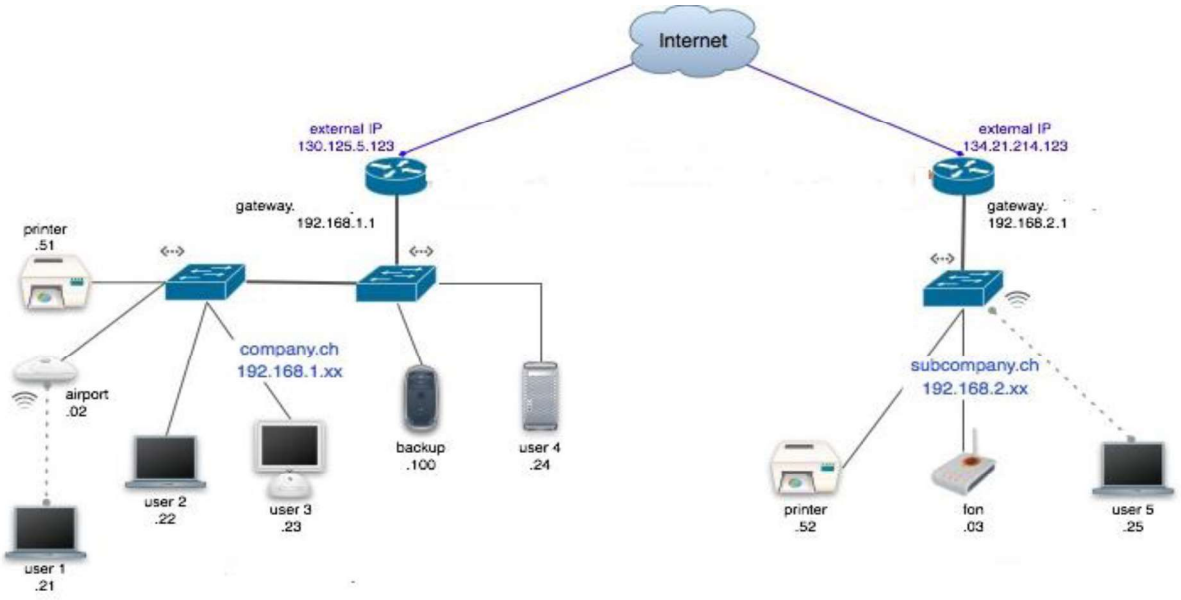
- Le client envoie au serveur une demande de connexion http sécurisée TLS.
- Le serveur lui envoie son certificat : sa clé publique, ainsi qu'une signature numérique (de la AC) sous forme de texte chiffré.
- Le navigateur du client déchiffre la signature numérique et récupère la clé publique du serveur.
- Le navigateur du client génère une clé de chiffrement symétrique, appelée clé de session, qu'il chiffre à l'aide de la clé publique contenue dans le certificat du serveur puis transmet cette clé de session au serveur.
- Dorénavant, les requêtes et réponses http sont chiffrés via cette clé de session

3. Déchiffrez le message '**cuskqxwmfwituk**' crypter avec Vigenère utilisant le mot de passe '**bgfbcdfbfdecdg'** et le mot de passe **'quauwtedbdisjg'** (a=0, b=1, etc). **(2 points)**

Avec mot de passe '**bgfbcdfbfdecdg'** : **bonjourlaterre.**
Avec mot de passe '**quauwtedbdisjg'**: **masquesjetable.**
Il est difficile de connaitre le vrai message clair.

Exercice 2 : « Cryptographie en pratique »

Soit le réseau suivant :



1. On souhaite connecter (en sécurisé) les deux réseaux du schéma, quelles sont les différentes solutions possibles ?
2. Expliquez le principe de fonctionnement global de chaque solution en montrant le rôle des certificats numériques.

Solution exercice 2 : « Cryptographie en pratique »

1. SSH et VPN
2. Principe de fonctionnement : cryptographie hybride=symétrique + asymétrique
Rôle des certificats numériques : éviter l'attaque man in the middle

Exercice 3 :

Soit le message : « **Cryptographiemodernes»**. Chiffrez le message avec les méthodes suivantes :

1. Hill

0	5	10
1	12	20
2	10	5

2. Vigenère, avec la clé « **symetrique »**
3. Affine, avec la clé (15,10)

4. Playfair, avec la matrice

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

5. Donnez une clef de vernam qui permet de déchiffrer le résultat du chiffrement de hill pour trouver le mot « **ACLUVWVCMNFINOPDDGCJC»**

Solution d'exercice 3

Soit le message : « **Cryptographiemodernes»**. Chiffrez le message avec les méthodes suivantes :

1. Hill

0	5	10
1	12	20
2	10	5

BQYPJUVIQZFAGSGWHRGLQ

2. Vigenère, avec la clé « **symetrique »**

UPKTMFOHUTZGQQHUMHHIK

3. Affine, avec la clé (15,10)

OFGBJMWFKBLASIMDSFXS U

4. Playfair, avec la matrice

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

ILZSNEDKXSMVITIYIXTOJY

5. Donnez une clef de vernam qui permet de déchiffrer le résultat du chiffrement de hill pour trouver le mot « **ACLUVWVCMNFINOPDDGCJC»**

