# Puces électroniques et sécurité numérique

Arnaud Tisserand

CNRS, IRISA, équipe-projet CAIRN

Fête de la science, octobre 2010

## Protection des données et des communications

**Applications :**


internet


signature électronique


carte bleue


vote électronique


décodeur

...

**Besoins :**

- Confidentialité ⇝ les informations sont non compréhensibles
- Authentification ⇝ garantie de l'identité de l'émetteur
- Intégrité ⇝ garantie que les informations sont complètes
- Non-répudiation ⇝ l'émetteur ne peut pas se dédire

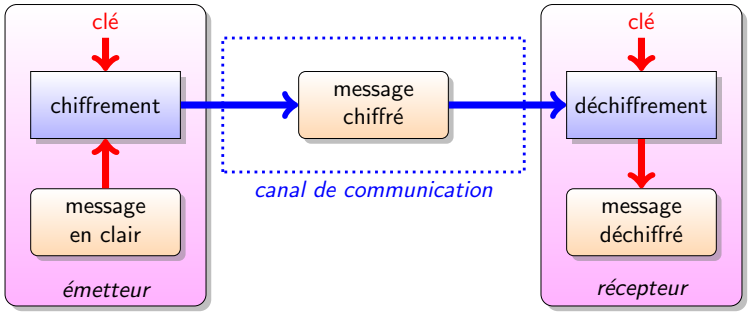


## Un peu de terminologie

**Cryptographie :** étymologiquement « écriture secrète », méthodes et outils pour rendre les messages incompréhensibles sans avoir la clé

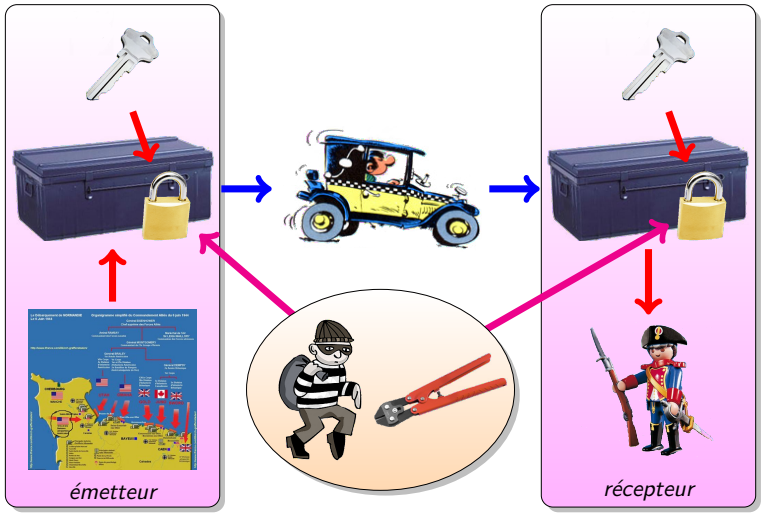
**Cryptanalyse :** analyse des cryptogrammes pour retrouver les informations secrètes (clé ou message en clair)

**Cryptologie :** cryptographie + cryptanalyse





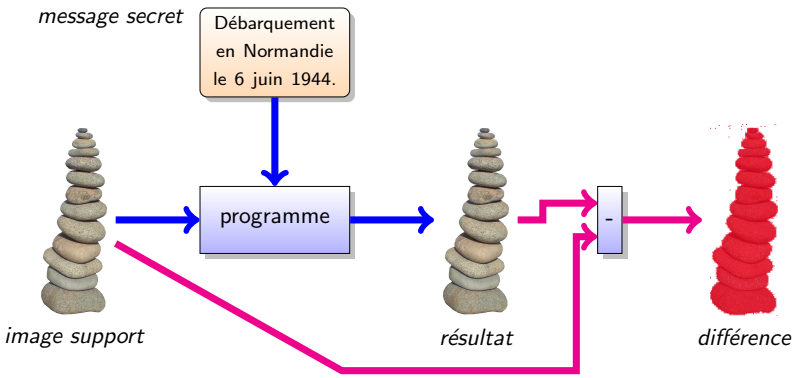

## Analogie avec un coffre et un cadenas



## Stéganographie

**Cryptographie :** art du secret
**Stéganographie :** art de la dissimulation

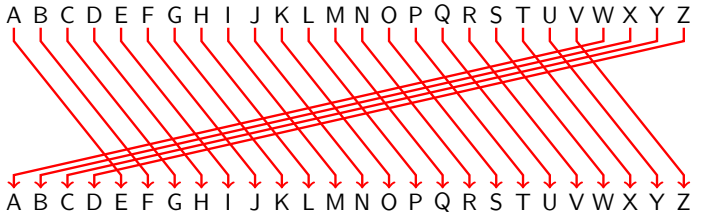
**Principe :** cacher un message (secret) dans un autre message (support)






