République Algérienne Démocratique Et Populaire
Ministère De L'enseignement Supérieur Et De La Recherche Scientifique
ECOLE NATIONALE POLYTECHNIQUE D'ORAN MAURICE AUDIN
Département Mathématiques et Informatique
Filière IMSI : 4ème année ingénieur

Sécurité des systèmes d'information

DR F.KABLI
kablifatima47@gmail.com

Introduction

- Qu'est-ce que la sécurité du système d'information ?
- La sécurité globale et les domaines d'application.
- La sécurité physique et environnementale
- La sécurité logique

Qu'est ce que la sécurité des systèmes informatiques ?

La sécurité des systèmes informatiques correspond à un ensemble de techniques mises en œuvre pour garantir la **sécurité** et l'**intégrité** d'un système informatique. Ces techniques peuvent être :

- *Fonctionnelles*
- *Organisationnelles*
- *Politiques*
- *Juridiques*
- *humaines …*

Introduction

La sécurité des systèmes informatiques ?

- La mise en place de la sécurité informatique est généralement ass-urée par un administrateur réseau en interne à l'entreprise ou une société indépendante.

- Il existe de nombreux techniques permettant d'assurer la protection d'un système informatique : **la cryptographie, la restriction d'accès par mot de passe, les antivirus, le pare-feu, un système de détection d'intrusion.**

Approche globale de la sécurité

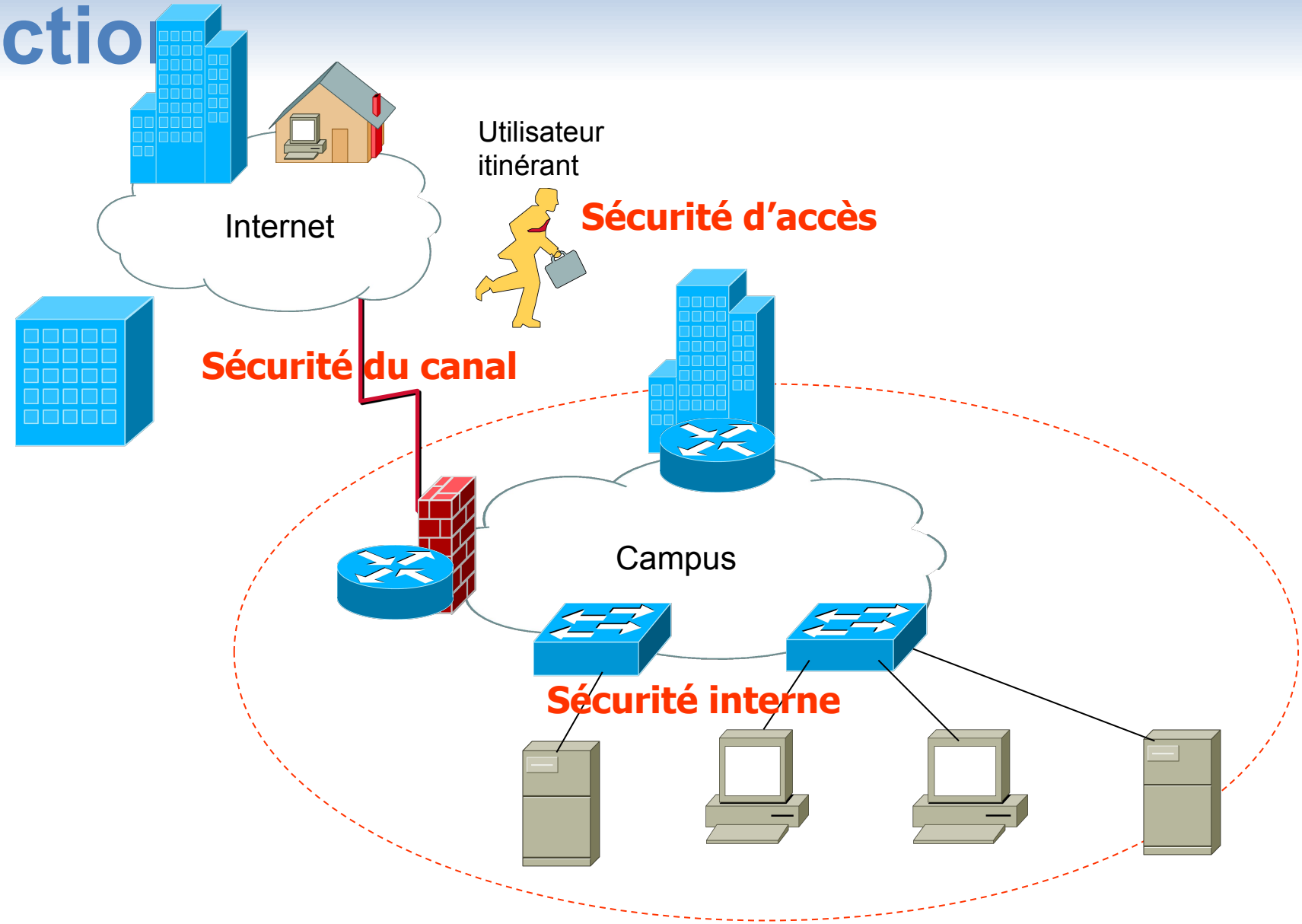
- Il faut traiter la sécurité d'un système informatique en sa totalité, car il est inutile d'avoir une porte blindée dans sa maison et en même temps avoir les fenêtres ouvertes sur le monde extérieur.

- Partant de cette idée, on doit donc aborder la sécurité dans son contexte global c'est–à–dire, on doit assurer les différents aspects de sécurité suivants :

Introduction

- La Sécurité Organisationnelle
- La sécurité physique et environnementale
- La sécurité des accès
- La sécurité des réseaux
- La sécurité des serveurs
- La sécurité des données
- La sécurité énergétique
- La sécurité antivirale (c'est la sécurité contre les virus informatiques)

Introduction



La Sécurité Organisationnelle

- Définir les rôles des différents acteurs : Qui fait quoi ?
- Sensibiliser les utilisateurs aux problèmes de la sécurité.
- Intégrer **le facteur sécurité** dans tout projet informatique dès sa conception jusqu'à sa réalisation.
- Mise en œuvre de la sécurité.

Introduction

La sécurité physique et environnementale

- Règles de sécurité des locaux qui abritent les serveurs sensibles et les équipements d'interconnexion : équiper ces locaux par des détecteurs d'incendie et par un système d'extinction automatique.
- Verrouillage des locaux contre le vol du matériel.
- Accès permis seulement aux personnes autorisées (utiliser des clés spéciales ou une carte à puce pour contrôler les accès à la salle informatique).

Introduction

Enquête :

- 89% des sociétés ont déjà été confrontées à un vol d'ordinateur portable.
- 67% des vols d'ordinateurs portables ont lieu au bureau
- Seulement 3% des ordinateurs portables volés sont récupérés

La sécurité des accès

- Sécurité des accès aux postes de travail et aux serveurs pour les utilisateurs et les administrateurs. L'accès doit être assuré par :
  - Nom utilisateur et mot de passe
  - Carte à puce : l'authentification par carte à puce est destinée à garantir l'identité d'une personne à assurer son identification via un code PIN et à protéger l'accès aux postes de travail par le biais d'un mot de passe dynamique
- Gestion des droits d'accès aux données et aux fonctionnalités des logiciels en fonction des profils des utilisateurs

Introduction

La sécurité des accès

Exemple:

- Serveur NIS : Yellow Pages » (YP)
- IDPrime MD est une carte à puce par certificats PKI à mini-lecteurs offrant un haut niveau de sécurité à l'identité de l'utilisateur qui essaie d'avoir un accès logique au réseau. Conçues à partir de la technologie éprouvée des cartes à puce, les cartes IDPrime MD sont des cartes robustes, mais simples à utiliser. En effet, elles ne contraignent pas les utilisateurs à saisir des mots de passe longs et compliqués ni à installer des appareils pénibles à utiliser.

La sécurité des réseaux

- Assurer la sécurité des topologies LAN et WAN pour garantir la continuité de transmission des données à l'intérieur et à l'extérieur de l'entreprise.
- Contrôler le flux des données entre le système d'information et le monde extérieur (c'est-à-dire l'Internet ou le WAN) pour éviter tout risque d'attaque (alors il faut installer serveur proxy avec un firewall).
- Détecter les intrusions qui viennent de l'extérieur et les éviter au préalable.
- Assurer la sécurité de transmission de données sur l'Internet en implantant des protocoles sécurisés (SSL (Secure Sockets Layer) et en faisant le cryptage des messages.

La sécurité des serveurs

- Classification des serveurs de l'entreprise (le serveur proxy doit être assez performant pour bien protéger le serveur de base de données)
- Audit sécurité des configurations des serveurs sensibles.
- Sécuriser les procédures d'exploitation et d'administration (avec des mots de passe)

Introduction

La sécurité des données

- Assurer une sauvegarde quotidienne et hebdomadaire des données.
- Faire la sauvegarde sur des supports multiples.
- Protéger les supports de sauvegarde, contre les incendies, dans une armoire inflammable.

Introduction

La sécurité énergétique

La sécurité énergétique est très importante quant au fonctionnement des équipements formant la plateforme technique. Il est recommandé d'équiper les armoires abritant les différents éléments par des onduleurs performants pour remédier aux petites coupures du courant ou aux chutes de la tension électrique. En revanche, pour les coupures de longue durée, il faut prévoir l'installation d'un groupe électrogène qui va assurer la continuité du courant nécessaire pour le bon fonctionnement.

Introduction

La sécurité antivirale (c'est la sécurité contre les virus informatiques)

- Un virus est un programme informatique qui peut infecter d'autres programmes dans le but de **les modifier** pour y ajouter une copie de lui-même, de **gêner leur fonctionnement** et **voire même les supprimer ou nuire à certaines composantes** de l'ordinateur.
- Les virus ne sont pas classés selon leurs dégâts mais selon

leur mode de propagation et d'infection.

La sécurité antivirale (c'est la sécurité contre les virus informatiques)

On distingue principalement quatre types de virus :

- *Vers*
- *Chevaux de Troie*
- *Bombes logiques*
- *Canulars*

L'analyse de risque

Différents aspects de la sécurité

Aspect :	**Exemple de mécanisme de protection :**
• Contrôle d'accès	
• Authentification	• Mot de passe, Firewall
• Confidentialité	• Signature
• Intégrité	• Cryptographie
• disponibilité	• Anti-virus
• Virus	

L'analyse de risque

Concepts

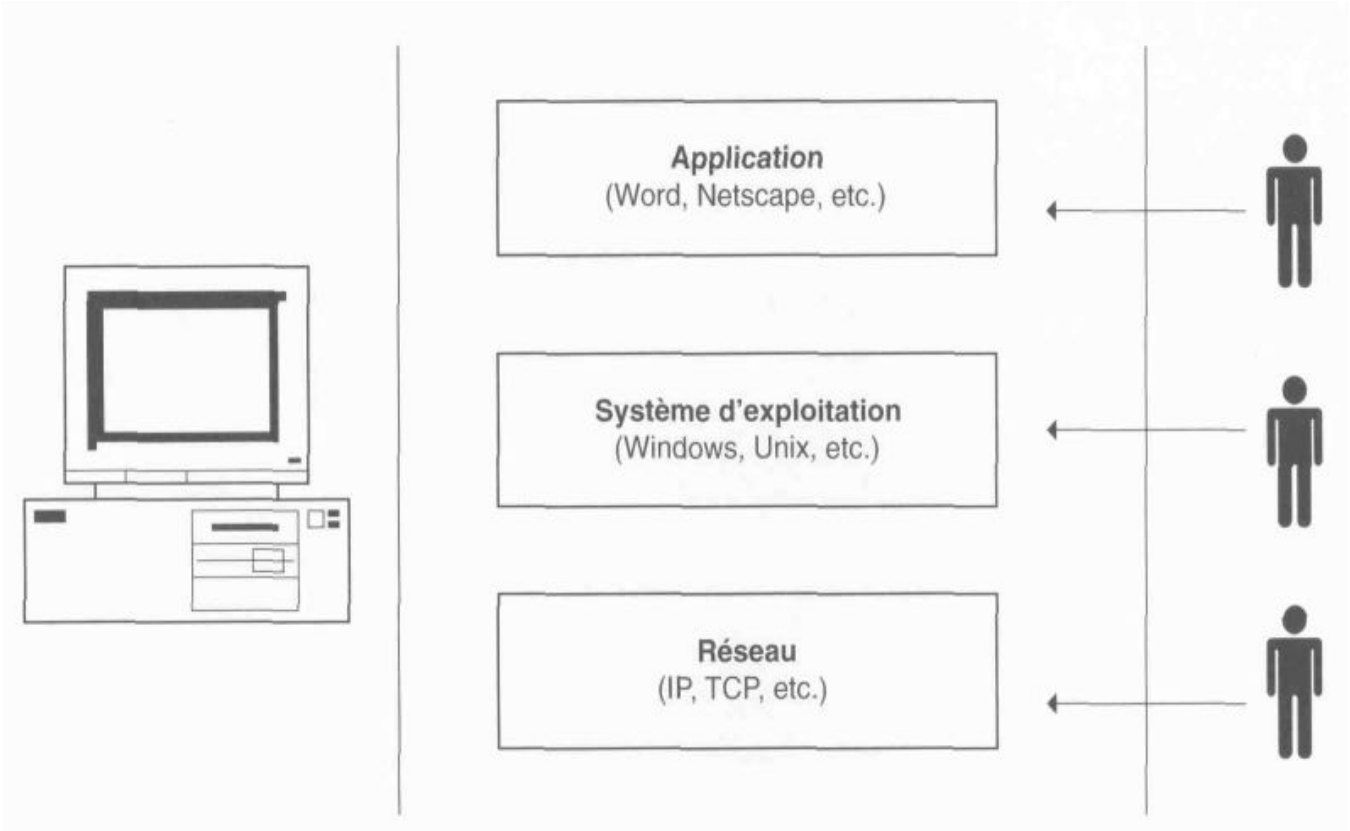
Sécurité d'un réseau: implique la sécurité de chaque machine (client, serveur) du réseau.

