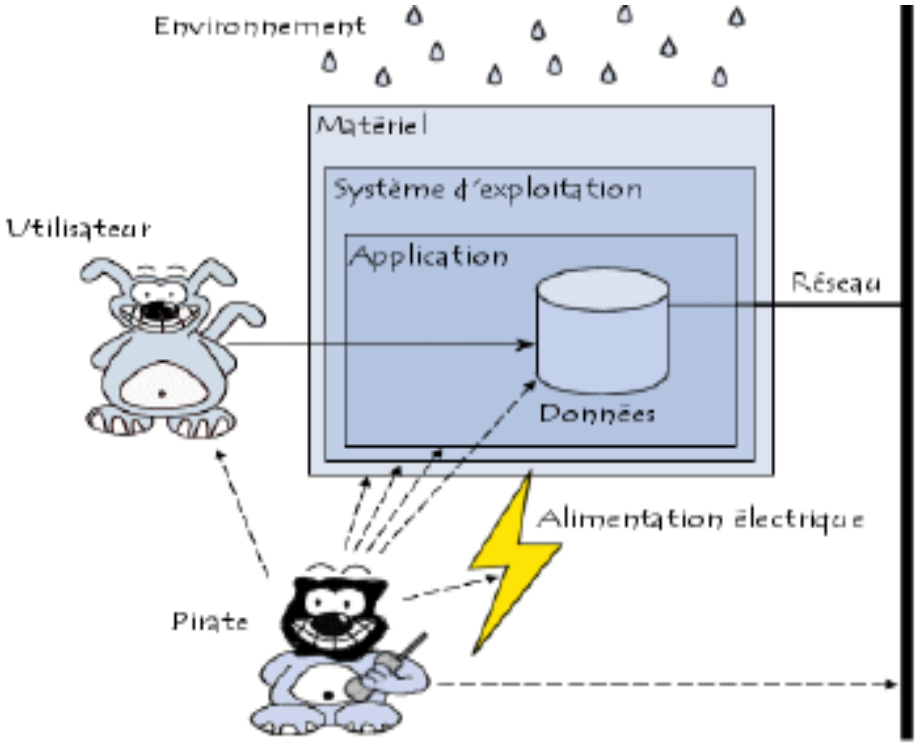
CONTRE-MESURES

Introduction

- Les systèmes informatiques mettent en œuvre différentes composantes, allant de l'électricité pour alimenter les machines au logiciel exécuté via le système d'exploitation et utilisant le réseau.

- Les attaques peuvent intervenir à chaque maillon de cette chaîne, pour peu qu'il existe une vulnérabilité exploitable. Le schéma ci-contre rappelle très sommairement les différents niveaux pour lesquels un risque en matière de sécurité existe :



Sécurité des utilisateurs

Gestion et contrôle des accès aux systèmes et aux informations

- **Objectif :** Veiller à ce que seules les personnes autorisées ont accès au système, et que la responsabilité individuelle est assurée.
- **Méthodes:**
  - attribution des identifiants/mots de passes, code PIN ou biométrie
  - Attribution des droits d'accès

Responsabilité liée à la sécurité des informations personnelles

- **Objectif :** Rendre les utilisateurs responsables de la protection de leurs informations d'authentification.
- **Utilisation d'informations secrètes d'authentification:**
- Pour préserver la confidentialité de l'authentification secrète :
- 1) Il est interdit de conserver les informations secrètes d'authentification (mot de passe, code PIN,… sur support papier, fichier électronique…) ;
- 2) Il est impératif de changer les informations secrètes d'authentification périodiquement et à chaque fois qu'il y a suspicion de compromission ;

Responsabilité liée à la sécurité des informations personnelles

3) L'organisme doit établir une politique de définition des mots de passe respectant notamment les mesures suivantes :

- a) la taille du mot de passe doit être supérieure à huit (08) caractères
- b) le mot de passe doit être composé de caractères alphanumériques (minuscules et majuscules) et de caractères spéciaux ;
- c) le mot de passe ne doit pas être facile à deviner (noms, prénoms, numéros de téléphone, dates d'anniversaire,….) ;
- d) ne pas utiliser des mots usuels (azerty, qwerty…) ;
- e) doivent être changés à la première connexion s'ils sont fournis par autrui.

- 4) Ne pas partager les informations secrètes d'authentification ;
- 5) Ne pas utiliser les mêmes informations secrètes d'authentification sur plusieurs comptes.

Formation et sensibilisation

Objectif : sensibiliser les utilisateurs aux risques liés à l'usage des TIC et améliorer leurs compétences.

- Sensibiliser les employés sur la sécurité informatique, notamment le risque lié au téléchargement et l'installation de logiciels non autorisés et les menaces liées au social engineering;
- Sensibiliser les utilisateurs sur les sanctions prévues en cas de tentative d'accès non autorisé ;
- Sensibiliser les utilisateurs sur les actions qui peuvent mettre en péril la sécurité ou le bon fonctionnement des ressources qu'ils utilisent.
- …

Sécurité physique

Sécurité physique

Objectif : empêcher tout accès physique non autorisé, tout dommage ou intrusion portant sur l'information et les moyens de traitement de l'information de l'organisme.

- **Contrôles physiques des accès**
- **Sécurisation des bureaux, des salles et des équipements (**Choisir un emplacement non accessible au public pour les équipements-clés**)**
- empêcher la perte, l'endommagement, le vol ou la compromission des actifs et l'interruption des activités de l'organisme.

Sécurisation des réseaux

SÉCURISATION DES RÉSEAUX

- **Objectif :** mettre en œuvre une architecture sécurisée afin de protéger le réseau des accès non autorisés.
- **méthodes:**
- **Configuration des équipements réseaux:**
  - Tous les mécanismes de protection du périmètre réseau notamment les routeurs et les pare-feu, et tous les équipements de connectivité tel que les commutateurs, points d'accès sans fil, etc. doivent être reconfigurés et personnalisés lors de leur installation
  - Les comptes par défaut doivent êtres désactivés ou renommés, et leurs mots de passe changés avant toute mise en service ;
  - …

Sécurisation des réseaux

- **Segmentation du réseau**
- Le réseau interne de l'organisme doit être séparé en zones pour protéger les serveurs des utilisateurs réseau ;

