



Sécurité - Cryptologie

Pr Fouzia Omary

Année: 2021-2022



Plan

- 🔦 Introduction

- 🔦 Notions générales sur la Sécurité

- 🔦 Outil de la Sécurité : Cryptologie

- Cryptographie à clé secrète

- Cryptographie à clé publique

- Fonctions de Hachage & Signatures



Plan (suite)

🔦 Applications

- Protocoles d'Authentification
- Pare feu, IDS
- SSL , TLS et IPSec
- Architectures de paiement électronique

Introduction générale (1)

🔦 **Historique** : De la Crypto → la Sécurité

➤ **Antiquité** : plus de 4000 ans

Sécurité = Cryptographie = Confidentialité

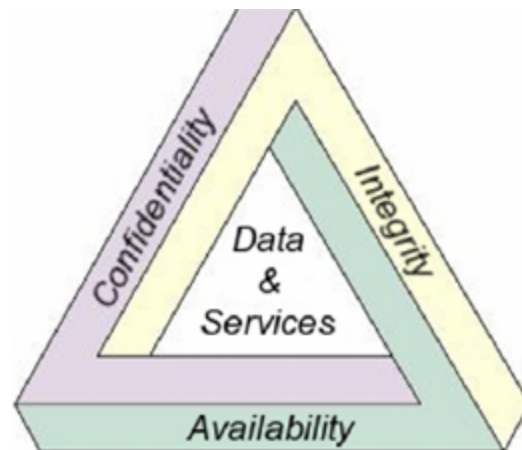
Milieux militaires et diplomatiques.

➤ **Evolution** de l'informatique et l'apparition de l'internet:

D'autres exigences sont apparues:

Authentification + Intégrité + Disponibilité +

Non-Répudiation

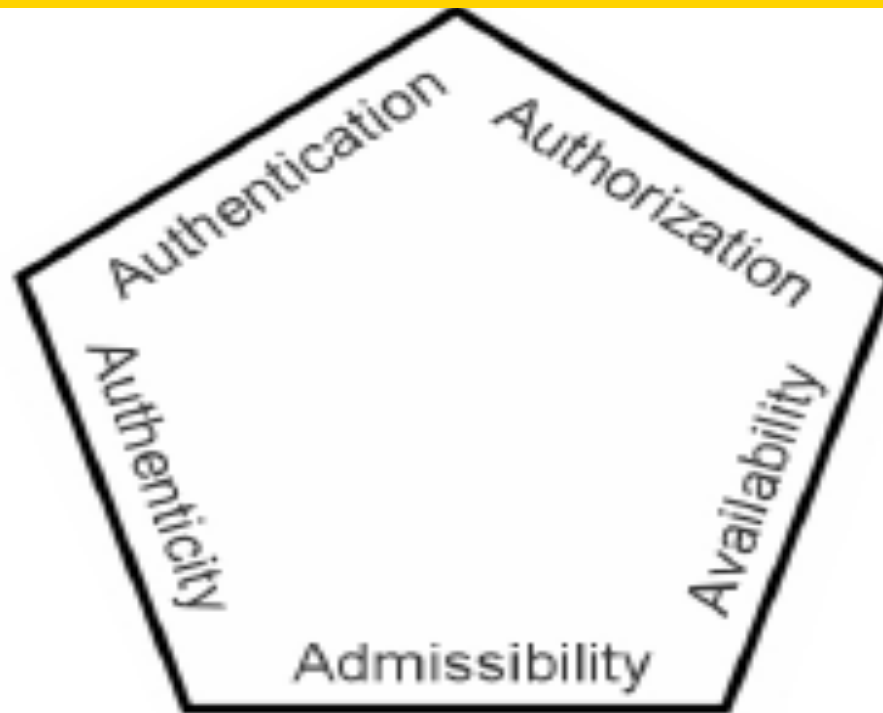


Triangle CIA (1987): Pilier immuable présentant les grands axes de la sécurité.



Hexagone de Parker(2002):

Utilité: Si la clé de déchiffrement est perdue, l'information chiffrée n'est plus utile, bien qu'elle est confidentielle, intègre disponible et que l'utilisateur y aie accès.



