1 Politique de sécurité SI

1.1 Haute disponibilité des données de l'entreprise et des systèmes

Parmi les moyens qu'on peut utiliser pour assurer ça :

1.1.1 Mise en place d'un système de gestion de redondance des disques (RAID)

- RAID 0 est utile pour installer un OS (linux, Windows server …)
- RAID 5 est très utilisé pour l'installation des bases de données (Oracle, SQL server…)
- RAID 0+5 est beaucoup plus sécurisé.

Remarque :

Pour un disque dur on a une vitesse de lecture / écriture sur le disque sous la forme : 10k rpm ou 10k tr/min qui représentent la vitesse d'écriture / de lecture sur le disque càd la vitesse avec laquelle il tourne.

On a aussi la vitesse d'échange entre le disque et la carte mère qui dépend du connecteur (IDE, SATA, SAS, SCSI …)

1.1.2 Mise en place d'un support de stockage externe supplémentaire

a- Lecteur LTO + Bandes magnétiques (équipement peu couteux)

Le lecteur LTO est branché au serveur via câble USB, et sur ce serveur il faut installer un logiciel de backup à configurer selon le type de sauvegarde (incrémental ou intégral) et la fréquence de sauvegarde.

Remarques :

L'inconvénient de cette solution est la durée de vie du matériel

La taille de stockage d'une bande magnétique ~ 800Go.

b- Robot de sauvegarde

Peut gérer des dizaines de centaines de bandes magnétiques. Le robot de sauvegarde est branché au réseau LAN via la fibre optique (pour des raisons de vitesse).

Remarque :

L'inconvénient encore une fois c'est la durée de vie des bandes.

c- Baie de stockage (solution la plus utilisées par les entreprises)

Contient plusieurs disques avec chacun une taille de 2To, une fois branchée sur le réseau, il va apparaitre comme un disque dur qu'on peut configurer selon le besoin.

Remarque :

Serveur Rackable => serveur qu'on peut mettre dans une armoire.

Serveur Blade => utile pour gérer les clusters.

1.1.3 Mise en place d'un réseau de stockage (SAN : Storage Area Network)

a- Haute disponibilité des systèmes

Pour assurer la disponibilité des systèmes, on va mettre en place des clusters (regrouper plusieurs serveurs qui de l'extérieur apparaissent comme un seul cluster).

On a deux catégories de clusters :

- Cluster Actif / Actif (Load balancing Cluster chez Microsoft):

Cluster à répartition de charge ; Le problème est que le serveur / site crache lors d'une connexion plus grande que la capacité, la solution est donc d'utiliser un NLB (Network Load Balancer) pour que le même site soit distribué sur plusieurs serveurs (charge répartie).

L'un des plus grands constructeurs est F5 (Big IP).

- Cluster Actif / Passif (Failover Cluster chez Microsoft) :

Cluster à basculement (pas très utilisé) consiste à avoir 2 serveurs un actif et un autre en hibernation / en mode veille ,s'il y a un problème avec le premier serveur , le cluster switch vers le 2ème serveur. Le problème ici est que cette méthode ne permet de gérer les sessions interrompues ce qui représente un problème pour les sites de e-commerce.

1.2 La confidentialité des données et des communications des données.

1.2.1 Cryptographie

Transformer les données pour les rendre illisibles.

- ⇨ Cryptographie symétrique
- ⇨ Cryptographie asymétrique
- ⇨ Signature numérique

1.2.2 Stéganographie

Cacher des données secrètes dans d'autres données.

1.3 L'intégrité des données.

Fonctions de hachages : MD5, sha-1, sha-256 … très utilisées dans les VPNs , wifi, https …

1.4 Identification et authentification des personnes qui vont accéder aux données.

- ⇨ Login et mot de passe
- ⇨ Cartes à puces
- ⇨ Biométrie

2 Cryptographie moderne

La grande différence entre la cryptographie classique et la cryptographie moderne réside dans l'utilisation des bits (binaire).

2.1 Utilisation de la substitution binaire

2.1.1 1.Substitution binaire simple

Suite binaire (1010) => S-Box => suite binaire de même taille (0101)

2.1.2 2.Substitution binaire compressive

Suite binaire (10101010) => S-Box => suite binaire de taille inférieure (0101)

2.1.3 3.Substitution binaire expansive

Suite binaire (1010) => S-Box => suite binaire de taille supérieure (01010101)

2.2 Utilisation de la permutation binaire

2.3 Cryptographie moderne asymétrique:

Utilisation d'une paire de clé; une clé secrète pour le décryptage et une clé publique pour le cryptage.

2.4 Cryptographie moderne symétrique:

Une seule clé est utilisée à la fois pour le cryptage et le décryptage.

2.4.1 Exemple

Supposons que nous avons 2 personnes un émetteur A et un récepteur B; si A veut chiffrer un message M (données claires) avec une clé secrète Ks, il va utiliser un algorithme (fonction) de cryptage par exemple DES, 3DES ,AES ,Blow Fish... pour crypter M, on aura alors un message crypté C=E(M, Ks) qu'on appelle aussi le cryptogramme. B va alors grâce à la clé secrète partagée Ks et le même algorithme de cryptage pouvoir décrypter le message C pour avoir le message de base M.