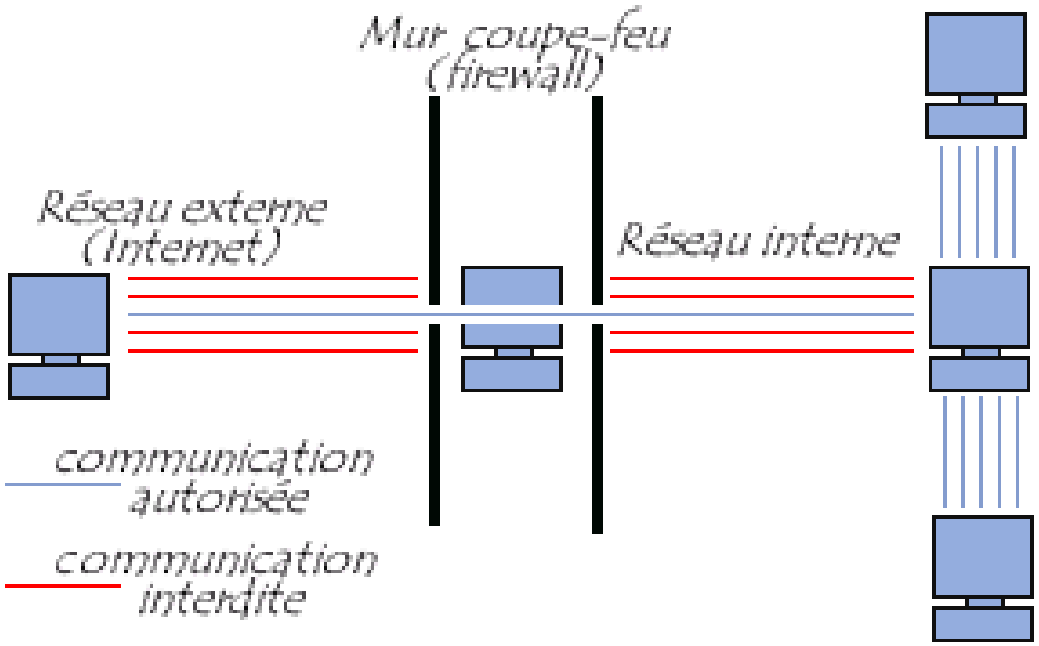
SÉCURISATION DES RÉSEAUX

- A titre d'exemple, la classification des zones réseaux peut être établie comme suit :

Zone	Contenu
Zone sécurisée	- Services base de données, - Services applicatifs, - Serveurs et stations contenant des données confidentielles,
Zone démilitarisé (DMZ)	- Interface utilisateur / Web,
Zone spécifique	- Développement, - Equipement de protection physique (onduleurs, caméras, etc.)
Zone utilisateur	- Les postes utilisateurs

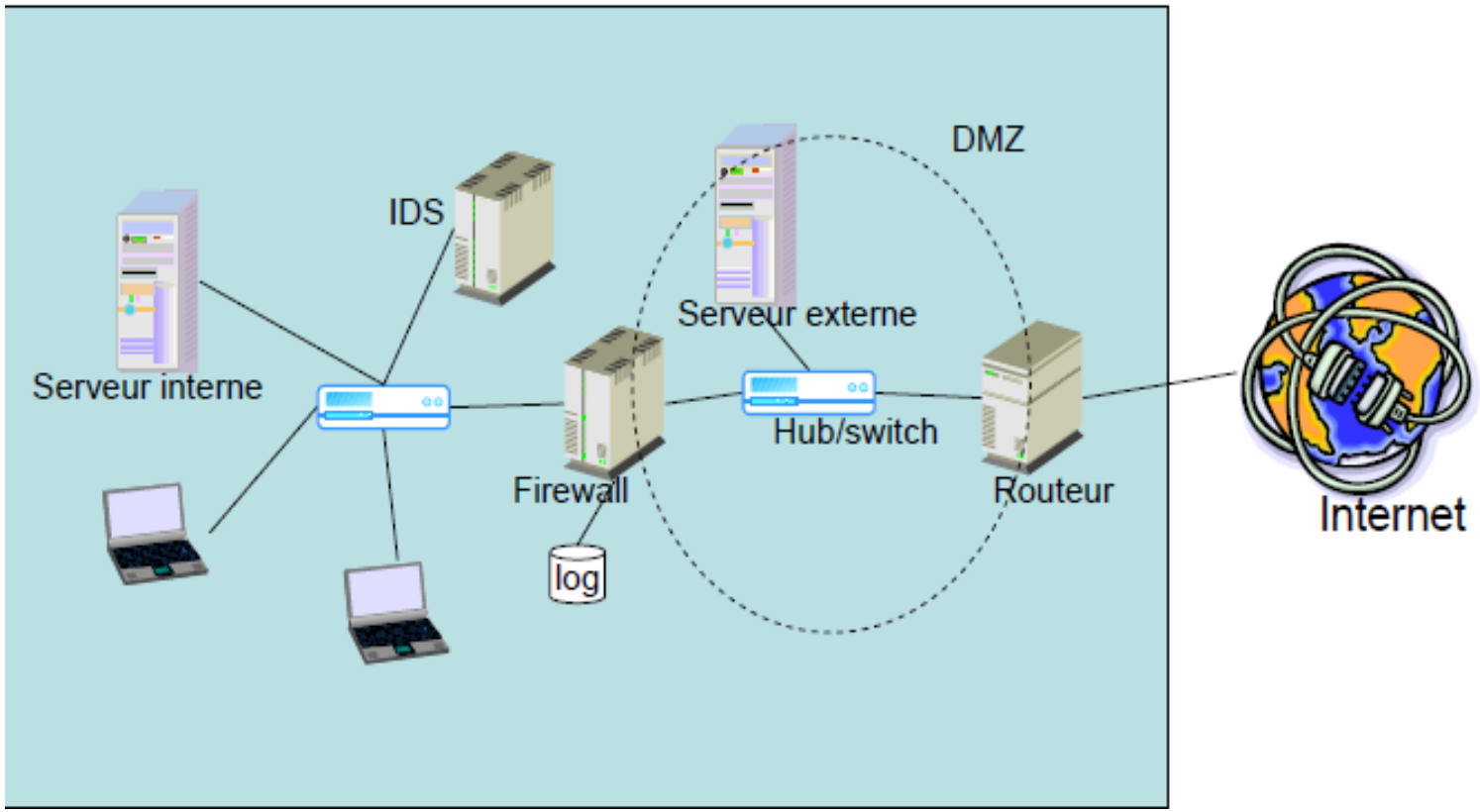
SÉCURISATION DES RÉSEAUX

- **Utilisation des pare-feux:** Le réseau doit être configuré pour surveiller et contrôler les communications aux limites externes du réseau, et à des points internes stratégiques ;



