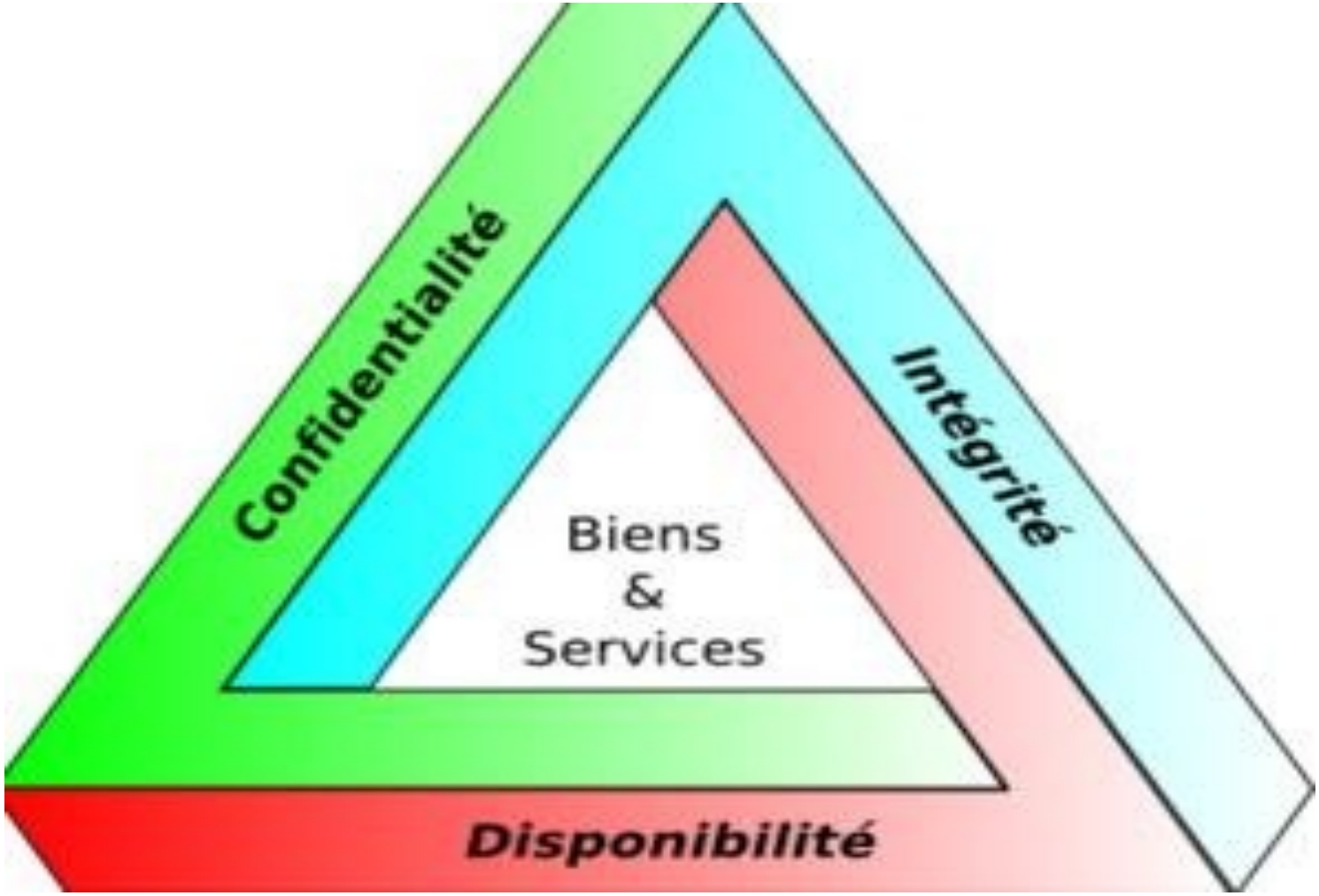
cours sécurité informatique

C1.1: *Définition*

- ***Sécurité informatique:*** est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, rétablir, et garantir la sécurité de l'information, des systèmes et ressources informatiques contre les menaces atteignant leur confidentialité, intégrité, et disponibilité.

les propriétés fondamentales de la sécurité



les propriétés (services) fondamentales de la sécurité

Confidentialité : protéger le contenu d'un message ou de données contre un espion qui écouterait les communications.

intégrité : certification de la non-altération des données, traitements et services.

Disponibilité : L'objectif de la disponibilité est de garantir l'accès à un service ou à des ressources.

authentification : vérification de l'identité de l'utilisateur et de ses autorisations (détermination de l'identité de l'interlocuteur).

non-répudiation : protection contre la négation d'une action accomplie : imputabilité, traçabilité, auditabilité.

Authenticité = authentification + intégrité .

Gestion des risques

- **Risque = (Menace x Vulnérabilité)/Contre_Mesures**
- **Menace:** Violation potentielle d'une propriété de sécurité.
- **type de menace:**

1) Accidentelles

- Catastrophes naturelles ("acts of God"): feu, inondation, …
- Actes humains involontaires : mauvaise entrée de données, erreur de frappe, de configuration, …
- Performance imprévue des systèmes : Erreur de conception dans le logiciels ou matériel, Erreur de fonctionnement dans le matériel,…

Gestion des risques

2) Délibérées

- Vol de systèmes
- Attaque de dénis de service
- Vol d'informations (atteinte à la confidentialité)
- Modification non-autorisée des systèmes.

Vulnérabilité: faiblesse / faille : faute accidentelle ou intentionnelle introduite dans spécification, conception ou configuration du système.

- **Attaque :** tentative volontaire de violer une ou plusieurs propriétés de sécurité.
- **Intrusion :** violation effective de la politique de sécurité.

Gestion des risques

- ***Contre_Mesures:*** est l'ensemble des actions mises en œuvre en prévention de la menace.

- ***Encryptage des données***

- ***Contrôles au niveau des logiciels***
  - Partie du système d'exploitation,
  - Contrôle du développement des logiciels

- ***Contrôles du matériel***
  - Contrôle de l'accès au matériel: identification et authentification.
  - Contrôles physiques: serrures, caméras de surveillance , gardiens, etc…

Logiciels malveillants

- **Virus:** Tout programme capable d'infecter un autre programme en le modifiant de façon à ce qu'il puisse se reproduire.

  - Les **macro-virus,**
  - Les **virus résidents**
  - Les **virus de boot**
  - Les **virus lents**
  - Les **virus défensifs ou rétrovirus**
  - Les **virus furtifs**

Infecte : Programmes, documents, secteurs de boot.

Logiciels malveillants

- **Ver (Worm):** Programme autonome qui se reproduit et se propage à travers le réseau.

- **Cheval de Troie:** Programme à l'apparence utile mais cachant du code pour créer une faille dans le système (back-door).

- **Bombes logiques:** est programme qui se déclenche automatiquement suite à un événement particulier (date, signal distant).

Logiciels malveillants

- **le logiciel espion (spyware) :** fait de la collecte d'informations personnelles sur l'ordinateur d'un utilisateur sans son autorisation. Ces informations sont ensuite transmises à une société en général pour du profilage.
- **Le pourriels(spamming) :** consiste à envoyer plusieurs milliers de messages identiques à une boîte aux lettres pour la faire saturer.
- **Spoofing (usurpation d'identité):** se faire passer pour quelqu'un d'autre afin de faire une action malveillante (ex: envoi virus, spam, …)

C1.2: Mise en œuvre d'une politique de sécurité

- **les moyens**

- moyens organisationnels et procéduraux:

- ✓ ensemble de règles qui doivent être mises en place et respectées

- moyens informatiques:

- ✓ Cryptographie, cryptanalyse.

- moyens matériels ou physiques:

- ✓ architecture des entreprises, les systèmes de *contrôle d'accès.*

Mise en œuvre d'une politique de sécurité

- **Contrôles d'accès**

Un ensemble de méthodes informatique à pour rôle de :

- Administrer l'accès aux ressources *(Administration).*
- Contrôler les droits d'accès.*(Identification* et *authentification).*
- Identifier les utilisateurs autorisés ou non *(autorisation).*

Mise en œuvre d'une politique de sécurité

* Les Contrôlesd'accès gouvernent et contrôlent l'accès d'un sujet à des objets.

La première étape de ce processus est appelée: l'***administration***, la deuxième étape est appelée: l'***identification***, la troisième étape est appelée: l'***authentification*** et la quatrième étape est appelée: l'***autorisation*** .

Mise en œuvre d'une politique de sécurité

- **Administration des contrôles d'accès**

✓ La gestion des comptes utilisateur.

✓ Le suivi des activités.

✓ **L'identification** est le processus par lequel un sujet prétend avoir une identité et donc une responsabilité(non répudiation) est engagée.

