Introduction to (Modern) Cryptanalysis

Maxime Bombar

Introduction and Preliminaries

Quelques mots de présentation

- Maxime Bombar
  `maxime.bombar@u-bordeaux.fr`
- Bureau 382, bâtiment A33 - IMB
- TODO: Site Web du Cours

Il n'y a pas de questions stupides !

Organisation du Cours

- CM les Mardis de 14h à 15h20 - A29 / Salle 104
- TD/TP de 15h30 à 18h20 - A28 / Salle 009
- TP en SageMath: Objectif, amusez vous dans ces TPs.

- Du contrôle continu: 50% de la note
  - Challenges de cryptanalyse ou DS de mi semestre.
  - Projet (implémentation) en seconde moitié de semestre.
- Un examen final (3h) en décembre, sur papier: 50% de la note.

Attention: Modification d'Emploi du Temps

- A priori, pas de cours le Mardi 10 Septembre.
- Décalé au Vendredi 13 (à confirmer ...)

Lectures Complémentaires (Librement Accessibles)

- A. Canteaut - Lecture Notes on Cryptographic Boolean Functions
- A. Canteaut - Lecture Notes on ECC and their Applications to Symmetric Crypto
- D. Boneh, V. Shoup - A Graduate Course in Applied Cryptography
- C. Swenson - Modern Cryptanalysis: Techniques for Advanced Code Breaking.
- Des notes sur la théorie de l'information: Par exemple E. Berardini, G. Zémor.
- Le poly de l'an dernier : G. Castagnos - Cryptanalyse

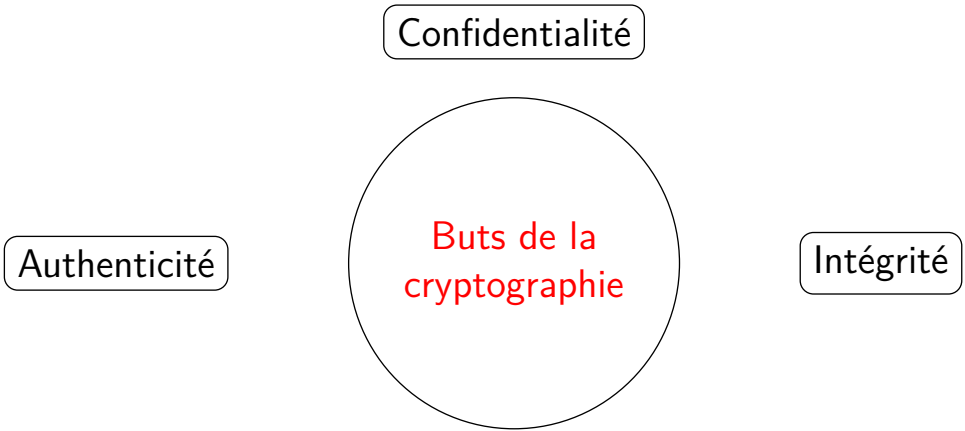
Autres Lectures Complémentaires

- G. Zémor - Cours de Cryptographie
- D. Vergnaud - Exercices et Problèmes de Cryptographie
- A. Joux - Algorithmic Cryptanalysis

