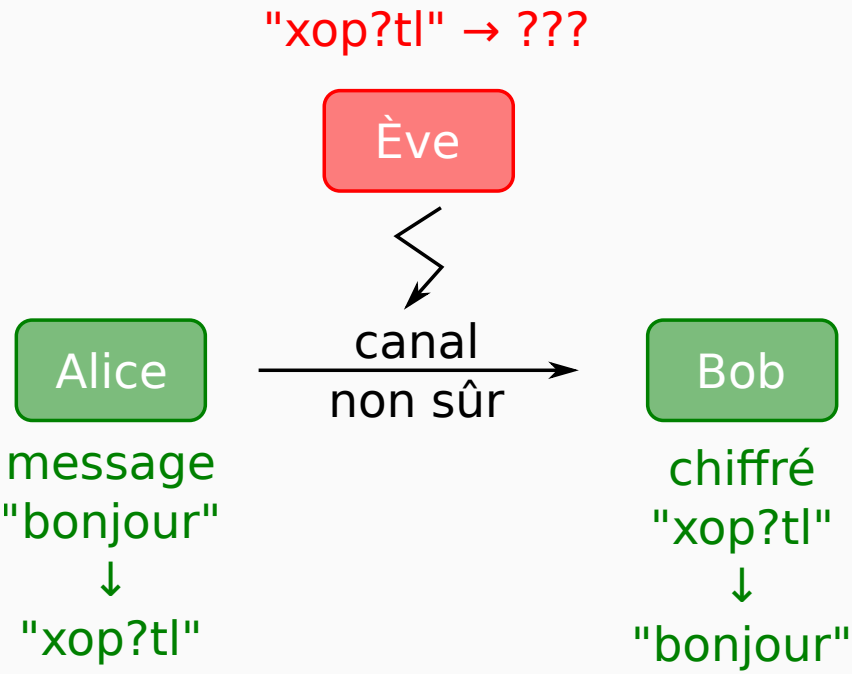
Cryptographie

Bruno Grenet

M1 MEEF Maths option Info – 2018 - 2019

Introduction

- Cryptologie = Cryptographie + Cryptanalyse
- But : « cacher » de l'information
- Autres possibilités, ex : stéganographie



- Objectifs : confidentialité, authentification, intégrité, non-répudiation

Principe de Kerckhoffs (1883)

« La méthode de chiffrement ne doit pas être secrète, elle doit pouvoir tomber aux mains de l'ennemi sans inconvénient. »

- Utilisation de *clefs de chiffrement et de déchiffrement*

Deux grandes familles

- Chiffrement symétrique
  - Même clef pour chiffrer ou déchiffrer
  - Historique : César, Vigenère, Vernam (masque jetable)
  - Moderne : DES (< 2000), AES (≥ 2000)
- Chiffrement asymétrique
  - Deux clefs : privée (secrète) et publique
  - Moderne : RSA, ElGamal, etc. (≥ 1970)

Chiffrement symétrique

Introduction

- **Idée :** secret partagé entre deux personnes
- **Image :** cadenas dont chacun possède une clef
- **Vocabulaire :** chiffrement symétrique ou à clef secrète

Chiffrement de César (50 av. J.-C.)

- Messages et chiffrés : mots sur 26 lettres
- Clef : entier $k < 26$
- Chiffrement : décalage de k lettres
- Déchiffrement : décalage de $-k$ lettres
- Exemple avec $k = 3$: `POLYNOMES` $\rightarrow$ `SROBQRPHV`
- Sécurité : extrêmement faible !

Chiffrement de Vigenère (XVI^{e} siècle)