Identification – suite

Un utilisateur fournissant un nom d'utilisateur, un ID de connexion, un numéro d'identification personnel (NIP), ou une carte à puce représente le processus d'identification.

Une fois le sujet s'est identifié, l'identité de ce sujet est tenue responsable pour toutes les actions de ce sujet.

Les systèmes de suivi (log et les fichiers journaux) permettent de garder les traces des usagers par leur identités.

L'identité permet au système de faire la distinction entre tous les utilisateurs de ce système.

Mise en œuvre d'une politique de sécurité

Authentification - Facteur d'authentification de type 3

* Un facteur d'authentification de type 3 représente quelque chose de nous même :

- ✓ Empreintes digitales,
- ✓ géométrie de la main,
- ✓ Reconnaissance du visage,
- ✓ Reconnaissance de l'iris,
- ✓ Reconnaissance de la rétine,
- ✓ La reconnaissance vocale,
- ✓ dynamique des signatures (signature-scan),…

Mise en œuvre d'une politique de sécurité

L'Autorisation

Une fois un sujet est authentifié, l'accès doit être autorisé:

- ✓Le processus d'autorisation garantit que l'accès à l'activité ou à l'objet demandé est possible compte tenu des droits et des privilèges accordés à ce sujet authentifié.

- ✓Dans la plupart des cas, le système évalue une matrice de contrôle d'accès, qui compare le sujet, l'objet, et l'activité. Si l'action spécifique est permise, le sujet est autorisé. Si l'action spécifique est interdite, le sujet n'est pas autorisé.

Important: gardez à l'esprit que juste parce qu'un objet a été identifié et authentifié ne signifie pas automatiquement qu'il a été autorisé.

Mise en œuvre d'une politique de sécurité

- **Les trois catégories de C.A**

* Les contrôles d'accès sont classés en trois catégories :

- ✓ Préventifs: Sont déployés pour ***stopper*** une activité non autorisée de se produire.
- Détectifs: Sont déployés pour ***détecter*** (découvrir) une activité non autorisée.
- Correctifs: Sont déployés pour ***restaurer*** les systèmes à un état normal après qu'une activité non autorisée ou non désirée soit produite.

Mise en œuvre d'une politique de sécurité

- **Implémentation des CA**

Elle peut être divisée en trois partie :

- ✓ CA administratifs: représentent un ensemble de politiques et de procédures pour mettre en œuvre et appliquer un contrôle d'accès global.
- ✓ CA logiques et techniques: représentent un ensemble de logiciels et de matériels capables de gérer et de protéger l'accès aux ressources demandées.
- ✓ CA physiques: représentent les barrières physiques déployés pour éviter le contact direct avec les systèmes.

Détection d'intrusion

- La détection d'intrusions consiste à analyser les informations collectées par les mécanismes d'audit de sécurité en utilisant un système qui effectue la détection d'intrusion d'une manière automatique, ce système est appelé « IDS: Intrusion Detection System ».

- Les IDS sont des systèmes software ou hardware conçus afin de pouvoir automatiser l'inspection des fichiers journaux , d'audits et les événements produits par le système en temps réel.

IDS: Intrusion Detection System

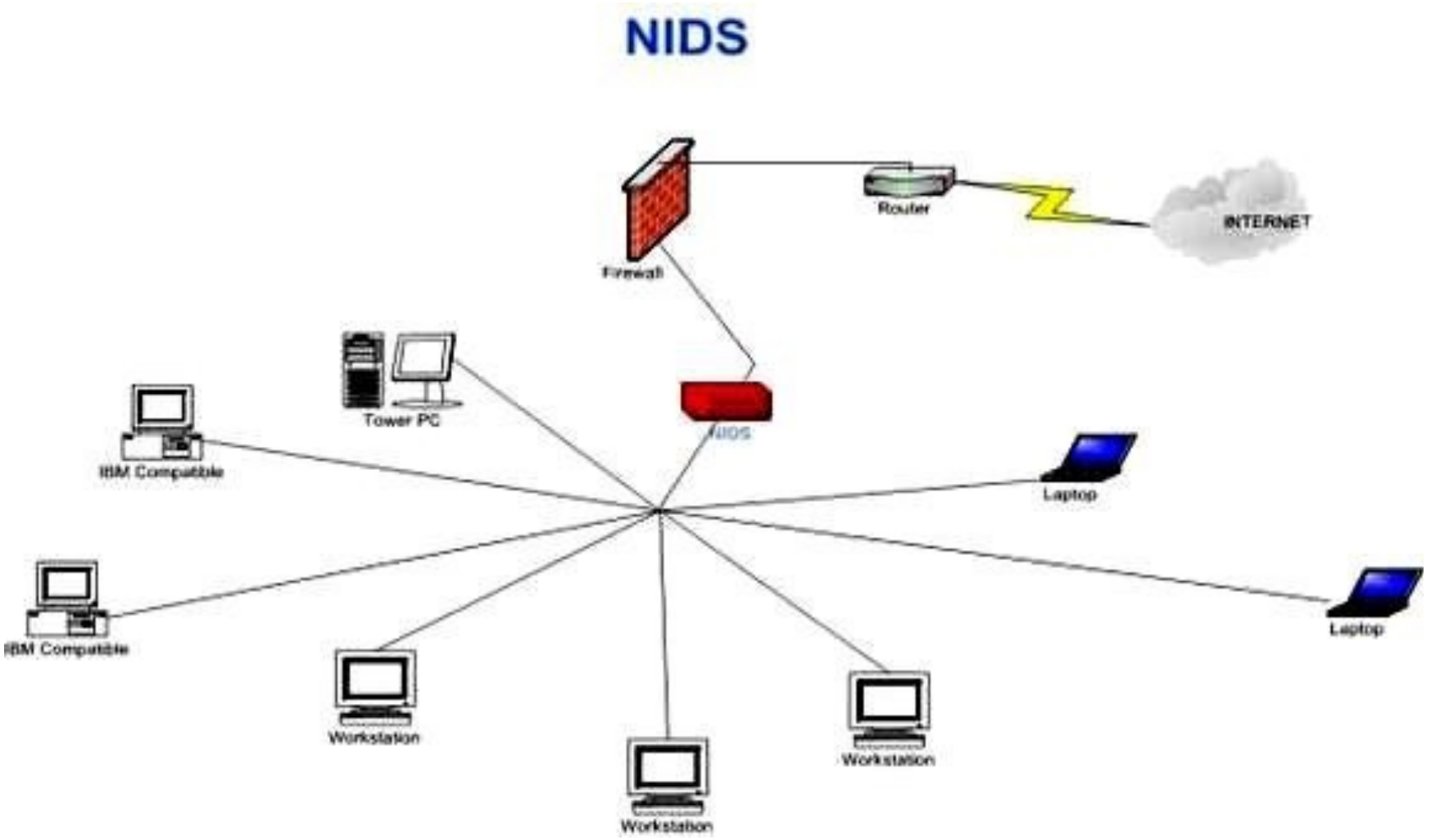
- Un IDS peut surveiller activement les activités suspectes.
- mettre en évidence les vulnérabilités, identifier le point d'origine de l'intrusion.
- reconfigurer les routeurs et les pare-feu pour empêcher les répétitions d'attaques découvertes.

Système de Détection d'intrusion (NIDS et HIDS)

- **Les NIDS (Network-Based IDS)** sont installés sur le réseau, ils permettent de détecter les attaques ou les anomalies par le biais de la capture et de l'évaluation des paquets réseau.

- Certaines versions de titres IDS basé sur le réseau utilisent des agents à distance pour recueillir des données provenant de divers sous-réseaux et de faire les reports à un système de gestion centrale.