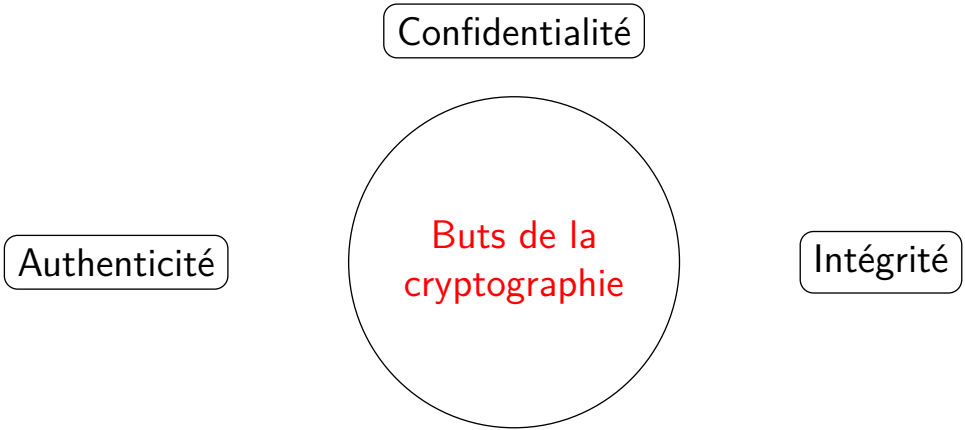
Objectifs du Cours

- Culture générale des techniques modernes en cryptanalyse.
- Développer la capacité de lire de véritables articles de recherche
  $\rightarrow$ Visitez `eprint.iacr.org`.
- Mettre en application ces techniques sur de la crypto “de la vraie vie”
  - Dans ce cours (TP)
  - Dans vos stages
  - Dans vos futurs jobs: Recherche ou entreprise (ou les deux, cf Ciffre)
- Mises en garde:
  - N'implémentez pas votre propre crypto vous même (mais cryptanalyse OK).
  - Plus efficace ne signifie pas forcément plus sûr.