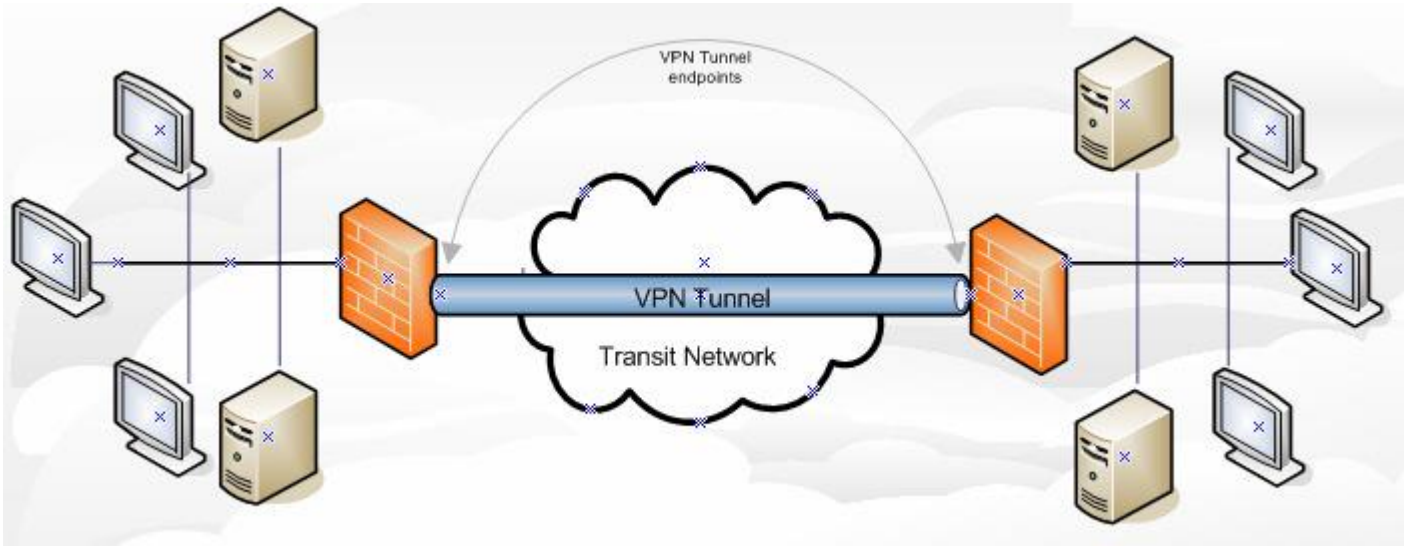
Sécurisation des réseaux

- **Utilisation des Systèmes de Détection et de Prévention d'Intrusion IDS/IPS:**



SÉCURISATION DES RÉSEAUX

- **Utilisation des VPN:** Un VPN (*Virtual Private Network*) est un tunnel (nous pouvons aussi parler de liaison virtuelle) sécurisé permettant la communication entre deux entités y compris au travers de réseaux peu sûrs comme peut l'être le réseau Internet



Se protéger de la perte de données

- La perte de données peut être provoquée par un virus, un effacement intentionnel de la part d'un autre utilisateur, un écrasement ou effacement accidentel de la part de l'utilisateur lui-même ou bien une panne matérielle (par exemple : une panne de disque dur).

- Contre-mesure: assurer des sauvegardes régulières

Confidentialité et intégrité des données

- **Confidentialité:** les données doivent être communiquées via un réseau de communication ou stockées sur un support de stockage chiffrées
  - ***Utilisation d'un mécanisme de chiffrement (symétrique ou asymétrique)***

- **Intégrité:** les données doivent être couplé avec une empreinte générée à partir des données elles-mêmes en utilisant les fonctions de hachage

Sécurité des systèmes et logiciels

- **Acquisition et l'installation des logiciels:**
- **Objectif** : Limiter les risques liés à la sécurité des systèmes d'information lors de l'acquisition des solutions et leur implémentation.
  - Il doit être strictement interdit d'acquérir et/ou utiliser des logiciels piratés. Tout logiciel ou système acquis doit disposer d'une License officielle.

Sécurité des systèmes et logiciels

- **Inspection et contrôle du code source des logiciels**
  - **Objectif :** protéger les systèmes contre toute tentative de détournement ou d'utilisation illicite.
    - Lorsqu'ils sont disponibles, les codes sources des applications critiques acquises ou développées doivent être inspectés.

- **Maintenance et mise à jour des logiciels**
- **Objectif :** Protéger les systèmes d'information des nouvelles vulnérabilités découvertes

La Cryptographie au Service de La Sécurité Informatique

Rappel Sur les Services de Sécurité et Mise en Œuvre

- Principaux Services de Sécurité

D	C	I	P
Disponibilité	Confidentialité	Intégrité	Preuve

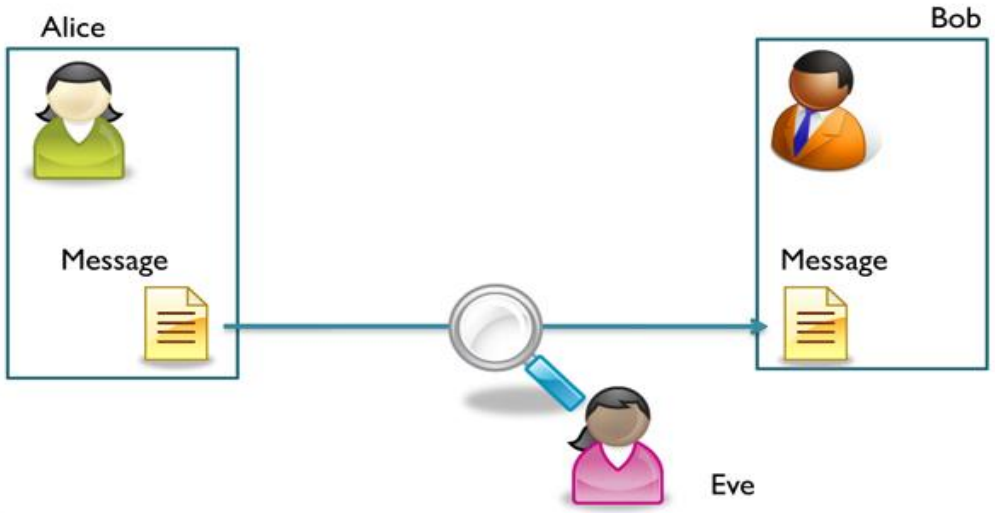
- Différents Moyens de Mise en œuvre
  - - Antivirus, **Cryptographie**, Pare-feu (Firewall), Contrôle d'Accès Logique, Sécurité Physique Locaux et Équipements, Audit, Formation/Sensibilisation, etc.
- Cryptographie: Fournit principalement les services **C I P**

Cryptographie: Rappel

- Définition: Étude des Techniques qui permettent de protéger l'information et les communications en termes de *Confidentialité*, *Intégrité* et Preuve (*Authenticité, Non Répudiation)*

