Cryptographie

Introduction

Gabriel Chênevert

3 novembre 2025

whoami

Gabriel Chênevert
gabriel.chenevert@junia.com

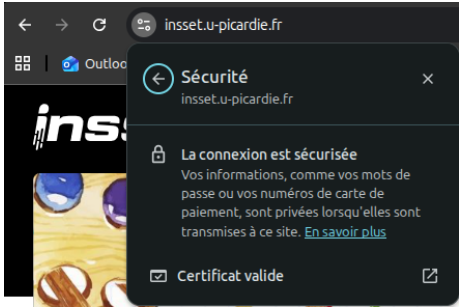
Responsable du département
Computer Science & Mathematics
JUNIA (ISEN) Lille

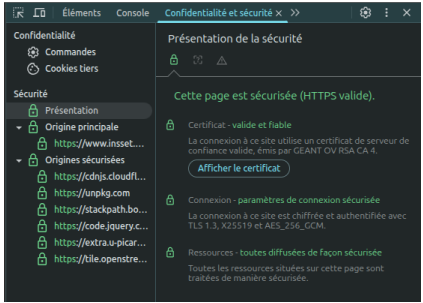
Spécialisé en théorie de l'information :

- traitement de signal
- correction d'erreur
- informatique quantique
- cryptographie

But du cours

Comprendre ce que signifie *vraiment* :





Organisation : 4 séances (cours + TP Python)

Supports de cours : `https://gch.ovh/insset`

Aujourd'hui

Introduction

Notion de canal sécurisé

Chiffrement par masque

Un peu de vocabulaire

- *Cryptographie* : ensemble de techniques (primitives, protocoles) permettant la communication sécurisée en présence d'*adversaires*
- *Cryptanalyse* : l'étude des façons d'essayer de contrecarrer (casser) ces techniques

Ce sont les deux composantes complémentaires formant le domaine de la *cryptologie*

Attention : en français on dit chiffrer

Ce que la cryptographie n'est pas

Ce qu'elle est

Un ensemble d'outils techniques fournissant permettant de garantir certaines propriétés de sécurité

tout comme : les cadenas, coffre-forts, sceaux, ...

Il est utile de comprendre comment ils fonctionnent, ce qu'ils font et ne font pas

cf. MIT Guide to lockpicking

Paradigme de conception

Principe de Kerckhoffs (1883)

Un cryptosystème doit demeurer sécurisé même si l'adversaire a la connaissance technique complète de système

sauf la clé

En d'autres termes : ne pas se fier à la sécurité par l'obscurité

En pratique : n'utiliser que des implémentations standard d'algorithmes reconnus

Aujourd'hui

Introduction

Notion de canal sécurisé

Chiffrement par masque

Modèle de la communication de Shannon

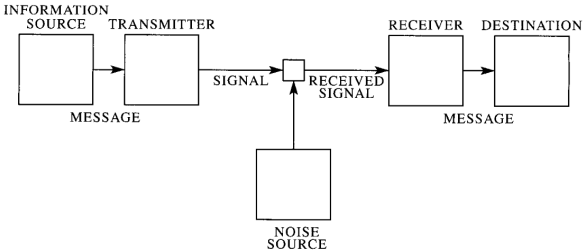


Fig. 1 — Schematic diagram of a general communication system.

Claude Shannon, *A mathematical theory of communication* (1948)

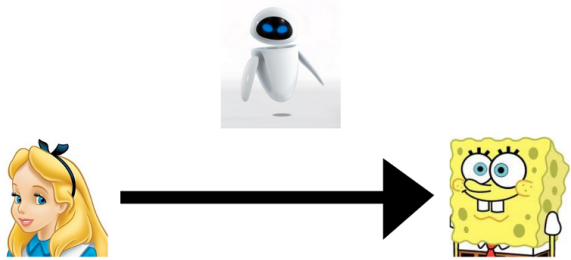
Encodage

De façon à pouvoir être envoyés sur le canal de communication, les messages doivent être *encodés* de façon appropriée (et décodés à l'arrivée).

Différentes propriétés souhaitables d'un encodage :

- existence
- compression
- intégrité
- confidentialité
- authentification
- non-répudiation

Le problème de la confidentialité



Alice veut envoyer un message à Bob, mais ne veut pas qu'Ève puisse le comprendre

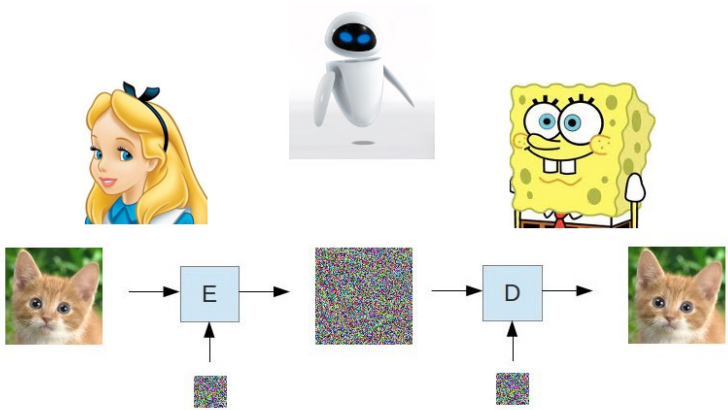
Chiffrement à clé secrète

Un *chiffre* (ou *cryptosystème*) *symétrique* est composé d'une paire de fonctions

où

- m est le message en clair ;
- c est le message chiffré ;
- k est la clé secrète partagée.

Illustration



Attaque par force brute

Ève pourra toujours essayer toutes les clés...

...et finira forcément par trouver la bonne !