'Hacker' : programmeur qui utilise des attaques pour pénétrer au systèmes informatiques sans être détecté .

'Cracker': utilise des attaques pour réaliser des bénéfices économiques.

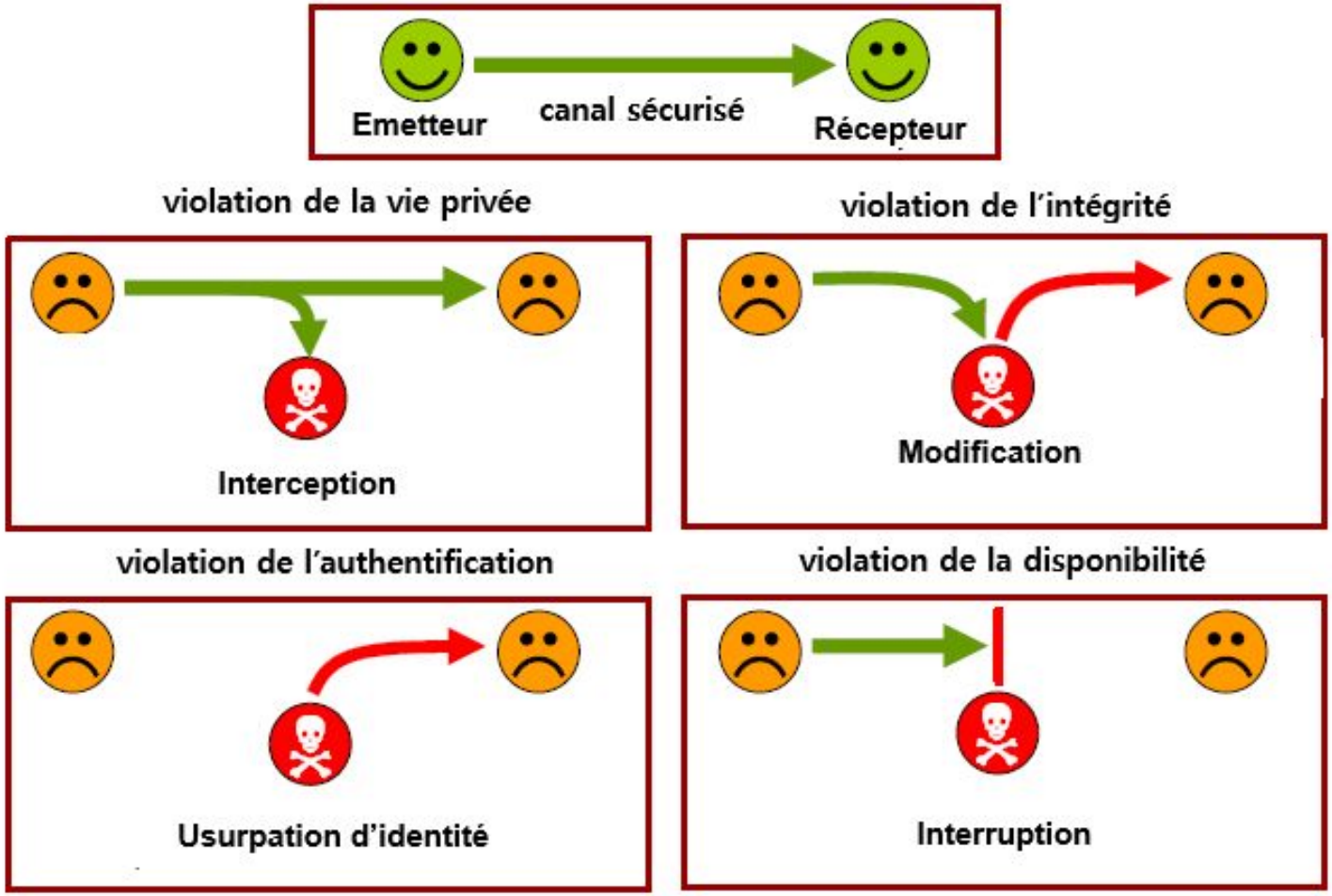
L'analyse de risque

Composantes d'un système susceptibles d'être attaquée



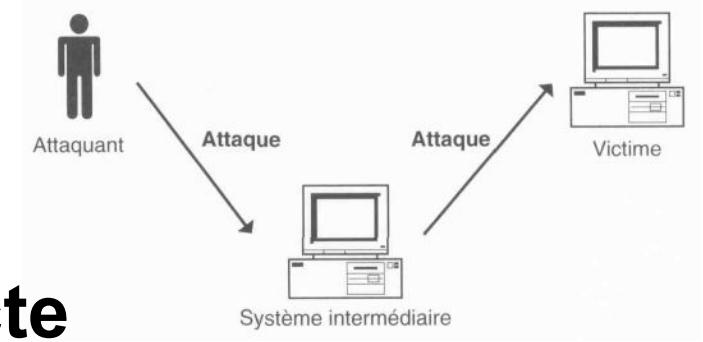
L'analyse de risque

Classification des Attaques

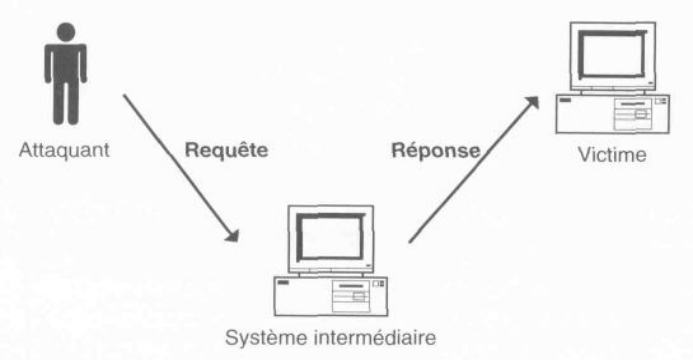


L'analyse de risque

Exemples d'attaques



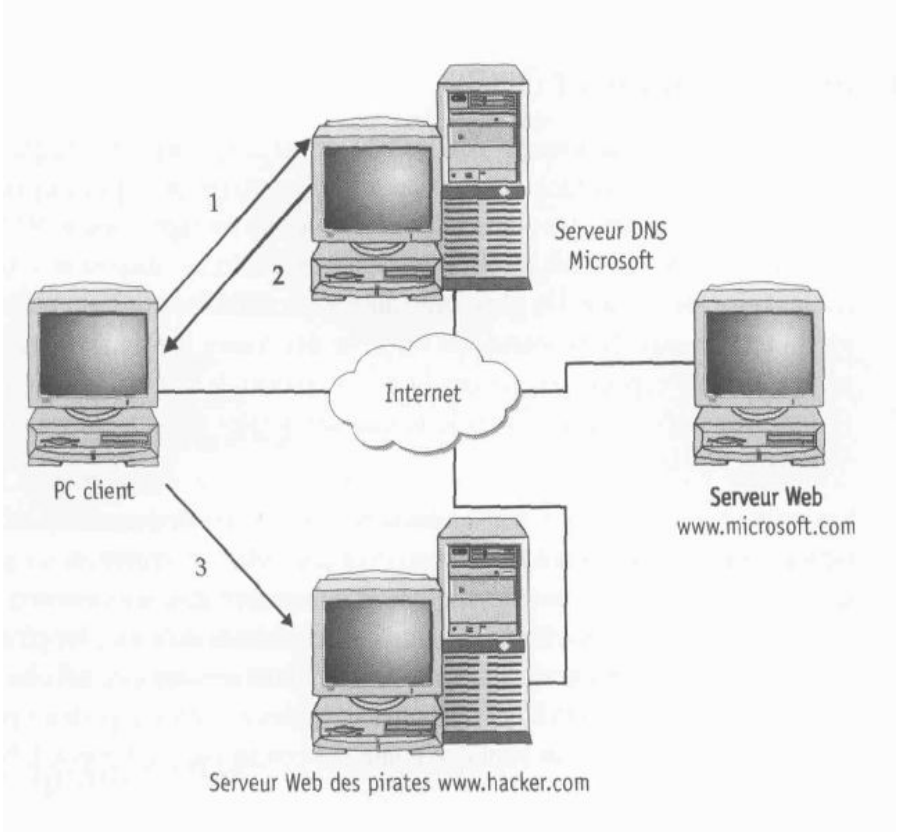
Attaque directe



Attaque indirecte par réponse

L'analyse de risque

Pollution du cache DNS



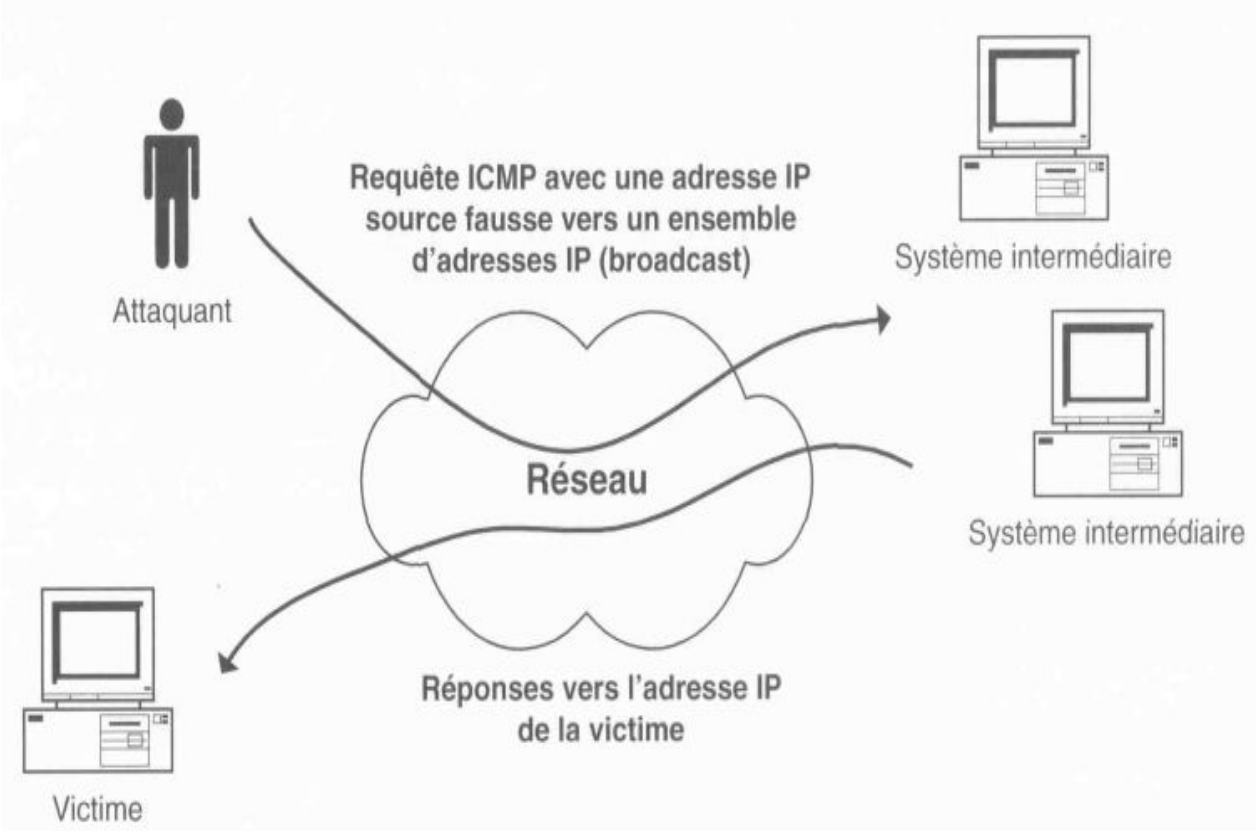
1) Le PC client demande à accéder au site Web de Microsoft. Le navigateur essaie de résoudre le nom *www.microsoft.com* en adresse IP.

2) Le cache du serveur DNS a été contaminé par un pirate et renvoie l'adresse IP *www.hacker.com* au lieu de celle de Microsoft.