BONVOYAGEMASTERTELECO

Exercice 4

Soit le message : « **Cryptographiemoderne »**. Chiffrez le message avec les méthodes suivantes :

6. Hill

0	5	10	11
1	12	20	21
2	10	5	4
3	4	5	6

7. Transposition, avec la clé « **symetrique »**
8. Donnez une clef de vernam qui permet de déchiffrer le résultat du chiffrement de la transposition pour trouver le mot « **recuperationdedonnee »**

Solution de l'exercice 4

Soit le message : « **Cryptographiemoderne »**. Chiffrez le message avec les méthodes suivantes :

1. Hill

0	5	10	11
1	12	20	21
2	10	5	4
3	4	5	6

vokpepkcyvdeyywjyhte

2. Transposition, avec la clé « **symetrique »**

ppgyroctarmeeerdhoni

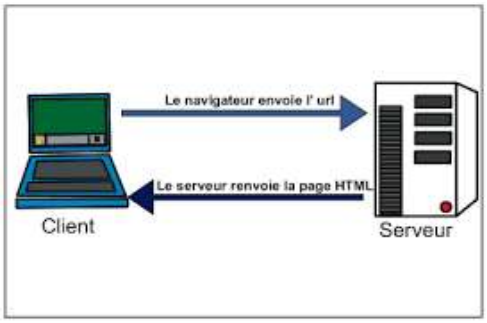
3. Donnez une clef de vernam qui permet de déchiffrer le résultat du chiffrement de la transposition pour trouver le mot « **recuperationdedonnee »**

yleecklthjyrbaopubje

Exercice 5

Soit la communication entre un client et un Serveur WEB, on veut rendre ce lien sécurisé.

1. Indiquer le rôle des composants d'une clé publique et d'une clé privée



2. Le client ne connait pas le serveur mais ce dernier lui affirme qu'il dispose d'une paire de clé délivrées par une entité tierce, comment appelle t on cette entité ?

3. Quelles sont les informations nécessaires qu'il faut avoir avec cette paire de clé ?

4. Que serait l'intérêt d'ajouter un système de cryptographie symétrique à ce schéma ?

5. Proposez les étapes de fonctionnement complet du nouveau système sécurisé.

6. Proposez un système d'authentification d'une requête HTTP

Exercice 6

Soit le message : « **Masterdeuxtelecomm »**. Chiffrez le message avec les méthodes suivantes :

4. Hill

5	10	11
12	20	21
10	5	4

5. Vigenère , avec la clé « **crypto** »
6. Donnez une clef de vernam qui permet de déchiffrer le résultat du chiffrement de Vigenère pour trouver le mot « **soutenancepfetelec** »
7. Playfair :

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

Exercice 7

Chiffrez puis déchiffrez le message **SECURITERESEAU** avec :

1. César, K= 17
2. Chiffrre de Hill

k k-1

$$\begin{pmatrix} 5 & 12 \\ 15 & 25 \end{pmatrix} \quad \begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$$

3. Chiffre de Vigenère, **k=MRRIAHLA**, essayez de le déchiffrer avec une autre clé et avoir un message utile
4. Verman, **k= aszerfdcnvbgtf**
5. Proposez un système de chiffrement qui évite les attaques par statistiques
6. Donnez l'utilisation et le but d'une clé de session

TD4.3. Exercices d'application extraits d'une série de TD

Exercice 1

Le chiffrement de César prend un texte composé de lettres, et décale chaque lettre d'un nombre constant de positions dans l'alphabet. Ce nombre de positions est la clé.

Tableau1. *Code de l'alphabet*

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

1. Chiffrer le message suivant avec clé =4 : **CHIFFREMENT DE CESAR**
2. Déchiffrer le message suivant avec clé=5 : **HJHTIJUJZYJYWJHFXXJ KFHNQJRJSY**
3. Montrer qu'il est très aisé de déchiffrer le message suivant sans connaitre la clé :

ZSGAS HWSFG RWBHS FBSH

4. Est-il plus facile de déchiffrer un texte long ou un texte court ?
5. Que remarquez-vous dans le cas où clef =13 ?

Exercice 2

Le chiffrement de Vigenère est une sorte de chiffrement de César amélioré. La clé est constituée non pas d'un, mais de plusieurs décalages. Cette clé est spécifiée sous la forme d'un mot.
Par exemple, la clé « BAC », de longueur trois, spécifie que pour chiffrer un message, on décale la première lettre d'une position (lettre B), la deuxième de zéro positions (lettre A), la troisième de deux positions (lettre C), et ainsi de suite en reprenant la clé au début.
(Les lettres ont une valeur de A=0 à Z=25).
1. Chiffrer le message suivant en utilisant la clé = **SECU :**

CHIFFREMENT DE VIGENERE

2. Sachant que le message a été chiffré, par la méthode de Vigenère, en utilisant la clé « CRYPTO », quel est le message en clair obtenu en déchiffrant le cryptogramme suivant :

OFBJESUVAJKWVVGCYCTDYIBEWV

3. Déchiffrer le message suivant chiffré par la méthode de Vigenère avec une clé de longueur 2 (sans connaître la clé)

OSFFBDWCJFDAPSGSYWJSQSUSQSVHSZXGFCQ
GLRHFHRHBRGMCXFVQRAPSXBSFRHRQRZHGXF

Exercice 3

Un groupe de n personnes souhaite utiliser un système cryptographique pour s'échanger deux à deux des informations confidentielles. Les informations échangées entre deux membres du groupe ne devront pas pouvoir être lues par un autre membre.
Le groupe décide d'utiliser un système symétrique de chiffrement.
1. Quel est le nombre minimal de clefs symétriques nécessaires ?
2. Donner le nom d'un algorithme de chiffrement symétrique connu.