Network-Based IDSs - NIDS

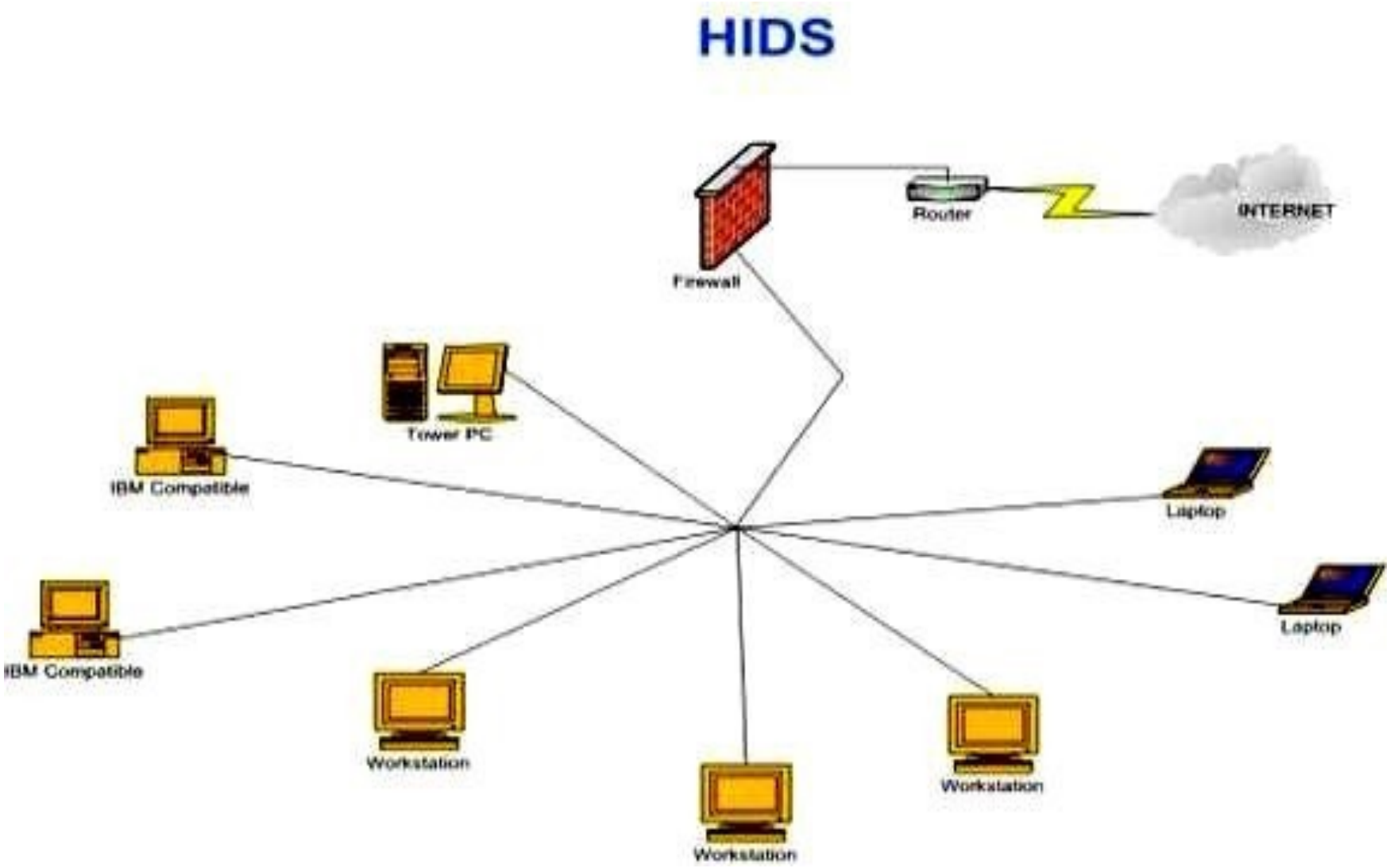


Host Based IDSs - HIDS

- **Les HIDS** (Host-Based **IDS)** sont installés sur les hôtes, ils permettent d'identifier les fichiers et les processus compromis ou employés par un utilisateur malveillant afin d'exercer une activité non autorisée.

- Les IDS hôtes (installé sur les PCs) peuvent Détecter les intrusions locales mais pas seules du réseaux.

Host Based IDSs - HIDS



Actions d’un IDS

- Journaliser l’événement,
- Avertir un système ou un humain par un message,
- Amorcer certaines actions sur un réseau ou hôte.

IDS : Méthodes de détection

1- Par signature:

- *Une signature d'attaque est un* ensemble de caractéristiques permettant d'identifier une activité intrusive : une chaîne alphanumérique, une taille de paquet inhabituelle, une trame formatée de manière suspecte, etc…

- ✓ Basé sur la *reconnaissances de schémas* déjà connus générés par une ou plusieurs *sondes de signatures* d'attaques qui sont contenues dans une *base de signatures.*

IDS : Méthodes de détection (Par Signature)

- Avantages
  - Simplicité de mise en œuvre,
  - Rapidité de diagnostic,
  - Précision (en fonction des règles),
  - Peu de faux-positifs.

- Inconvénients
  - Ne détecte que les attaques connues,
  - Maintenance de la base,
  - Techniques d'évasion possibles dès lors que les signatures sont connues.

IDS : Méthodes de détection

2- Par comportement

- Le comportement observé du système cible est comparé aux comportements normaux et espérés.

- Si le comportement du système est significativement différent du comportement normal, on dit que le système cible présente des anomalies et fait l'objet d'une intrusion.

- Une alerte est levée dès lors qu'une déviation est constatée entre le comportement appris et le comportement observée.

IDS : Méthodes de détection (Par comportement)

- Avantages
- Permet la détection d'attaque inconnue,
- Facilite la création de règles adaptées à ces attaques,
- Difficile à tromper.

- Inconvénients
- Les faux-positifs sont nombreux,
- Générer un profil est complexe,
- Diagnostics long en cas d'alerte.

IDS : évaluation

L'évaluation de l'efficacité des IDS est basée sur les trois critères ci-dessous:

- ✓ **L'exactitude :** les IDS déclarent comme malicieux une activité légale. Ce critère correspond au faux positif.
- ✓ **La performance :** Si le taux de traitement des événements est faible, la détection en temps réel est donc impossible.
- ✓ **La complétude :** Si IDS rate la détection d'une attaque. Ce critère est le plus difficile parce qu'il est impossible d'avoir une connaissance globale sur les attaques. Ce critère correspond au faux négatif.

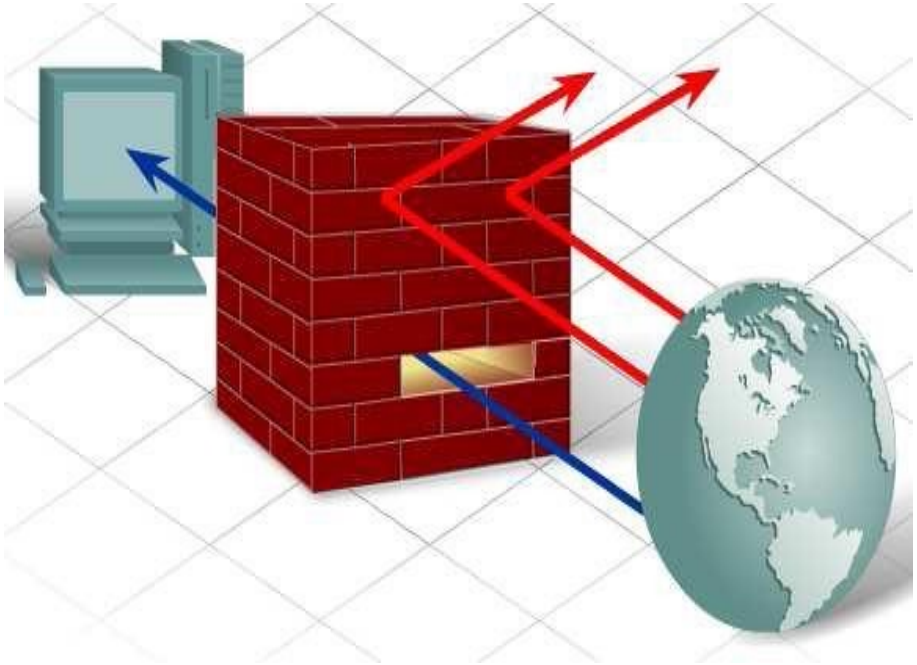
Points négatifs des IDS

- Technologie complexe,
- Nécessite un degré d'expertise élevé,
- Réputer pour générer de fausses alertes,
- Encore immature.

Les Pare-feux (firewalls)

pare- feu (Firewall) : est un mur qui empêche la propagation d'un incendie dans un bâtiment .

Pare-feu : en informatique une protection d'un réseau contre des attaques.



- Un pare-feu est un système physique (matériel) ou logique (logiciel) servant d'interface entre un ou plusieurs réseaux afin de contrôler et éventuellement bloquer la circulation des paquets de données, en analysant les informations contenues dans les couches 3, 4 et 7 du modèle OSI.

Le rôle d'un pare-feu

Le pare-feu joue le rôle de **filtre** et peut donc intervenir à plusieurs niveaux du modèle OSI:

- déterminer le type de trafic qui sera acheminé ou bloqué,
- limiter le trafic réseau et accroître les performances,
- autoriser un administrateur à contrôler les zones auxquelles un client peut accéder sur un réseau,
- Enregistrer le trafic.

Les types de pare-feux

- Il existe trois types de principaux de pare-feu :

- ✓ Pare-feux statique (stateless),
- ✓ Pare-feux dynamique (*stateful),*
- ✓ Pare-feux applicatifs (*proxy).*

Les types de pare-feux (stateless)

1) **Pare-feux statique** (*Filtrage de paquets sans état)* : Les pare-feux de filtrage de paquets sans état sont généralement des routeurs qui permettent d'accorder ou de refuser l'accès en fonctions des éléments suivants :

- l'adresse source,
- l'adresse destination,
- le numéro de port,
- le protocole.