3) Le système des pirates se fait maintenant passer frauduleusement pour *www.microsoft.com*

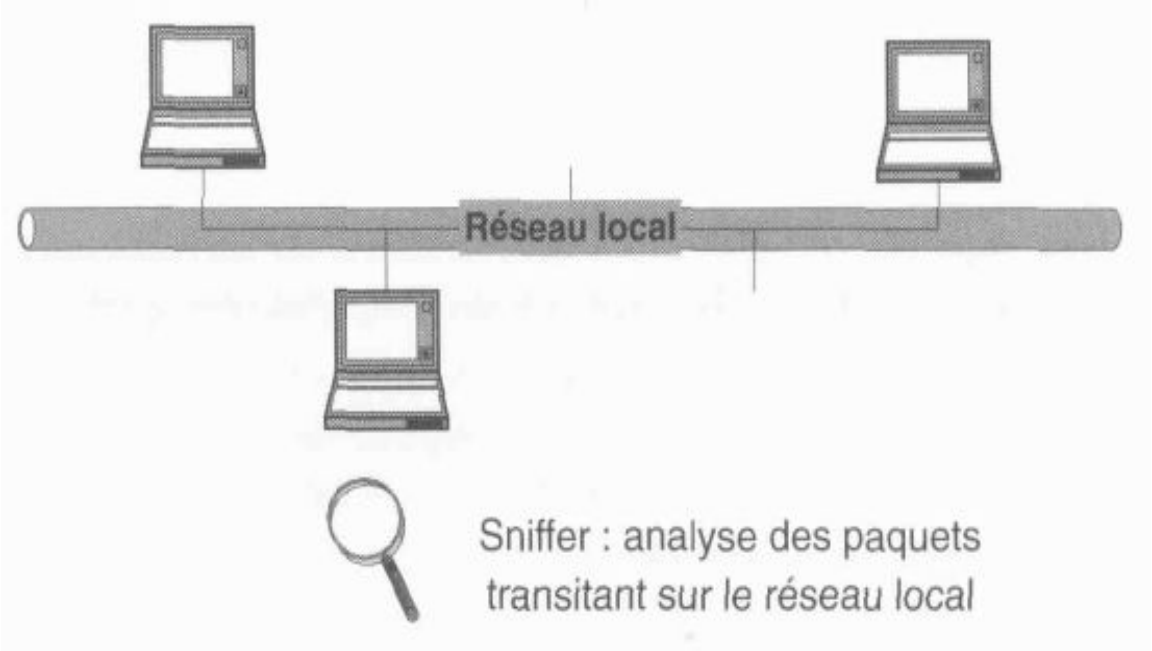
L'analyse de risque

Inondation de Ping : ICMP



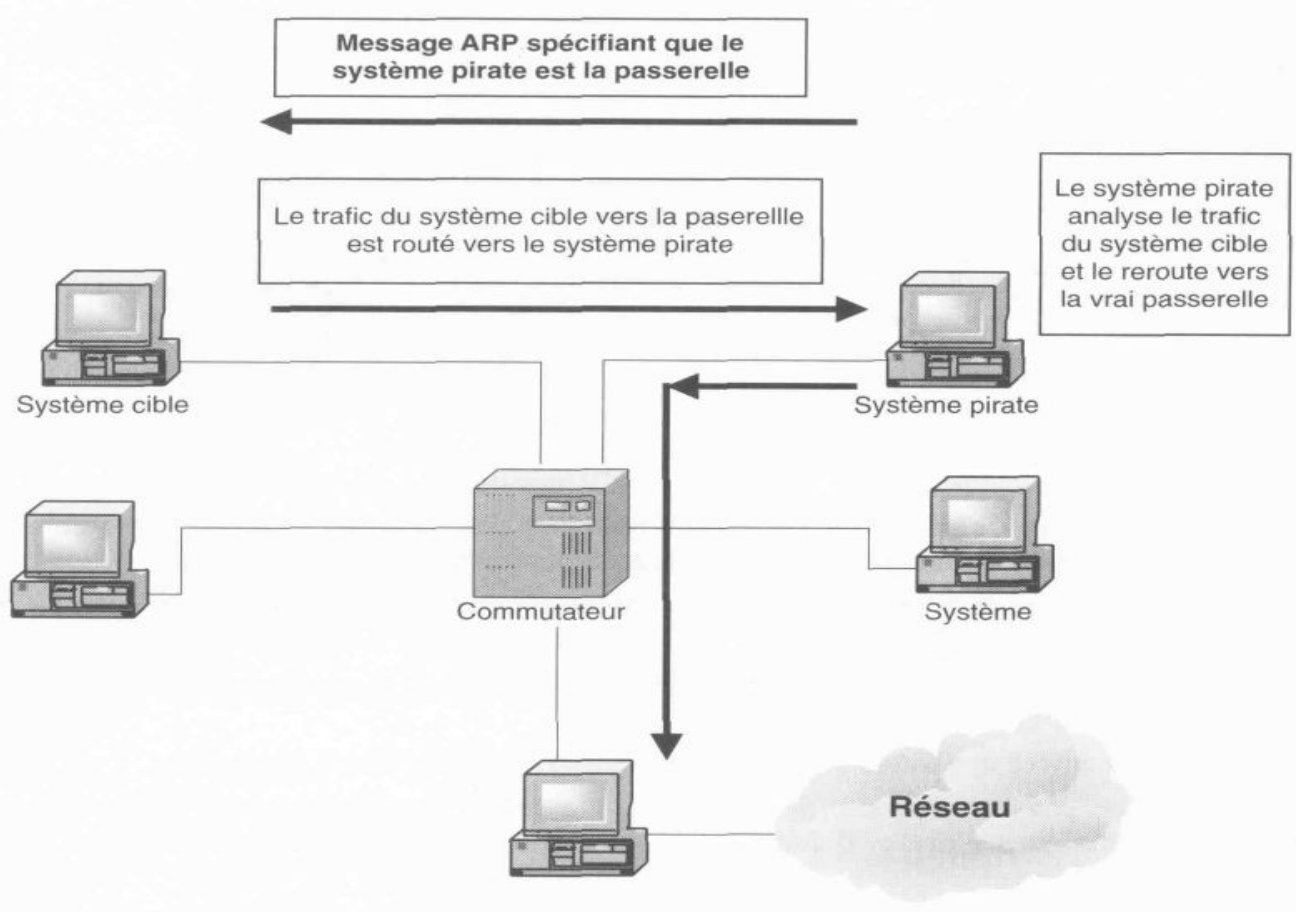
L'analyse de risque

Écoute sur un réseau local



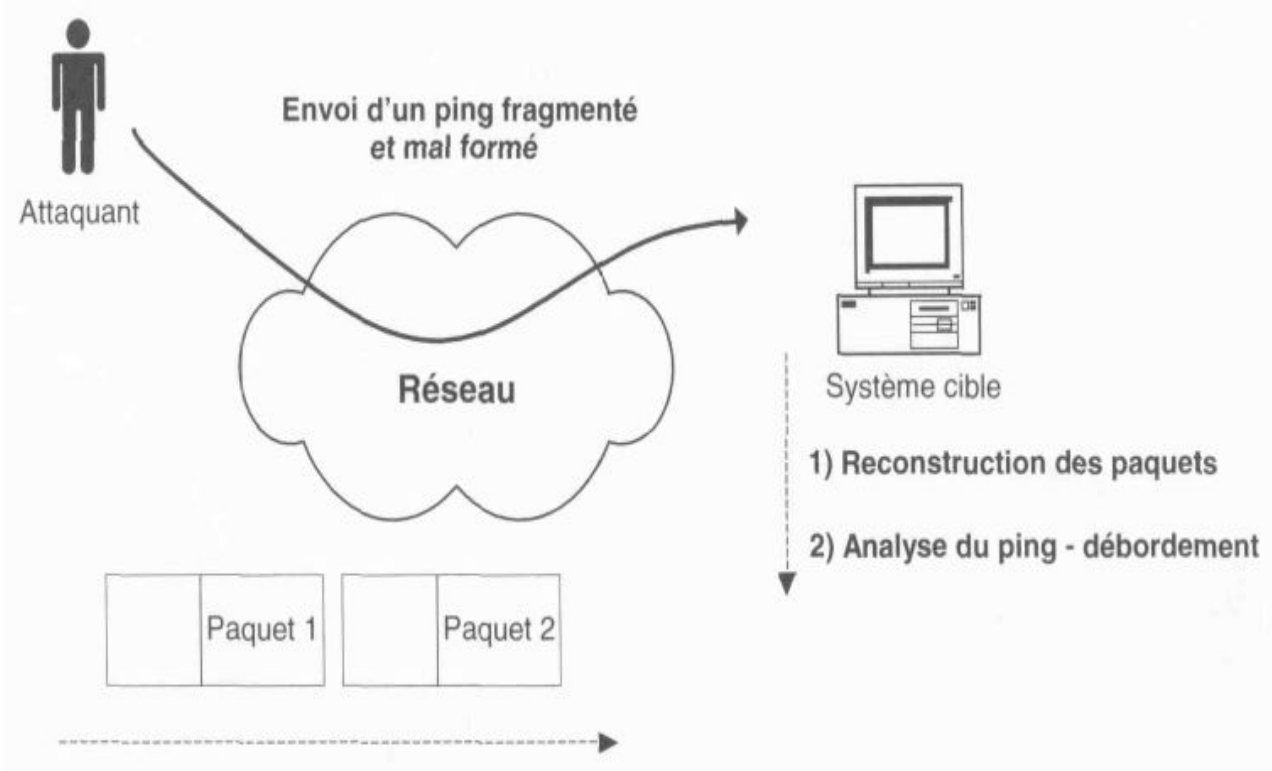
L'analyse de risque

L'attaque ARP spoofing



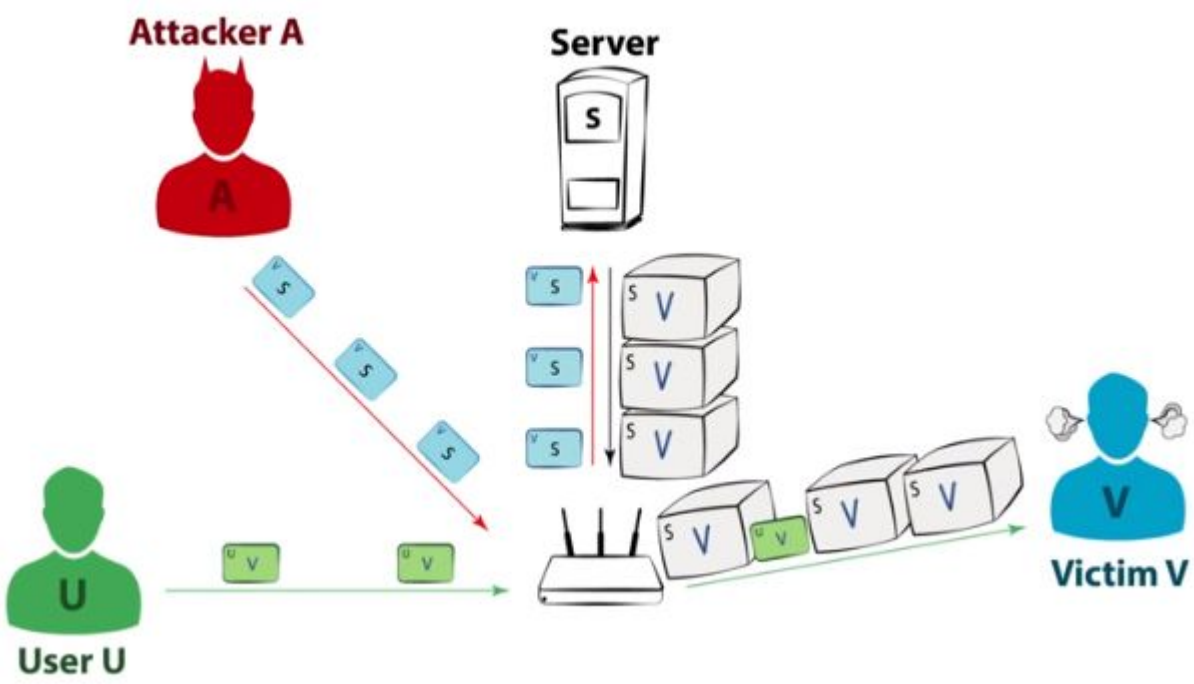
L'analyse de risque

L'attaque ping de la mort



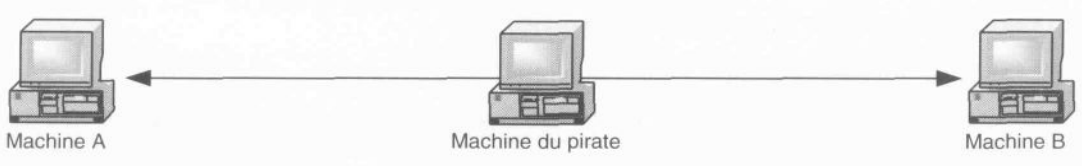
L'analyse de risque

L'attaque IP spoofing

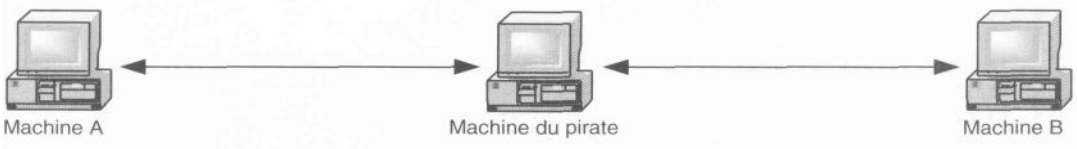


L'analyse de risque

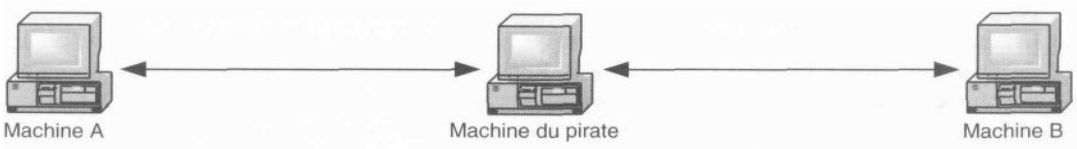
Machine du pirate (Man-in-the-middle)



en tant que relais transparent



en tant que relais applicatif



en tant que hijacker

L'analyse de risque

Les Attaques :

- **Attaques réseaux**
  - ✔ Connexion réseaux
  - ✔ Service
  - ✔ ……
- **Attaques systèmes**
  - ✔ Fichier mot de passe
  - ✔ Page web

La cryptographie et ses applications

- Les algorithmes cryptographiques se basent sur des fonctions mathématiques qui dépendent d'une clés secrète.