## Méthode de chiffrement très simple (mais peu fiable)

**Idée :** remplacer les lettres de l'alphabet par une version décalée de l'alphabet (chiffre de César)




Le secret est la valeur du décalage

**Exemple :**

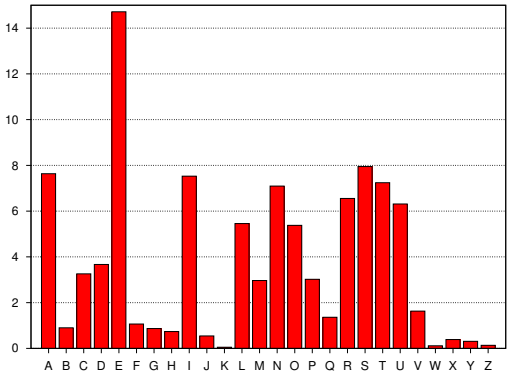
| F | E | T | E | | D | E | | L | A | | S | C | I | E | N | C | E |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ↓ | ↓ | ↓ | ↓ | | ↓ | ↓ | | ↓ | ↓ | | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ |
| J | I | X | I | | H | I | | P | E | | W | G | M | I | R | G | I |



## Fréquence d'apparition des lettres en français

**Constat :** il y a plus de e ou de a que de z dans nos textes

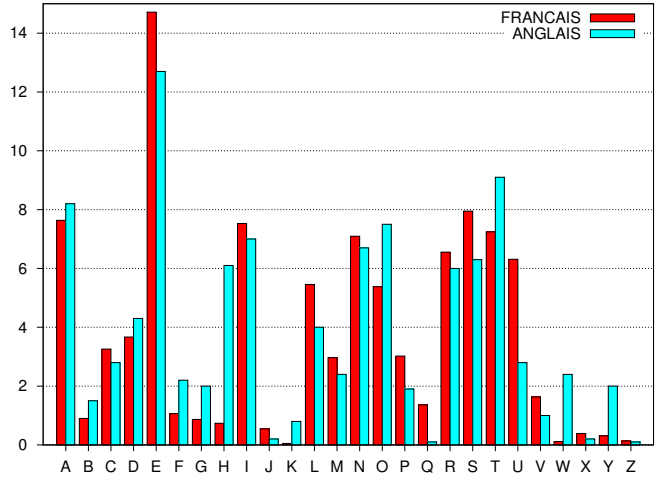
Pourcentage mesuré des apparitions des lettres en français :




Application : les valeurs des lettres du jeu Scrabble



## Comparaison des fréquences d'apparition des lettres



## Attaque par analyse fréquentielle des lettres (1/4)

Exemple de texte chiffré :

> Szwxpd pelte lddtd opaftd awfdtpfcd spfcpd dtw-pyntpfdpxpye ; dzy ozd wzyr pe xtynp pelte nzfcmp dfc fy mznlw op nstxtp, olyd wpbfpw tw xpwlyrplte opd aczofted o'fyp zopfc ylfdplmzyop ezfep alcetn-fwtpcp. Dl epep pelte apynspp dfc dl aztectyp pe tw cpacpdpyelte, l xpd jpfi, w'txlrp o'fy rclyo ztdplf xltrcp lf awfxlrp rctd, l wl szfaap yztcp.

**But :** trouver la clé secrète du décalage

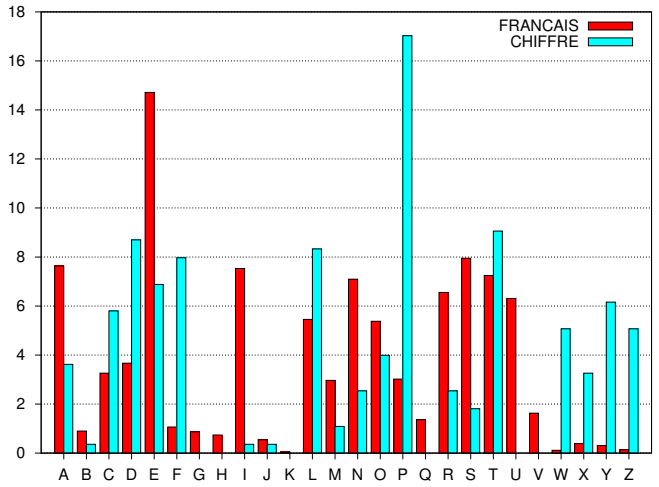
**Méthode pour attaquer :**

1. calculer les fréquences d'apparition des lettres du texte chiffré
2. comparer les distributions obtenue et de référence



