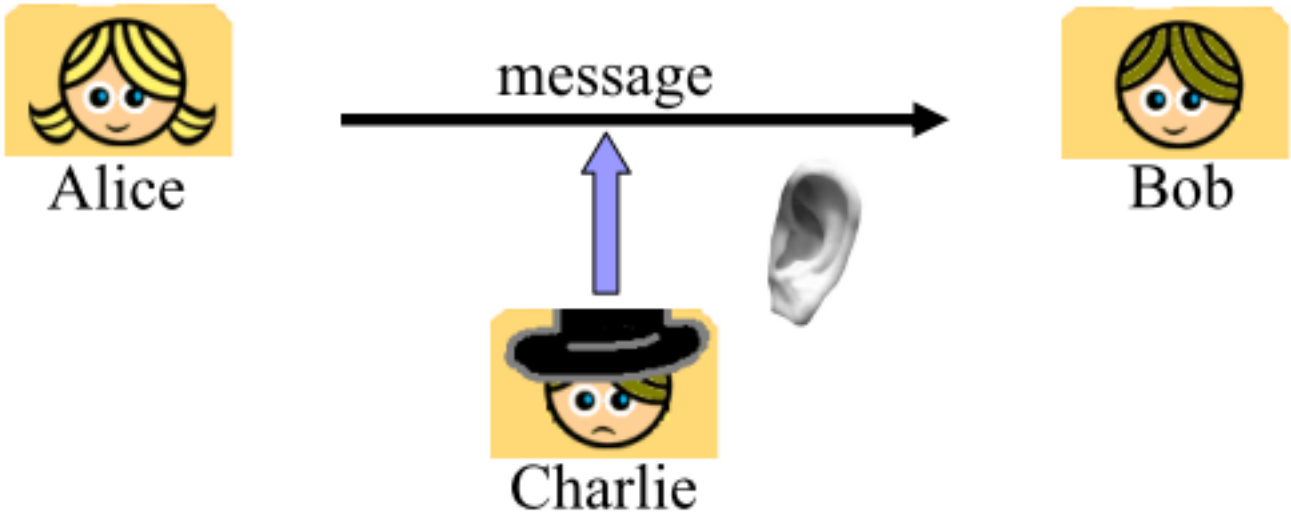
Chapitre 1

INTRODUCTION

Menaces : utilité de la cryptographie

- **Attaques passives**

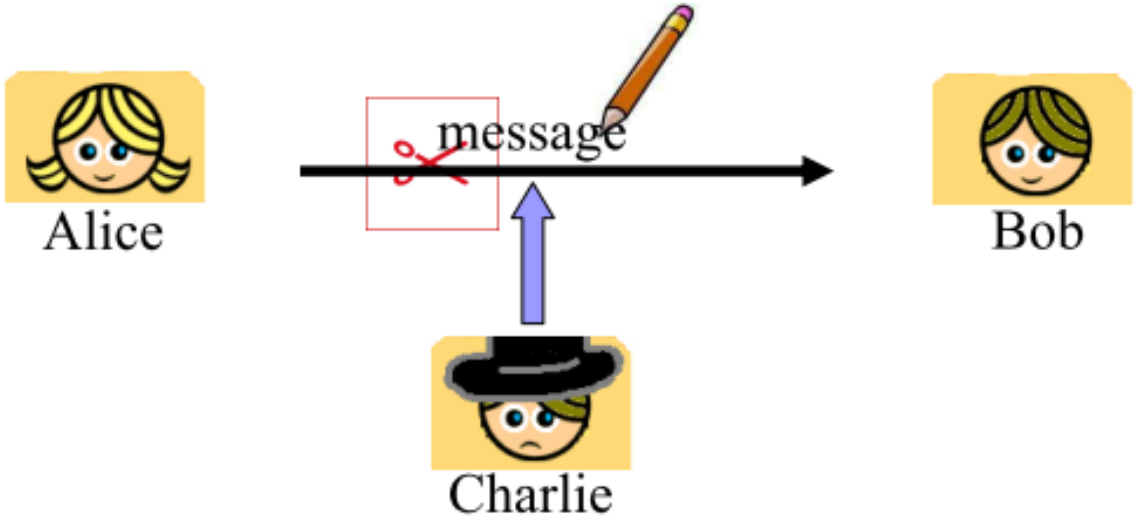


- Menace contre la **confidentialité** de l'information :