- La sécurité est au niveau clés, pas au niveau algorithmes cryptographiques.

- Les algorithmes cryptographiques sont publiées est connu par tout le monde.

Définition : Un message en clair est **transformé** en une forme ambigüe, **incompréhensible** par le public.

- Lors de sa réception, seul le destinataire **légitime** peut renverser le processus et obtenir le message **original** en clair.

- La **cryptologie** peut être définie littéralement comme la *science du secret*. Elle se compose de deux grandes branches distinctes :

  « La Cryptographie , La Cryptanalyse »

La cryptographie et ses applications

- Le verbe **crypter** est parfois utilisé le verbe **chiffrer**.

- **Les modifier** de telle façon à les rendre **incompréhensibles,** d'une part (le résultat de cette modification [le message chiffré] est appelé **cryptogramme** [en anglais ***ciphertext***] par opposition au message initial, appelé message en **clair** [en anglais ***plaintext***]).

- Les termes **chiffrement/ déchiffrement** sont généralement confondus avec les termes **cryptage /décryptage.**

- **Chiffrement** : processus de transformation du message M de telle manière à le rendre incompréhensible :
  - ✔ On se base sur une **fonction** de **chiffrement « E »**
  - ✔ On génère ainsi un message chiffré C = E(M)

- **Déchiffrement** : processus de reconstruction du message clair à partir du message chiffré
  - ✔ On se base sur une fonction de **déchiffrement « D »** .
  - ✔ On a donc D(C) = D(E(M)) = M .

La cryptographie et ses applications

Opérations de base

- **Substitution :**

  Remplacement de chaque élément (bit, lettre, groupe de bits ou de lettres) dans le texte clair par un autre élément.

- **Transposition :**

  réarrangement des éléments du texte clair.

- **Opérations algébriques simples :**

  La plupart des systèmes utilisent plusieurs étapes de transposition et de substitution.

La cryptographie et ses applications

Opérations de base

Substituer un caractère ou un groupe de caractères par un autre dans le texte à chiffrer.

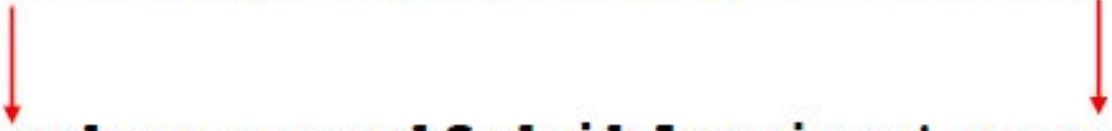
Exemple :

- Mono alphabétique
- Homophonique
- ……..

La cryptographie et ses applications

Exemple1：

plaintext: abcdefghijklmnopqrstuvwxyz



ciphertext: mnbvcxzasdfghjklpoiuytrewq

Plaintext: bob. how are you. alice

ciphertext: nkn. akr moc wky. mgsbc

La cryptographie et ses applications

Exemple 2 :

Table des fréquences d'apparition des lettres pour un texte français :

Lettre	Fréquence %
A	9.42
B	1.02
C	2.64
D	3.39
E	15.87
F	0.95
G	1.04
H	0.77
I	8.41
J	0.89
K	0.00
L	5.34
M	3.24

Lettre	Fréquence %
N	7.15
O	5.14
P	2.86
Q	1.06
R	6.46
S	7.90
T	7.26
U	6.24
V	2.15
W	0.00
X	0.30
Y	0.24
Z	0.32

La cryptographie et ses applications

Lettre	Fréquence	Symboles
A	8,01	09, 12, 33, 47, 53, 67, 78, 92
B	0,88	48
C	3,23	13, 41, 62
D	3,91	01, 03, 45, 79
E	17,52	14, 16, 24, 25, 31, 39, 44, 46, 55, 57, 64, 74, 81, 82, 87, 98
F	1,06	10
G	1,06	6
H	0,88	23
I	7,35	32, 50, 70, 73, 83, 88, 93
J	0,44	15
K	0,05	4
L	5,77	26, 37, 51, 84, 88
M	2,9	22, 27, 56
N	7,22	18, 39, 58, 59, 66, 71, 91
O	5,43	00, 05, 54, 72, 90
P	2,94	07, 38, 95
Q	1,14	94
R	6,69	29, 35, 40, 42, 77, 80
S	8,17	11, 19, 36, 43, 65, 76, 86, 96
T	7,07	17, 20, 30, 49, 69, 75, 97
U	6	08, 52, 60, 61, 63, 99
V	1,41	34
W	0,02	89
X	0,47	28
Y	0,3	2
Z	0,12	21

La cryptographie et ses applications

- Avec le tableau de substitution précédent, le mot **EVENEMENT** pourra être codé **25345558875614 9117**

- Si ce tableau tombait dans des mains ennemies, tous les messages chiffrés devenaient lisibles!

La cryptographie et ses applications

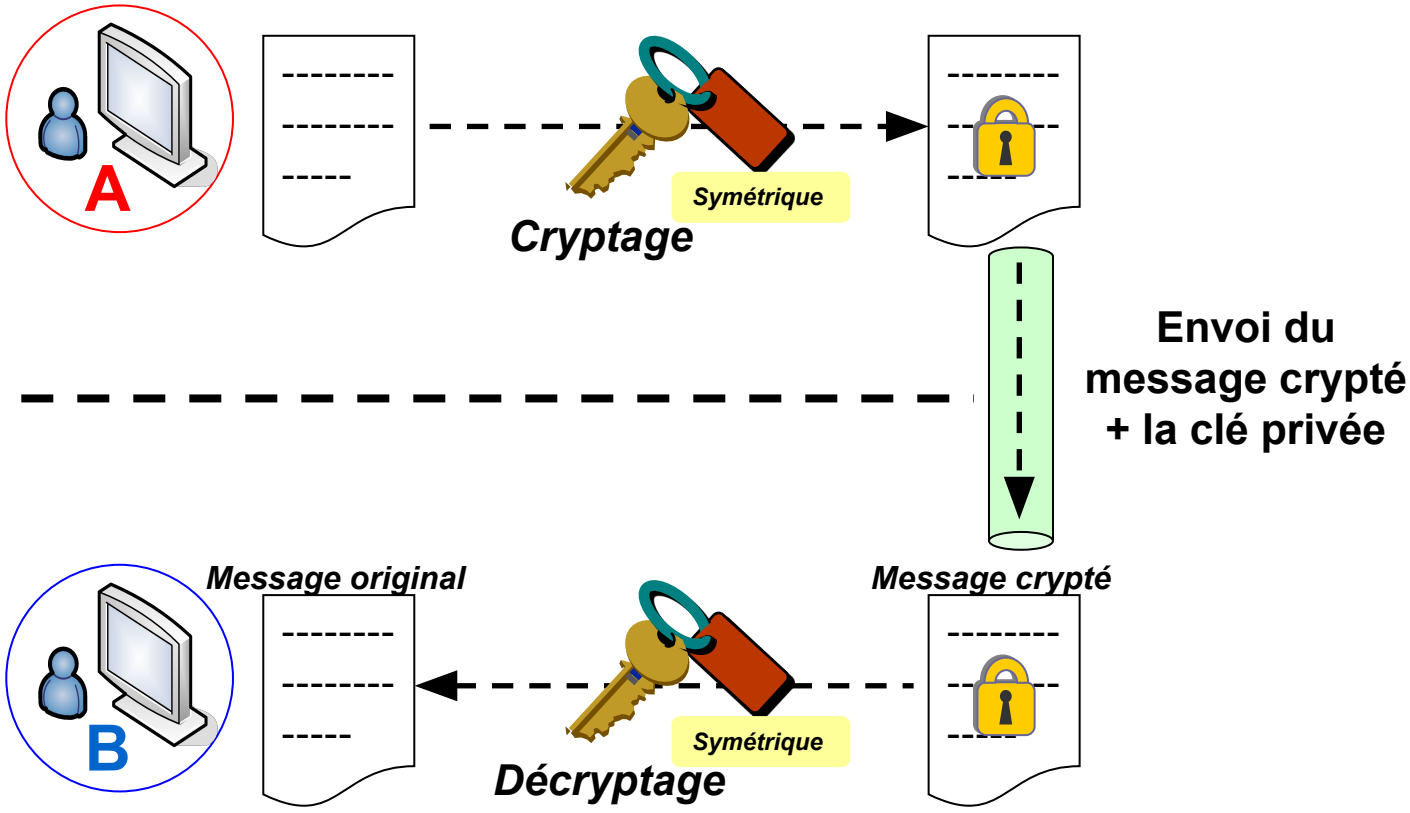
Principales techniques de cryptographie ou de chiffrement de l'information :

- Cryptage par clé symétrique
- Cryptage par clé publique
- Cryptage par clé secrète partagée
- Cryptage par clé de session

La cryptographie et ses applications

Cryptographie à clé symétrique :

- Utilisation de la même clé pour crypter et décrypter



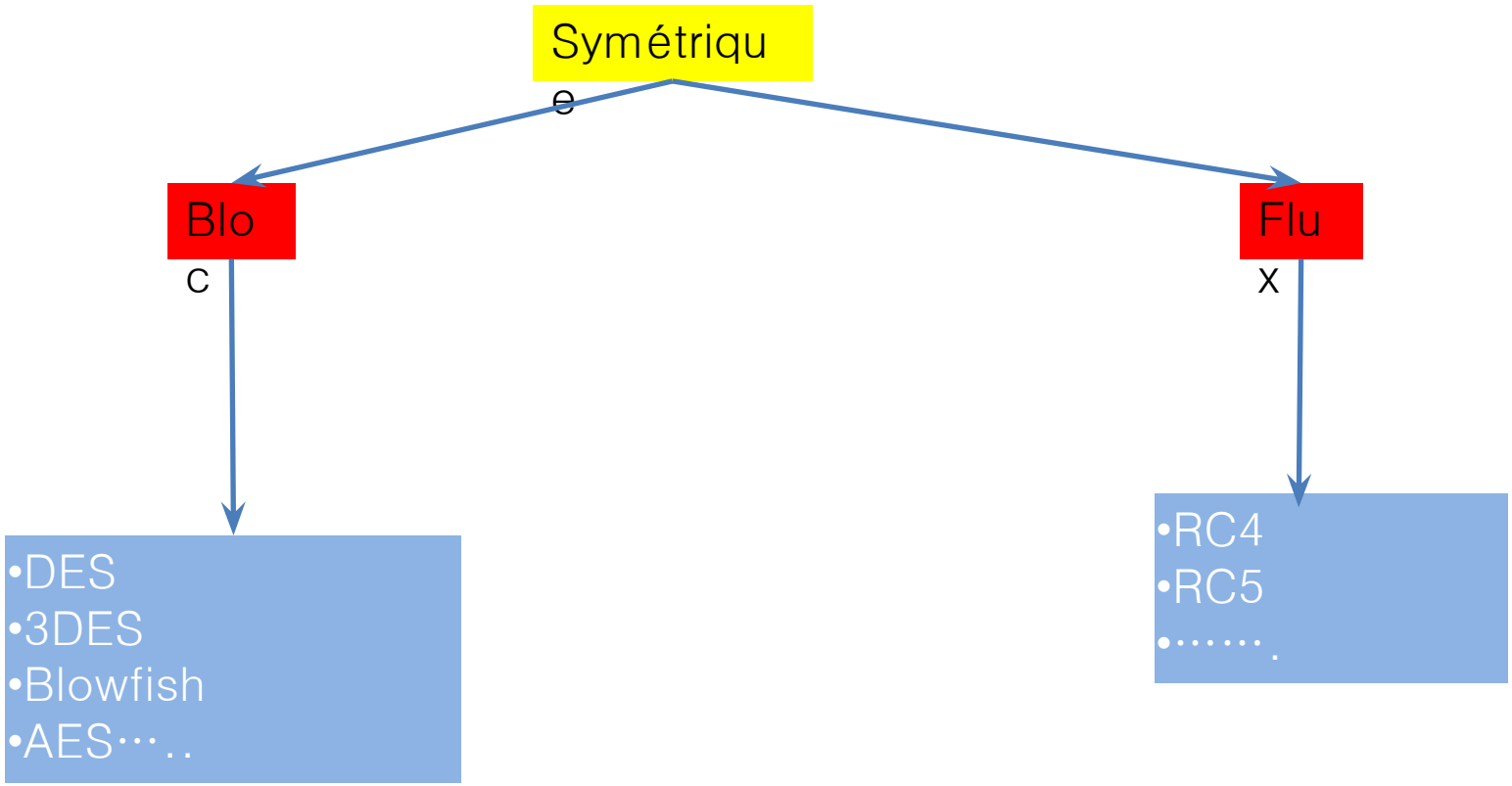
La cryptographie et ses applications

Cryptographie à clé symétrique (ii)

- **Avantage**
  - Mécanisme très rapide
- **Inconvénients**
  - Nécessite la distribution de la clé
  - Si une personne arrive à lire le message et la clé, peut déchiffrer le message
- **Exemples d'algorithmes à clé symétrique**
  - DES (Data Encryption Standard)
  - 3DES (Triple DES)
  - RC2, RC4, RC5
  - AES (Advanced Encription Standard)

La cryptographie et ses applications

- Il y a deux catégories de systèmes à clé privée: les chiffrements **par blocs** et les chiffrements **de flux**.