Les types de pare-feux (stateful)

***2)* Pare-feux dynamique** (*filtrage de paquets avec état):* conserve les états des connexions : 4 types d'états:

- **NEW :** un client envoie sa première requête vers un serveur web.
- **ESTABLISHED :** connexion a déjà été initiée (après un NEW).
- **RELATED :** ce peut être une nouvelle connexion, mais elle présente un rapport direct avec une connexion déjà connue.
- **INVALID :** un paquet qui n'a rien à faire là dedans.

Les types de pare-feux (applicatifs)

- ***3) Pare-feux applicatifs (proxy):*** analyse du trafic échangé au niveau application (couche 7) pour appliquer une politique de sécurité spécifique de chaque application.

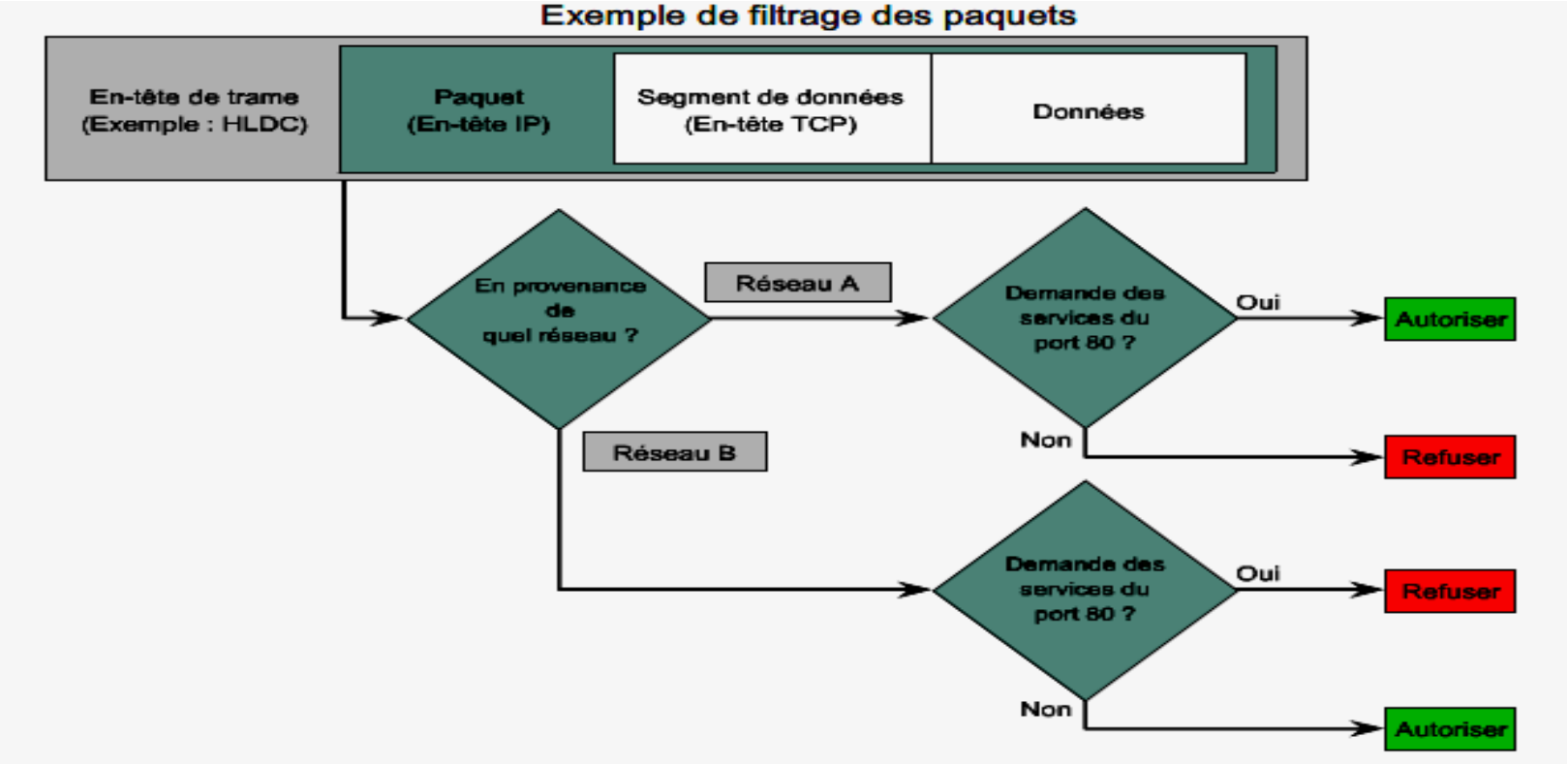
- Ces systèmes se substituent au serveur ou au client qu'ils ont pour mission de défendre pour :

✓ traiter les requêtes et réponses à la place du système à protéger,

✓ les transmettre, après d'éventuelles modifications ou les bloquer.

Exemple de Firewall (Filtrage de paquets) : Listes de contrôle d'accès

- **ACL** = bout d'un pare-feu dans un routeur.
- LES ACL (Access Control List) : sont des Collections d'instructions permettant d'autoriser ou de refuser des paquets en fonction d'un certain nombre de critères



Création d'une ACL: Exemple CISCO

- Créer la liste de contrôle d'accès en mode de configuration globale.
- **Syntaxe**: Router(config)# access-list *numéro d'ACL*
  { permit | deny } instruction

- ✓ ***numéro d'ACL*** doit être compris entre 1 et 99 ou entre 1300 et 1999,
- ✓ ***deny*** pour interdire le trafic,
- ✓ ***permit*** pour autoriser le trafic,
- ✓ ***instruction*** invoque une information sur un protocole ou une adresse.

Les types d'ACL

- Il existe 3 types de liste de contrôle d'accès :

- ✓ ***les ACLs standards***: uniquement sur les IP sources,
- ✓ ***les ACLs étendues*** : sur quasiment tous les champs des en-têtes IP, TCP et UDP,
- ✓ ***les ACLs nommées***: peuvent être soit standards, soit étendues ; mais n'ont pour but que de faciliter la compréhension et de connaître la finalité de l'ACL.

Les ACLs standard

1) **ACL standard** permet de créer des règles dont les conditions ne prennent en compte que les adresses IP sources des datagrammes IP analysés.

Syntaxe: access-list *ACL_number* {deny | permit} *adresse_Source masque_générique*

- *Pour l'activation sur une interface d'un routeur CISCO*

Syntaxe: ip access-group [*ACL_number* | ***name [in | out]]***

- On peut compléter par: **access-list *ACL_number remark test***

La sécurité des donnés : Cryptologie

- **Définitions**

- Cryptologie : Il s'agit d'une science mathématique comportant deux branches : la cryptographie et la cryptanalyse.

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

- Cryptanalyse : Opposée à la cryptographie, elle a pour but de retrouver le texte clair à partir de textes chiffrés en exploitant les failles des algorithmes utilisés.