Essence de la Cryptographie

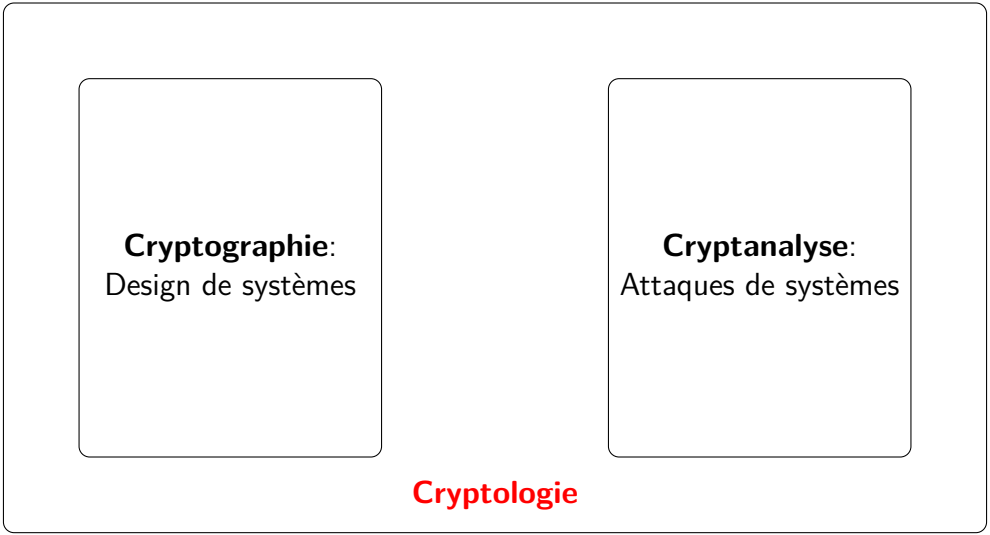


Essence de la Cryptographie

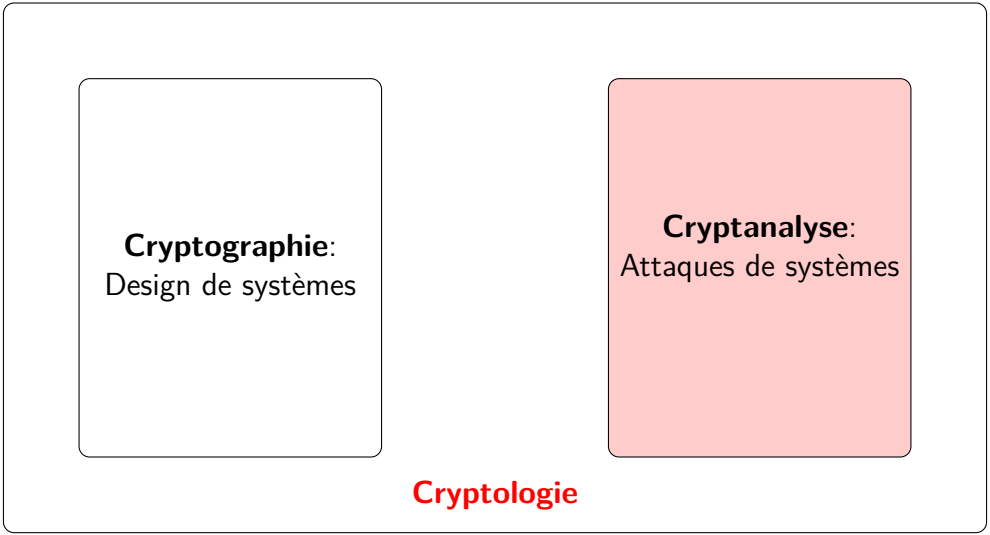


Cryptanalyse: Menacer n'importe quelle de ces propriétés.

Cryptologie



Cryptologie



Cryptologie

Cryptographie:
Design de systèmes

Cryptanalyse:
Attaques de systèmes

Crypto symmétrique

Cryptologie

Réussir en Cryptanalyse (dans la vraie vie)

- La cryptanalyse, c'est difficile.
- Nécessite
  - Du temps et de la persévérance
  - De l'intuition
  - De la pratique
  - De la chance
- C'est probabiliste.

Parfois aussi, une question de perspectives

Parfois aussi, une question de perspectives

Parfois aussi, une question de perspectives

Contenu du cours (tentative)

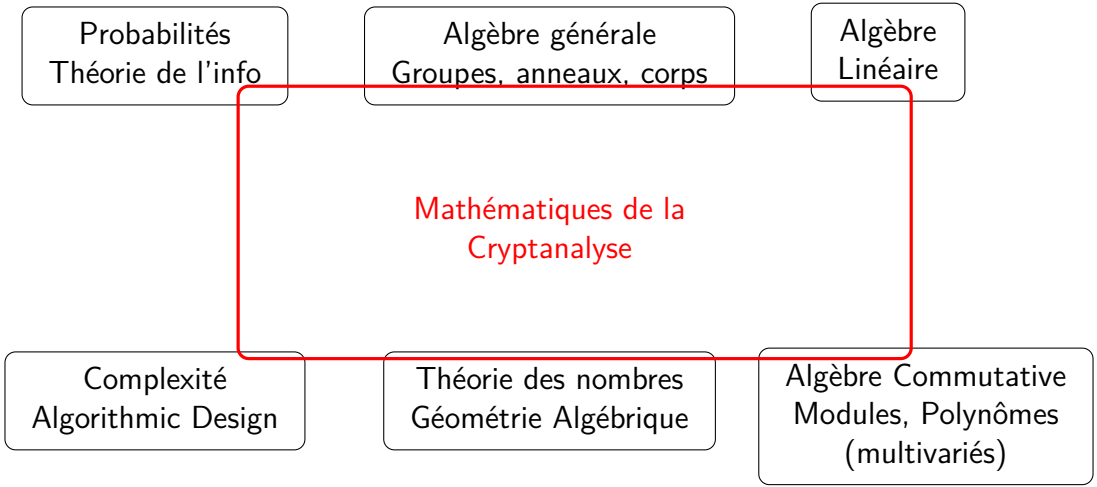
- Chiffrement par blocs
- Chiffrement par flot
- Fonctions de hachage

- Cryptanalyse Linéaire
- Cryptanalyse Différentielle
- Cryptanalyse Algébrique

Attaques sur crypto asymétrique:

- Réduction de réseaux ?
- Fuite d'information dans les signatures ?

Outils Mathématiques



Principe de Kerckhoffs

Auguste Kerckhoffs
(1835-1903)

- L'algorithme du cryptosystème ne doit pas être secret.
  $\rightarrow$ Le cryptanalyste connaît l'algorithme.
- Seule la clé doit être secrète.
  $\rightarrow$ La clé détermine une instance particulière du cryptosystème.

Types de Cryptanalyse

Chiffré Seul
Retrouve la clé ou le clair

Clair Connu
Retrouve la clé à partir de couples *(clair, chiffré)*.
Exemples: Recherche exhaustive, Enigma.