## Attaque par analyse fréquentielle des lettres (2/4)

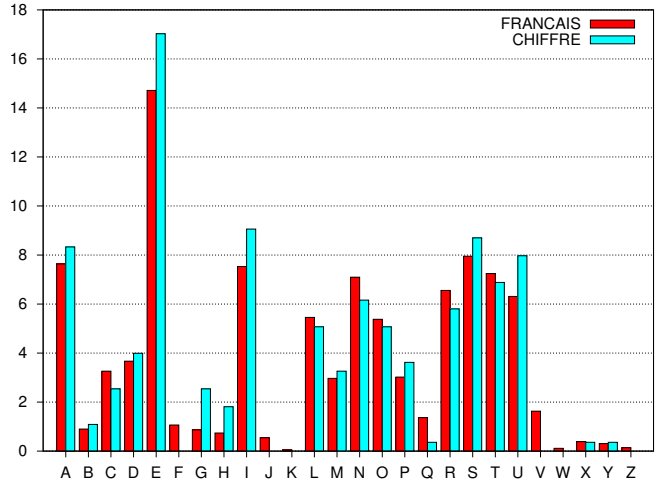
Les distributions ne semblent pas proches






## Attaque par analyse fréquentielle des lettres (3/4)

Mais avec un décalage de 11 vers la gauche on a :






## Attaque par analyse fréquentielle des lettres (4/4)

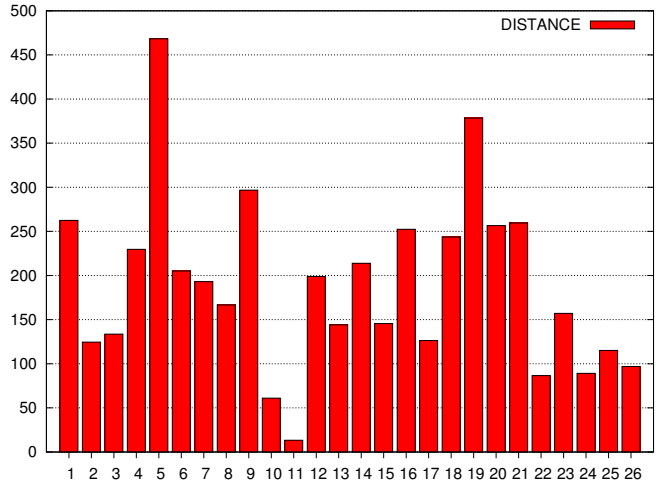
On a alors le text déchiffré suivant :

> Holmes etait assis depuis plusieurs heures silencieusement ; son dos long et mince etait courbe sur un bocal de chimie, dans lequel il melangeait des produits d'une odeur nauseabonde toute particuliere. Sa tete etait penchee sur sa poitrine et il representait, a mes yeux, l'image d'un grand oiseau maigre au plumage gris, a la houppe noire.

Remarque : extrait d'une nouvelle sur les aventures de Sherlock Holmes écrite par Arthur Conan Doyle (1903) et intitulée *Les Hommes dansants* (*The Adventure of the Dancing Men*)

## Pouvons nous trouver le secret par le calcul ?

Oui, en utilisant le calcul d'une distance entre les distributions






## Attaques par force brute

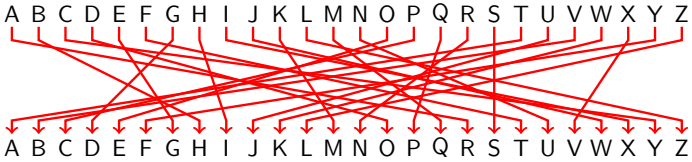
**Principe :** tester toutes les clés possibles

**Limite :** possible que si le nombre de clés possibles est raisonnable

Exemple du chiffrement par décalage de l'alphabet :

seulement 26 clés possibles

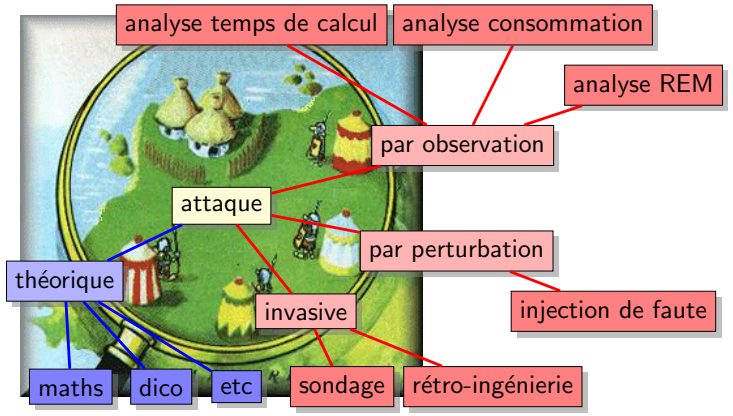
Exemple du chiffrement par permutation des lettres de l'alphabet :