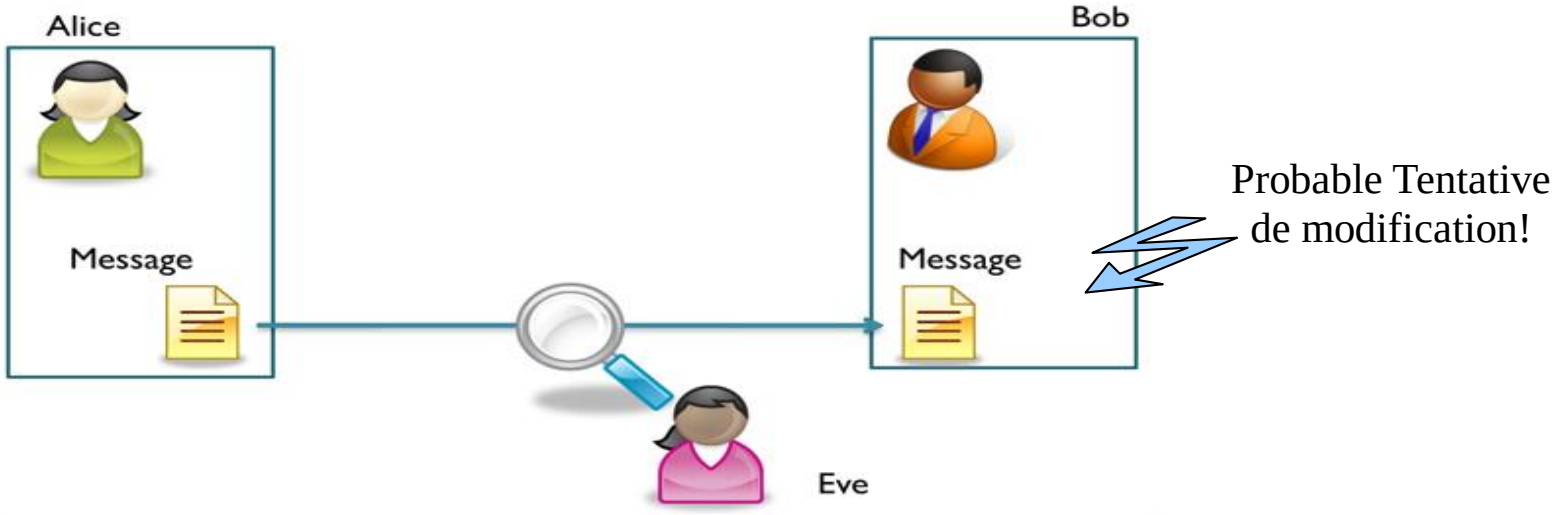
CONFIDENTIALITÉ

- L'information n'est accessible/lisible qu'aux entités autorisés (ex, Alice, Bob)