Clairs connus Aléatoires
Retrouve la clé à partir de couples *(clair, chiffré)*, mais où *clair* est aléatoire.

Canaux Auxiliaires
Utilise de l'information supplémentaire (consommation énergétique, injection de fautes...)
cf: UE Cartes à Puces

Cryptanalyse quantique
Shor, Grover
cf: UE Algo Arithmétiques

Rappel: Chiffrement Symétrique

Formellement, couple (E, D)

$$E : \mathcal{M} \times \mathcal{K} \to \mathcal{C}$$

et

$$D : \mathcal{C} \times \mathcal{K} \to \mathcal{M}$$

telle que

$$D_K(E_K(m)) = m$$

Recherche Exhaustive: attaque à clair connu

Attaquant connaît (m, c) et calcule $D_K(c)$ pour toutes les clés K jusqu'à $D_K(c) = m$.

Si $|\mathcal{K}| = 2^n$, recherche exhaustive réussi avec en moyenne $O\left(2^{n-1}\right)$ essais (Exercice).

Grandes Familles de Chiffrement Symétriques

Une sécurité uniquement estimée par la cryptanalyse.

- Chiffrement par substitutions
- Chiffrement par transpositions

Cryptanalyse: analyse fréquentielle, et autres outils statistiques (voir TD).

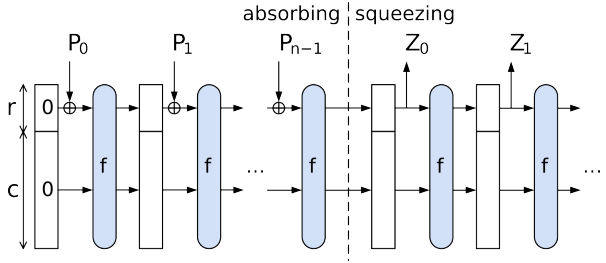
Cryptographie historique

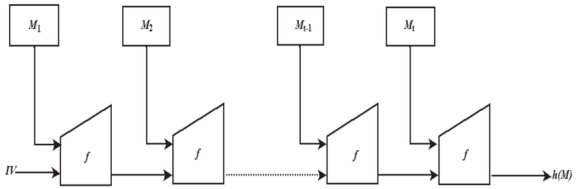
- Chiffrement par blocs (AES)
- Chiffrement par flot (ChaCha20)

Cryptanalyse: Linéaire, Différentielle, Algébrique

Cryptographie moderne

Ne pas oublier





- Fonctions de Hachage
- Cryptanalyse
- Contre-mesures

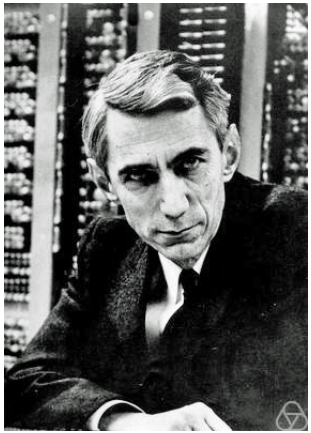
Rappel: Chiffrement à Clé Publique

- **Attaque sur les messages** - Retrouver le texte clair uniquement à partir des données publiques.
- **Attaque sur les clés** - Retrouver une clé secrète à partir des données publiques.

- Idéalement: repose sur des problèmes bien étudiés (Hypothèse Calculatoire) Sécurité Réductioniste (cf UE Crypto Avancée).
- Cryptanalyse et réductions sont deux faces d'une même pièce.

Shannon Theory of Secrecy

Chiffrement Inconditionnellement Sûr ?



Claude Shannon
(1916-2001)

Peut-on construire un chiffrement de sorte que les chiffrés soient indépendants des messages?

Quelle information sur le message est contenue dans le chiffré ?

Rappel: Entropie d'une variable aléatoire

Soit X une variable aléatoire à valeurs dans un ensemble fini $\mathcal{X}$.