Pentagone de Confiance: Pliscitello(2006)

Il précise la notion d'accès à un système. indépendamment des notions définies dans CIA, il précise la confiance que doit avoir l'utilisateur en présence d'un système informatisé

Introduction générale(2)

- ☀ Ce qui peut arriver à votre machine
 - Refuser de faire quoique ce soit (plantage)
 - Faire trop tôt ou trop tard ce qu'elle devait faire (mauvaise réactivité).
 - Accomplir des actions différentes de celles attendues
 - Etre attaquée par un pirate → attaque
 - La destruction de vos données
 - La transformation de votre écran en une œuvre d'art minimaliste
 - L'inondation de la planète de message pornographiques

Introduction générale(3)

- L'espionnage de votre comportement et la vente de ces informations
- L'utilisation de votre machine comme relai d'attaque
- L'implantation d'un module de surveillance étatique
- Conséquences
 - Dans la majorité des cas, des conséquences assez bénignes:
 - « Retaper » deux ou trois fois la même chose, suite à la perte d'un fichier



Introduction générale(4)

- Perdre des emails, des photos, des textes
- Subir de la publicité
 - Mais pour une entreprise, des conséquences considérables:
 - La paralysie des serveurs
 - Le vol de sommes considérables
 - la faillite d'une entreprise qui ne peut plus facturer
 - Dans le futur?
 - L'échec d'un tir de fusée
 - la création d'embouteillages monstrueux
 - une panne de courant paralysant une métropole

Introduction générale (5)

✱ Pourquoi est-ce si important de prévenir?

■ Dommages potentiels importants

- Indisponibilités des systèmes
- Manipulations des données/ systèmes
- Destruction des données /systèmes
- ET si la puce de votre carte d'identité crash?

✱ Coûts importants de remise en marche

- Financiers
- Temporels



Introduction générale(6)

- Humains (juristes, informaticiens)
- Matériels (serveurs de sauvegarde, ...)

- Coûts importants de maintien en état

- Analyse des données de surveillance
- Analyse des machines

Introduction générale(7)

Conséquence: ne pas renoncer aux bénéfices de l'informatisation, mais:

Centres de préoccupations → Sécurité :

- Sécurité locale (sur une machine)
- Sécurité réseau
- **Les utilisateurs !!!**
 - Education comportementale
 - . Peur de l'ordinateur
 - . La non compréhension des outils informatiques



Introduction générale(8)

- Identification des maillons faibles (personnes à risques)
 - Cadre juridique et sociale
- 🔦 **Conclusion:**
 - Faire appel à des spécialistes pour définir:
 - Quels types d'attaques l'entreprise peut subir
 - Quels moyens de protections sont à mettre en place



Introduction générale(10)

- Quelles mesures (contre-mesures) utiliser en cas d'attaque
- Quels sont les contrôles à effectuer et à quelle fréquence
 - Il n'y a aucun système sûr à 100% .
 - Il faut savoir choisir son degré de protection en fonction de ses besoins
 - Adéquation des moyens et des objectifs
 - C'est une obligation juridique



Notions générales sur la sécurité



Terminologie Et Concepts

- ✱ **Sûreté** : protection contre les actions non intentionnelles
- ✱ **Sécurité** : protection contre les actions intentionnelles malveillantes
- ✱ **Menace** : moyen potentiel par lequel un attaquant peut attaquer un système
- ✱ **Risque** : prise en compte à la fois de la probabilité d'une menace et de sa gravité si elle réussit



Terminologie Et Concepts(2)

- ✱ la **vulnérabilité** (en anglais « vulnerability »., appelée parfois faille ou brèche) représente le niveau d'exposition face à la menace .
- ✱ Enfin la **contre-mesure**: ensemble des actions mises en oeuvre en prévention de la menace.

Terminologie Et Concepts(3)

$$\text{Risque} = \frac{\text{Menace} \times \text{Vulnérabilité}}{\text{Contre-mesure}}$$

Terminologie Et Concepts(4)

- ✱ **Entité** : gouvernement, entreprise, particulier,...
- ✱ **Identifier**: obtenir l'identité d'une personne ou d'une entité
- ✱ **Authentifier**: vérifier qu'une personne ou une entité correspond bien à son identité déclarée
- ✱ **Autoriser** : vérifier qu'une personne ou une entité a les droits nécessaires pour accéder à ou modifier une ressource

Terminologie Et Concepts(5)

Définition de la SSI

Définition1: Système d'Information (Odile Papini:université de la Méditerranée)

