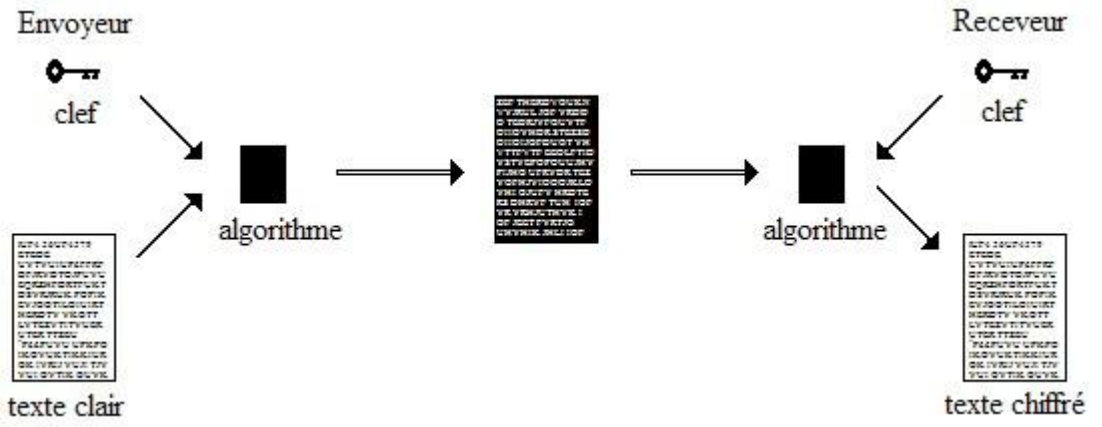
Cryptologie

Faculté des Sciences – Département de mathématique

Denis Longree, Thomas Makkink, Nicolas Roobaert, Chimed Sammut

Introduction

La **cryptologie** est une science divisée en deux branches : la ***cryptographie*** -l'écriture secrète- et la ***cryptanalyse*** -l'analyse des écritures secrètes.



tiré de *THE CODE BOOK* par Simon Singh

Buts de l'exposé

Notre exposé est axé sur trois aspects :

- Un **aspect mathématique** : au travers d'exemples de méthodes de chiffrement et d'attaques sur ces méthodes, nous présentons des concepts mathématiques sous-jacents.
- Un **aspect pédagogique** : nous apportons du matériel pédagogique ainsi que des jeux pour tous âges permettant aux visiteurs de participer de manière active et interactive.
- Nous abordons **les origines** de la cryptologie via une partie historique.

Les Mathématiques en cryptologie

Pour analyser la sûreté d'une méthode de chiffrement, il est utile de commencer par calculer le nombre de ***clés secrètes*** possibles qui peuvent être associées à un ***algorithme*** de chiffrement pour s'assurer qu'un message ne peut être déchiffré simplement en testant toutes les clés possibles.
Si par exemple un message est chiffré par une permutation de ses symboles, le nombre de permutations augmente très vite avec la taille du texte : par exemple, si le texte clair comporte seulement 10 caractères nous avons déjà *3628800* permutations possibles ce qui rend la permutation utilisée difficile à deviner. Nous montrerons comment des **raisonnements combinatoires** permettent de calculer le nombre de clés possibles pour différentes méthodes de chiffrement.

Nous parlerons d'**arithmétique modulaire** et illustrerons son utilité via différentes méthode de chiffrement. Pour *k* et *n* deux nombres entiers positifs, *k modulo n* est le reste de la division euclidienne de *k* par *n*. On a par exemple *6 = 6 (mod 7)* car *6 = 0x7 + 6* mais *8 = 1 (mod 7)* car *8 = 7x1 + 1*. Sur le cadran d'une horloge, lorsque l'heure a avancé, on additionne modulo 12. Par exemple, lorsqu'on est 3h après 11h, il est 2h car *11 + 3 = 14 = 2 (mod 12)*.

Nous parlerons également de **nombres premiers** et du **petit théorème de Fermat**. Un nombre entier positif est dit premier s'il possède exactement 2 diviseurs : par exemple, *7* et *11* sont premiers car ils ne sont divisibles que par 1 et par eux-mêmes ; *4* n'est pas premier car il est divisible par 1,2 et lui-même mais est factorisable en un produit de nombres premiers : 2x2. On peut montrer que chaque entier *k>1* possède une unique factorisation en nombres premiers. Le petit théorème de Fermat énonce que « si *p* est un nombre premier et si *a* est un entier non divisible par *p*, alors $a^{p-1} - 1$ est un multiple de *p* ».

L'**arithmétique modulaire** et le **petit théorème de Fermat** interviennent dans le **chiffrement RSA** qui est une méthode très utilisée pour échanger des données confidentielles sur internet et dont la sécurité repose sur le temps incroyablement long qu'il faut à un ordinateur pour factoriser un grand nombre en un produit de nombres premiers.

Origines de la cryptologie

Même si la cryptologie n'est considérée que depuis récemment comme une véritable science, on en retrouve de nombreuses traces dans les temps anciens.

Le **Kâmasûtra** (écrit aux alentours des VI-VIIèmes siècles PCN) recommande aux amants de communiquer en chiffrant leurs messages pour conserver le caractère intime de leurs conversations.

Bien avant cela Jules César (100-44 ACN) codait des messages par un simple décalage des lettres de l'alphabet connu sous le nom, devenu célèbre, de **code César**. Par exemple, si César voulait chiffrer le texte clair "J'aime le printemps des sciences !" avec une clé 3, le message chiffré serait "M'DLPH OH SULQWHPSV GHV VFLHQFHV!" ; "Un scientifique" deviendrait "FY ESZXLDNZYYZC" avec une clé 11 ; ...

Il suffisait alors à son destinataire, connaissant la clé, d'appliquer le décalage en sens inverse pour pouvoir déchiffrer le message.

Le chiffre César fait partie de la famille des chiffrements dits par ***substitution monoalphabétique*** car chaque lettre de l'alphabet est remplacée par une et une seule autre lettre lors du chiffrement.

Ce type de chiffrement a dominé la cryptographie pendant des siècles jusqu'à l'avènement de la cryptanalyse fréquentielle par Al-Kindi au IXème siècle PCN.

Ce processus permet de retrouver l'alphabet de chiffrement en analysant les fréquences d'apparitions des lettres de l'alphabet dans le message chiffré et en les comparant aux fréquences des lettres dans un long texte : par exemple pour la langue française, on peut exploiter les faits que la lettre « **e** » est celle qui a tendance à apparaître le plus souvent dans un texte et que des mots tels que « **un**, **une**, **le**, **la**, **les** » sont plus fréquents que d'autres mots.

Actualité

Les découvertes en cryptologie font l'objet de beaucoup de convoitises, comme le montre la récente nouvelle de février 2014 qui annonça que l'internationalement célèbre cryptographe belge Jean Jacques Quisquater était surveillé par les cryptanalystes de la **NSA**, intéressés par son travail de cryptographe.