La sécurité des donnés : Cryptologie

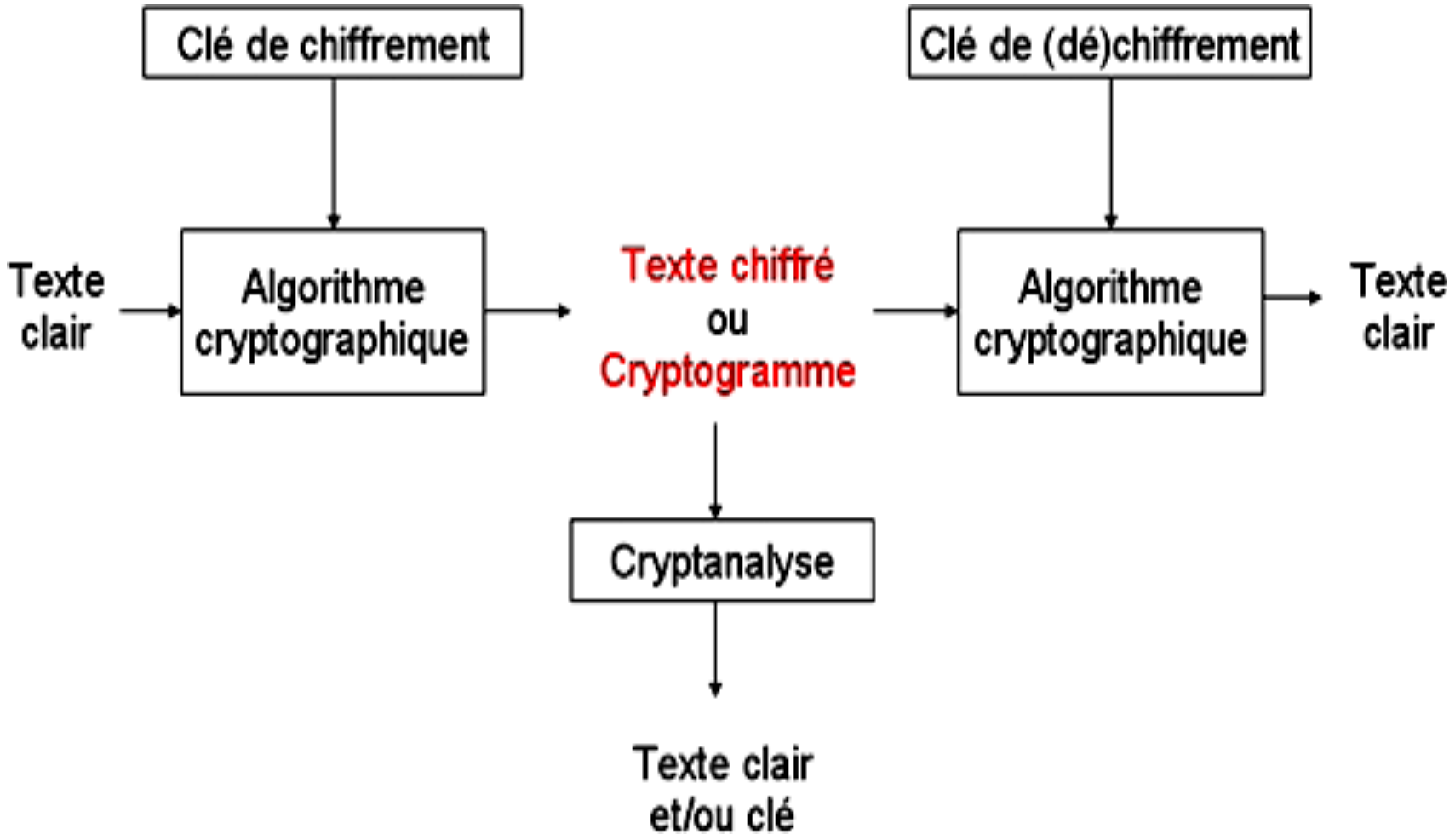
- **Définitions**

- Crypto-système : Il est défini comme l'ensemble des clés possibles (espace de clés), des textes clairs et chiffrés possibles associés à un algorithme donné.

- Texte chiffré : Appelé également cryptogramme, le texte chiffré est le résultat de l'application d'un chiffrement à un texte clair.

- Clé : Il s'agit du paramètre impliqué et autorisant des opérations de chiffrement et/ou déchiffrement.

Cryptologie : Vocabulaire de base



A. Cryptographie classique

- I- **Chiffrement par substitution:** Cette méthode correspond à substituer un caractère ou un groupe de caractères par un autre dans le texte à chiffrer.

- Plusieurs types de **Chiffrement par substitution :**

I.1- **mono-alphabétique :** consiste à remplacer chaque lettre du message par une autre lettre de l'alphabet ;

Chiffrement par substitution: mono-alphabétique

- 1ère **méthode :** sub-mono-alph:alphabétique
- **Exemple:**Chiffre de César (50 av. J-C)
- Décalage de 3 positions à gauche.

Clair : ABCDEFGHIJKLMNOPQRSTUVWXYZ

Chiffré : DEFGHIJKLMNOPQRSTUVWXYZABC

2ème méthode : sub-mono-alph: numérique

- Pour le chiffrement, on aura la formule:$C = E(p) = (p + k) \bmod 26$
- Pour le déchiffrement, il viendra: $p = D(C) = (C - k) \bmod 26$

- p est l'indice de la lettre de l'alphabet
- k est le décalage

Chiffrement par substitution: mono-alphabétique

Chiffrez DCODEX avec César, un décalage de 3 caractères

A	B	C	D	E	F	G	H	I	J	K	L	M
D	E	F	G	H	I	J	K	L	M	N	O	P
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	R	S	T	U	V	W	X	Y	Z	A	B	C
14	15	16	17	18	19	20	21	22	23	24	25	26

- **1ère méthode :** alphabétique , **Chiffrement :** GFRGHA

- **2ème méthode :** numérique
- **Chiffrement:**C = E(p) = (p + k) mod 26, D ?(4+3) mod 26=7=G
- **Déchiffrement :**P = D(C) = (C − k) mod 26, A ?(1-3) mod 26=24=X

Chiffrement par substitution: poly-alphabétique

- 1.2-**poly-alphabétique :** consiste à utiliser une suite de chiffrement, mono-alphabétique réutilisée périodiquement ;

- Utilisation d'une clef secrète : on répète la clef autant de fois jusqu'à satisfaire tout le texte.

- ***Deux méthode :***

1ère méthode Par calcul au modulo 26

Pour coder : DCODE avec une clef CLE,

DCODE , CLECL ⟶ pour chiffrer : DCODE + CLECL

D:4+3=7mod26=7=G donc : texte chiffré=GOTGQ

Chiffrement par substitution: poly-alphabétique

2ème méthode par carré de vigenère (1568).

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

TEXTE=DCODE et la clé=CLE texte chiffré= croisement des L/C)

DCODE (1ère ligne)

C L EC L (1ère colonne)

D et C =F, C et L=N, O et E = S… FNSFP

II. Chiffrement par transposition

- Toutes les lettres du message sont présentées, mais *dans un ordre différent.*
- C'est un chiffrement de type *anagramme.* Il utilise le principe mathématique des **permutations** (par colonne par exemple). *Seul l'ordre est changé*.

- **II.1- Transposition par blocs :** on écrit le message ***horizontalement*** dans une matrice prédéfinie (chiffrement) et on lit le message ***verticalement*** (déchiffrement),
- i.e: Chaque bloc de n lettres est mélangé d'une certaine manière.

II.1.1 Transposition par blocs

- **Exemple**: blocs de 3*3
- « le monde ne sera pas détruit par ceux qui font le mal».

l	e		n	e		a	s		t		p	x		q	t	l	e
m	o	n	s	e	r	d	é	t	a	r		u	i			m	a
d	e		a		p	r	u	i	c	e	u	f	o	n	l		

- On lit ensuite par colonne:
- Lmdeoe n nsaee rpadrséu titac rep uxuf ioq nt iim ea

II.2 Transposition à base matricielle

- Le message en clair est écrit dans une matrice.
- La clé est la matrice.
- La technique de transposition de base consiste à lire la matrice en colonne.
- Exemple (6,5):

M	**E**	**S**	**S**	**A**	**G**
E		**S**	**E**	**C**	**R**
E	**T**		**A**		**T**
R	**A**	**N**	**S**	**P**	**O**
S	**E**	**R**			

Le message **en clair** est :