- Matériels informatiques et les équipements périphériques
- Les logiciels et les microprogrammes
- Les algorithmes et spécifications internes aux programmes
- La documentation

Terminologie Et Concepts(6)

✱ Les moyens de transmission, les procédures, les données **et**

les informations qui sont collectées, gardées, traitées recherchées ou transmises par ces moyens ainsi que les ressources humaines qui les mettent en oeuvre

Terminologie Et Concepts (5)

Définition 2: Sécurité informatique

- ✱ Le fait de maintenir un système informatique en état de fonctionner normalement.
- ✱ Restreindre l'accès à certaines informations aux utilisateurs autorisés à les utiliser.

Terminologie Et Concepts (6)

Définition 3: Sécurité d'un SI

☛ Ensemble des règles et techniques qui assurent que les ressources du système d'information (matérielles ou logicielles) d'une organisation sont utilisées uniquement dans le cadre où il est prévu qu'elles le soient.

Objectifs: La sécurité vise cinq objectifs primordiaux, désignés par les cinq piliers de base :

Terminologie Et Concepts (7)

✚ Les 5 piliers de la sécurité sont:

- Authentification
- Non répudiation
- Intégrité
- Confidentialité
- Auditabilité

Terminologie Et Concepts (8)

✶ Propriété de sécurité: l'authentification

C'est la propriété qui assure la reconnaissance sûre de l'identité d'une entité

- L'authentification protège de l'usurpation d'identité
- Signature assure Authentification
- Entités à authentifier:
 - Une personne /organisme

Terminologie Et Concepts (9)

- Une machine dans un réseau
- Un programme qui s'exécute (processus)

✶ Propriété de sécurité : la non répudiation

C'est la propriété qui assure que l'auteur d'un acte ne peut ensuite dénier l'avoir effectué

■ Signature= Authentification+ Non répudiation

-Seconde idée contenue dans la notion habituelle de signature

-Le signataire s'engage à honorer sa signature

Terminologie Et Concepts (10)

- Engagement contractuel/juridique, on ne peut pas revenir en arrière
 - Deux aspects spécifiques de la non répudiation dans les transactions électroniques:
 - a) La preuve d'origine : un message (une transaction) ne peut être nié par son émetteur.
 - b) La preuve de réception: Un récepteur ne peut ultérieurement nier avoir reçu un ordre s'il ne lui a pas plu de l'exécuter alors qu'il le devait juridiquement

Terminologie Et Concepts (11)

✶ Propriété de sécurité : l'intégrité

C'est la propriété qui assure qu'une information n'est modifiée que par des entités habilitées
(selon des contraintes précises)

Exemples:

- le code binaire des programmes ne doit pas pouvoir être altéré
- Les messages de l'ingénieur système doivent pouvoir être lus et non modifiés

Terminologie Et Concepts (12)

✶ Propriété de sécurité: la confidentialité

C'est la propriété qui assure qu'une information ne peut être dévoilée que par des entités habilitées

■ Exemple:

- Un mot de passe ne doit jamais être lu par une autre personne que son possesseur
- Un dossier médical ne doit pouvoir être consulté que par les malades et le personnel médical habilité
- On ne doit pas pouvoir intercepter le contenu d'un courrier

Terminologie Et Concepts (13)

✳️ Propriété de sécurité: l'auditabilité

C'est la propriété qui assure la capacité à détecter et à enregistrer de façon infalsifiable les tentatives de violation de la politique de sécurité

Audit: Examen méthodique d'une situation relative à un produit, un processus, une organisation.

Il est réalisé en coopération avec les intéressés en vue de vérifier :

-la conformité de cette situation aux dispositions préétablies



Terminologie Et Concepts (14)

-l' adéquation de ces dernières à l'objectif recherché.

✱ **Auditabilité** : Garantir une maîtrise complète et permanente du système et en particulier pouvoir retracer tous les événements au cours d'une certaine période.

Types d'attaques (1)

☀ Attaque sur l'authentification

- Usurpation de l'identité: se faire passer pour quelqu'un d'autre pour pénétrer dans un système.
- Exemple:
 - simulation d'interface de système sur écran,
 - simulation de terminal à carte bancaire

☀ Attaque sur l'intégrité

- **Intégrité des données:** Modification des messages, de données.

Types d'attaques (2)

➤ Intégrité des protocoles:

- Espionnage.

