Introduction à la Cryptographie

Ludovic Perret

Université Paris VI
ludovic.perret@lip6.fr

Premier Semestre 2009–2010

Plan du cours

Le triptyque de la cryptographie

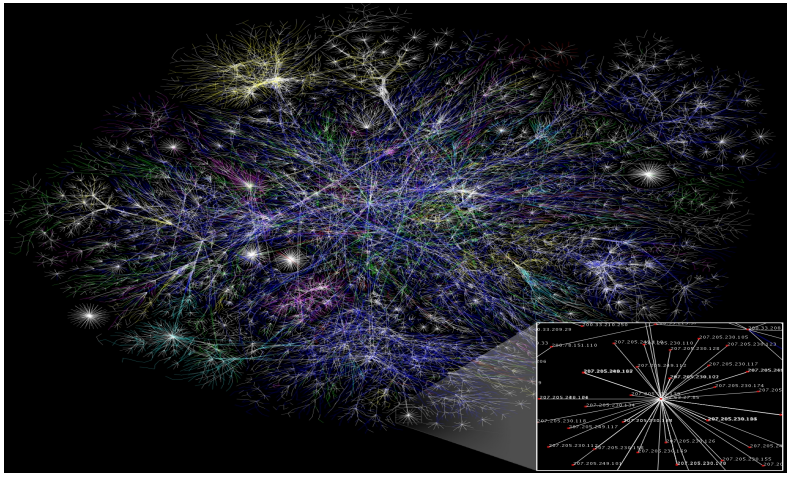
Objectif

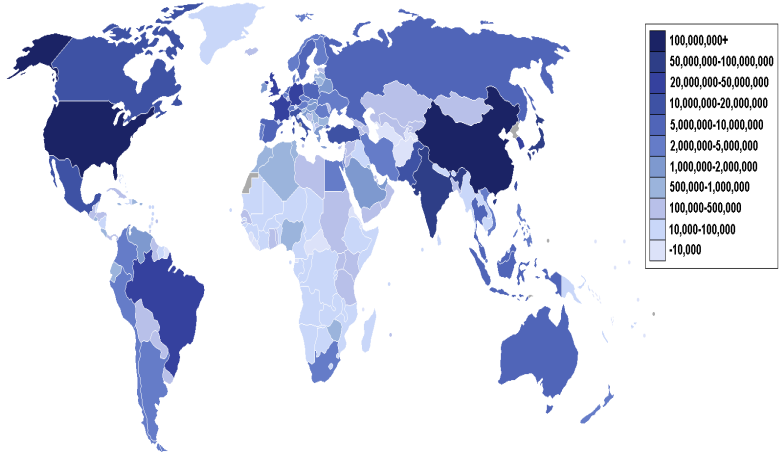
Assurer la « protection » de l'information.

- Confidentialité : garantir le caractère secret de l'information
- authenticité : garantir l'origine de l'information
- intégrité : empêcher la modification de l'information

La Cryptographie : les enjeux

- Militaires/diplomates et grandes entreprises
  - stratégique
  - . . .
- Grand public/internet
  - liberté individuelle (utilisateur)
  - économique
  - . . .





Vocabulaire

- cryptographie, étymologiquement *écriture secrète*, devenue par extension la discipline s'attachant à protéger la confidentialité de l'information.
- cryptosystème : un mécanisme (algorithme) dont l'objectif est de protéger l'information.
- La cryptanalyse est complémentaire de la cryptographie. C'est une discipline s'attachant à évaluer la sécurité des cryptosystèmes.
- cryptologie – *science du secret* – discipline qui englobe la cryptographie et la cryptanalyse.

J. Stern.
"La Science du Secret."
Éditions Odile Jacob (204 pages).

Plan du cours

Les trois périodes de la cryptologie

1. La période artisanal (– fin de la première guerre mondiale)
2. La période mécanique (1919 – 1975)
3. La période scientifique (1976 –)

La scytale

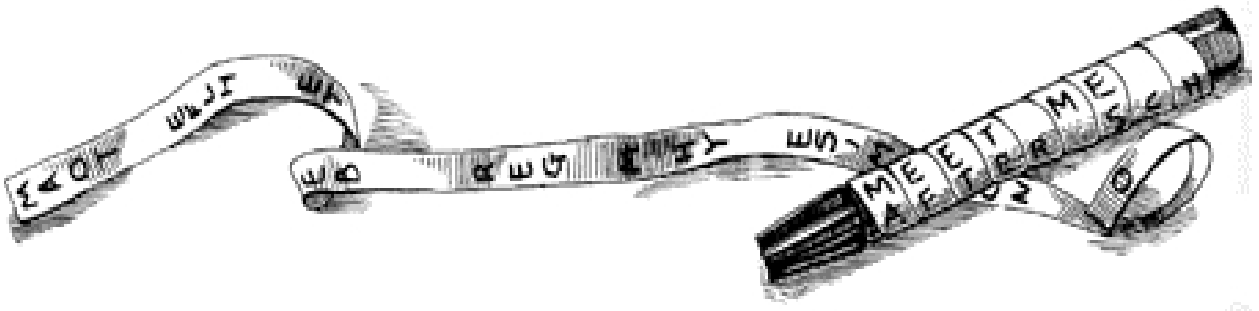
Bâton de bois utilisé pour chiffrer un message. C'est le plus ancien dispositif de cryptographie militaire connue.

Chiffrement (par transposition)

On écrit son message sur toute la longueur de la scytale. On déroule ensuite la bande.

Déchiffrement

Le destinataire enroulera alors cette bande sur son bâton (de même diamètre) pour lire le message clair.



Chiffrement par transposition

Principe

On change la position de chaque lettre du message.