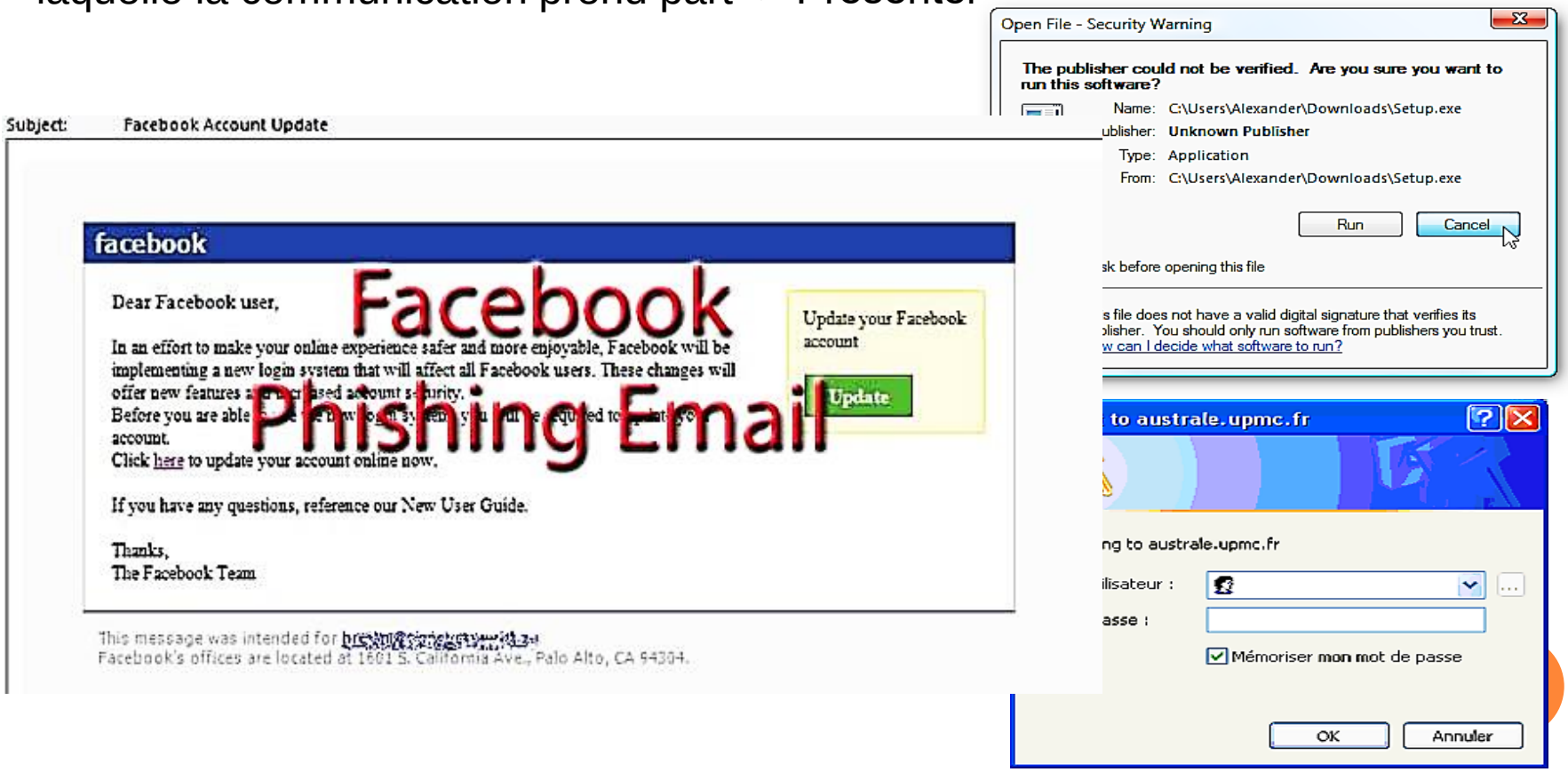
INTÉGRITÉ

- Protéger l'information contre toute modification/altération non autorisée



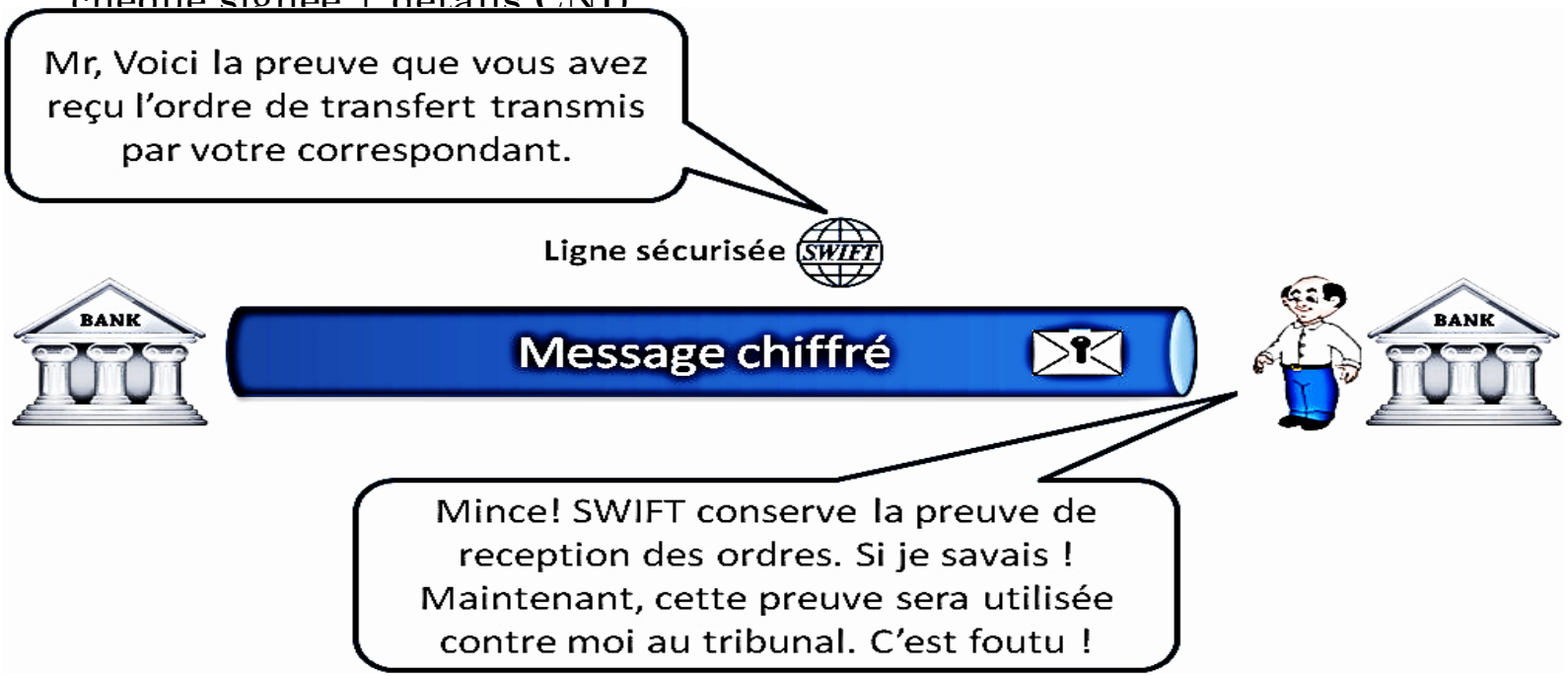
Authenticité (Preuve)

- S'assurer de l'identité de l'entité (personne, machine, programme, etc...) avec laquelle la communication prend part -> Présenter la preuve de son identité



Non Répudiation (Preuve)

- Pouvoir prouver qu'une action a bien eu lieu --> Déterminer les responsabilités en cas de litige
  - - Prouver l'envoi/réception d'un message (*Analogie*, A/R lettre)
  - - Prouver avoir effectuer une opération bancaire (retrait, virement, etc,) (Analogie chèque signée + détails CNI)

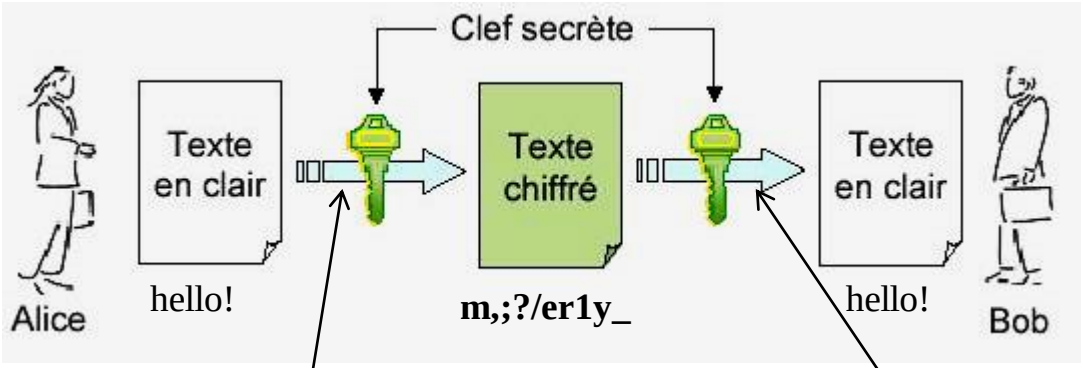


Cryptographie et Secrets

- La cryptographie est pratiquement lié, si ce n'est pas toujours, à l'utilisation d'un (ou plusieurs) **secret(s)**, en plus de techniques

  - - Les techniques – SW/HW- sont supposés être publique (*Analogie*, les serrures)
  - - Le(s) secret(s), ne l'ai (le sont) pas (*Analogie*, clefs de serrures)