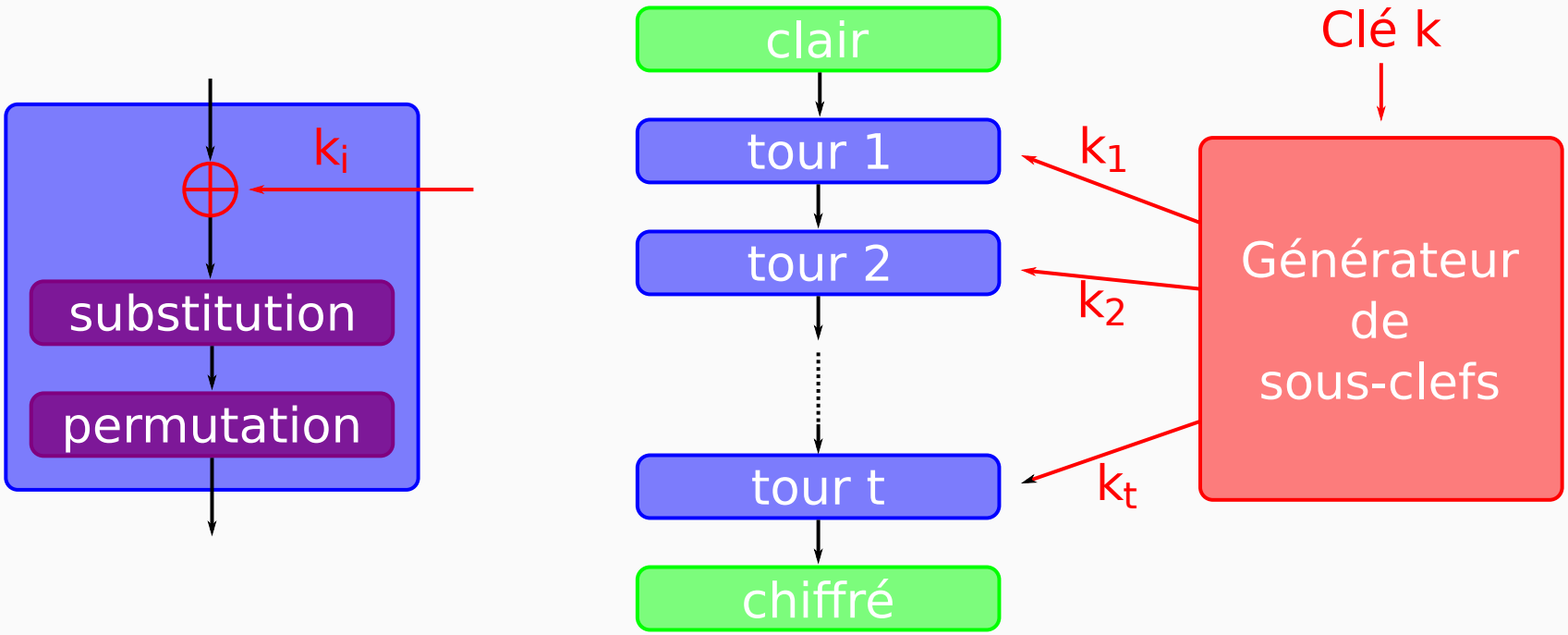
- Messages et chiffrés : mots sur 26 lettres
- Clef : mot de k lettres, vu comme suite de décalages
- Exemple avec `CAFE` : `POLYNOMES` $\rightarrow$ `SPRDQPSJV`
- Déchiffrement similaire
- Sécurité : mieux... mais faible !
- Cryptanalyse : analyse des fréquences des lettres

Vernam ou masque jetable (fin XIX^{e} siècle)

- Messages et chiffrés : suites de bits
- Clef : suite de bit de la longueur du message
- Chiffrement : $c = m \oplus k$
- Déchiffrement : $m = c \oplus k$
- Sécurité : inconditionnellement sûr...
- ... si utilisation unique !

Schéma général

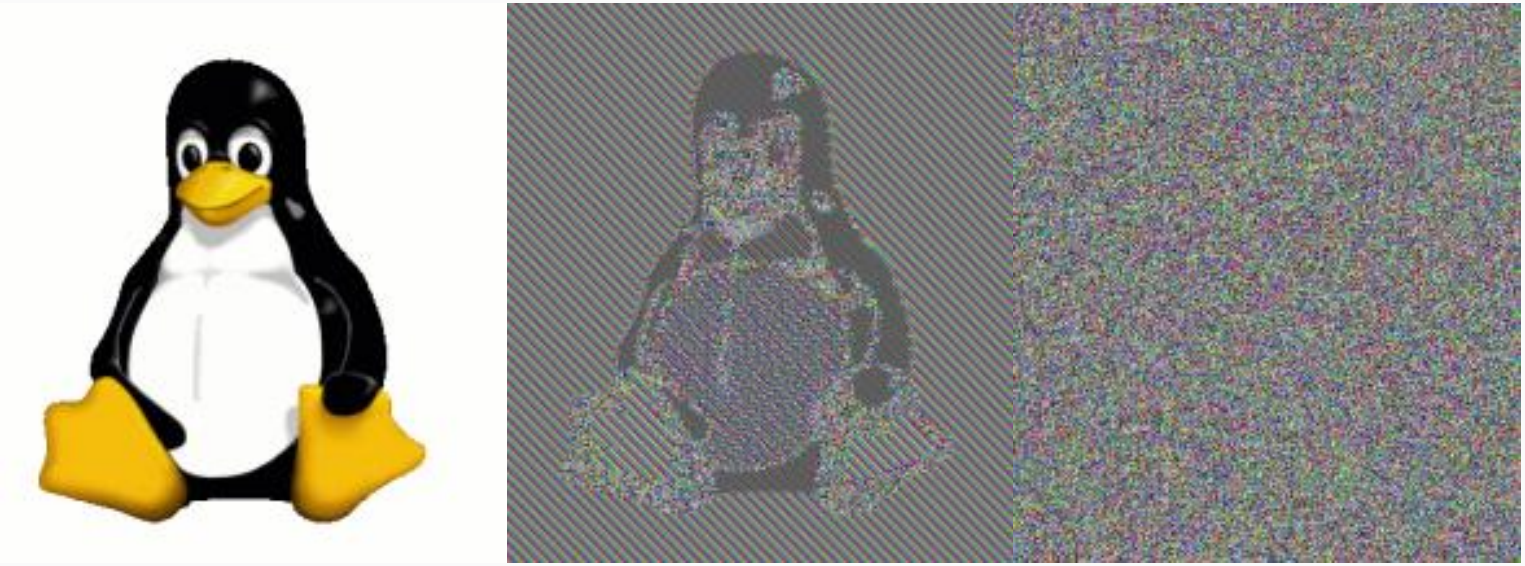
Idée : Utiliser une variante de Vernam, avec des petites clefs réutilisables