On considère un message $m = m_1 \cdots m_n$ de longeur n

- La clef secrète est une *permutation* sur $\pi : \{1, \ldots, t\}$
- Pour chiffrer, on le divise le message m en blocs M_i de t lettres. On calcule ensuite :

$$c = \underbrace{M_{1,\pi(1)} \cdots M_{1,\pi(t)}}_{C_1} \underbrace{M_{2,\pi(1)} \cdots M_{2,\pi(t)}}_{C_2} \cdots$$

- Pour déchiffrer c, on le découpe en blocs C_i de t lettres :

$$M_{1,\pi^{-1}(1)} \cdots M_{1,\pi^{-1}(t)} M_{2,\pi^{-1}(1)} \cdots M_{2,\pi^{-1}(t)} \cdots$$

Chiffrement par permutation – exemple

La clef secrète est $\pi : (2, 4, 1, 3)$.

$$1 \to 2, 2 \to 4, 3 \to 1, 4 \to 3.$$

Message
HELLOBOB

Cryptogramme
LHLEOOBB

Le chiffrement Atbash (≈ -500)

Le chiffrement Atbash (≈ -500)

Il consiste simplement à inverser l'ordre des lettres de l'alphabet.

- substitution

Remarque

Le mot « **Atbash** »est composé à partir des lettres **A**leph, **t**au, **b**eth et **sh**in, les deux premières et les deux dernières de l'alphabet hébreux.

Troisième Testament, tome III, p. 38,éditions Glénat

Chiffrement par substitution (monoalphabétique)

Principe

Chaque lettre du message est remplacée par une autre lettre de l'alphabet.

On considère un message $m = m_1 \cdots m_n$ de longeur n sur un alphabet $\mathcal{A} = \{A, B, C, \ldots, Z\}$

- La clef secrète est une *permutation* π sur les lettres de $\mathcal{A}$
- Pour chiffrer $m = m_1 \cdots m_n$:

$$c = \pi(m_1) \cdots \pi(m_n).$$

- Pour déchiffrer $c = c_1 \cdots c_n$, on calcule :

$$\pi^{-1}(c_1) \cdots \pi^{-1}(c_n).$$

Exemple

Message

CE TEXTE EST CHIFFRE PAR SUBSTITUTION

$$\begin{pmatrix} A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,P,Q,R,S,T,U,V,W,X,Y,Z \\ D,X,Y,W,V,H,N,A,I,B,T,U,G,S,C,R,O,J,Q,P,E,Z,K,F,M,L \end{pmatrix}$$

Cryptogramme

YV PVFPV VQP YAIHHJV RDJ QEXQPIPEPICS

En route vers la période mécanique

Auguste Kerckhoffs.
La cryptographie militaire.
Journal des sciences militaires, 1883.

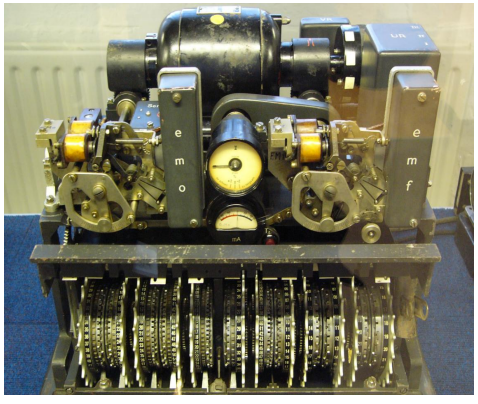
Les principes Kerckhoffs

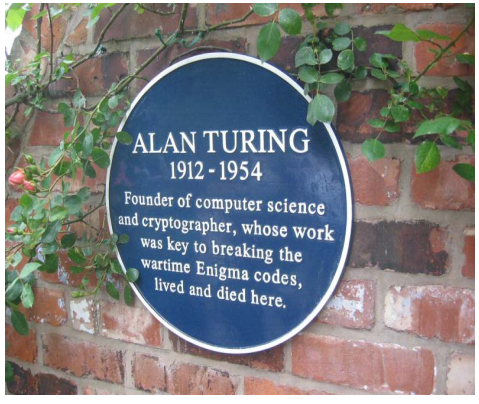
- La sécurité d'une primitive cryptographique ne doit pas reposer sur son caractère secret ; seule la taille de la clé doit suffire à assurer la sécurité.
  - « l'adversaire connaît le système »

La période mécanique

- Machines chiffrante (Enigma, Lorenz)
- premier ordinateur : Collossus

Alan Mathison Turing
(1912 – 1954)





En route vers la période scientifique

Théorie de l'information

« La sécurité se mesure »

C.E. Shannon.
A Mathematical Theory of Communications.
Bell System Technical Journal, 1949.

C.E. Shannon
(1916 – 2001)

Chiffrement de Vernam (1917)

- La clef est une suite de caractères aussi longue que le message à chiffrer.
- Les caractères composant la clef doivent être choisis de manière totalement aléatoire.
- Chaque clef, ou « masque », ne doit être utilisée qu'une seule fois (d'où le nom de masque jetable)

Avantages/Inconvénients

- simplicité du chiffrement/déchiffrement, sécurité théorique absolue
- Difficultés de mise en oeuvre
  - comment produire une clef totalement aléatoire.
  - comment transmettre une clef, comment gérer les clefs

La période scientifique

- 1967 – *The Codebreakers*, David Kahn.
- 1976 – invention de la cryptographie à clef publique par Diffie et Hellman.
- 1977 – Data Encryption Standard (DES)
  - 1973 – National Bureau of Standards création d'un chiffrement standard
- 1978 – RSA (Rivest – Shamir – Adleman) un algorithme asymétrique de crypto. à clef publique