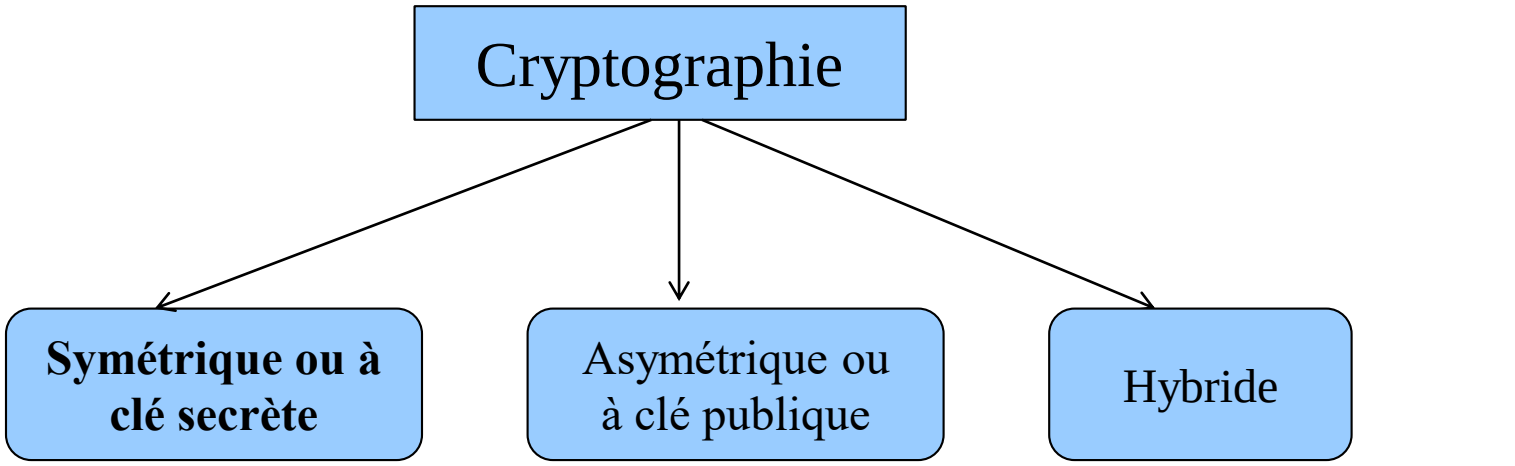
- Secret: Peux être assimilé tout simplement à une <u>suite binaire</u> d'une certaine longueur, souvent connue sous le nom de « clé/clef »



Technique produisant un texte **illisible**

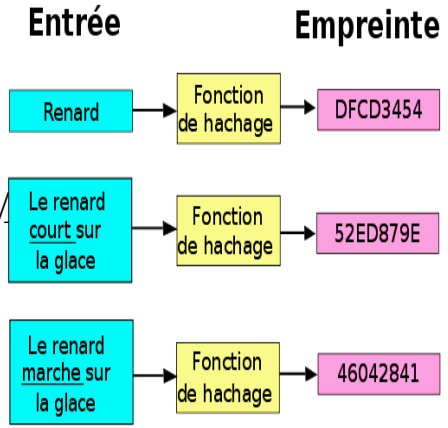
Technique produisant le texte **lisible**

Classification de la Cryptographie



TERMINOLOGIE

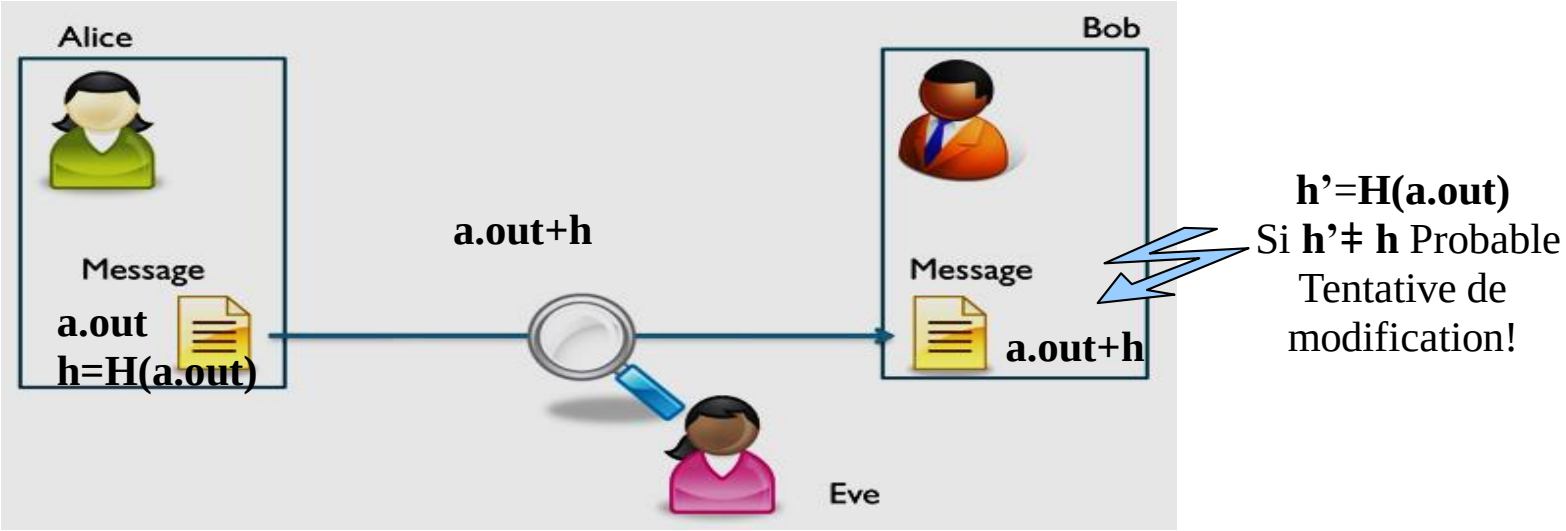
- **Fonction de hachage**: Une fonction **H** qui prend en entrée un message d'une taille arbitraire, et retourne un message appelé *empreinte* ou *haché h* de taille fixe *l*= 160, 256, 384, 512, ... bits



- **H**: {0, 1}* --> {0, 1}l
- Propriétés
  - *Calculabilité*: étant donnée M, il est facile de calculer *h*=H(M
  - *Irréversible*: étant donnée un haché *h,* il est *impossible en pratique* de trouver M tel que H(M)=*h*
  - *Résistance aux collisions:* Il est *impossible en pratique* de trouver deux messages M, M' tel que H(M)=H(M')
- Exemples: *MD4, MD5 (128 b), SHA-1 (160 b), SHA-256/384/512,* fonctions de hachage publique
- Est ce que la longueur du haché à une quelconque influence?

Quel Service Peut nous fournir une fonction de hachage?