Le groupe décide ensuite de remplacer ce système par un système asymétrique.
3. Quel est le nombre minimal de couples de clefs asymétriques nécessaires pour que chaque membre puisse envoyer et recevoir des informations chiffrées/signées ?
4. Bob souhaite envoyer des informations chiffrées et signées à Alice (Bob et Alice appartiennent tous les deux au groupe). Quelle(s) clef(s) Bob doit-il utiliser ?
5. Donner le nom d'un algorithme de chiffrement asymétrique connu.

Le groupe décide finalement d'utiliser un système hybride pour le chiffrement (c'est-à-dire qui utilise la cryptographie symétrique et asymétrique).
6. Donner les raisons qui ont poussé ce groupe à utiliser un tel système.

Exercice 4

Bob, qui utilise souvent la messagerie sécurisée de son entreprise, vient de perdre sa clef privée mais dispose encore de la clef publique correspondante.
1. Peut-il encore envoyer des courriers électroniques chiffrés ? En recevoir ?

2. Peut-il encore signer des courriers électroniques qu'il envoie ? Vérifier les signatures des courriers électroniques qu'il reçoit ?

3. Que doit-il faire pour être de nouveau capable d'effectuer toutes les opérations mentionnées ci-dessus ?

Exercice 5

Pour résoudre le problème de l'authentification d'une clef publique, on utilise très souvent la solution des certificats.

1. Qu'est-ce qu'un certificat et quelles sont les informations qu'il contient ?

2. Discuter les deux scénarios suivants en termes de sécurité :

- Deux certificats différents sont signés par la même clef privée.
- Deux certificats différents contiennent la même clef publique.

Solutions des exercices des parties 1, 2 et 3

Solution du TD1. Travaux dirigés du chapitre I

TD1.1. Questions QCM

1. L'analyse de la situation lors de l'analyse de risque permet de :
   - Définir un périmètre de sécurité **
   - Définir le contexte de la politique de sécurité
   - Définir les éléments du système à protéger**
   - Faire un audit de sécurité
2. L'analyse de risque permet de :
   - Mesurer la fréquence d'apparition des incidents***
   - Installer des systèmes contre les risques identifiés
   - Préparer une politique de sécurité ***
   - Faire des audits de sécurité.
3. Le respect de la vie privée permet de :
   - Assurer l'anonymat des utilisateurs**
   - Assurer l'authentification des utilisateurs
   - Assurer la confidentialité des informations des utilisateurs**
   - Assurer la non répudiation
4. Le rôle de la sécurité en entreprise est :
   - Réduire le risque à un niveau acceptable**
   - Prévenir tout risque
   - Empêcher les employés de travailler correctement
   - Surveiller le bon fonctionnement des systèmes**
5. La politique de sécurité permet de :
   - De répondre aux incidents de sécurité selon leur fréquence et cout***
   - Installer des systèmes contre les risques identifiés
   - Préparer une analyse de situation
   - Faire des audits de sécurité.
6. La non répudiation :
   - Permet de garder la trace de qui a fait quoi****
   - Permet d'assurer la vie privée des personnes
   - A besoin des signatures numériques***
   - Est un objectif de sécurité***
7. La politique de sécurité permet de :
   - Préparer des mécanismes de sécurité***
   - Définir le contexte de la politique de sécurité
   - Définir les incidents possibles sur le système à protéger
   - Faire un audit de sécurité
   - Répondre aux incidents de sécurité selon leur fréquence et cout***
8. Quand on a un risque à cout faible mais à haute fréquence :
   - On installe des serveurs miroirs***
   - On accepte le risque
   - On installe des mécanismes de sécurité
   - On tente d'assurer la disponibilité des données et des services***

TD1.2. Exercices

Exercice 1 « Méthode d'analyse de risque »

La banque WDZ subit chaque année six infections par des malwares (virus, vers….) et quatre déformations de son site internet. La restauration du bon état des machines âpres une infection requiert deux jours de travail à l'administrateur, avec un cout de 200 000 DZD. Le design du site internet peut être réparé en 06 heures, avec un cout de 100 000 DZD.

Une société tierce de sécurité informatique propose le déploiement et la maintenance d'un antivirus et d'un outil de protection du site internet avec un cout annuel de 2 500 000 DZD.

1. Calculer le risque annuel

Si on se base uniquement sur les données financière, le risque est calculé comme suit :

La solution locale coute 6(fois)*200 000(DZD) + 4(fois)*100 000(DZD)=1 200 000+400 000=1 600 000 DZD par an

La solution de la société tierce coute 2 500 000 par an

Il est clairement indiqué que la solution locale est beaucoup moins couteuse que la solution de la société tierce. Donc la banque perdrait de l'argent en achetant une telle solution

2. Est-il bénéfique pour l'entreprise WDZ d'acheter la solution proposée par la société tierce ? Pourquoi ?

D'autres risques avec des conséquences dramatiques n'ont pas été prises en considération dont :

Le problème de disponibilité : le site n'est pas disponible pendant 6(fois)*2(jours) + 4(fois)*6(heurs)= 12 jours + 24 heures= 13 jours par an. Site internet d'une banque absent 13 jours par an, C'est énorme ! Pourtant la disponibilité est l'un des principes de base de la sécurité informatique.