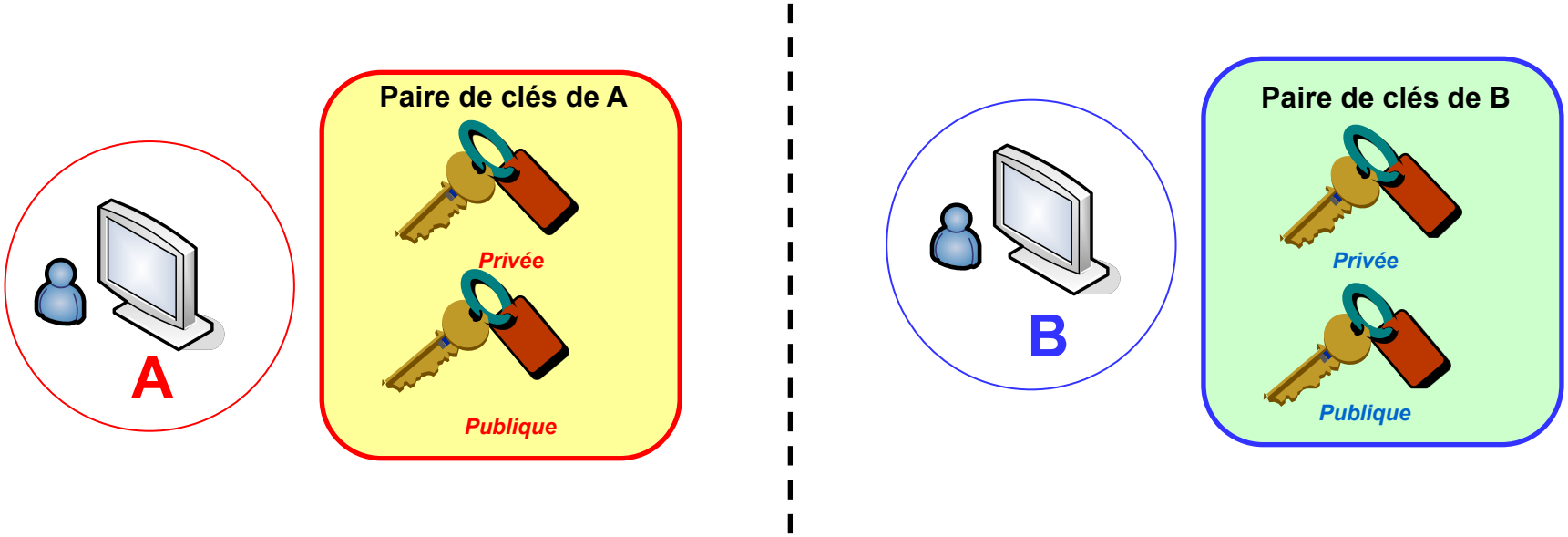


La cryptographie et ses applications

Cryptographie à clé asymétrique ou publique :

Chaque utilisateur du système possède une paire de clés:

- ✔ **Une clé privée**: est connue seulement par son propriétaire
- ✔ **Une clé publique**: est connue par tous les utilisateurs



La cryptographie et ses applications

La paire de clés est **complémentaire :**

- Message chiffré avec la **CLE PRIVEE**

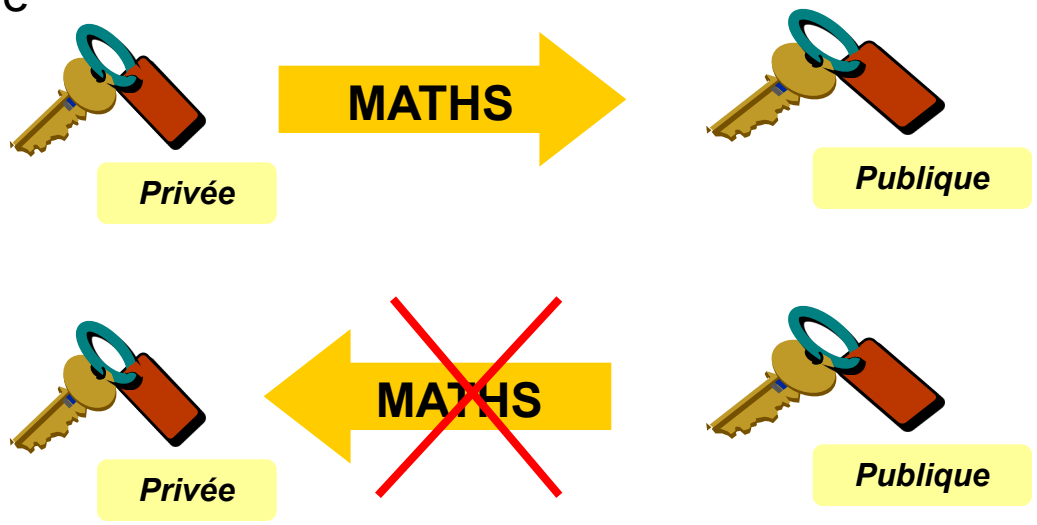
 Seule la clé publique est utilisée pour la déchiffrer

- Message chiffré avec la **CLE PUBLIQUE**

  Seule la clé privé est utilisée pour la déchiffrer

Relation mathématique entre les clés :

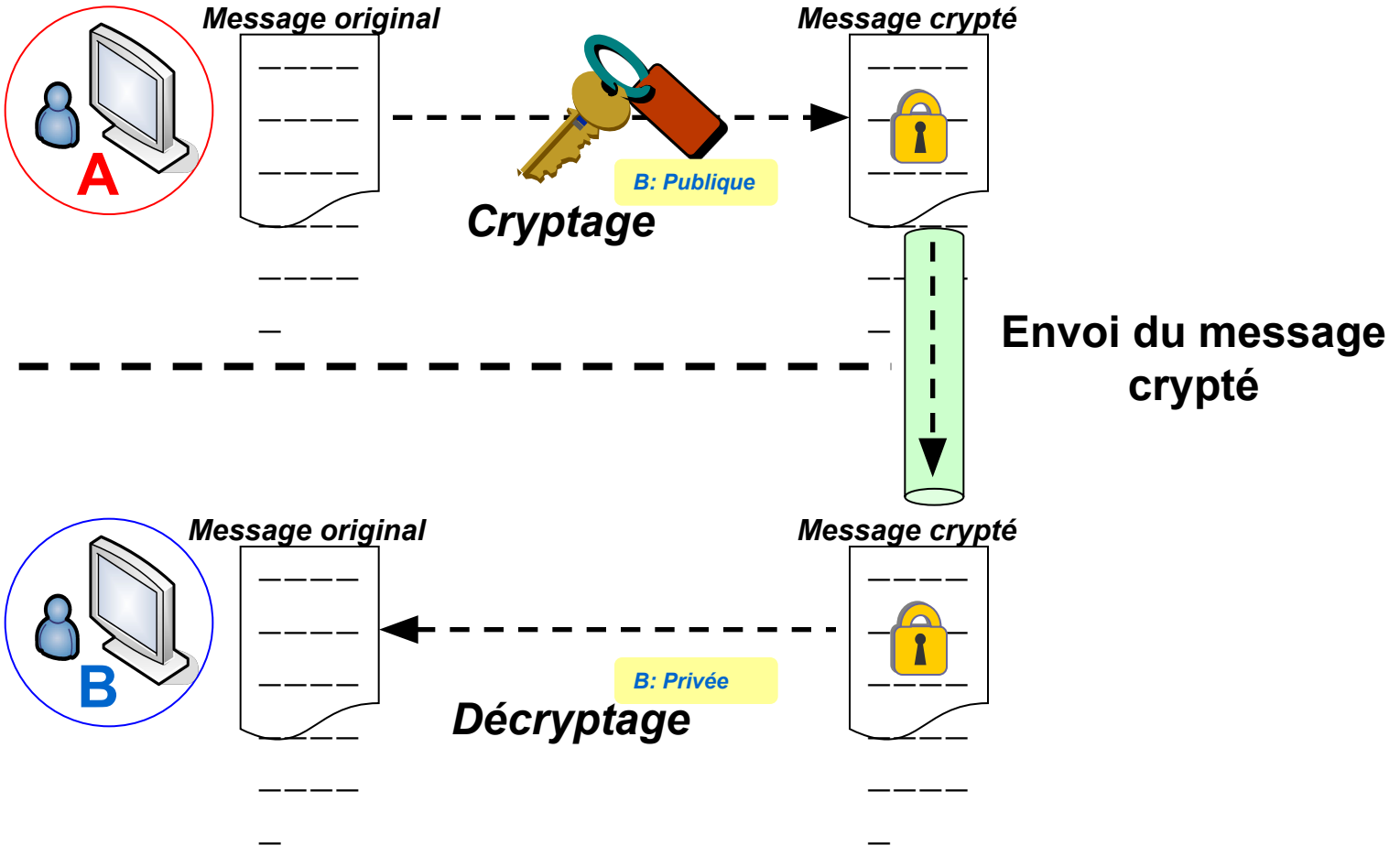
- La clé publique est générée mathématiquement à partir de la clé privé
- Par contre, obtenir la clé privé à partir de la clé publique est mathématiquement et impossible



La cryptographie et ses applications

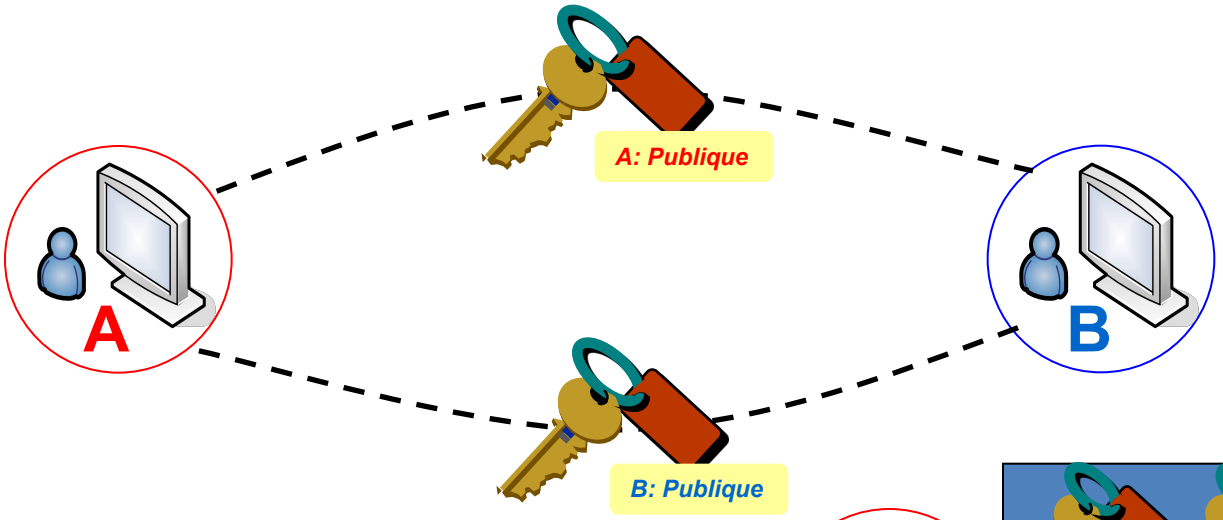
Cryptographie à clé asymétrique ou publique (iii)