403 291 461 126 605 635 584 000 000 clés possibles



## Quelques types d'attaques

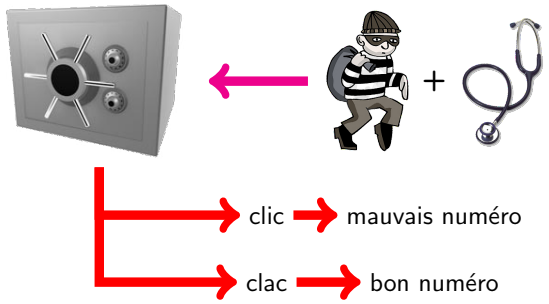



REM = rayonnement électromagnétique



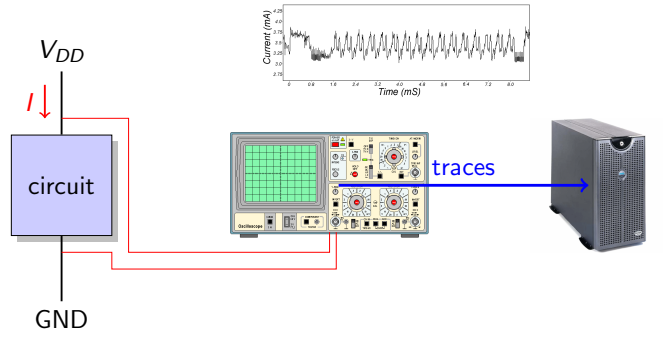
## Attaques par canaux cachés, une nouvelle technique ?

Pas vraiment ! Vous connaissez tous des attaques par canaux cachés...



## Attaque par mesure de la consommation d'énergie

**Principe :** mesurer le courant $I$ qui alimente le dispositif



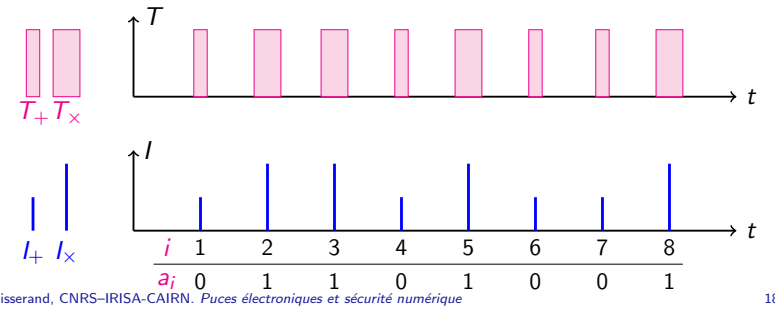

**Notations** : $V_{DD}$ tension d'alimentation (5, 3, 2.5, 1.2 V), GND la masse



## Exploiter les différences

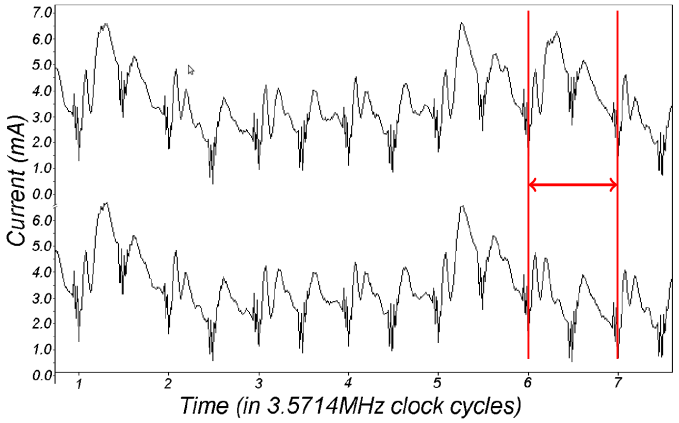
Un algorithme a une signature en courant et en temps de calcul :

```
r = c0
pour i allant de 1 à n faire
  si ai = 0 alors
    r = r + c1
  sinon
    r = r × c2
```






## Analyse simple de la consommation






## Niveau de sécurité

Nombre d'opérations à effectuer pour ≪ casser ≫ le système