L'image de marque de la banque : les clients ne sont surtout pas contents de ne pas pouvoir effectuer leurs transactions bancaires plusieurs fois par an, ce qui les pousserait à changer de banque !

En conclusion : la solution de la société tierce s'avère plus pertinente, voir indispensable, même si elle coute plus cher.

Exercice 2 « questions sur la sécurité des systèmes d'information»

1. Pourquoi le niveau réel de sécurité d'un système d'information est toujours inferieur au niveau estimé par un RSSI ?

Par ce que du jour au lendemain on détecte de nouvelles attaques et failles de sécurité au niveau :

1. Des outils automatisant les systèmes d'information
2. Des outils de sécurité eux-mêmes

Le problème est que si on ne prend pas de précautions, cette différence de niveau de sécurité tend à augmenter avec le temps.

2. Décrire le genre de mesures à prendre pour éviter une baisse du niveau de sécurité.

Il faut être vigilant, attentif et surtout se tenir informer aux nouvelles failles de sécurité. Ainsi, il faut

- installer les mises ajours correctifs de sécurité sur les systèmes d'exploitation, des serveurs de base de données, logiciels et outils de sécurité,…etc
- Effectuer des audits réguliers et revoir à chaque fois la politique de sécurité

3. Les systèmes d'information des entreprises sont plus exposés aux attaques informatiques aujourd'hui, donner quelques raisons ?

- L'utilisation des réseaux sociaux dans un environnement professionnel,
- L'augmentation du nombre d'utilisateurs et dispositifs connectés à internet
- L'ouverture des systèmes d'information aux partenaires des entreprises

4. On souhaite sécuriser l'accès des personnes à une entreprise, donnez les différentes méthodes à utiliser pour avoir des systèmes d'authentification efficaces.

- Utiliser une carte magnétique pour y accéder
- Utiliser un système de reconnaissance faciale ou par empreinte
- Utiliser un mot de passe d'accès

Pour avoir une authentification forte, on combine au moins deux des trois systèmes d'accès précédents

5. Expliquez l'impact des réseaux sociaux (Facebook, twitter, etc.) sur la sécurité des systèmes d'information des entreprises.

Un pirate peut se faire des amis avec les employés de l'entreprise via ces Réseaux pour récupérer des informations confidentielles de l'entreprise.

Exercice 3 « Etapes de sécurisation des systèmes d'information »

Remplir le tableau ci-dessous par les actions suivantes

Analyse de la situation	Analyse de risque	Politique de sécurité	Mesures de sécurité	Implémentation	Validation
5	**6, 9**	**2, 11**		**3, 4, 7, 8**	**1, 10**

12. Essayer de pirate ma propre politique de sécurité.
13. Le serveur Web tombe fréquemment en panne il faut prévoir une redondance
14. Recruter un ingénieur en sécurité informatique
15. Installer un système de détection d'intrusion
16. Déterminer le périmètre du système à protéger
17. Le serveur web tourne sur une vielle machine avec une alimentation faible
18. Recruter un administrateur réseau compètent
19. Installer un antivirus
20. Le serveur web tourne sur une vielle machine
21. Tester les vulnérabilités du système de sécurité mis en place.
22. Le serveur ftp tombe fréquemment en panne il faut prévoir une redondance

Exercice 4 « Objectifs de sécurité »

2. Pour chaque risque ci-dessous, fournissez les vulnérabilités et montrez s'il s'agit d'un problème de confidentialité (**C**), d'intégrité (**I**) ou de disponibilité (**D**)

Risque	Vulnérabilité	C	I	D
Certains employés se connectent à internet avec leurs smartphone via le réseau de l'entreprise	**Propagation virus dans le réseau**	*	*	*

Le vice-président de la comptabilité est recruté par un concurrent	**Divulguer des informations secrètes**	*		
L'entreprise envoie des données sans signatures numériques	**Modifier les messages sans autorisations**		*	
L'administrateur réseau de l'entreprise travail comme consultant chez un concurrent	**Divulguer des informations secrètes**	*		
Certains utilisateurs utilisent leurs PCs portable personnels dans l'entreprise	**Propagation virus dans le réseau**	*	*	*
Certains utilisateurs insèrent leurs clés USB non scannées dans les PCs de l'entreprise	**Propagation virus dans le réseau**	*	*	*
L'entreprise utilise un mot de passe par défaut pour accéder à ses applications de gestion.	**Des pirates peuvent accéder à ses application : problème d'authentification**			

Solution du TD2. Travaux dirigés du chapitre II

Exercice 1 : « QCM rapide »

1. Une attaque passive :
   - Consiste à briser l'intégrité des messages
   - Consiste à effectuer une attaque DOS
   - Consiste à effectuer une attaque d'espionnage**
   - Consiste à effectuer une attaque visant la confidentialité**

2. Une attaque de déni de service consiste à :
   - Refuser l'accès d'un client à un serveur en se faisant passer par ce dernier
   - Empêcher les utilisations légitimes d'avoir accès à un système**
   - Casser la clé de chiffrement d'un échange de données
   - Utiliser une erreur de programmation dans un système donné pour le compromettre **

3. Quels sont les problèmes de sécurité relatifs à une attaque par interruption
   - Déni de service***
   - Fabriquer de faux message d'erreur
   - Modifier illégalement la clé du réseau wifi
   - Vol de mot de passe

Exercice 2 : « Questions de compréhension »

1. Donnez la définition, avec un exemple d'attaque en réalité de chaque catégorie : Interruption, interception, modification et fabrication.