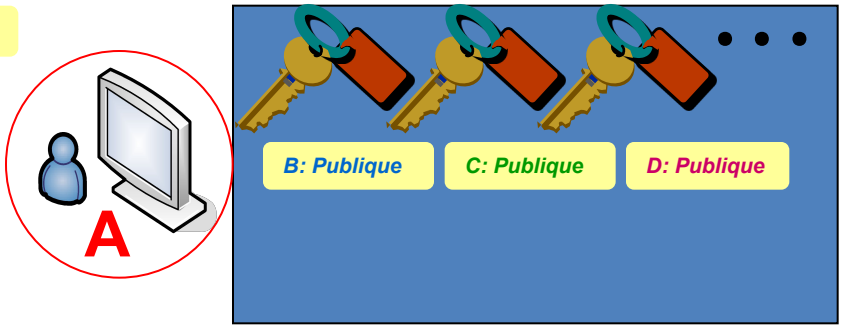
- Fonctionnement



La cryptographie et ses applications

Nécessité d'inter changer les clés publiques





- Collection des clés publiques des autres utilisateurs

La cryptographie et ses applications

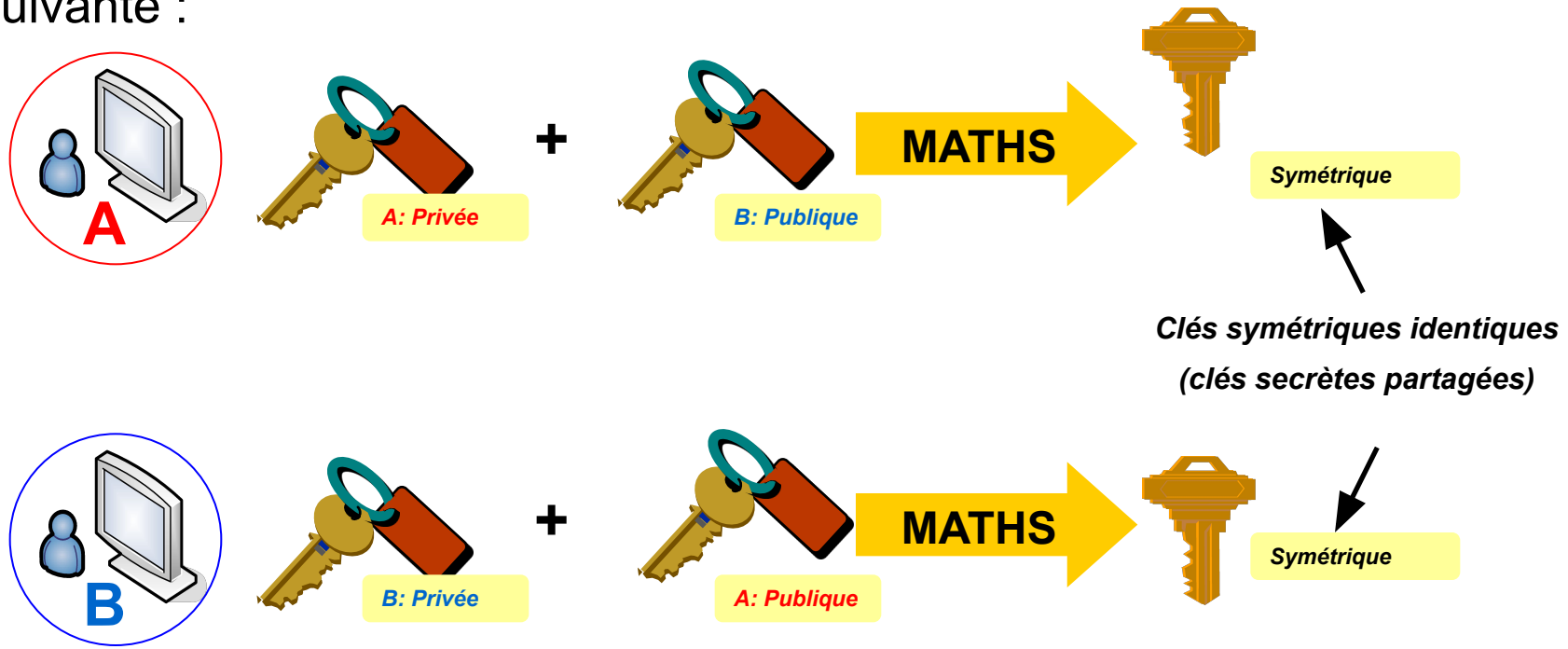
Cryptographie à clé asymétrique ou publique(V)

- **Avantage**
  - Plus sécurisée
- **Inconvénients**
  - Processus de chiffrement lent
  - Peu recommandée pour les messages très longs
- **Solution :** combiner le mécanisme à clé symétrique avec le mécanisme à clé asymétrique
- **Exemples d'algorithmes à clé asymétrique**
  - RSA (Rivest, Shamir y Adleman)

La cryptographie et ses applications

Cryptographie à clé secrète partagée (i)

- Basée sur la clé symétrique
  - La clé privée ne s'inter change pas
  - Elle est générée par chacun des utilisateurs d'extrémité de la manière suivante :



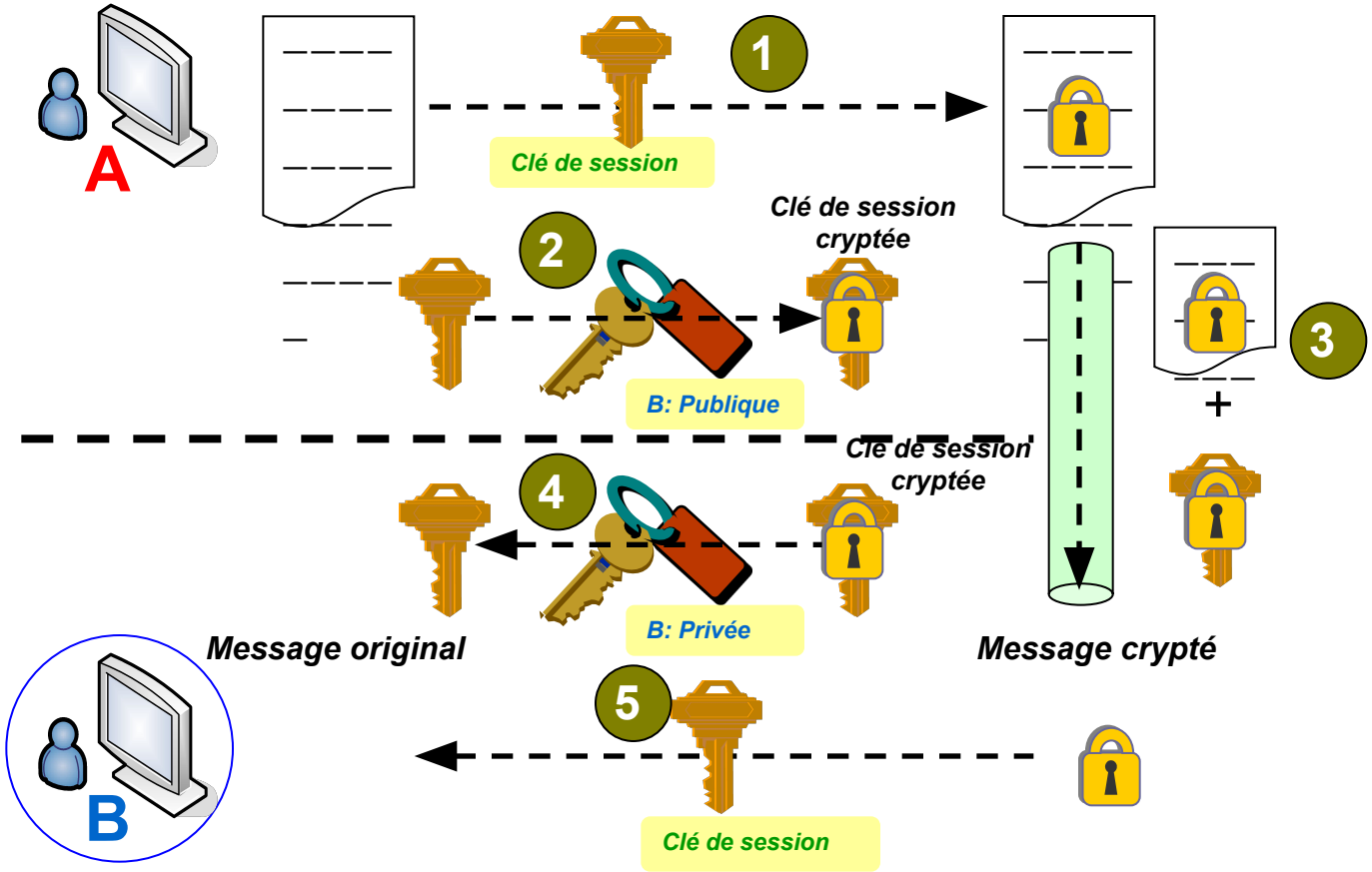
La cryptographie et ses applications

Cryptographie à clé secrète partagée (ii)

- **Avantage**
  - Rapide
  - Sécurisée : pas de clés inter changées
- **Inconvénients**
  - Utilisation de la même clé (toujours)
    - risque de reconnaître cette clé
- **Exemples d'algorithmes**
  - Diffie-Hellman

La cryptographie et ses applications

Cryptographie par clé de session (i)



La cryptographie et ses applications

Cryptographie par clé de session (ii)

- **Avantages**
  - Rapide
  - Sécurisée :
    - La clé de session est envoyée cryptée
    - Pour chaque transmission, on utilise une clé de session distincte
- **Exemples d'algorithmes**
  - SSL (*Secure Socket Layer*) : utilisé dans les serveurs Web sécurisés (https) ou dans les applications de e-commerce.

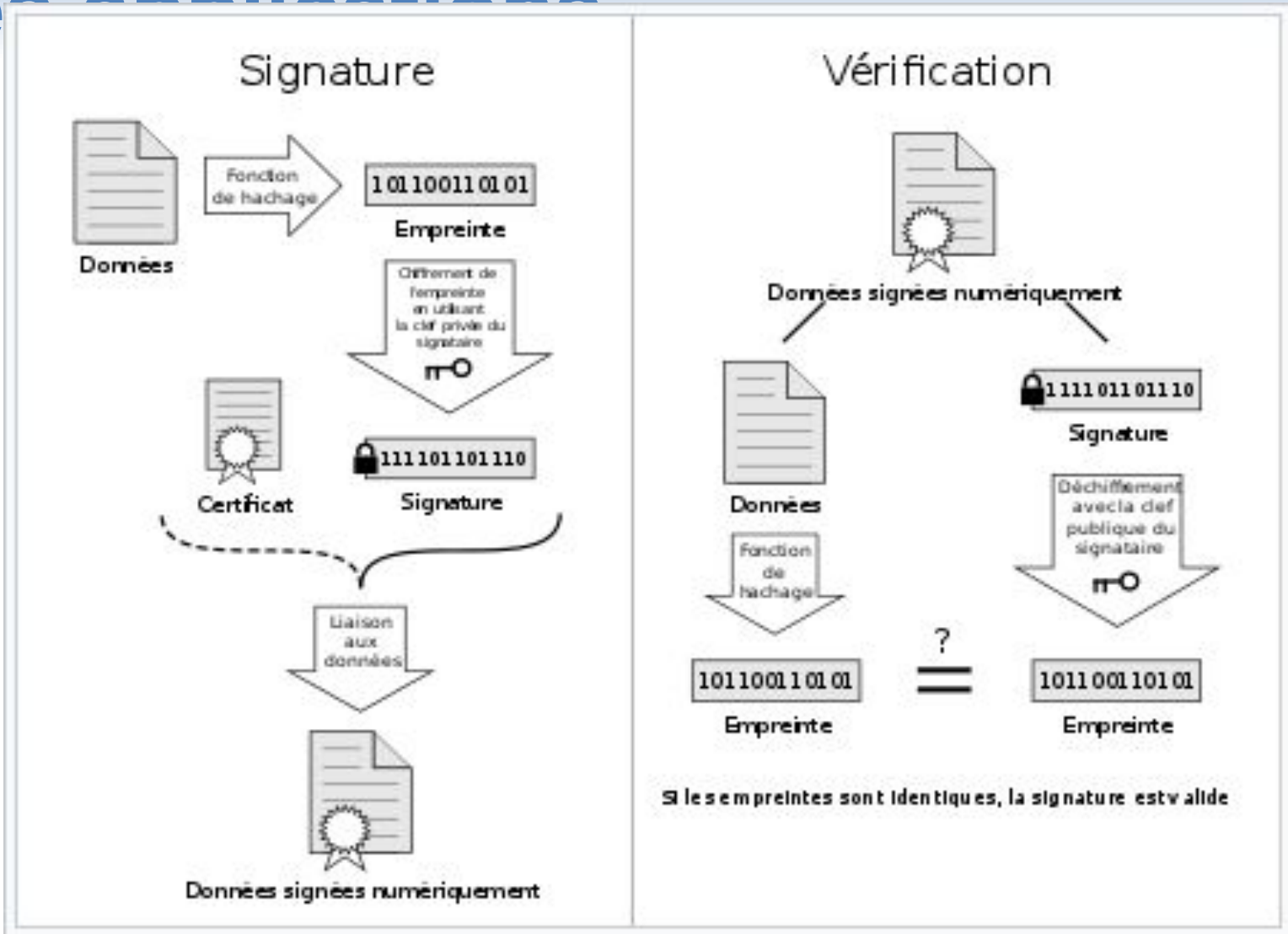
La cryptographie et ses applications

Fonction de hachage et **Signature digitale :**

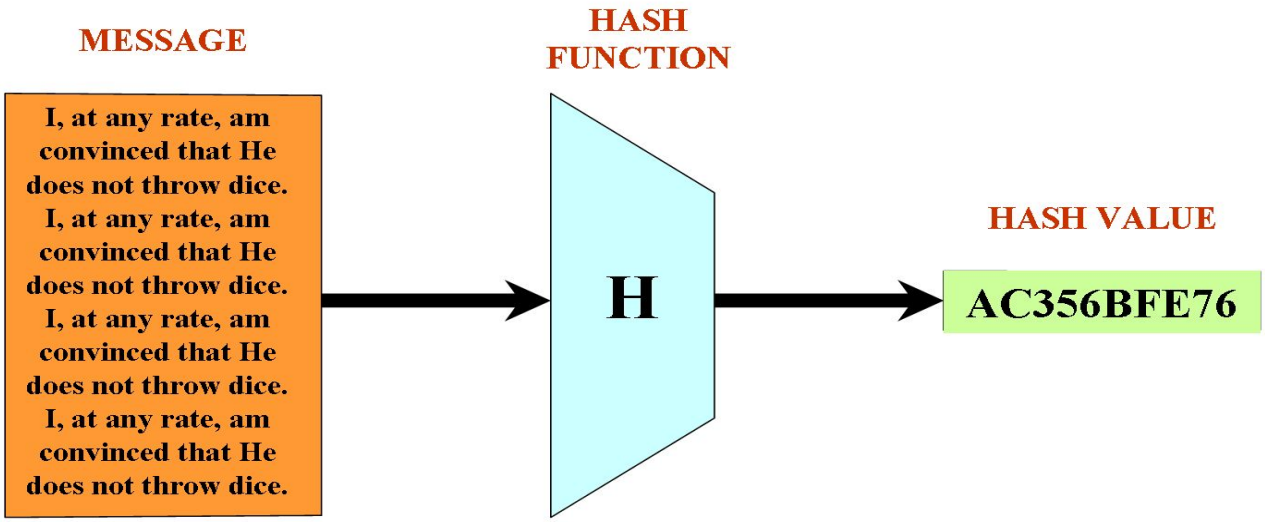
A quoi ça sert une signature digitale ?