- d'une interface,

- d'une voie de communication

- Répétition de l'opération pour obtenir une fraude

- Exemple :plusieurs fois la même opération de crédit d'un compte bancaire.

➤ Intégrité des programmes:



Types d'attaques (3)

Les modifications peuvent être:

- À caractères frauduleuses

Pour s'attribuer des avantages

Exemple: virement des centimes sur un compte

- À caractères sabotage

Pour détruire des systèmes ou des données

Les types de modifications:

- Infections informatiques à caractère unique

Exemple: Bombe logique, cheval de Troie



Types d'attaques (4)

- Infections auto reproductrices

Ex:Virus(repro rapide,), ver(repro lente)

- ✶ **Attaque sur la confidentialité:**

But : le vol d'information via un réseau par espionnage des transmissions de données

- Analyse de trafic:

- Observer le trafic de messages échangés
- En déduire des informations sur les décisions d'entité.



Types d'attaques (5)

Exemple:

Bourse: augmentation des transitions sur une place financière

➤ Inférence:

- Obtenir des informations confidentielles non divulguables à partir de questions autorisées

-Exemple:

Le fichier de l'hôpital, la divulgation interdite par la loi, mais autorise des opérations statistiques

Types d'attaques (6)

🔦 Attaque sur la disponibilité:

➤ Attaque par violation de protocole:

- Envoie de données non prévues

➤ Attaque par saturation:

- Envoi de messages trop nombreux provoquant un écroulement des systèmes et réseaux.

Exemple: Distributed Denial of Service

Types d'attaques (7)

Attaque sociale:

Dans la majeure partie des cas le maillon faible est l'utilisateur lui-même !

- Par méconnaissance ou duperie → l'utilisateur ouvre une brèche dans le système.
- Comment?
 - En donnant des informations (mot de passe par exemple) au pirate informatique
 - En exécutant une pièce jointe.
 - En discutant sur du chat.

Description Des Processus de la Sécurité

Les processus de la sécurité informatique se résument en :

- Analyse de risques ;
- Politique de sécurité ;
- Techniques de sécurisation.



Analyse de risques

On ne peut se protéger que contre les risques qu'on connaît, il importe :

☀ De mesurer ces risques:

- probabilité et fréquence de leur apparition
- leurs effets possibles.

☀ De mettre en oeuvre des protections raisonnables.

Analyse de risques (2)

Huit étapes pour réaliser ces tâches

- Identifier ce qu'il faut protéger
- Identifier les menaces

Ex: danger des CDs ou des clefs USB

Ex: Autoriser les accès aux sites de crack

- Identifier les points faibles

Ex: Arrivée/Départ de personnel, sortie de documents, entrée d'appareils électroniques, ..

Ex : arrêt d'un firewall



Analyse de risques (3)

- Estimer la probabilité des risques
- Calculer les Prévisions de Pertes Annuelles pour chaque point faible (P.P.A.)
- Identifier les mesures protectrices nécessaires
- Estimer(statistiquement) la réduction du PPA pour chaque mesure protectrice
- Sélectionner les meilleures mesures de protection
(Rapport prix / Réduction du PPA)

Exemples de méthodes d'analyse de Risques (1)

- ✱ La méthode **EBIOS(1995)** (Expression des besoins et identification des objectifs de sécurité), développée par ANSSI (logiciel gratuit).
- ✱ La méthode **MARION(1980):** par le **CLUSIF**
(Méthode d'analyse de risque informatiques optimisés par niveau)
- ✱ La méthode MEHARI(1995) Harmonisée d'Analyse du Risque, développé par le CLUSIF.

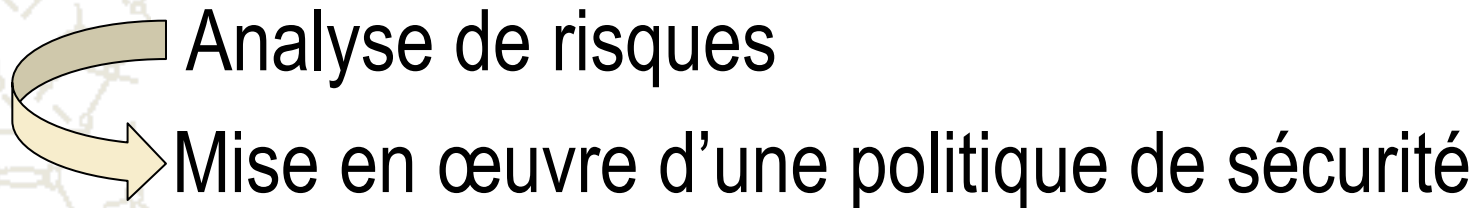
Exemples (2)

✱ La Méthode **OCTAVE(1999)** (Operationally Critical Threat, Asset, and Vulnerability Evaluation) développée par l'Université de Carnegie Mellon (USA).