Interruption : Bloquer le fonctionnement d'un routeur critique (qui mène vers plusieurs destinations) sur internet

Interception : Intercepter le mot de passe d'accès à une base de données en espionnant le réseau wifi

Modification : augmenter illégalement le montant du compte bancaire d'un pirate

Fabrication : générer de faux messages d'alerte à un administrateur réseau

3. Donnez et expliquez deux exemples d'attaques passives et actives.

Attaque passive :

4. Espionner les conversations téléphoniques
5. Comprendre la signification des messages circulants à travers un réseau pour préparer une attaque active.

Attaque active :

6. Le pirate change illégalement le contenu d'une conversation sur Skype entre deux utilisateurs victime
7. Le pirate falsifie les informations de routage pour saturer la table de routage des routeurs par des chemins fictifs

4. Comment assurer le principe de la disponibilité ?
Assurer la disponibilité des services : (déployer des serveurs miroirs).
Duplication des données,

5. Donner deux exemples d'attaques par interruption

Déni de service : DOS
Déni de service distribué : DDOS

TD3. Travaux dirigés du chapitre III

TD3.1. « Questions QCM »

1. Un screenlogger est :
   - Une préparation d'une attaque passive
   - Un cheval de Troie***
   - Une préparation d'une porte dérobée***
   - Logiciel Espion ***

2. Un mail de ma banque m'avertit que mon compte a été débité de 78 DZD par erreur. Pour me faire rembourser, je suis invité à cliquer sur le lien dans le message afin de confirmer mes coordonnées de compte. Quel est le piège à éviter ?
   - Je clique sur le lien et je tombe sur le site de ma banque avec les cases à remplir. Je les remplis, c'est très simple. ***
   - Je vais sur le site de ma banque en utilisant mes favoris dans mon navigateur pour voir ce qu'il en est.
   - Je détruis le mail sans me soucier de la mise à jour de mes données bancaires.
   - Je téléphone à ma banque et je traite cela par téléphone.

3. Mon petit frère a téléchargé un petit jeu sympa sur Internet que j'amènerais bien au bureau pour montrer aux collègues. Quelle est la meilleure attitude à adopter ?
   - Je l'amène au bureau sur une clé USB que j'ai passée à l'anti-virus à la maison.
   - Je l'amène au bureau sur une clé USB que j'ai passée à l'anti-virus au bureau.
   - Je l'amène au bureau sur une clé USB que j'ai passée à l'anti-virus à la maison ET au bureau.
   - Je ne l'amène pas au bureau. ***

4. Je trouve une clé USB dans ma boîte à lettres. Quelle est la meilleure action ?
   - Je la connecte à mon ordinateur pour en voir le contenu.
   - Je l'analyse avec un anti-virus, on ne sait jamais.
   - Je la jette, une clé peut contenir un virus.***

5. Un virus de démarrage est :
   - Un virus qui se cache derrière le secteur MBR***
   - Un virus qui se cache dans la FAT
   - Un virus qui modifie son code est la façon de changer son code
   - Une bombe logique

6. Je reçois un mail m'annonçant que je peux gagner une voiture. Il suffit d'envoyer un mail à l'adresse qui apparaît dans le message : winner@tombola.com. Quelle sont les menaces possibles ?
   - Je serai victime d'un cheval de Troie
   - Le pirate tentera de de m'envoyer un ver en réponse à mon émail***
   - Je serai victime d'un hoax***

7. Un pirate installe un ransomware pour :
   - Préparer une porte dérobée
   - Chiffrer illégalement les données confidentielles d'une entreprise victime***
   - Faire du chantage à une victime***
   - Exécuter un rootkit

TD3.2. « Questions de compréhension de la partie III »

8. Quelle est la différence entre un virus et un ver
   Un virus est un programme malveillant qui se propage à l'aide d'un autre programme, alors qu'un ver est un programme malveillant autonome

9. Dans quel cas les vers deviennent plus dangereux que les virus
   Dans le cas des réseaux informatiques, puisque le ver est autonome, donc il peut se déplacer dans les dossiers partagés et/ou en créant des sockets et se diriger avec d'autres machines distantes.

10. Certains vers circulant sur internet ne cause pas de dommages sur les machines victimes, c'est quoi le danger ?
    Ils encombrent la bande passante du réseau, donc ralentissent le bon fonctionnement des équipements.

11. Certains concepteurs d'antivirus recommandent de scaner une machine avec un antivirus de démarrage se trouvant sur supports de stockage externe, pourquoi ?
    Parfois le système d'exploitation de la machine lui-même est infecté, donc si on installe notre antivirus dessus, il risque de ne rien détecter. Un antivirus de démarrage verra notre machine comme un élément externe à scaner complétement, y compris le système d'exploitation.