→ une information sensible parvient à une personne autre que son destinataire légitime

Menaces : utilité de la cryptographie

- **Attaques actives : interventions sur la ligne**



  - Menace contre l'**intégrité** et l'**authenticité** de l'information
  - Exemples :
    - Impersonification : modification de l'identité de l'émetteur / récepteur
    - Altération des données (modification du contenu)
    - Destruction des données
    - Retardement de la transmission
    - Répudiation du message = l'émetteur nie l'envoi du message

Services de sécurité

- Fournir un certain nombre de services de sécurité

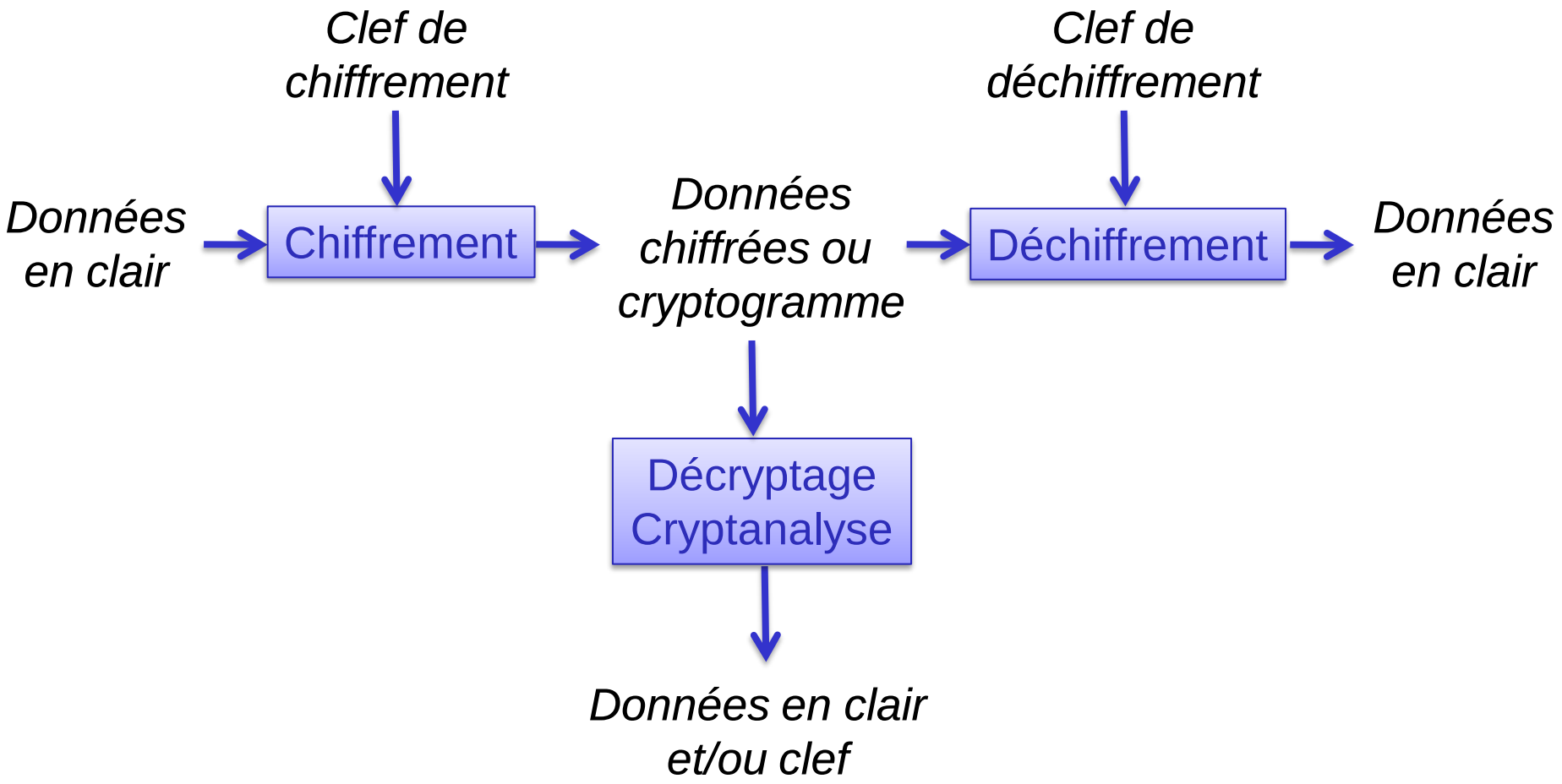
1. ***Confidentialité***
   - Fait de garder quelque chose privé et secret vis-à-vis de tout le monde sauf de ceux qui sont autorisés à le voir.
2. ***Intégrité***
   - Assurance que les données n'ont pas été modifiées (par des personnes non autorisées) pendant le stockage ou la transmission
3. ***Authentification*** de l'origine des données ou d'un tiers
   - Assurance qu'un tiers non autorisé n'est pas à l'origine des données
4. ***Non-répudiation***
   - Assurance que l'émtteur ne puisse pas nier l'envoi d'un message.
5. ***Preuves à divulgation nulle de connaissance***
   - Désigne un protocole sécurisé dans lequel un tiers veut prouver au second tiers qu'il connait une information, mais sans lui dévoiler.