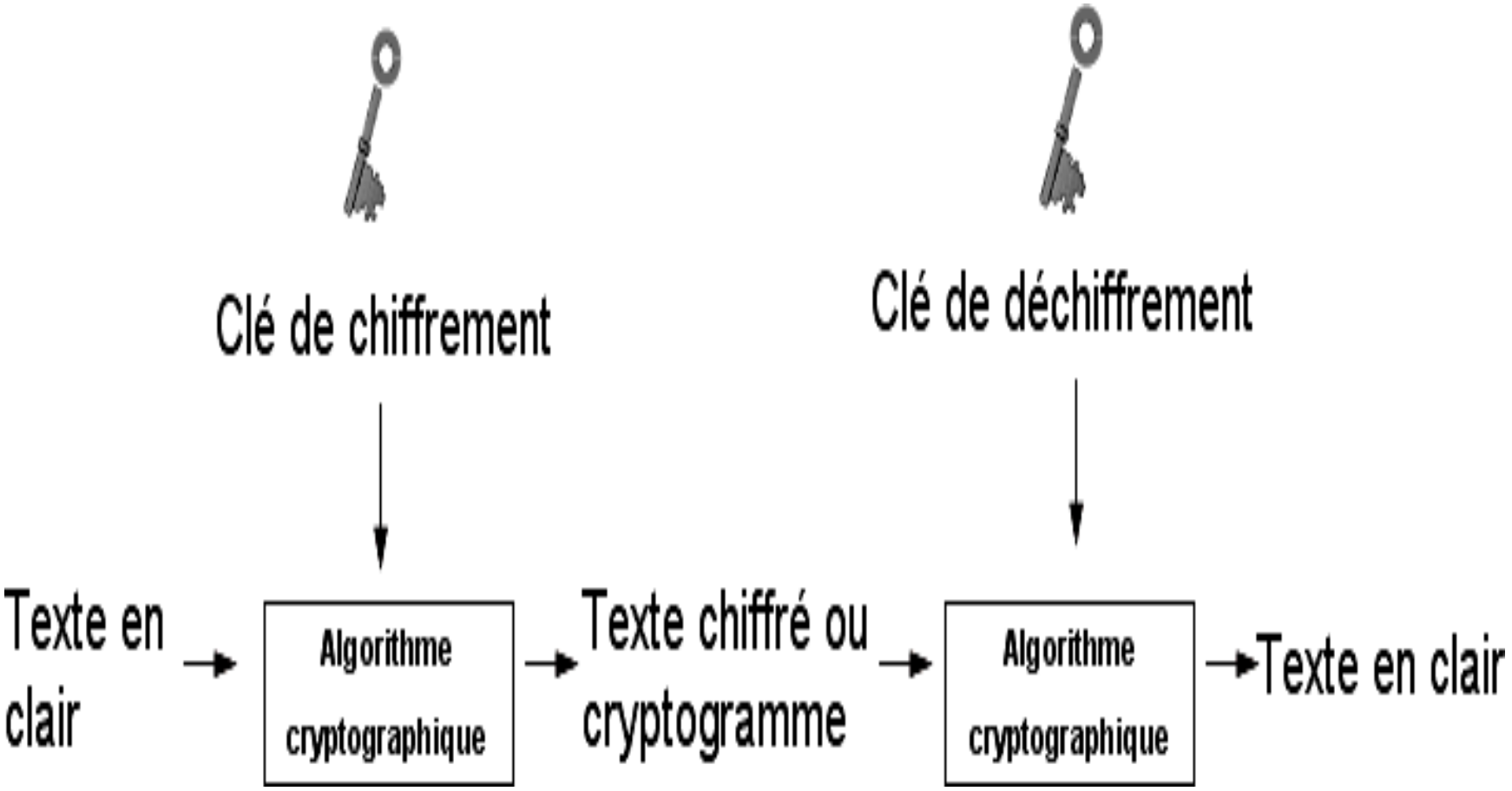
« MESSAGE SECRET A TRANSPOSER »

Le message **crypté** est donc:

« MEERSE TAESS NRSEAS AC P GRTO »

B. La cryptographie moderne : Chiffrement symétrique

1.Cryptographie à clefs privés:



- Nécessite :

- Un algorithme F de chiffrement symétrique
- Ou 2 algos (F1 pour chiffrer, F2 pour déchiffrer)
- Une clé K partagée entre E et R

- Principe :

- E chiffre le message M en C = F1(K,M)
- E envoie le message C à R
- R le décrypte et retrouve M = F2(K,C)

B.1 La cryptographie moderne (DES)

- **1.1 Algorithme Data Encryption Standard (DES)**

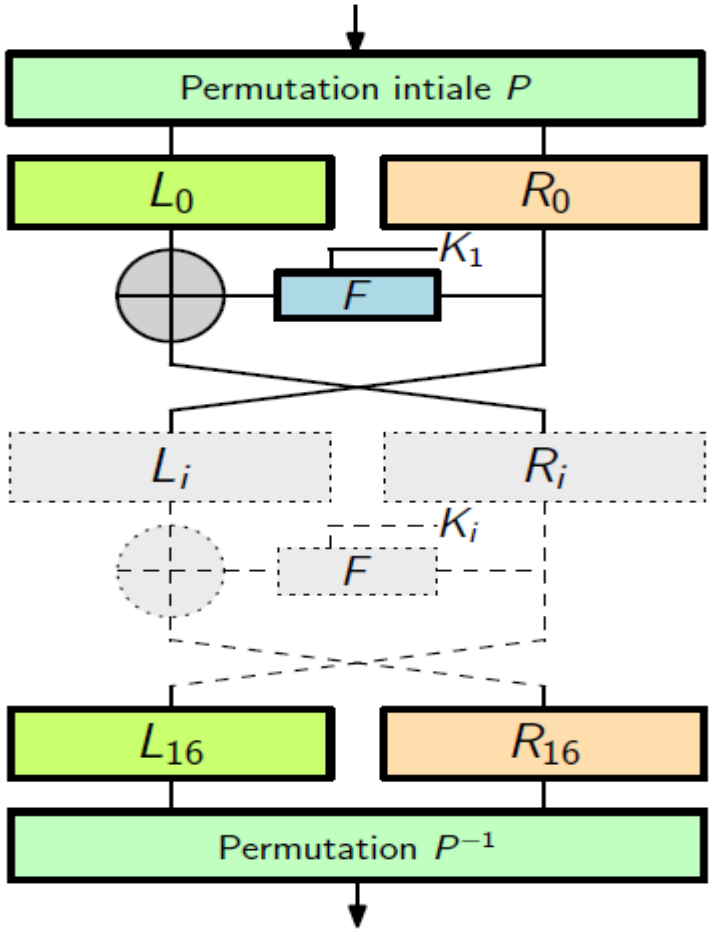


Schéma de Feistel à 16 tours

Le DES est un algorithme de chiffrement symétrique par blocs qui permet de chiffrer des mots de 64 bits à partir d'une clef de 56 bits + 8 bits de parité.

* Le déchiffrement est identique au chiffrement, à condition de prendre les sous-clés dans l'ordre inverse.

B.1 La cryptographie moderne (DES)

- Les avantages du DES

- Les avantages du DES

- la rapidité :

- la rapidité :

- Le chiffrement symétrique est typiquement 100 fois plus rapide que le chiffrement asymétrique.

- Il est particulièrement adapté à la transmission de grandes quantités de données.

B.1 La cryptographie moderne (DES)

- **- Les limites du DES**
- L'inconvénient est l'explosion combinatoire du nombre de clefs : pour que n personnes communiquent il faut O(n^2) clefs qui doivent être échangées de façon sûre. Au lieu de O(n) clefs en cryptographie asymétrique.

- -taille des clés : la recherche exhaustive, 2^56 devient réalisé.

- Taille des blocs 64 bits est devenu court et présente des risque d'attaques.

B.1 La cryptographie moderne (AES)

- 1.2 algorithme Advanced Encryption Standard (AES):

- est un algorithme de chiffrement par blocs à plusieurs tours similaire à DES mais avec une taille de blocs de 128 bits et de clefs supérieures et variables, choisis entre 128, 192 et 256 bits.

- Algorithme de chiffrement par:

  -Traitement itératif de ces blocs en fonction de la taille de la clé secrète :

  - 10 itérations pour des clés de 128 bits
  - 12 itérations (clés de 192 bits)
  - 14 itérations (clés de 256 bits)

B.1 La cryptographie moderne (AES)

- **Initialisation**
  - Le bloc de 128 bits (=16 octets) est recopie verticalement dans un tableau « d'etat » 4x4 .
    - XOR avec la sous-clé numéro 0.
- **Itérations (10, 12 ou 14 fois) sur le tableau d'état :**

  -Confusion : substitution indépendante sur chaque bloc, basée sur les inverses dans le corps fini 2^8

  -Décalage des trois dernières lignes suivant un pas différent
  - Diffusion : multiplication polynomiale des colonnes
  - XOR avec la sous-clé numéro i
- **Lecture du résultat final dans le tableau d'etat.**

B.1 La cryptographie moderne (AES)

- **Les atouts de l'A.E.S**

- Il existe beaucoup plus de clés possibles :