12. Donnez les étapes d'installation d'une porte dérobée

1. Installer un programme malicieux (ou utile) qui en cache un autre.
2. Le programme caché est en principe un "keylogger".
3. Le premier programme malicieux ouvre les ports de communication.
4. Le deuxième programme malicieux, le "keylogger" copie toutes ces données, elles seront envoyées et connues par le programmeur de ce code malicieux.
5. Résultat : Ordinateur téléguidé donc botnet : Backdoor: Accès caché à un ordinateur

13. Donnez les étapes d'installation d'un cheval de troie

14. Installer un programme malicieux (ou utile) qui en cache un autre.
15. Le programme caché est en principe un "keylogger".
16. Le premier programme malicieux ouvre les ports de communication.

17. Donner deux méthodes implémentées dans certains virus pour les rendre indétectables par les antivirus

    Virus polymorphes
    Virus furtifs

TD3.2. « Exercice de reflexion »

1. Donnez quelques conséquences des vers :

- Le ralentissement de l'appareil infecté
- Surcharge de la bande passante d'un réseau
- Le Blocage de services ou du système d'exploitation de la machine victime.

2. Donnez les étapes adoptées par un pirate pour mettre en place une porte dérobée (Backdoor)

6. Un programme malicieux (ou utile) qui en cache un autre.
7. Le programme caché est en principe un "keylogger".
8. Le premier programme malicieux ouvre les ports de communication.
9. Le deuxième programme malicieux, le "keylogger" copie toutes ces données, elles seront envoyées et connues par le programmeur de ce code malicieux.
10. Résultat : Ordinateur téléguidé donc botnet : Backdoor: Accès caché à un ordinateur

Remarque : les étapes 1+2+3+4 =cheval de Troie

Echantillons d'examens

Exercice 1 (10 points): Cocher la ou les bonnes réponses

1. Pour cacher l'existence d'un pirate dans un système d'information, on utilise :
   - L'effacement des fichiers journaux des serveurs
   - Les rootkit
   - La cryptanalyse
   - Les botnets

2. Un attaquant manipule le fichier log d'un serveur pour :
   - Installer des rootkit
   - Installer des malwares et rester invisible
   - Casser les algorithmes de cryptographie utilisés
   - Effectuer une attaque CSS

3. Les certificats numériques permettent de :
   - S'assurer que les messages arrivent sans interruption
   - S'assurer qu'on parle avec le bon destinataire
   - S'assurer que le message n'a pas été lu par une personne non autorisée
   - S'assurer qu'on chiffre les données utilisant la bonne clé publique

4. Quelle sont les menaces possibles quand je réponds aux emails d'inconnus?
   - Je serai victime d'un cheval de Troie
   - Un spammeur peut me rajouter dans sa liste de victimes
   - Le pirate essayera de voler mon compte de messagerie
   - Je serai victime d'un hoax

5. Une méthode de signature numérique :
   - Permet d'envoyer la clé à son interlocuteur pour que celui-ci puisse décrypter les données
   - Permet de hacher les données en plus du chiffrement asymétrique
   - Est utilisée pour assurer l'intégrité des échanges
   - Est utilisée pour assurer la confidentialité des échanges

6. L'utilisation des fonctions de hachage dans les signatures permet de :
   - S'assurer qu'on parle avec le bon destinataire
   - S'assurer que les messages arrivent sans modifications
   - S'assurer que le message n'a pas été lu par une personne non autorisée
   - S'assurer qu'on respecte l'intégrité des données

7. L'analyse de la situation permet de :
   - Définir le risque de sécurité
   - Définir le périmètre de sécurité à protéger
   - Déterminer les services d'une entreprise à protéger
   - Faire un audit de sécurité

8. Le protocole SSH
   - Utilise le HTTPs
   - Remplace le protocole SSL
   - Utilise la cryptographie hybride pour l'administration à distance des serveurs
   - Est un protocole de téléchargement de fichiers sécurisé

9. Un screenlogger est :
   - Un cheval de Troie
   - Une préparation d'une attaque spam
   - Une préparation d'une porte dérobée
   - Un rootkit

10. Une Infrastructure à clés publiques :
    - Permet de stocker les clés publiques des individus
    - Permet de hacher les données en plus du chiffrement asymétrique
    - Permet de stocker les clés symétriques des individus
    - Permet de stocker des certificats numériques

11. Parmi les étapes de création d'une porte dérobée, on trouve :
    - Bloquer le serveur DNS
    - Bloquer un site web
    - Espionner le clavier de la victime
    - Installer un cheval de Troie

12. L'attaque par force brute consiste à :
    - Diriger le trafic vers un pirate
    - Envoyer des paquets ICMP vers une adresse de diffusion
    - Essayer tous les cas possibles pour casser un algorithme de cryptographie
    - Effectuer une attaque de déni de service utilisant le protocole ICMP

13. Le protocole HTTPs
    - Utilise le DNS
    - Utilise la cryptographie hybride
    - Utilise le protocole SSL
    - Est un protocole de téléchargement de fichiers sécurisé

14. Un pirate installe un ransomware pour :
    - Chiffrer illégalement les données confidentielles d'une entreprise victime
    - Préparer une attaque sql injection
    - Faire du chantage à une victime
    - Exécuter un rootkit