✱ La norme ISO 17799 ➡ ISO 27002
✱ (organisation internationale de normalisation)



Politique de sécurité



Définition de la politique:

- Règles concernant les ressources informatiques
Ressources immatériels/ données
- Règles concernant les ressources physiques
Documents papiers, accès aux batiments

Politique de sécurité (2)

- ✱ Elaborer des règles et des procédures
→ les mettre en oeuvre dans les différents services de l'organisation pour les risques identifiés.
- ✱ Identifier les techniques de sécurisation à mettre en place dans les différents services.
- ✱ Surveiller et détecter les vulnérabilités du système.
- ✱ Définir les actions à entreprendre et les personnes à contacter en cas de détection d'une menace .
(y compris sensibilisation des utilisateurs)



Techniques de sécurisation

Elles assurent:

- ✱ la disponibilité (garantir l'accès aux services et informations pour personnes autorisées),
- ✱ l'intégrité (seules les personnes autorisées peuvent modifier les informations et les services),
- ✱ la confidentialité (l'information est accessible uniquement à ceux qui y ont droit).



Techniques de sécurisation (2)

Les techniques de sécurisation incluent :

- ✱ Audit de vulnérabilités.
- ✱ Sécurité des données: chiffrement, authentification, contrôle d'accès ;
- ✱ Sécurité du réseau : pare-feu, IDS;
- ✱ Surveillance des informations de sécurité;
- ✱ Education des utilisateurs.



Proverbe : **Sagesse populaire**

☛ « Une chaîne est aussi forte que son maillon le plus faible »

☛ Principe:

Si différents mécanismes de sécurité jouent le même rôle, le système est aussi sûr que le plus faible de ces mécanismes.



Outil de base de la Sécurité: Cryptologie


• Historique

- Discipline très antique (Avant J.C.)
- Evolution dans le temps
- Développement de la communication: → indispensable de nos jours

• Objectifs

- Assurer CAIN des informations stockées ou échangées

La Cryptologie (2)

 Définition: - C'est une science désignée par la « Science du secret » utilisant des concepts issus de plusieurs domaines (Mathématiques, informatique, électronique..)

-Comporte deux composantes complémentaires:

La cryptographie: Conception et étude de techniques ou procédés permettant de protéger des données (i.e assurant confidentialité, intégrité, authentification) sur un support donné.

La Cryptologie (3)

N.B : Les procédés de la cryptographie sont déterminés par un algorithme généralement non secret, mais faisant intervenir une information tenue secrète:

la clef

La cryptanalyse 1: Oposée à la cryptographie, elle a pour but de retrouver les données (ou messages) protégés en se basant sur les failles des techniques de la cryptographie

La Cryptologie (4)

🔦 **Cryptanalyse 2:** Ensemble de techniques permettant de déterminer le contenu du message chiffré à partir du message clair en déterminant les failles des algorithmes utilisés en cryptographie.



Cryptographie: Terminologie

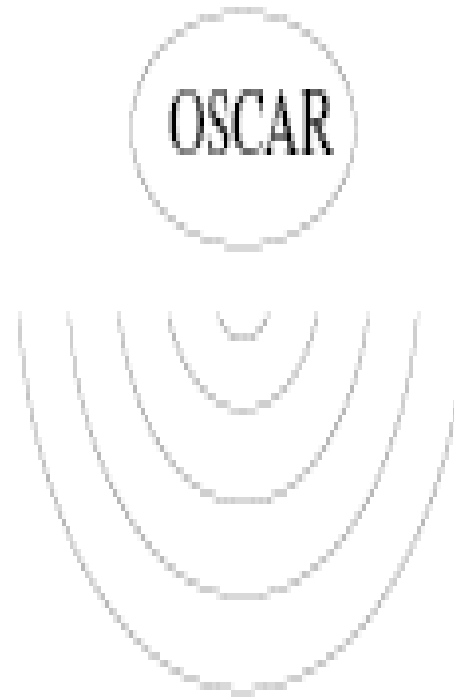
Protagonistes traditionnels:

- Alice et Bob souhaitent se transmettre des informations.
- Oscar: Un opposant qui souhaite espionner Alice et Bob.