Idée : rendre cette attaque inenvisageable en pratique

i.e. la rendre trop LONGUE

Le secret est protégé tant qu'Ève n'a pas terminé

Parenthèse : ordres de grandeur

- 2^4 : nombre de personnes dans cette salle
- 2^9 : nombre d'étudiants sur ce campus
- 2^{16} : nombre de personnes dans cette ville
- 2^{26} : nombre de personnes dans ce pays
- 2^{33} : nombre de personnes sur cette planète
- 2^{34} : nombre de visionnements de la vidéo YouTube la plus populaire

Constantes astronomiques

- 2^{34} : âge de l'univers (en années)
- 2^{59} : âge de l'univers (en secondes)
- 2^{63} : nombre de grains de sable sur Terre
- 2^{79} : nombre d'atomes dans un gramme de carbone
- 2^{226} : nombre de façons de mélanger un jeu de 52 cartes
- 2^{250} : nombre d'atomes dans l'univers observable

Ressources informatiques

- 2^{32} : nombre d'adresses IPv4
- 2^{71} : nombre d'opérations par seconde effectuées par l'ensemble des CPU
- 2^{74} : capacité mondiale totale de stockage numérique (en bits)

  cf. Hilbert & Lopez (2011)
- 2^{70} : nombre d'empreintes SHA256 par seconde calculées par le réseau Bitcoin
- 2^{128} : nombre d'adresses IPv6

Niveau de sécurité

Une clé cryptographique n'est (comme tout le reste) qu'une suite de bits.

Nombre total de clés à n bits possibles : 2^n

Une attaquante cherchant à retrouver une clé de taille n par force brute devra donc effectuer 2^n calculs.

Définition

Le *niveau de sécurité* d'un cryptosystème est le $\log_2$ de la complexité temporelle (nombre d'étapes de calcul) de la meilleure attaque connue contre celui-ci.

Niveau de sécurité

Le niveau de sécurité d'une primitive :

- peut changer abruptement si une nouvelle attaque est découverte
- n'est jamais supérieur à la taille de la clé (attaque par force brute)
- peut être inférieur s'il existe de meilleures attaques...

Recommendation actuelle (2025) : **128 bits de sécurité** devraient suffire pour garantir la confidentialité des communications pour les 25 prochaines années

(256 si on est paranoïaque)

Niveau de sécurité

Exercice

Niveau de sécurité de ce cadenas ?

- attaque par force brute : pas plus que $\log_2(10^4) = 4\log_2(10) \approx 13{,}3$ bits
- avec un peu d'habilté : sans doute plus près de $\log_2(4 \cdot 10) \approx 5{,}3$ bits

Aujourd'hui

Introduction

Notion de canal sécurisé

Chiffrement par masque

Une opération binaire réversible

Sur l'ensemble $\mathcal{M} = \{0,1\}^n$ des messages de longueur n on a une opération :

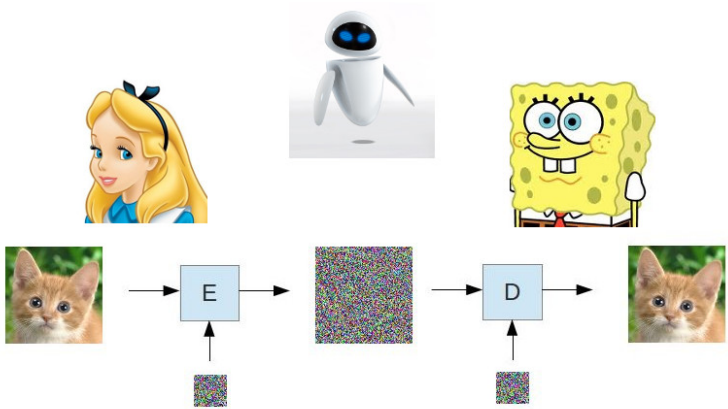
addition modulo 2 (ou exclusif) dans chaque composante,

notée XOR ou $\oplus$

Exemple

$$010011 \oplus 111000 = 101011$$

Rappel : chiffrement symétrique



Chiffrement par masque

Cas particulier du chiffrement symétrique où :

- $m, c \in \{0,1\}^n$
- $E(k, m) = m \oplus \text{pad}(k)$
- $D(k, c) = c \oplus \text{pad}(k)$

où $\text{pad}(k)$ est un masque de taille n obtenu à partir de la clé k.

Remarque

Lorsque Bob déchiffre le message chiffré reçu d'Alice :

$$D(k, E(k, m)) = E(k, m) \oplus \text{pad}(k) = (m \oplus \text{pad}(k)) \oplus \text{pad}(k)$$

$$= m \oplus (\text{pad}(k) \oplus \text{pad}(k)) = m \oplus 0 = m$$

donc Bob récupère bien, après déchiffrement, le message m initial

Chiffre de Vernam

(Miller 1882, Vernam 1917)

On prend comme clé $k = \text{pad}(k)$ le masque lui-même.

$$\begin{cases} E(k, m) = m \oplus k \\ D(k, c) = c \oplus k \end{cases}$$

Théorème (Shannon, 1949)

Le chiffre de Vernam fournit une confidentialité parfaite (la connaissance du message chiffré n'aide pas Ève à deviner quel message a été envoyé).

Problèmes avec le chiffre de Vernam

- La clé est aussi longue que le message !

  Mais : on a tout de même un transfert de confidentialité (de m à k)

- La clé ne doit **jamais** être réutilisée

  En effet, si $c_1 = m_1 \oplus k$ et $c_2 = m_2 \oplus k$, alors

  $$c_1 \oplus c_2 = m_1 \oplus m_2$$

  ce qui met sérieusement à mal la confidentialité... (*cf.* TP)