Exercice 2 (5 points):

1. Remplir le tableau ci-dessous par les actions suivantes

Analyse de la situation	Analyse de risque	Politique de sécurité	Mesures de sécurité	Implémentation	Validation

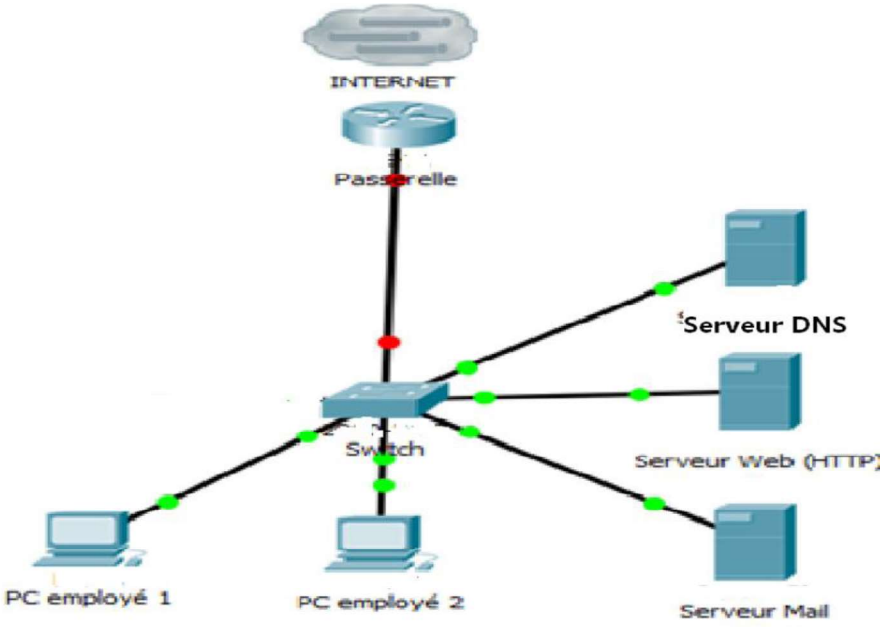
A. Formation des utilisateurs du système d'information
B. Installer un antivirus
C. Déterminer le périètre à sécuriser
D. La climatisation des serveurs n'a pas été maintenues depuis longtemps
E. Auditer mon système de sécurité
F. Le serveur de messagerie tombe fréquemment en panne il faut prévoir une redondance

2. Remplir le tableau suivant par les actions à effectuer (la politique de sécurité)

	Incidents à cout cher	Incidents à cout faible
Incidents fréquents		
Incidents rares		

Exercice 3 (5 points):

Soit le réseau local suivant :



1. L'administrateur souhaite installer au niveau du réseau un système de cryptographie hybride comme PGP avec certificat numérique, donner tous les éléments nécessaires

Solution de l'échantillon d'examen

Exercice 1 (10 points): Cocher la ou les bonnes réponses

1. Pour cacher l'existence d'un pirate dans un système d'information, on utilise :
   - L'effacement des fichiers journaux des serveurs***
   - Les rootkit***
   - La cryptanalyse
   - Les botnets

2. Un attaquant manipule le fichier log d'un serveur pour :
   - Installer des rootkit***
   - Installer des malwares et rester invisible***
   - Casser les algorithmes de cryptographie utilisés
   - Effectuer une attaque CSS

3. Les certificats numériques permettent de :
   - S'assurer que les messages arrivent sans interruption
   - S'assurer qu'on parle avec le bon destinataire***
   - S'assurer que le message n'a pas été lu par une personne non autorisée***
   - S'assurer qu'on chiffre les données utilisant la bonne clé publique***

4. Quelle sont les menaces possibles quand je réponds aux emails d'inconnus?
   - Je serai victime d'un cheval de Troie
   - Un spammeur peut me rajouter dans sa liste de victimes***
   - Le pirate essayera de voler mon compte de messagerie
   - Je serai victime d'un hoax***

5. Une méthode de signature numérique :
   - Permet d'envoyer la clé à son interlocuteur pour que celui-ci puisse décrypter les données
   - Permet de hacher les données en plus du chiffrement asymétrique***
   - Est utilisée pour assurer l'intégrité des échanges***
   - Est utilisée pour assurer la confidentialité des échanges

6. L'utilisation des fonctions de hachage dans les signatures permet de :
   - S'assurer qu'on parle avec le bon destinataire
   - S'assurer que les messages arrivent sans modifications***
   - S'assurer que le message n'a pas été lu par une personne non autorisée
   - S'assurer qu'on respecte l'intégrité des données***

7. L'analyse de la situation permet de :
   - Définir le risque de sécurité
   - Définir le périmètre de sécurité à protéger***
   - Déterminer les services d'une entreprise à protéger***
   - Faire un audit de sécurité

8. Le protocole SSH
   - Utilise le HTTPs
   - Remplace le protocole SSL
   - Utilise la cryptographie hybride pour l'administration à distance des serveurs***
   - Est un protocole de téléchargement de fichiers sécurisé

9. Un screenlogger est :
   - Un cheval de Troie***
   - Une préparation d'une attaque spam
   - Une préparation d'une porte dérobée***
   - Un rootkit