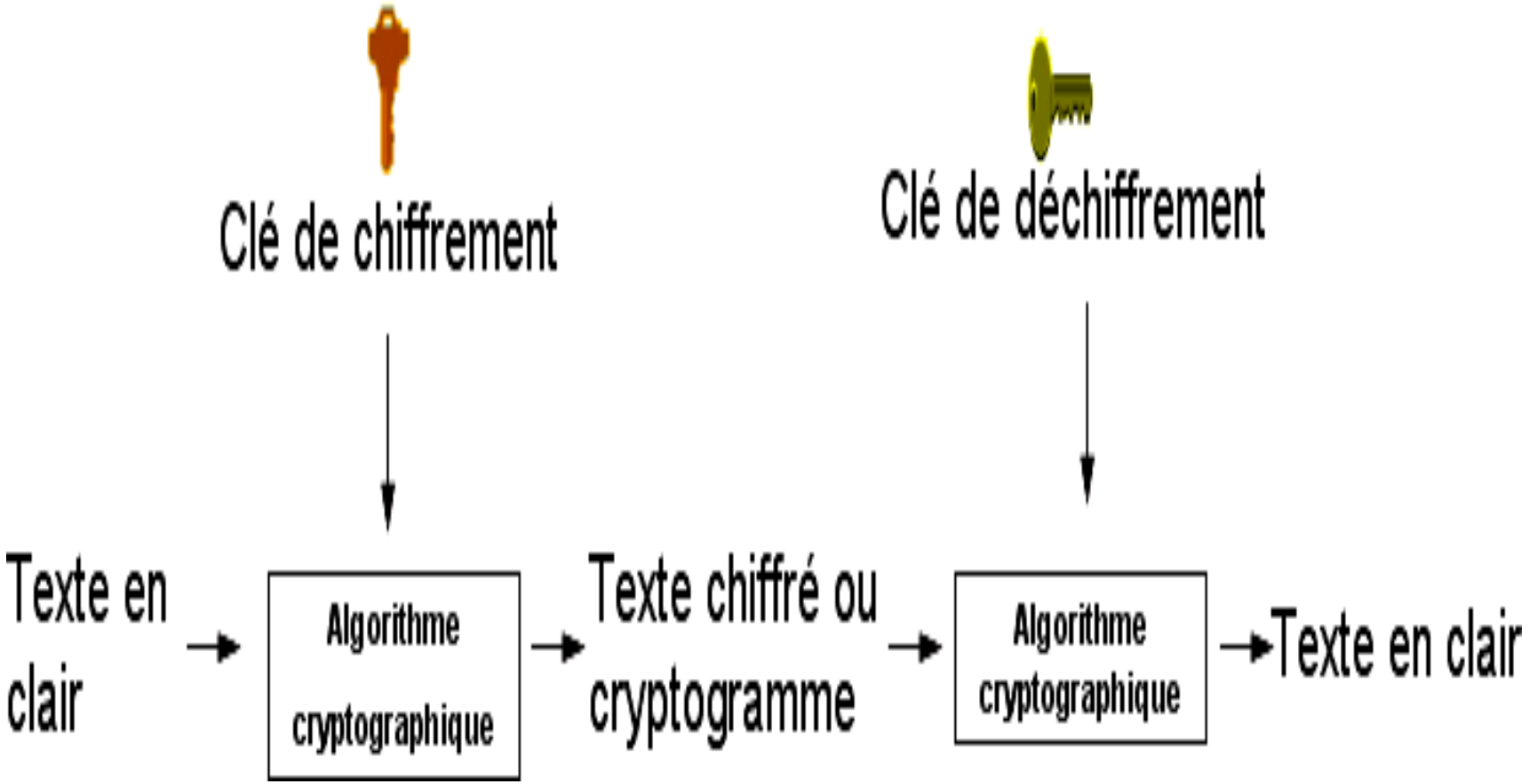
2^128 clés de 128 bits contre 2^56 clés pour le DES, soit environ 10^21 fois plus de solutions.

- Aucune clé ≪ faible ≫ n'est connue actuellement : toutes les clés sont utilisables.

- Resistance à la cryptanalyse différentielle et linéaire.

B.2 La cryptographie moderne : Chiffrement asymétrique

2.Cryptographie à clefs publiques :



Diffie et Hellman résolvent l'échange de clés (1976)

- Le protocole repose sur une fonction de la forme :

$K = W^X \bmod P$, avec P premier et $1<W<P$.

- Une telle fonction est très facile à calculer, mais la connaissance de K ne permet pas d'en déduire facilement X.

- Cette fonction est publique, ainsi que les valeurs de W et P.

Diffie et Hellman résolvent l'échange de clés (1976)

- Exemple

- Prenons W = 7 et P = 11
- Alice et Bob veulent échanger la clé secrète SK
- Alice choisit A=3 et Bob choisit B=6
- $SK = W^{B.A} \bmod P$
- Alice calcule $\alpha = W^A \bmod P = 7^3 \bmod 11 = 2$
- Bob calcule $\beta = W^B \bmod P = 7^6 \bmod 11 = 4$
- Echange des clés α et β entre Alice et bob.

- Alice calcule $\beta^A \bmod P$ qui est $(WB)^A \bmod P$, soit $4^3 \bmod 11 = 64 \bmod 11 = 9$

de la même manière

- Bob calcul $\alpha^B \bmod P = 2^6 \bmod 11 = 9$

2.1 RSA (1977) : Ronald Rivest, Adi Shamir et Leonard Adleman

- L'algorithme est remarquable par sa simplicité. Il est basé sur les nombres premiers.
- Pour crypter un message, on fait: **c = m^e mod n**
- Pour décrypter: **m = c^d mod n**

m = message en clair

c = message crypté

(e,n) constitue la clé publique

(d,n) constitue la clé privée

n est le produit de 2 nombres premiers

^ opérateur de puissance (a^b : a puissance b)

mod est l'opération de modulo (reste de la division entière)

2.1 RSA : Comment faire ?

1. Prendre deux nombres premiers **p** et **q** (***de taille à peu près égale***).
2. Calculer **n = p x q**.
3. Choisir **e** qui n'a aucun facteur en commun avec:**(p-1)(q-1)=z**.
4. Calculer l'inverse de **e** (mod **z**), c'est-à-dire **d** tel que : **e x d** = 1 mod **z**.
5. Le couple **(e,n)** constitue la clé publique **PK** et **(d,n)** est la clé privée **SK**. ***i.e ;*** **PK= (e,n) , SK= (d,n)**

2.1 RSA : Problèmes et limites

- Trouver de grands nombres premiers (sont choisis au hasard).
- (on prend en fait des nombres premiers en probabilité).

- Choisir des clés secrètes et publiques assez longues.

- Limitation des calculs du fait de la puissance de calcul disponible (**RSA carte bancaire**).

- Même clé publique pour tout le monde.

1.présentation des réseaux sans fil

- Un réseau sans Fil est un réseau informatique où la connexion entre les postes et les différents systèmes se fait par ondes radio.

- **1.1 Types de réseaux sans Fil :**
- **1.1.1.En fonction de la taille**
- ***1.1.1.1 Réseaux personnels sans fils (WPAN) :***concerne les réseaux sans fils d'une faible portée : de l'ordre de quelques dizaines mètres.
- ***1.1.1.2 Réseaux locaux sans fils (WLAN):*** est un réseau permettant de couvrir l'équivalent d'un réseau local d'entreprise, dont la portée va jusqu'à 500 m.(campus, hôpital, aéroport,…).

SÉCURITÉ DES RÉSEAUX SANS FIL

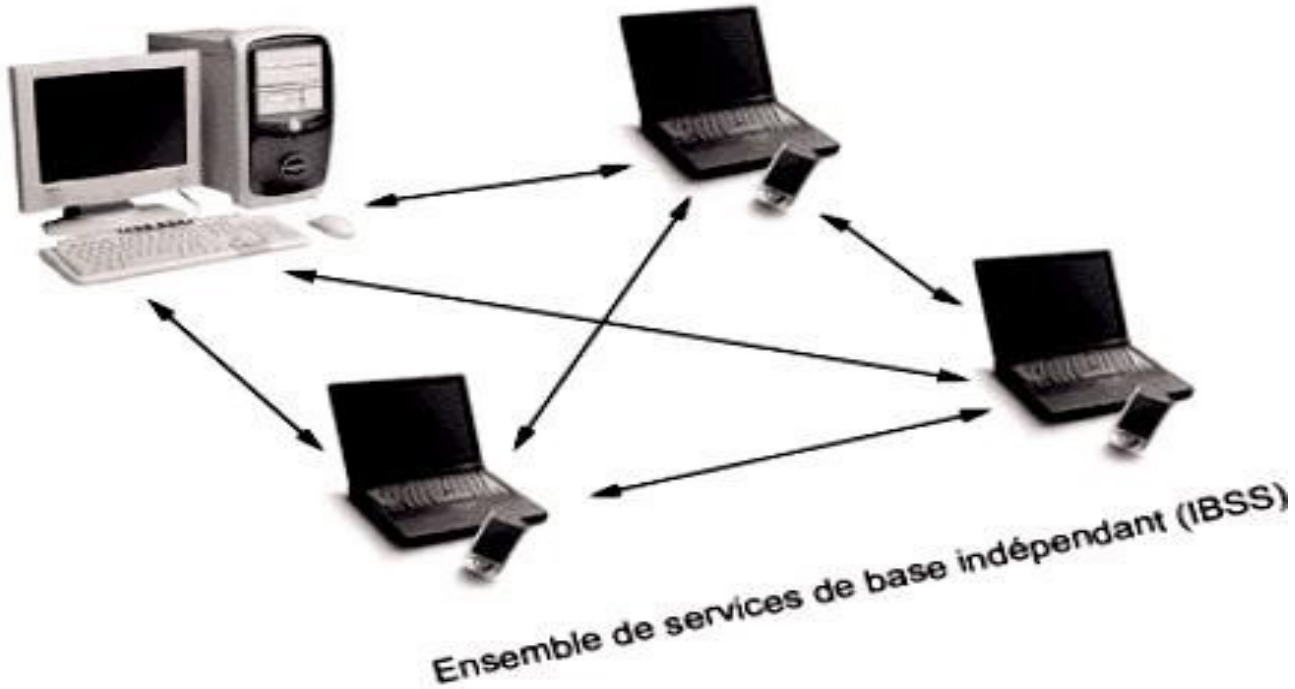
- *1.1.1.3 Réseaux métropolitains sans fils (WMAN):*Les WMAN sont basés sur la norme IEEE 802.16. Ce type de réseau utilise le même matériel que celui qui est nécessaire pour constituer un WLAN mais peut couvrir une plus grande zone de la taille d'une ville avec une portée de 50km.