- Permet au récepteur de vérifier l'identité de l'expéditeur
  - l'authentification
- Permet au récepteur de vérifier que l'information n'a pas été modifiée pendant son acheminement
  - l'intégrité
- La signature est générée à partir de:
  - **La clé privée de l'expéditeur**
    - L'expéditeur doit disposer d'une paire de clés privée et publique
    - La clé privée est employée pour générer la signature digitale
    - Ceci garantit *l'authentification*
  - **Le message original**
    - Au message original, s'applique une fonction de hachage (hash)
    - Le message haché est crypté avec la clé privée formant la signature digitale de l'expéditeur
    - Ceci garantit *l'intégrité*

La cryptographie et ses applications



La cryptographie et ses applications



Conditions de base d'une fonction de hachage :

1. L'entrée peut être de dimension variable.
2. La sortie doit être fixe.
3. H(m) doit être relativement facile à calculer.
4. H(m) doit être une **fonction à sens unique**.
5. H(m) doit être **sans collision**.

La cryptographie et ses applications

Exemples : Algorithmes de hachage

- MD5 (Message Digest 5).
- SHA1 (Secure Hash Algorithm 1)
- SHA 256
- Tiger
- Whirlpool

La cryptographie et ses applications

Préparation du message signé

Un Emetteur (A) prépare le message signé, pour cela :

Il produit un résultat de hachage du message par la fonction de hachage choisie **H(M)** ;
Il chiffre ce résultat grâce à la fonction de chiffrement **C** en utilisant sa clé privée K_{pr}. Le résultat obtenu est la signature du message : $S_M = C(K_{pr}, H(M))$
Il prépare le message signé en plaçant le message en clair **M** et la signature S_M dans un conteneur quelconque : $M_{signé}=(S_M, M)$.

(A) transmet $M_{signé}$, le message signé, à (B) par un canal non sécurisé

La cryptographie et ses applications

Réception du message signé

(B) réceptionne le message signé, pour vérifier l'authenticité du message :
il produit un résultat de hachage du texte clair en utilisant la fonction de hachage : $H(M)$;
il déchiffre la signature en utilisant la fonction de déchiffrement D avec la clé publique K_{pb} soit : $D_{Sm}=D(K_{pb},S_M)$;
il compare D_{Sm} avec $H(M)$.
Dans le cas où la signature est authentique, D_{Sm} et $H(M)$ sont égaux car, de par les propriétés du chiffrement asymétrique : $D_{Sm}=D(K_{pb},S_M)=D(K_{pb},C(K_{pr},H(M)))=H(M)$. Le message est alors authentifié.

La cryptographie et ses applications

Buts de la cryptographie

- Confidentialité des informations stockées/manipulées
- Intégrité des informations stockées/manipulées
- Authentification d'utilisateurs/de ressources
- Non-répudiation des informations

Sécurité du périmètre « Firewall »

Sécurité du périmètre Firewall

Introduction

Un système parefeu (firewall) est un dispositif conçu pour examiner et éventuellement bloquer les échanges de données entre réseaux.

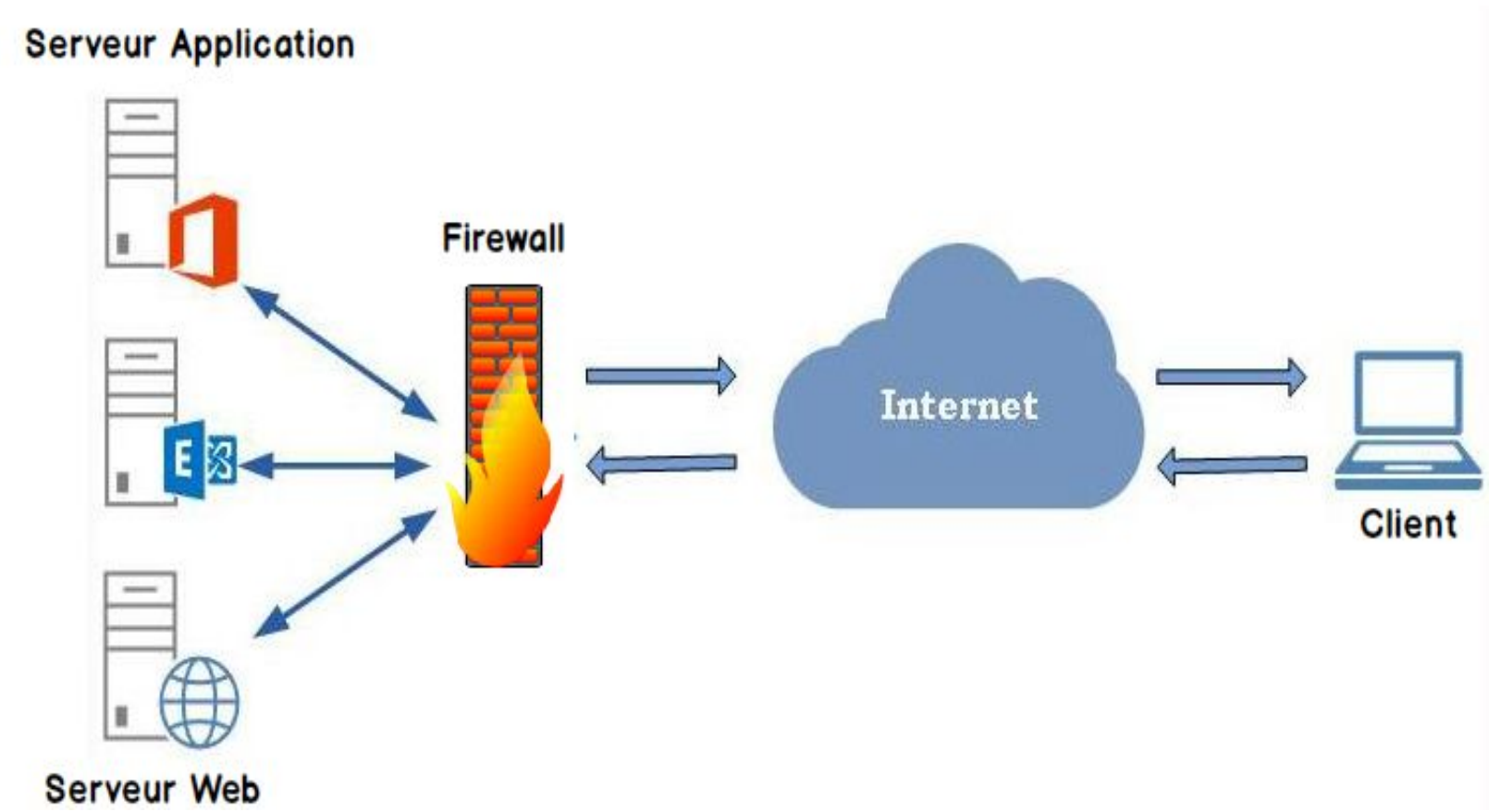
C'est donc un élément de sécurité d'un réseau qui peut être :

- un ordinateur
- un routeur
- un matériel propriétaire

Dans tous les cas, un système parefeu est une combinaison d'éléments matériels et logiciels

Sécurité du périmètre Firewall

Un système parefeu :



Sécurité du périmètre Firewall

Principe

Le parefeu
joue le rôle de filtre et peut donc intervenir à plusieurs niveaux du modèle OSI.
Il existe trois types de principaux de parefeu :

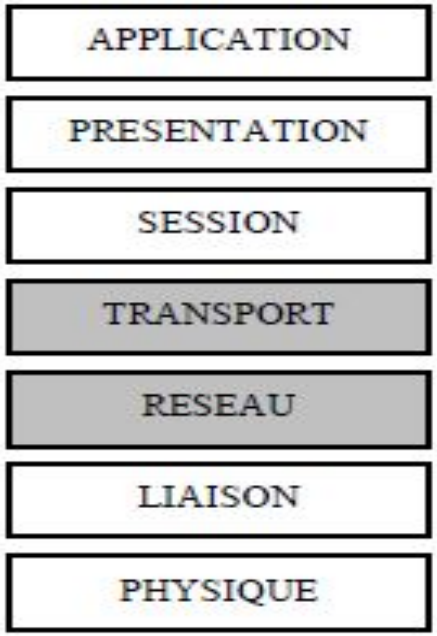
- filtrage de paquets
- filtrage de paquets avec état (firewall stateful)
- proxy

Sécurité du périmètre Firewall

Filtrage de paquets

Les pare-feu de filtrage de paquets 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 protocole
- ☐ le numéro de port