10. Une Infrastructure à clés publiques :
   - Permet de stocker les clés publiques des individus***
   - Permet de hacher les données en plus du chiffrement asymétrique
   - Permet de stocker les clés symétriques des individus
   - Permet de stocker des certificats numériques***

11. Parmi les étapes de création d'une porte dérobée, on trouve :
   - Bloquer le serveur DNS
   - Bloquer un site web
   - Espionner le clavier de la victime***
   - Installer un cheval de Troie***

12. L'attaque par force brute consiste à :
   - Diriger le trafic vers un pirate
   - Envoyer des paquets ICMP vers une adresse de diffusion
   - Essayer tous les cas possibles pour casser un algorithme de cryptographie***
   - Effectuer une attaque de déni de service utilisant le protocole ICMP

13. Le protocole HTTPs
   - Utilise le DNS
   - Utilise la cryptographie hybride ***
   - Utilise le protocole SSL***
   - Est un protocole de téléchargement de fichiers sécurisé

14. Un pirate installe un ransomware pour :
    - Chiffrer illégalement les données confidentielles d'une entreprise victime***
    - Préparer une attaque sql injection
    - Faire du chantage à une victime***
    - Exécuter un rootkit

Exercice 2 (5 points):

1. Remplir le tableau ci-dessous par les actions suivantes

Analyse de la situation	Analyse de risque	Politique de sécurité	Mesures de sécurité	Implémentation	Validation
C	**D**	**F**		**A et B**	**E**

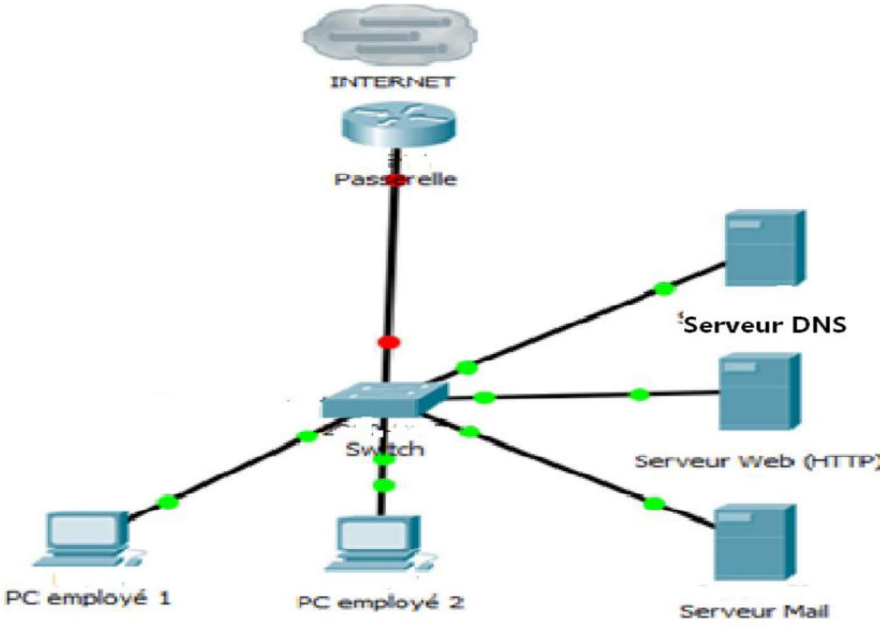
G. Formation des utilisateurs du système d'information
H. Installer un antivirus
I. Déterminer le périètre à sécuriser
J. La climatisation des serveurs n'a pas été maintenues depuis longtemps
K. Auditer mon système de sécurité
L. Le serveur de messagerie tombe fréquemment en panne il faut prévoir une redondance

2. Remplir le tableau suivant par les actions à effectuer (la politique de sécurité)

	Incidents à cout cher	Incidents à cout faible
Incidents fréquents	**Mettre en place des mécanismes de sécurité** **•Recruter** **•Former**	**Assurer la disponibilité (serveurs miroirs. etc)**
Incidents rares	**S'assurer**	**Accepter**

Exercice 3 (5 points):

Soit le réseau local suivant :



1. L'administrateur souhaite installer au niveau du réseau un système de cryptographie hybride comme PGP avec certificat numérique, donner tous les éléments nécessaires

- L'ensemble des clés possibles (espace de clés) : clés pub, privées et clés de session
- Les algorithmes de chiffrement et déchiffrement : RSA, AES, SHA **(0,5 pt)**
- Les fonctions de hachage **et** Les certificats numériques
- L'infrastructure PKI

Référence

- L'ISO/CEI 27001 : la norme internationale de sécurité des systèmes d'information
- ISO 27005 : La gestion des risques
- ISO 19011 : Audit des systèmes de management
- Documents de certification PECB Lead auditor
- Guy Pujolle « Les réseaux ». Edition Eyrolles, 2010.
- Wolfgang Kandek, "Vulnerability Management", Chichester, West Sussex, England, 2015.
- Joanna Rutkowska, « Introducing Stealth Malware Taxonomy », *Black Hat Federal Conference*, COSEINC Advanced Malware Labs, November 2006
- T. Chothia and K. Chatzikokolakis, A Survey of Anonymous Peer-to-Peer File-Sharing. In Proceedings of EUC Workshops, pages 744-755, 2005.