- Taille de message fixée
- DES puis AES

Messages de longueur quelconque

- Chiffrement par blocs :
  - couper le message en blocs de même taille
  - chiffrer chaque bloc, mais clef adaptative !



- Chiffrement par flot : Vernam avec générateur pseudo-aléatoire

Chiffrement asymétrique

Introduction

- **Idée :** utiliser des fonctions faciles à calculer, dures à inverser
- **Image :** Cadenas :
  - Alice ferme un coffre avec le cadenas de Bob (= clef publique)
  - Bob est le seul à pouvoir l'ouvrir avec sa clef (= clef privée)
- **Vocabulaire :** chiffrement asymétrique ou à clef publique

Protocole de Diffie et Hellman (1976)

But : se mettre d'accord sur une clef secrète commune

1. Alice et Bob choisissent
   - un groupe cyclique G d'ordre q
   - un générateur g de G
2. Alice choisit x aléatoire et calcule $k_A = g^x$

   Bob choisit y aléatoire et calcule $k_B = g^y$
3. Alice et Bob s'échangent publiquement k_A et k_B
4. Alice et Bob calculent chacun $k = g^{xy} = k_A^y = k_B^x$

Exemple : $g = \mathbb{Z}/p\mathbb{Z}^\times$

Propriétés

- Correction :
  - Alice peut calculer $k = k_B^x$
  - Bob peut calculer $k = k_A^y$
- Sécurité : problème du « logarithme discret » supposé *difficile*
  - Étant donnés g et $k = g^x$, trouver x
  - Étant donnés g, $k_A = g^x$ et $k_B = g^y$, trouver $k = g^{xy}$
- Très utilisé en pratique, avec différents groupes
  - courbes elliptiques
  - réseaux euclidiens
  - ...

Introduction

Idée : chiffrer avec la clef publique / déchiffrer avec la clef privée

Plusieurs systèmes proposés, dont :

- RSA
- ElGamal
- ...

RSA : Rivest, Shamir, Adleman (1978)

- Messages : éléments de $\mathbb{Z}/N\mathbb{Z}^\times$, avec $N = p \cdot q$
- Clef privée : d aléatoire tq $d \wedge \varphi(N) = 1$
  - $\varphi(N) = (p-1)(q-1)$
- Clef publique : $e = d^{-1} \mod \varphi(N)$ et N

Protocole :

- Chiffrement : $m \mapsto (c, r)$ où r aléatoire, $c = (m + r)^e \mod N$
- Déchiffrement : $(c, r) \mapsto m' = c^d - r \mod N$

Correction et sécurité :

- $m' + r = c^d = (m + r)^{ed} = (m + r) \mod N$ (théorème d'Euler)
- Calcul de $\varphi(N)$ et $e^{-1} \mod \varphi(N)$ *difficile* $\leftrightsquigarrow$ factorisation

ElGamal (1985)

- Messages : éléments d'un groupe cyclique G d'ordre q
- Clef privée : $x \in \{1, \ldots, q-1\}$, aléatoire
- Clef publique : un générateur g de G, $h = g^x$

Protocole :

- Chiffrement : $m \mapsto (g^y, m \cdot h^y)$ avec y aléatoire
- Déchiffrement : $(c_1, c_2) \mapsto c_2 \cdot (c_1^x)^{-1}$

Correction et sécurité :

- $c_2 \cdot (c_1^x)^{-1} = m \cdot h^y \cdot (g^y)^{-x} = m \cdot g^{xy} \cdot g^{-xy} = m$
- logarithme discret

Conclusion

Conclusion

- Deux grands systèmes : symétrique et asymétrique
- Échange de clef : un entre-deux
- Systèmes historiques inutiles de nos jours
- Ingrédients importants des systèmes modernes :
  - hypothèses de théorie de la complexité
  - utilisation de l'aléatoire
- Domaine en pleine expansion !