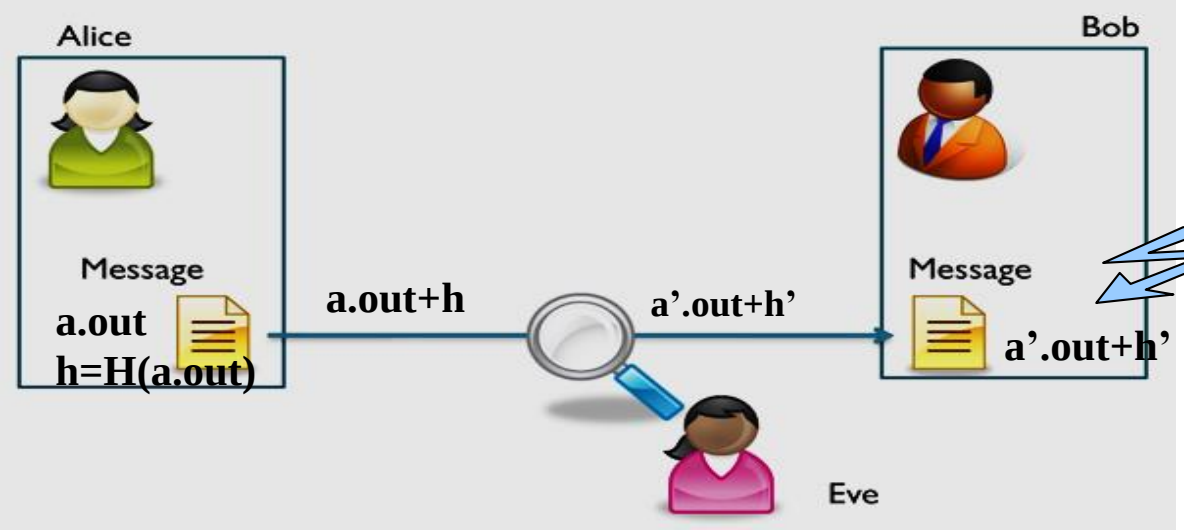
- **Intégrité**: Protection contre les modification accidentels (erreur transmission)



- ***Problème***: on peut changer le message, mais l'empreinte respectivement aussi! > Pas de trace de violation d'intégrité!

Quel Service Peut nous fournir une fonction de hachage?

- **Intégrité**: Protection contre les modification intentionnelles ?



- La fonction de hachage seule ne permet pas de **détecter** une violation d'intégrité intentionnelle, mais plutôt une violation suite à une erreur de transmission

- Toutefois, associé à **un secret partagé**, elle pourra fournir le service d'intégrité

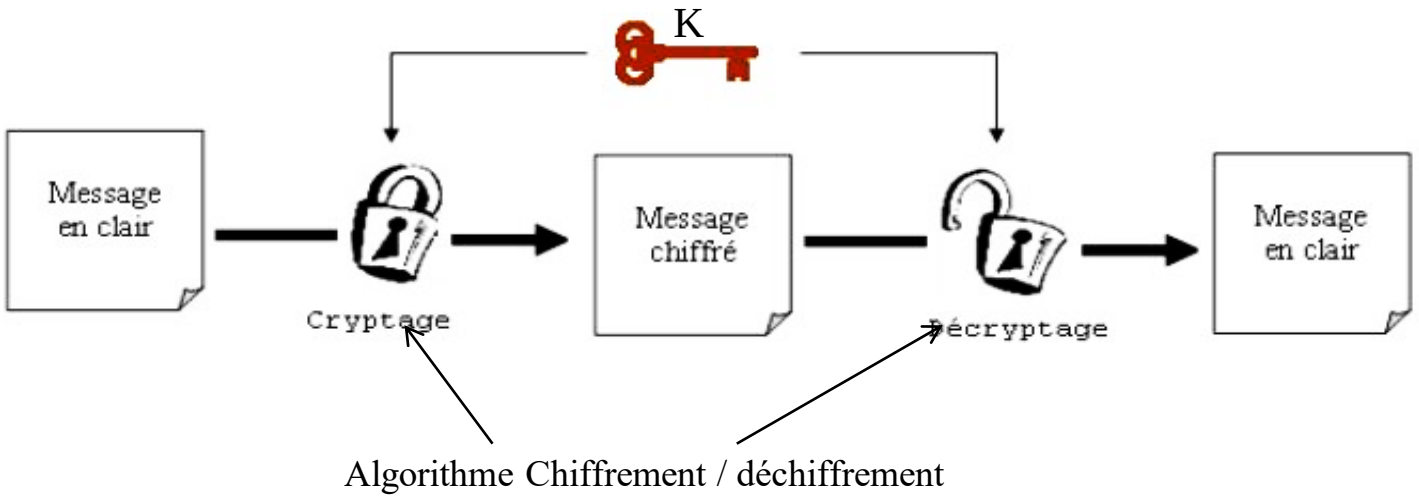
La mise en œuvre des services CIP via la cryptographie symétrique

- **Chiffrement**
- Intégrité de Données
- Authentification
- Non-répudiation

CHIFFREMENT

- **Algorithme de Chiffrement**: Un algorithme, qui étant donné un message en clair **M** et une clé secrète **K** produit un message chiffré/crypté **M'** qui ne peut être lisible (déchiffré/décrypté) qu'aux détenteur de **K**

- **E:** $\{0,1\}^* \times \{0,1\}^{|K|} \rightarrow \{0,1\}^*$



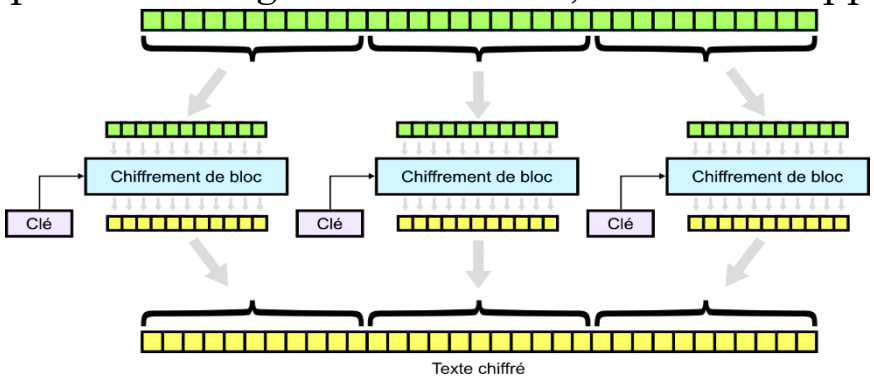
- Analogie: une serrure, un coffre fort, un cadenas --> ont tous besoin de clés (matériel et/ou numérique) pour les fermer/ouvrir