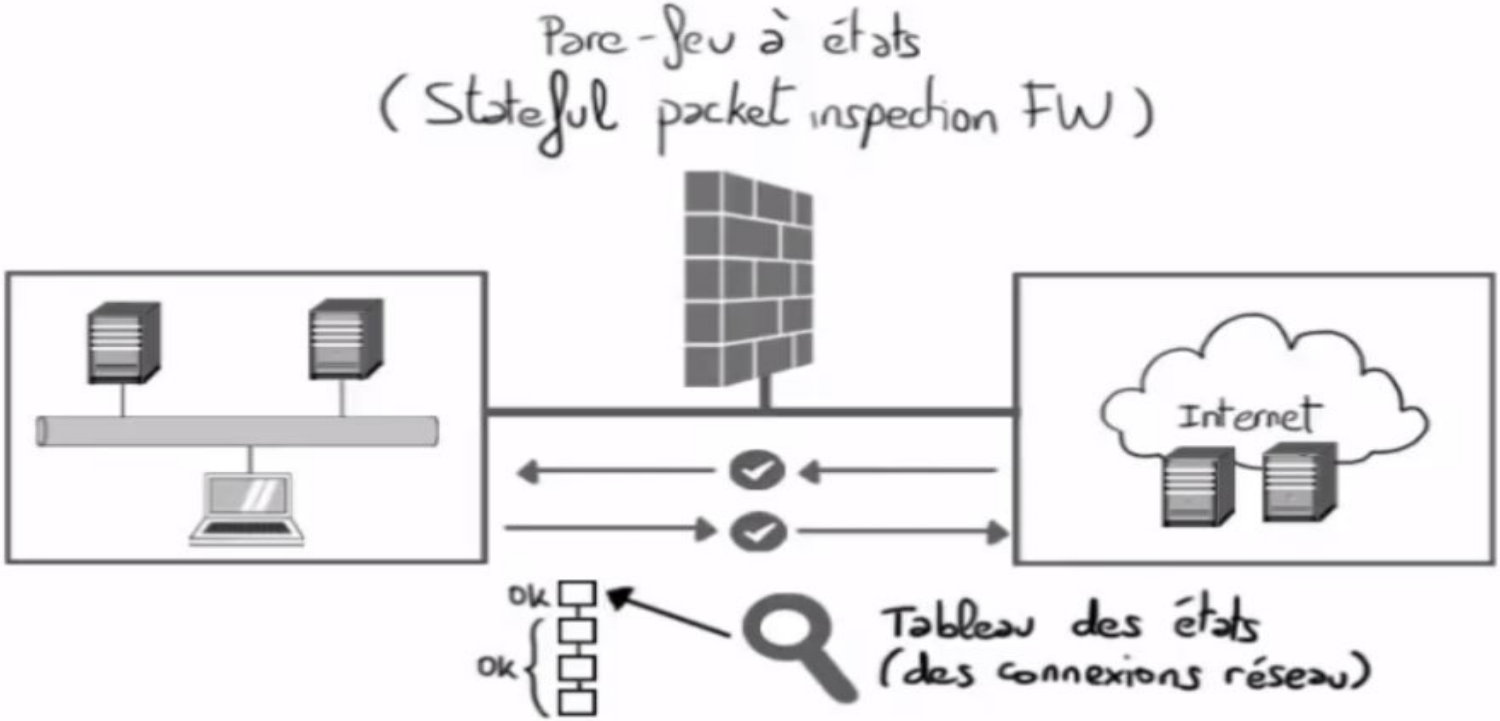


Sécurité du périmètre Firewall

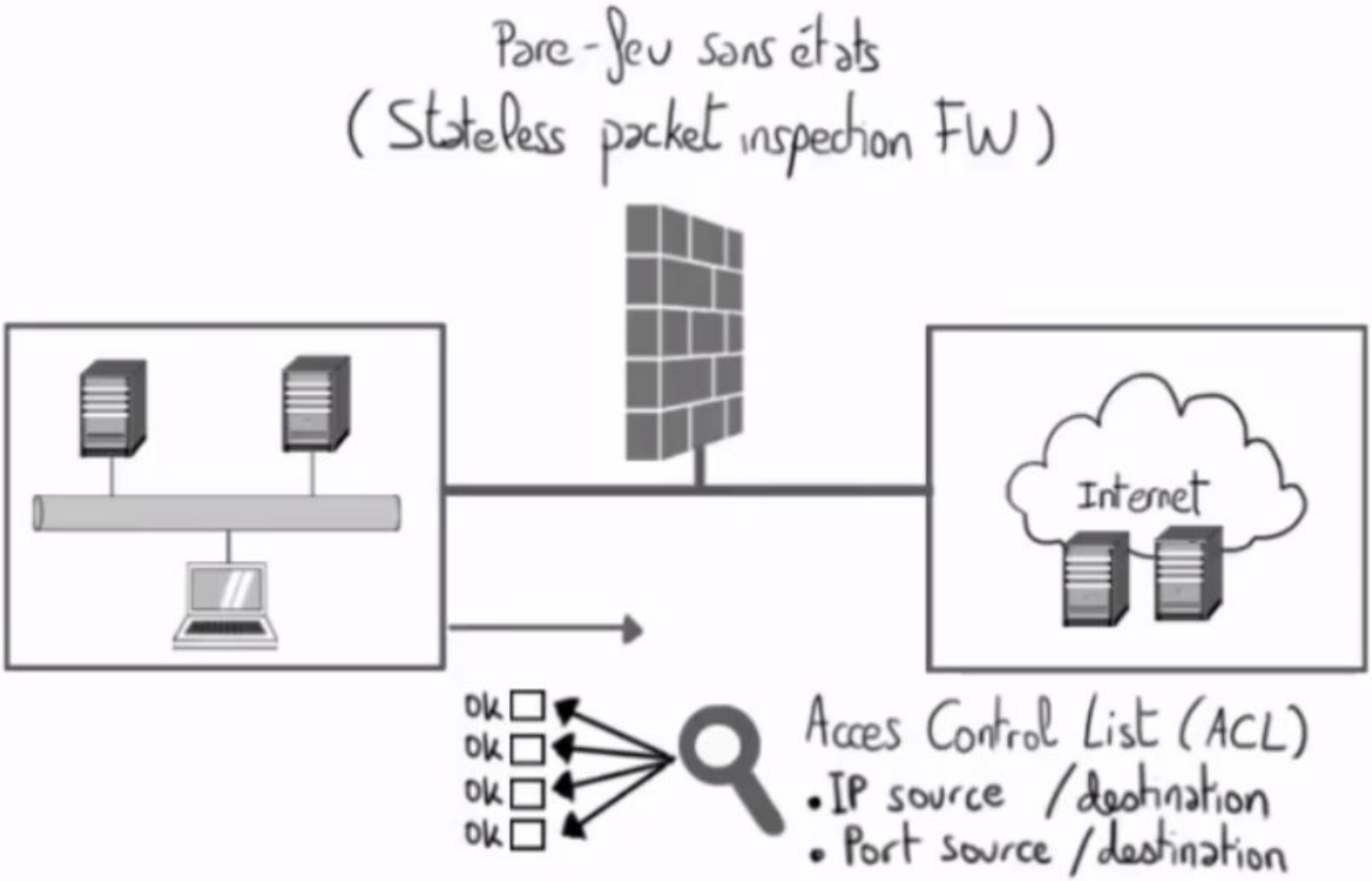
Filtrage de paquets avec état (firewall stateful) :

L'amélioration par rapport au filtrage simple, est la conservation de la trace des sessions et des connexions dans des tables d'états internes au Firewall. Le Firewall prend alors ses décisions en fonction des états de connexions,

et peut réagir dans le cas de situations protocolaires anormales



Sécurité du périmètre Firewall



Sécurité du périmètre Firewall

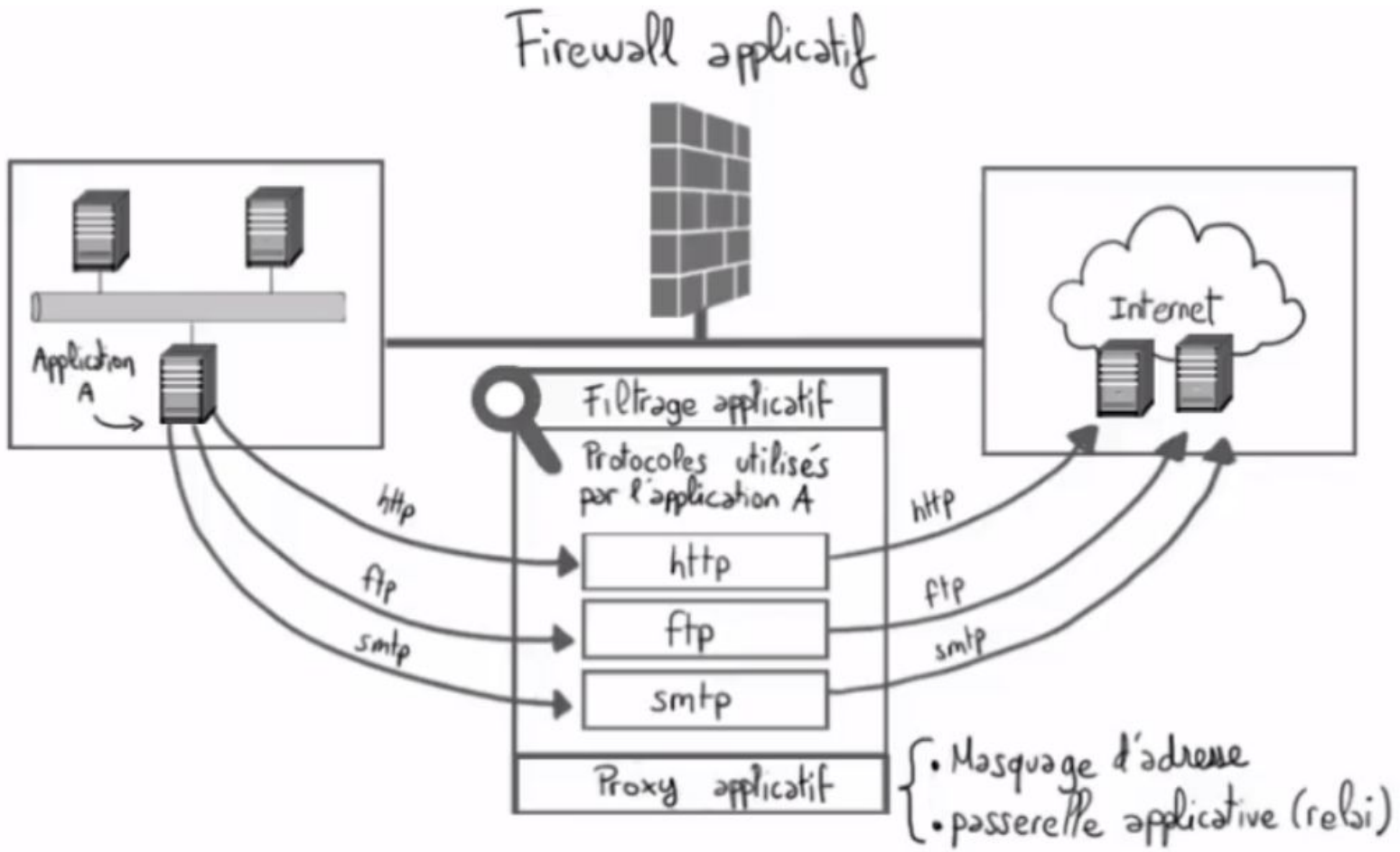
Proxy :

Le filtrage applicatif est comme son nom l'indique réalisé au niveau de la couche Application. Pour cela, il faut bien sûr pouvoir extraire les données du protocole de niveau 7 pour les étudier. Les requêtes sont traitées par des processus dédiés,
par exemple une requête de type Http sera filtrée par un processus proxy Http.

Le pare-feu rejettera toutes les requêtes qui ne sont pas conformes aux spécifications du protocole. Cela implique que le pare-feu proxy connaisse
toutes les règles protocolaires des protocoles qu'il doit filtrer.

Sécurité du périmètre Firewall

Proxy :



Sécurité du périmètre Firewall

Architecture réseau

Réseaux externes

C'est le réseau généralement le plus ouvert. L'entreprise n'a pas ou très peu de contrôle sur les informations, les systèmes et les équipements qui se trouvent dans ce domaine.

Réseaux internes

Les éléments de ce réseau doivent être sérieusement protégés. C'est souvent dans cette zone que l'on trouve les mesures de sécurité les plus restrictives et c'est
donc le réseau le moins ouvert.

Réseaux intermédiaires

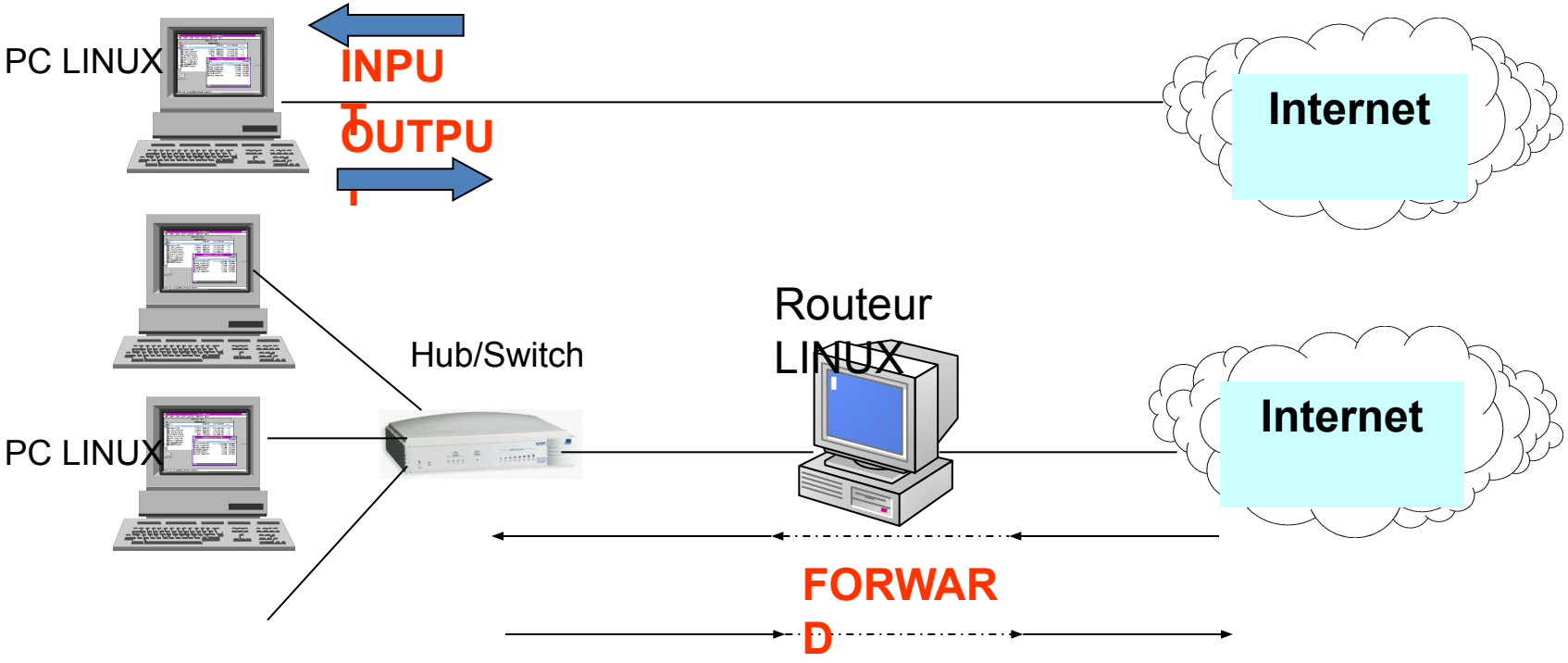
Ce réseau est composé de services fournis aux réseaux internes et externes. Les services publiquement accessibles (serveurs de messagerie, Web, FTP et DNS le plus souvent) sont destinés aux utilisateurs internes et aux utilisateurs par Internet. Cette zone, appelée réseau de service ou de zone démilitarisée (DMZ
DeMilitarizedZone), est considérée comme la zone moins protégée de tout le réseau.

Sécurité du périmètre Firewall

Firewalls personnels: IPtables de Linux

Règles de filtrage

INPUT, OUTPUT, FORWARD



Sécurité du périmètre Firewall

Firewalls personnels: IPtables de Linux

Principaux critères de filtrage

Option / exemple	signification
-A INPUT -A OUTPUT -A FORWARD	**Ajouter une règle à la chaîne d'entrée** **Ajouter une règle à la chaîne de sortie** **Ajouter une règle à la chaîne FORWARD (cas d'un routeur)**
-s 192.168.1.1 -d 140.10.15.1	**Filtrage pour @ip origine** **Filtrage pour @ip destination**
-p tcp -p udp -p icmp	**Filtrage d'un paquet TCP** **Filtrage d'un paquet UDP** **Filtrage d'un paquet ICMP**

Sécurité du périmètre Firewall

Principaux critères de filtrage

Option / exemple	signification
-sport 3000 -dport 80 -icmp 8	Filtrage pour N° port origine (pour TCP/UDP) Filtrage pour N° port destinat. (pour TCP/UDP) Filtrage de code d'un paquet ICMP (pour ICMP)
-i eth0 -o eth1	Filtrage pour interface réseau d'entrée Filtrage pour interface réseau de sortie

Sécurité du périmètre Firewall

Filtrage pour l'état de connexion

Option	signification
-m state --state NEW	Filtrages de paquets correspondant aux nouvelles connexions (le premier paquet vu dans une connexion)
-m state --state ESTABLISHED	Filtrages de paquets correspondant aux connexions déjà établies
-m state --state RELATED	Filtrages de paquets en rapport avec d'autres connexions existantes (ex: connexion de données FTP, ou paquets ICMP)
-m state --state INVALID	Filtrages de paquets n'appartenant à aucun des états précédents

Sécurité du périmètre Firewall

Actions

Option / exemple	signification
-j ACCEPT	Le paquet est accepté
-j DROP	Le paquet est rejeté

Sécurité du périmètre Firewall

Exemple:

1. Iptables –A INPUT –i eth0 –s 192.168.10.0 –p icmp –j Accept
2. Iptables –A OUTPUT –o eth1 –s 192.168.10.0 –p icmp –j Accept
3. Iptables –A FORWARD –m state —state ESTABLISHED, RELATED –j Accept