- *1.1.1.4 Réseaux étendus sans fils (WWAN):* est également connu sous le nom de réseau cellulaire mobile, dont la zone de couverture est très large à l'échelle mondiale.

- **2. En fonction du mode opératoire**
- **2.1 le mode infrastructure**

➢ chaque ordinateur station se connecte à un point d'accès via une liaison sans fil. L'ensemble formé par le point d'accès et les stations situés dans sa zone de couverture est appelé ensemble de services de base (en anglais *Basic Service Set, noté BSS).*

- **2.1 le mode Ad Hoc:** En mode **ad hoc,** les machines sans fil clientes se connectent les unes aux autres afin de constituer un **réseau point à point (*peer to peer en anglais).***
-



Mode Ad Hoc

Les attaques d'un réseau WIFI

- **Le War-driving:** il consiste à se promener en voiture avec une antenne **WiFi** et à noter la position et les caractéristiques de tous les AP que l'on puisse trouver.
- **L' Espionnage :** WIRESHARK
- **L'intrusion :** Un réseau sans fil non sécurisé représente de cette façon un point d'entrée royal pour le pirate au réseau interne d'une entreprise ou une organisation.
- **Le Dénis de Service:** Le but de ce type d'attaque n'est pas de détruire ou de récupérer les données stockées sur le serveur visé mais simplement de le rendre indisponible.
- **Usurpation d'adresse MAC:** Spoofing.

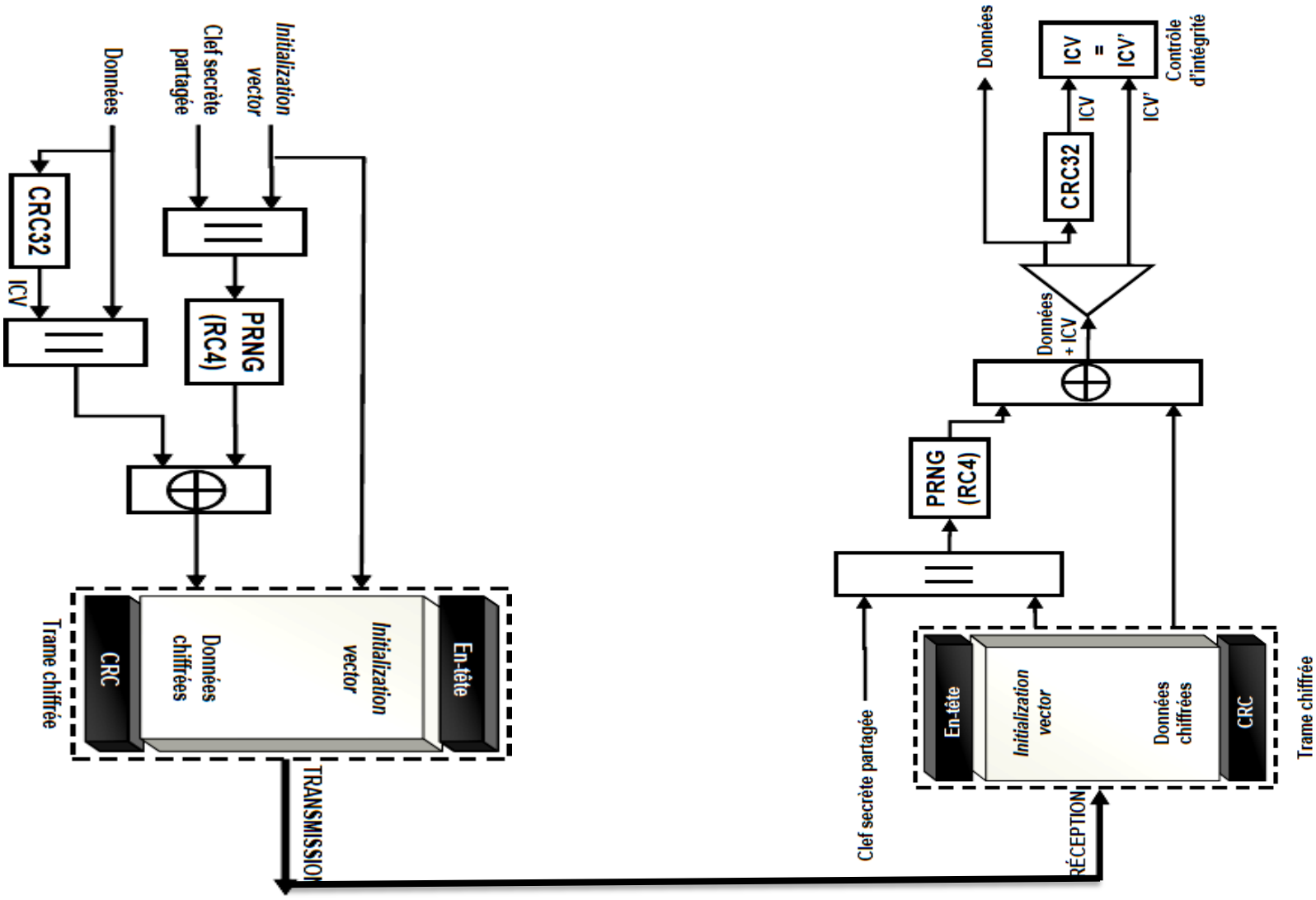
Solutions pour sécuriser un réseau WIFI (WEP)

- **1. WEP (Wired Equivalent Privacy)**

Est un protocole de sécurité pour les réseaux sans fils défini dans le standard 802.11, il utilise :

- ✓ l'algorithme de chiffrement RC4 (**confidentialité**),
- ✓ la somme de contrôle **CRC-32 (Intégrité),**
- ✓ les clés statiques de 64 ou 128 bits **(authentification).**

Fonctionnement du WEP (chiffrement des données)



LES FAILLES DU WEP

- Faiblesse de certaines clés RC4.
- Le principal problème est qu'une clé de flux ne peut pas être réutilisée.
- Théoriquement, une fois que les 2^24 clés possibilités ont été utilisées, il est nécessaire de changer de clé secrète.
- La norme ne spécifie pas de méthode précise de gestion de clés.
- En pratique, les clés secrètes ne sont quasiment jamais changées.

Solutions pour sécuriser un réseau WIFI (WPA / WPA2)

- **2. WAP / WAP2 : Wi-Fi Access Protocol,** Appelé aussi **WPA (*Wi-Fi Protected Access*)**

- **WPA:** son fonctionnement repose sur un système d'échange de clés dynamiques, renouvelées tous les 10 ko de données Ce procédé, appelé TKIP (*Temporal Key Integrity Protocol).*

- **WPA2** : protocole d'authentification de WPA , il Utilise CCMP.

Propriétés du WPA / WPA2

- **confidentialité:** Utilisation d'un protocole (TKIP) pour pallier les failles de WEP.
- **Intégrité** : Utilisation d'un code de vérification d'intégrité (MIC) en remplacement de CRC.
- **Authentification:** Deux modes de fonctionnements :
- WPA est conçu pour fonctionner avec un serveur d'authentification 802.1X (un serveur radius en général) qui se charge de la distribution des clés à chaque utilisateur.
- WPA propose aussi un mode moins sécurisé (PSK) basé sur un secret partagé commun à tous les utilisateurs.

Quelques protocoles d'authentification sous WPA/WPA2

- **EAP (Extensible Authentification Protocol)** : est un mécanisme d'authentification universelle.

- WPA et WPA2 implémentent 5 types d'EAP :
  - ✓1. EAP-TLS,
  - ✓2. EAP-TTLS/MSCHAPv2,
  - ✓3. PEAPv0/EAP-MS-CHAPv2,
  - ✓4. PEAPv1/EAP-GTC,
  - ✓5. EAP-SIM/EAP-AKA.

Solutions pour sécuriser un réseau WIFI (@MAC / VPN)

- **3. Filtrage par adresse Mac**

  Cette technique consiste à limiter l'accès au réseau à un certain nombre de machines en se basant sur leurs adresses MAC.

- **4. VPN (Virtual Private Network)**

  Cette technologie, est très utilisée dans le monde de l'entreprise, permet de créer un tunnel (une liaison virtuelle), via Internet, entre deux réseaux physiques géographiquement distants et ce, de manière transparente pour ses utilisateurs.