Algorithmes de Chiffrement: Deux Grandes Catégories

- Pour pouvoir chiffrer des messages de taille **quelconque :**

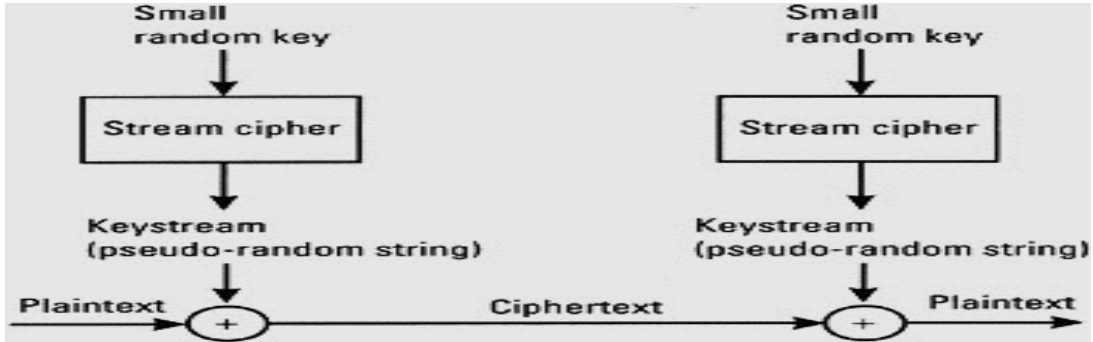
➢ Par **Bloc**: Le chiffrement s'opère sur des blocs de taille fixe (128, 192, … bits)

- - Découper le message clair en blocs, et ensuite appliquer le chiffrement sur les blocs



DES, 3DES, AES, …

➢ Par **Flux**: Le message n'est pas divisé en blocs, il est traité comme un flux continu d'octets



RC4, A5/1

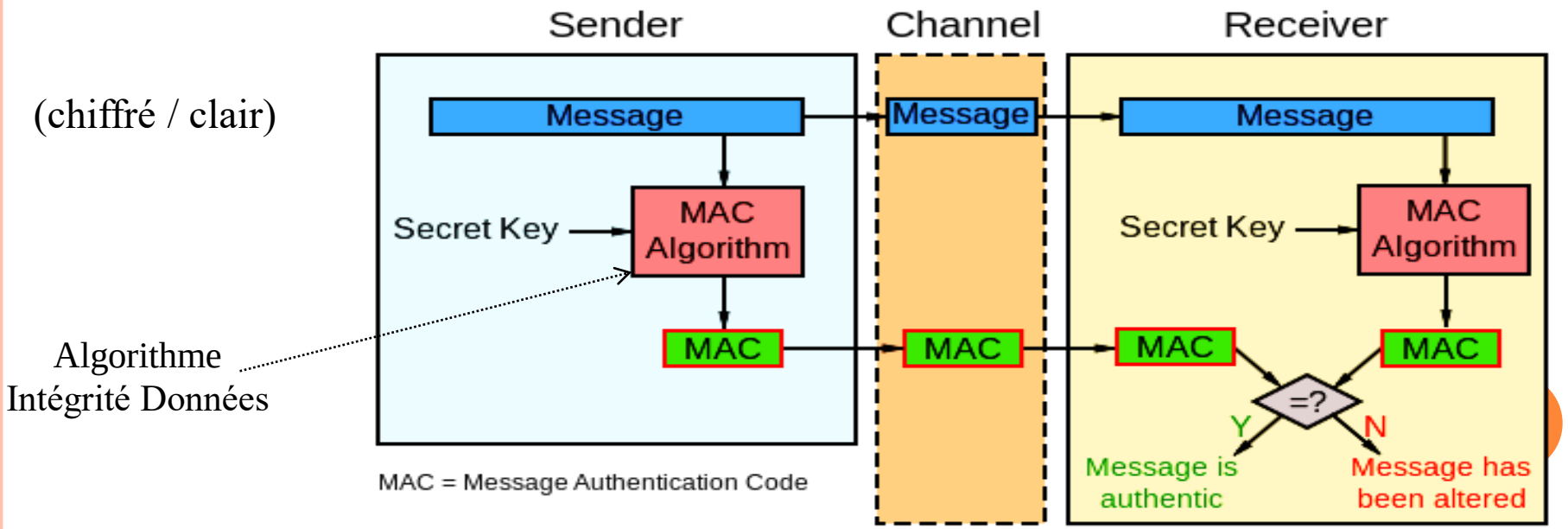
La mise en œuvre des services CIP via la cryptographie symétrique

- Chiffrement
- **Intégrité de Données**
- Authentification
- Non-répudiation

Intégrité des Données

- Algorithme d'Intégrité des données: un algorithme qui étant donnée un message **M**, ainsi qu'une clé **K**, produit un code de taille fixe appelée **MAC** (Message Authentification code) ou code d'intégrité de donnée, permettant de vérifier si **M** a été modifié. On parle aussi de fonction/algorithme MAC

  - Fonction MAC: $\{0,1\}^* \times \{0,1\}^{|K|} \rightarrow \{0,1\}^l$



La mise en œuvre des services CIP via la cryptographie symétrique

- Chiffrement
- Intégrité de Données
- **Authentification**
- Non-répudiation

AUTHENTIFICATION (PREUVE)

•Un procédé, protocole, par lequel une entité **A** **s'assure** de **l'identité** d'une entité **B** avec laquelle elle communique / par lequel une entité **B** **prouve** son identité à une entité **A**

•**A**, **B** peuvent être: des machines, des applications, utilisateurs, etc.

▪Ouverture de session Windows/Linux

▪Connexion à votre compte email, FB, BDD, etc.

➢La machine/serveur vérifie si vous avez un compte, et si vraiment vous êtes le propriétaire

▪Retrait d'argent du distributeur de billet par carte bancaire (CIB, etc.)

▪Paiement par carte bancaire via un borne monétique

➢Vérification si vous êtes réellement le porteur de la carte bancaire

AUTHENTIFICATION (PREUVE)

Principe général

> Le serveur « met à l'épreuve » le client en lui faisant effectuer une opération que seul le client légitime est en mesure de mener à bien correctement

- A travers cet épreuve, le Client doit **prouver** son identité au Serveur
- Différents facteurs d'authentification existent pour fournir une telle preuve:
  - Une information que seul le client connait (ex: mot de passe)
  - Une information unique que seul le client possède (Token de sécurité, ex USB)
  - Une information que seul le client peut produire (paramètre biométrique: IRIS …)
  - Etc.

La mise en œuvre des services CIP via la cryptographie symétrique

- Chiffrement
- Intégrité de Données
- Authentification
- **Non-répudiation**

Non-répudiation

- **Définition:** Impossibilité, pour une personne ou pour toute autre entité engagée dans une communication par voie informatique, de nier avoir reçu ou émis un message.

- **Mise en œuvre:** mécanisme de signature numérique

NON-RÉPUDIATION

Signature numérique: La signature numérique est un mécanisme permettant de garantir l'intégrité d'un document électronique et d'en authentifier l'auteur, par analogie avec la signature manuscrite d'un document papier

→Utilisation de la cryptographie à clé publique + fonction de hachage