ACTIVITÉ 3 - RÉSEAUX EUCLIDIENS

Antoine Douteau[1]

[1]Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC, 14000 Caen, FRANCE

[1]en thèse dirigée par Adeline Roux-Langlois

antoine.douteau@unicaen.fr

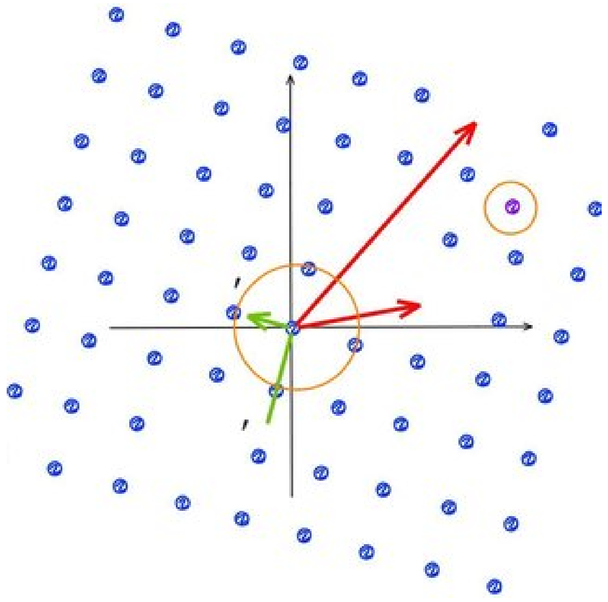


Figure 1: *Un exemple de réseau*

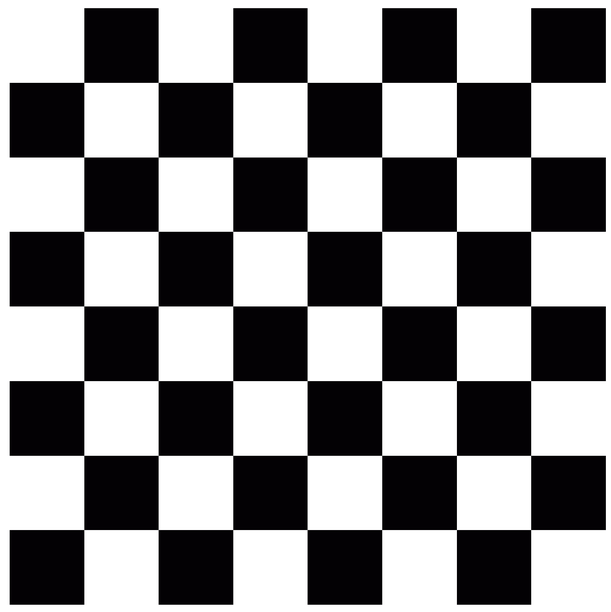


Figure 2: *Un damier : un autre exemple de réseau*

Réseaux euclidiens

Nous avons vu divers schémas de chiffrements lors de l'**activité 1** où les messages clairs étaient des mots utilisant les 26 lettres de l'alphabet. Mais en réalité, on exploite souvent des nombres ou d'autres éléments mathématiques servant à représenter les données.
Un **réseau euclidien** est un outil mathématique qui a deux aspects : un aspect calculatoire et un aspect visuel géométrique.

Un **réseau euclidien** est un ensemble de points, d'objets, ou de cases régulièrement espacés, c'est-à-dire avec une structure visuelle qui se repètent. On peut voir les deux exemples si dessus.

- La première figure représente un ensemble de points disposés avec régularité selon les flèches,
- La seconde représentant un damier UI est un réseau euclidien bien connu où l'on colorie les cases 1 fois sur 2.

Le réseau qu'on utilise est décrit grâce à deux choses : un **"point" initial** et un **"mouvement" de répétition**. Le mouvement de répétition créé de nouveaux éléments à partir du point initial. Puis, on repète l'action de répétition sur les nouveaux points créés et ça de manière infinie. Le mouvement de répétition n'est pas unique par exemple dans la figure 1 les flèches rouges et les flèches vertes vont engendrer le même réseau.

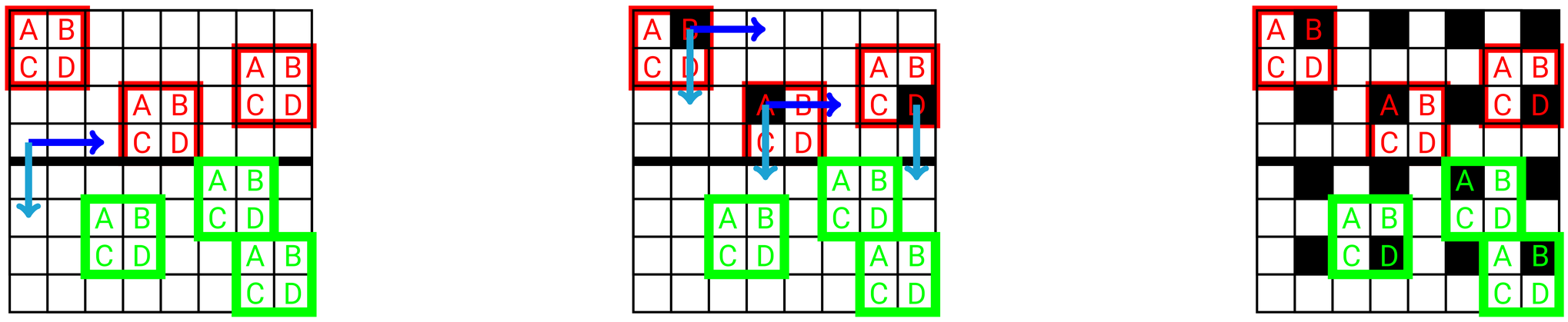
- Pour le premier exemple, le point initial est le point $(0, 0)$, le mouvement répétif est défini avec les flèches créant de nouveaux points. Les flèches sont ensuite répétées sur les nouveaux points créés, etc, etc.
- Pour le damier, notre point initial est que l'on colorie la case la plus en bas à gauche, la répétition est implicitement définie ici. Essayez de la deviner.