Entropie

$$H(X) \stackrel{\text{def}}{=} -\sum_{x \in \mathcal{X}} \mathbb{P}_X(X = x) \log \mathbb{P}_X(X = x) \text{ avec } 0 \times \infty = 0.$$

L'entropie de X est maximale lorsque X est **uniformément distribuée**, et on a alors

$$H(X) = \log |\mathcal{X}|.$$

L'entropie mesure le degré d'incertitude de la variable aléatoire.

Entropie Conditionnelle et Information Mutuelle

Soient X, Y deux variables aléatoires à valeurs dans des ensembles finis $\mathcal{X}$ et $\mathcal{Y}$.

Entropie Conditionnelle

$$H(X \mid Y) \stackrel{\text{def}}{=} -\sum_{x,y} \mathbb{P}(X = x, Y = y) \log \mathbb{P}(X = x \mid Y = y)$$

Information Mutuelle

$$I(X, Y) \stackrel{\text{def}}{=} H(X) - H(X \mid Y)$$

$H(X \mid Y)$ mesure l'incertitude résiduelle que l'on a sur X étant donnée Y.

Système de Chiffrement au Sens de Shannon

Shannon propose une abstraction de système de chiffrement.

Un système de chiffrement pour une variable aléatoire M (le message) est un couple de variables aléatoires (K, C) (respectivement la clé et le chiffré) tel que

- M et K sont indépendantes.
- $H(M|K, C) = 0$

La seconde condition signifie que le déchiffrement est toujours unique.

Chiffrement Parfait

Definition

Un chiffrement (K, C) pour un message M est dit **parfait** lorsque $I(M; C) = 0$ ou de manière équivalente

$$H(M|C) = H(M).$$

Dit autrement, la connaissance d'un chiffré n'apporte aucune information sur la valeur du message original.

Un exemple Pertinent: le Chiffrement de Vernam

Alias: Masque jetable (*One-Time Pad*)

Dans le chifrement One-Time Pad, $\mathcal{M}, \mathcal{K}, \mathcal{C}$ sont identifiés à un même groupe abélien G. Pour une clé $K \in G$, et un message $M \in G$, le chiffré est

$$C = E_K(M) \stackrel{\text{def}}{=} M + K.$$

Prop. Le *One-Time Pad* est un chiffrement parfait.

Condition pour un Chiffrement Parfait

Théorème de Shannon pour le Chiffrement

Si (K, C) est un chiffrement parfait pour un message M, alors

$$H(K) \geqslant H(M)$$

Preuve:

$$\begin{aligned} H(M) &= H(M \mid C) && \text{puisque le chiffrement est parfait} \\ &\leqslant H((M,K)|C) \\ &= H(K \mid C) + H(M \mid (K,C)) && \text{règle de la chaîne.} \\ &= H(K \mid C) && \text{chiffrement au sens de Shannon.} \\ &\leqslant H(K). \end{aligned}$$

Cryptographie en Pratique

- Pour $G = (\mathbb{Z}/2\mathbb{Z})^n$, la condition d'entropie implique que la clé doit être **au-moins aussi longue que le message** pour avoir un chiffrement parfait.
- En pratique, un adversaire est **limité en ressources**.
- Comment estimer la sécurité d'un cryptosystème, étant donné cette limitation ?

Cryptographie en Pratique

- Pour $G = (\mathbb{Z}/2\mathbb{Z})^n$, la condition d'entropie implique que la clé doit être **au-moins aussi longue que le message** pour avoir un chiffrement parfait.
- En pratique, un adversaire est **limité en ressources**.
- Comment estimer la sécurité d'un cryptosystème, étant donné cette limitation ?
  $\rightarrow$ Sécurité calculatoire et **Cryptanalyse** !

Remarque: Le *One-Time Pad* est utilisé en cryptographie dans le **partage de secrets** par exemple.

Remarque 2: Sécurité parfaite ne veut pas dire résistance à la cryptanalyse: OTP est vulnérable à une attaque à clairs connus.

Séance Prochaine: Chiffrement par flot

Idée: Remplacer une clé aléatoire, par une clé **Pseudo-aléatoire**.