2.4.2 Avantages

Les avantages de la cryptographie moderne symétrique c'est qu'elle est rapide, facile à implémenter sur des circuits électriques. Quant à l'inconvénient de la cryptographie moderne symétrique est le partage de manière sécurisée de la clé secrète (la solution est d'utiliser l'algorithme de Diffie Hellman D.H).

2.4.3 Différence entre les algorithmes de cryptage

La différence principale des algorithmes de cryptage est la taille des données à chiffer et la taille de la clé secrète utilisée.

Pour **DES (M = 64bits, Ks = 56bits, C= 64bits)** si on donne des données de taille plus grande M > 64bits l'algorithme va diviser le messages M1, M2, ...Mi de taille convenable avant de les crypter ,si on a un bloc de données M < 64bits il faut ajouter des données de Bourrages (caractères aléatoires ou 0s ou (0s et 1s)...).

Pour **3DES (M = 64bits et Ks = 112 ou 168 bits)** qui est mieux sécurisé pour éviter ce qu'on appelle l'attaque par force brute c'est à dire essayer des combinaisons jusqu'à trouver la bonne combinaison pour la clé.

Pour **AES** , qui est le plus utilisé on a augmenté la taille des données à **M = 128bits** et on a la possibilité d'utiliser une des clés **Ks = 128 ou 192 ou 256bits.**

Pour **Blowfish** qui est 5fois plus rapide que 3DES repose sur un chiffrement par bloc avec des clés de longueur variable **(M = 64bits et KS entre 32 et 448bits)**

2.4.4 Remarques

A l'aide des méthodes cryptographiques modernes, il devient possible d'assurer :

- Confidentialité
- Authenticité
- Intégrité

Dans le cryptage symétrique il y'a deux méthodes :

1. Cryptage par bloc (Bloc Cipher) :
    - Le texte est divisé en différents blocs de taille fixe.
    - Un bloc est traité à la fois avec la même clé de cryptage
    - Le bloc de données doit être entièrement disponible avant le traitement
2. Cryptage par flux (Stream Cipher) :
    - Traite les éléments d'entrée de façon continue, produisant à la fois un élément de sortie crypté
    - La clé est aussi longue que le flux de données
    - Mode adapté pour la communication en temps réel

Propriété	ECB (Electronic Codebook)	CBC (Cipher Block Chaining)
Principe	Chaque bloc de texte clair est chiffré indépendamment avec la clé.	Chaque bloc est chiffré après avoir été combiné avec le bloc précédent (XOR), créant une dépendance entre les blocs.
Aléatoire	Non aléatoire : un même bloc de texte clair produit toujours le même bloc chiffré.	Introduit de l'aléatoire grâce au chaînage (sauf pour le premier bloc, qui utilise un IV).
Diffusion	Aucune : une modification d'un bloc de texte clair n'affecte que son bloc chiffré correspondant.	Bonne diffusion : une modification d'un bloc affecte aussi tous les blocs suivants.
Sécurité	Faible : des motifs répétitifs dans le texte clair apparaissent dans le texte chiffré.	Plus sécurisé : masque les motifs du texte clair grâce au chaînage.
Avantage	Rapidité et parallélisation possible (chaque bloc peut être chiffré séparément).	Plus sécurisé contre l'analyse statistique et les attaques par répétition.
Inconvénient	Peu sécurisé : vulnérable aux attaques par analyse fréquentielle et aux attaques sur les motifs répétitifs.	Plus lent : le chiffrement et le déchiffrement doivent être effectués séquentiellement (non parallélisable).

3 La Cryptographie Par Substitution Monoalphabétique

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

- Le texte clair à coder est le suivant : **Bienvenue à l'ENSA**
- Le texte codé (chiffré) est alors : **XCYASYARY W IYAMW**

3.1 Le Code De César

La substitution est définie par un **décalage de lettres 3 positions à gauche.**

- Le chiffrement se fait par : $C_i = (X_i + 3)\ mod\ 26;$

  X_i: représente une lettre du texte clair;

  C_i: représente une lettre du texte chiffré.