Objectif fondamental de la cryptographie:

- permettre à Alice et Bob de communiquer sur un canal peu sûr.
- Oscar ne doit pas comprendre ce qui est échangé.

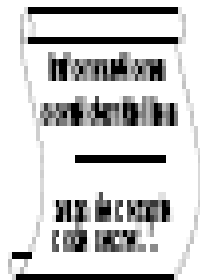
OSCAR



BOB

Canal de communication

ALICE



message M



Terminologie(suite)

- ✪ **Texte clair** : information qu'Alice souhaite transmettre à Bob.
- ✪ **Texte chiffré** ou **cryptogramme**: résultat d'application d'un chiffrement à un texte clair
- ✪ **Chiffrement**: processus de transformation d'un message M de telle manière à le rendre incompréhensible.
 - Basé sur une fonction de chiffrement
 - On génère ainsi un message chiffré $C=E(M)$.
- ✪ **Déchiffrement**: processus de reconstruction du message clair à partir du message chiffré
 - Basé sur une fonction de déchiffrement D
 - On a donc $D(C) = D(E(M)) = M$ (D et E sont injectives)

Exemple

- Représentation mathématique de E et D
- Pour permettre l'analyse des systèmes cryptographiques:
 - ✓ Représentation mathématique des messages M et C. EX:

a	b	...	y	z	0	1	...	9	␣	▪
0	1	...	24	25	26	27	...	35	36	37

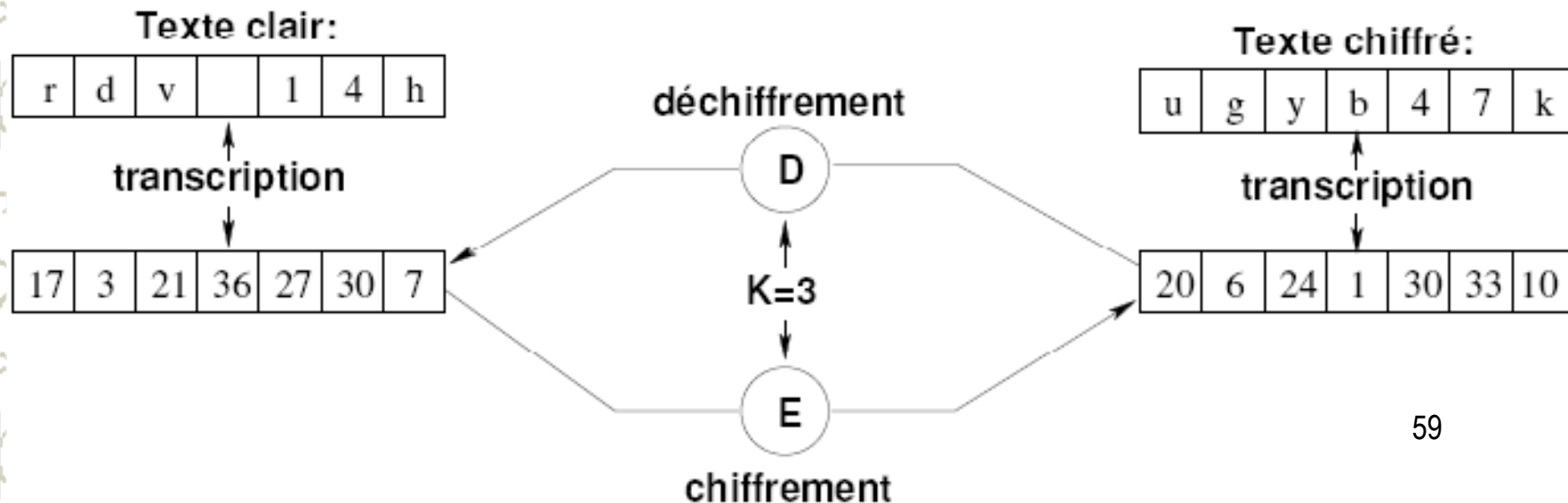
Ici:vocabulaire de n=38 caractères (code ASCII: n=256)