Exemple d'algorithme de chiffrement

Afin d'introduire la notion, nous allons premièrement identifier un exemple. Nous allons ici construire des messages de 3 lettres composés de A, B, C ou D grâce à des boîtes positionées dans le damier. Initialisons notre exemple : les boîtes rouges donneront les positions initiales de 3 points grâce à un unique mot. Les flèches bleues représentent le mouvement de répétition. Les boîtes vertes en bas de la feuille définissent notre mot chiffré (ici le chiffré n'est ni un mot, ni un nombre, il s'agit bien de la position des boîtes dans la grille). Afin de déchiffrer le message, il est nécessaire de remplir notre damier de la bonne manière. La clé est donc ici le mouvement répétitif défini par les flèches et le mot initial. L'exemple ci-dessus montre le chiffrement du message DAB.

La difficulté ici va être de colorier le damier de la bonne manière, en effet, sans coloration, le damier est vide (à gauche) et il est impossible de savoir le clair à partir du chiffré.

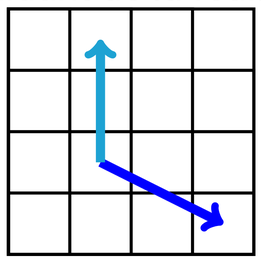
- Le mot initial est BAD, on colorie B dans la première boite, A dans le deuxième et D dans la dernière (comme dans la figure du milieu)
- La coloration est définie par les flèches bleues. On repète en coloriant où pointe la flèche quand elle part d'une case coloriée.
- On repète le processus avec nos nouvelles cases coloriées.
- On remarque bien une fois le réseau complété (à droite) qu'il n'y a qu'une seul possibilité de clair, ici DAB.



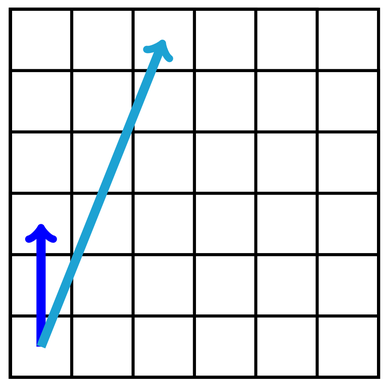
Activité 3

A vous de jouer : déchiffrer les différents messages chiffrés en vous aidant de la feuille plastifiée disponible :

Niveau 1 : Le message initial du réseau est $ABDB$ et la clé utilisée est :

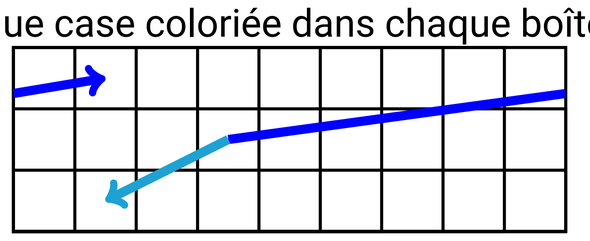


Niveau 2 : Le message initial du réseau est brouillé $A\cdots$ et la clé utilisée est :



Niveau 3 : Vous ne possédez pas le message initial mais vous savez plusieurs informations :

- le demi-boîte visible à droite est vide,
- la partie gauche de la troisième boîte est vide,
- l'intersection entre les deux boîtes à gauche est vide,
- aucune ligne ne peut être totalement coloriée,
- **Rappel :** il y a une unique case coloriée dans chaque boîte rouge et verte,
- la clé est donnée par :



Comment et pourquoi utiliser ça en pratique ?

Comme on le remarque à travers l'activité, plus les flèches sont grandes plus il est difficile de construire notre damier. Mais pourtant, on constate que les damiers coloriés sont identiques bien vous ayez plus rapidement construit le niveau 1. Ce phénomène se produit quand la répétition est la même.

On dit que les flèches sont mauvaises quand elles sont grandes et pointant des directions relativement éloignées.

On utilise les réseaux euclidiens pour les constructions cryptographiques asymétriques (**Voir l'activité 2.2**), on garde les petites flèches pour nous (**clé privée**) et on donne les grandes flèches (**clé publique**) aux personnes souhaitant communiquer avec nous, car grâce aux grandes flèches, l'utilisateur peut judicieusement placer les différentes boîtes vertes, que nous pourrons facilement recolorier grâce à nos petites flèches.

Bien que cet exemple inclue des notions mathématiques, il représente l'idée de ce qui est utilisé actuellement : une paire mauvaises flèches/-petites flèches. À noter que cela peut vous sembler tout le temps facile : cela est du au fait que nous nous basons uniquement sur un damier, mais la même chose se fait dans un cube ou sur des dimensions beaucoup plus grandes $64, 256$ ou encore 1024, rendant le problème pertinent. Il est très difficile avec des grandes flèches de compléter le réseau entier de la meilleure des manières.

La cryptographie post-quantique

Les réseaux euclidiens sont majoritairement exploités pour construire des nouveaux protocoles cryptographiques car ils sont résistants à tout type d'attaque, notamment celles utilisant un ordinateur quantique qui est supposé être plus puissant que l'ordinateur actuel.

Activité sur les réseaux reprise de `challenge AlKindi 2018`..