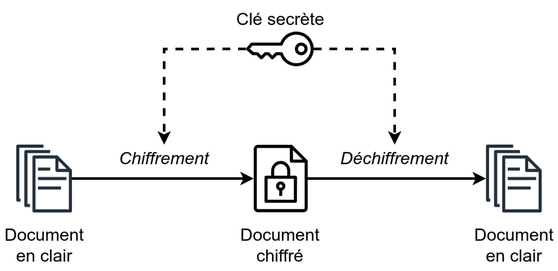
INTRODUCTION À LA CRYPTOGRAPHIE

Antoine Douteau[1]
[1]Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC, 14000 Caen, FRANCE
[1]en thèse dirigée par Adeline Roux-Langlois financée par la région Normandie
antoine.douteau@unicaen.fr

GREYC
Laboratoire de recherche en sciences du numérique

1. Mais qu'est ce que la cryptographie ?

Cryptographie vient des mots en grec ancien *kruptos* signifiant "caché" et *graphein* pour "écrire". C'est l'art de **sécuriser les échanges entre deux personnes**. Contrairement à la stéganographie qui est, elle, une technique de dissimulation totale du message.



On peut considérer la cryptographie comme la manière de **rendre un message impertinent ou inintelligible** pour qui n'est pas de droit.

2. Histoire de la cryptographie ?

On identifie les **premières traces d'utilisation de la cryptographie** vers -1900 en Egypte ancienne utilisant des nouveaux hiéroglyphes :

Le **premier document chiffré** connu est une tablette d'argile contenant une recette datant du XVI^{e} siècle av. J-C retrouvée en Iraq actuel.

L'auteur·e avait supprimé les consonnes des mots et modifié l'orthographe afin de rendre inintelligible sa propre recette. On peut imaginer que le phénomène était répandu dans toutes les civilisations.

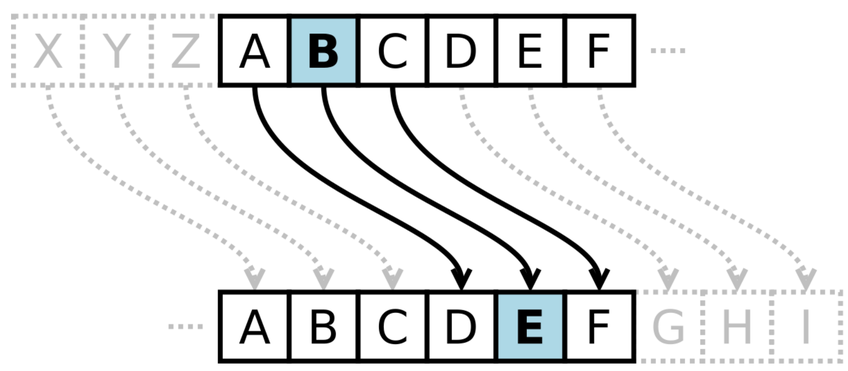
3. Vocabulaire

Comme tout domaine scientifique, la cryptographie a son vocabulaire :

- **clair** : un message est appelé clair ou message clair quand celui-ci est non-dissimulé et devant être transmis,
- **chiffrement** : modification d'un clair en un nouveau message inintelligible pour qui n'est pas de droit, à l'aide d'une clé secrète,
- **chiffré** : un message est chiffré quand on applique un chiffrement servant à modifier le contenu visible du message,
- **déchiffrement** : restitution d'un chiffré en son message initial,
- **clé secrète** : la clé secrète permet de chiffrer et de déchiffrer correctement de manière à pouvoir restituer le bon clair associé à un chiffré.

4. Quelques exemples de chiffrement

Jules César chiffrait ses messages grâce à son propre code :
Le code de César : décalage mono-alphabétique.



Par exemple : $MATHS \xrightarrow{+3} PDWKV$

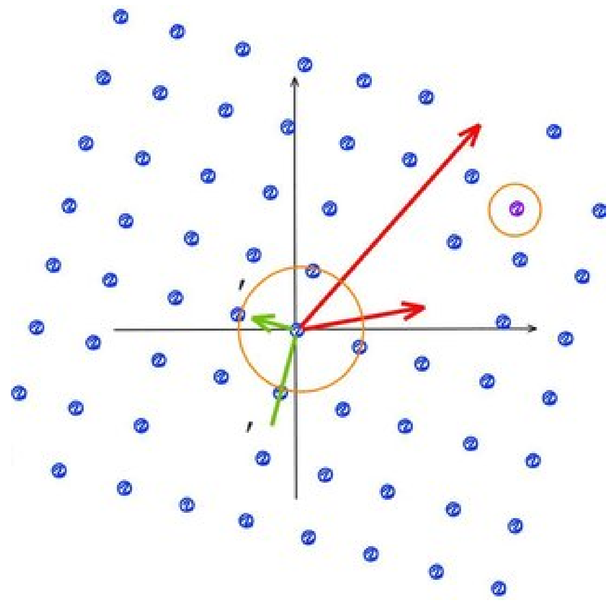
Le clair est $MATHS$, le chiffré est $PDWKV$ et la clé est 3.
Voir l'activité 1.1 sur le chiffrement de César.
Les **activités 1.2** et **1.3** montrent d'autres chiffrements similaires.

Pour que deux personnes communiquent de manière sécurisée, il faut également qu'elles connaissent la même clé pour se comprendre (c'est-à-dire chiffrer et déchiffrer correctement les messages).

L'**Activité 2** permet d'avoir un aperçu de comment cela fonctionne.

5. Au sein du laboratoire GREYC

L'**Activité 3** est une initiation aux **réseaux euclidiens**, un outil mathématique récent où les clés ne seront pas des simples nombres.



Mon travail de recherche consiste en la recherche de nouveaux problèmes mathématiques difficiles ainsi qu'en la construction de nouveaux schémas cryptographiques basés sur les réseaux euclidiens.

Informations

Recommandation de lecture et sources : David Kahn, The Codebreakers.
Icones et images : Wikipedia Commons, icon-icons, et Dr. Ganesh's lattice image.
Activité sur les réseaux reprise de AlKindi 2018.

Initiation à la cryptographie