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

- Lorsque on utilise un décalage **d**, le chiffrement devient : $C_i = (X_i + \boldsymbol{d})\ mod\ 26;$

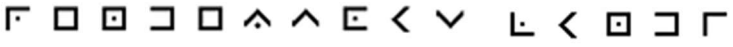
- Le texte clair à coder est le suivant : **ENSA**

- Le texte codé (chiffré) est alors : **HQVD**

3.2 Code de Pig-Pen

On remplace chaque lettre du texte claire par un symbole en utilisant la table suivante :

Texte clair: r e n d e z v o u s | u n d i



3.3 Chiffre De Vigenère

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

- Le chiffrement se fait par : $C_i = (X_i + clé)\ mod\ 26;$
- Chiffre de **Vigenère:**
  - ✓ On répète la clé aussi souvent que nécessaire pour que sous chaque lettre du message à coder, on trouve une lettre de la clé
  - ✓ Exemple: mot clair= SALAM ALIKOUM; clé= ENSA

Texte clair	S	A	L	A	M	A	L	I	K	O	U	M
	18	0	11	0	12	0	11	8	10	14	20	12
clé	E	N	S	A	E	N	S	A	E	N	S	A
	4	13	18	0	4	13	18	0	4	13	18	0
Texte Chiffré	22	13	29	0	16	13	29	8	14	27	38	12
	W	N	D	A	Q	N	D	I	O	B	M	M

ENSA KÉNITRA

3.4 Chiffre De Beaufort

- Le même principe que le chiffre de Vigenère mais on va soutraire le texte clair de la clé .
- Le chiffrement se fait par : $C_i = (clé - X_i)\ mod\ 26;$
- Chiffre de **Beaufort:**
  - ✓ Exemple: mot clair= SALAM ALIKOUM; clé= ENSA

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

Texte clair	S	A	L	A	M	A	L	I	K	O	U	M
	18	0	11	0	12	0	11	8	10	14	20	12
clé	E	N	S	A	E	N	S	A	E	N	S	A
	4	13	18	0	4	13	18	0	4	13	18	0
Texte Chiffré	-14	13	7	0	-8	13	7	-8	-6	-1	-2	-12
	M	N	H	A	S	N	H	S	U	Z	Y	O

ENSA KÉNITRA

3.5 Code De Vernam

- Chiffre de **Vernam** appelé aussi OTP (One Time Pad)
  - ✓ incassable

- Le même principe que le chiffre de Vigenère mais:
  - ✓ Taille de la clé = taille du message en clair
  - ✓ La clé est aléatoire
  - ✓ La clé de chiffrement est utilisée pour chiffrer un seul message (One Time)

Texte clair	S	A	L	A	M	A	L	I	K	O	U	M
	18	0	11	0	12	0	11	8	10	14	20	12
clé	X	V	S	B	R	A	T	C	Q	I	L	F
	23	21	18	1	17	0	19	2	16	8	11	5
Texte Chiffré	15	21	3	1	1	0	4	10	0	22	5	17
	P	V	D	B	B	A	E	K	A	W	F	R

3.6 Attaques Par Analyse Fréquentielle

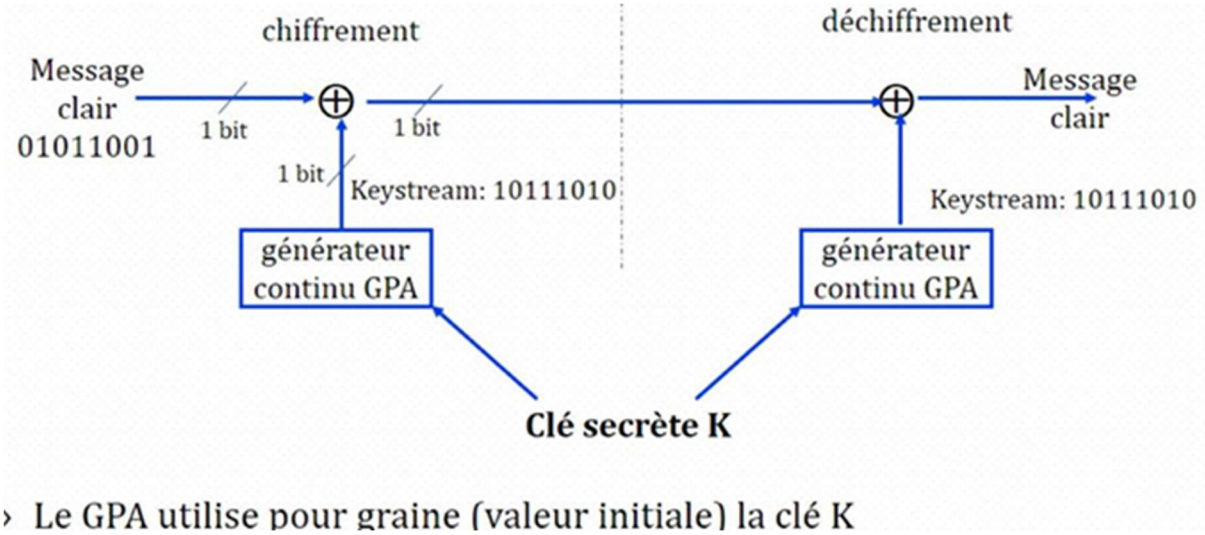
Exemple d'un texte crypté: **IKIOK YZATZ KYZJK IXEVZ UMXGV NOK**

La lettre la plus fréquente est « K ». Le décalage d = « K »- « E » = 10 - 4

Donc d= 6.

Le déchiffrement se fait par $X_i = (C_i - \boldsymbol{d}) \; mod \; 26$;

4 Chiffrement par flux



› Le GPA utilise pour graine (valeur initiale) la clé K