Exemple (suite)

- ✓ Fonctions E et D vues comme des fonctions mathématiques
 - Basés le plus souvent sur l'arithmétique modulaire
 - Exemple: chiffrement par décalage

$$E_k(M) = M + K \pmod{n}$$

$$D_k(C) = C - K \pmod{n}$$



Objectifs de la cryptographie : CAIN

✱ Assurer CAIN (Confidentialité-Authentification-Intégrité-Non répudiation):

- **Confidentialité** des informations stockées /échangées
 - Utilisation d'un algorithme de chiffrement
 - Empêcher l'accès aux infos pour ceux qui ne sont pas autorisés
- **Authentification** d'utilisateurs et ressources.
 - Utilisation d'algorithmes d'authentification
 - Alice s'identifie à Bob en prouvant qu'elle connaît un secret S (ex: un mot de passe)
- **Intégrité** des informations stockées/manipulées
 - Vérifier que les informations transmises n'ont pas subi d'altérations

CAIN (Suite)

- **Non- répudiation des informations**

- Utilisation d'algorithme de signatures
- Empêcher un utilisateur de se dédire

Remarque: Authentification+Intégrité → Authenticité

Les grands types de menaces

☛ Menaces accidentelles

Aucune préméditation

☛ Menaces intentionnelles

Reposent sur l'action d'un tiers désirant s'introduire et relever des informations

- Passive: L'intrus tente de dérober l'info par Audit ce qui rend sa détection difficile
(en effet: cet audit ne modifie pas les fichiers ni altère les systèmes)

Les grands types de menaces(suite)

- Active: la détection est facile mais il peut être déjà trop tard lorsque celle-ci a eu lieu

(Ici l'intrus aura modifié volontairement les fichiers ou système en place pour s'en emparer)

- ☀ Les menaces actives appartiennent principalement à quatre catégories:

- Interruption: lié à la disponibilité des données
- Interception: lié à la confidentialité des données
- Modification: lié à l'intégrité des données
- Fabrication: lié à l'authentification des données

Attaques sur Chiffrement

- ✱ **Cryptanalyse** : étude des systèmes cryptographiques, notamment de leur faiblesse

But : Retrouver les messages clairs correspondants à des messages chiffrés dont on n'est pas destinataire.

- ✱ **Cryptanalyste (ou attaquant)** : personne qui tente de déchiffrer des messages sans connaître la clé.

Niveaux d'attaques possibles

1. Texte chiffré connu: seul C est connu d'Oscar
2. Texte clair connu: Oscar connaît C et M correspondant
3. Texte clair choisi : $\forall M$, Oscar peut obtenir C
4. Texte chiffré choisi: $\forall C$, Oscar peut obtenir M

Garantir la confidentialité \rightarrow Oscar ne peut pas :

- Trouver M à partir de $E(M)$
- Trouver **la clé** de déchiffrement D à partir d'une séquence $\{M_i, E(M_i)\}$

Algorithmes d'attaques

✶ Attaque brutale

- Énumérer toutes les valeurs possibles de clés
- 64 bits $\rightarrow 2^{64}$ clés = $1.844 \cdot 10^{19}$ combinaisons
 - Un milliard de combinaisons /s \rightarrow 1 an sur 584 machines

✶ Attaque par séquences connues

- Deviner la clé si une partie du message est connue
 - Ex: en-têtes de standard de courriels

✶ Attaque par séquences forcées

- Faire chiffrer par la victime un bloc que l'attaquant en connaît le contenu, puis on applique l'attaque précédente...



✶ Attaque par analyse différentielle

- Niveau: Texte clair choisi
- Utiliser des faibles différences entre paires de textes
- la possibilité d'attribuer des probabilités à chaque clé possible

✶ Attaque par analyse linéaire

- Niveau: Texte clair connu
- Modéliser l'algorithme de chiffrement par une approximation linéaire, en le simplifiant.
- En augmentant le nombre de couples disponibles (texte en clair, texte chiffré), on améliore la précision de l'approximation et on peut deviner la clé.



Algorithmes d'attaques(3)

→ on améliore la précision de l'approximation et on peut deviner la clé

Exemple d'application: DES a été attaqué par la cryptanalyse linéaire.