Mécanismes et services de sécurité

- **Moyens mis en œuvre :**
  - Mécanismes de sécurité construits au moyen d'outils cryptographiques (fonctions, algorithmes, générateurs aléatoires, protocoles…)
    - Chiffrement / déchiffrement
    - Scellement et signature
    - Certification
    - Protocoles d'authentification mutuelle avec échange de clefs

- **Cryptologie**
  - Science regroupant :
    - La cryptographie
    - Et la cryptanalyse

Principe d'une transmission sécurisée



Cryptographie

- **Définition :**
  - Conception de mécanisme de cryptologie destinés à garantir les notions de sécurité à des fins de :
    - **confidentialité**,
    - d'**authenticité**
    - et d'**intégrité** de l'information,
  - mais aussi pour d'autres notions comme :
    - l'**anonymat**
    - et la **non-répudiation** de l'information

Cryptanalyse

- **Définition :**
  - Reconstruction d'un message chiffré en clair à l'aide de méthodes mathématiques.

- **Pourquoi ?**
  - Tout cryptosystème doit nécessairement être **résistant** aux méthodes de cryptanalyse.
  - Lorsqu'une méthode de cryptanalyse permet de déchiffrer un message chiffré à l'aide d'un crypto-système, on dit alors que l'algorithme de chiffre-ment a été « **cassé** ».

- On appellera « **attaque sur texte** » une méthode de cryptanalyse permettant de déchiffrer un message donné.

Cryptanalyse

- **Méthodes d'attaque :**
  - attaque texte chiffré seul (*cyphertext-only attack*) :
    - l'attaquant possède une copie du texte chiffré.
  - attaque texte clair connu (*known plaintext attack*) :
    - l'attaquant possède une copie du texte clair et une copie du texte chiffré.
  - attaque texte clair choisi (*chosen plaintext attack*):
    - l'attaquant possède temporairement un accès à la machine de chiffrement. Il peut choisir librement un texte clair et le chiffrer.
  - attaque texte chiffré choisi (*chosen cyphertext attack*) :
    - l'attaquant possède temporairement un accès à la machine de déchiffrement et peut choisir des textes chiffrés et les déchiffrer.
  - attaque par force brute (*brute force attack*) :
    - on essaie toutes les clés possibles.
  - attaque par devinette (*riddle attack*) :
    - Soit un espace de clé défini. Si un utilisateur utilise un sous-espace seulement (par exemple seulement des mots français) on peut facilement faire une recherche sur les mots français. Ceci réduit grandement le nombre de clés possibles.