# 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

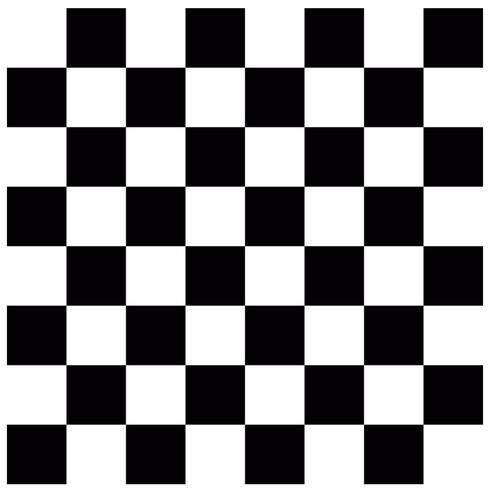


**Figure 1:** *Un damier : un exemple de réseau*

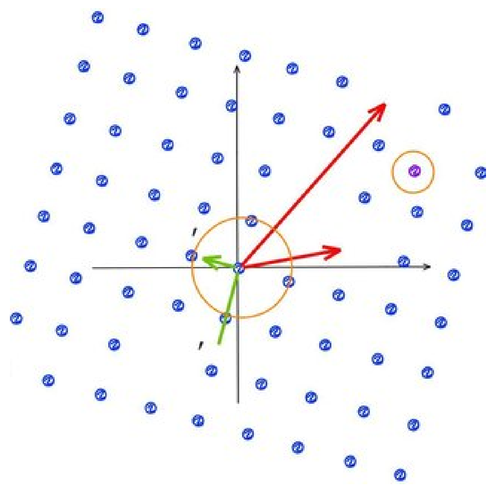


**Figure 2:** *Un autre exemple de réseau*

## Réseaux euclidiens

Nous allons étudier un nouvel outil mathématique assez peu étudié, pourtant facile à comprendre : les **réseaux (euclidiens)**.
Un réseau est un objet mathématique composé d'une structure répétitive, il est à la fois calculatoire et géométrique.

- Les damiers en sont un bon exemple (**Figure 1**), une case sur deux est coloriée en noir. On identifie facilement la structure répétitive.
- Pour les plus matheux, sur un repère orthonormée (**Figure 2**), si on colorie tous les points ayant en abscisse et en ordonnée des nombres relatifs (sans virgule), alors cet ensemble de points est un réseau euclidien car sur chaque axe tous ces points ont le même écart.

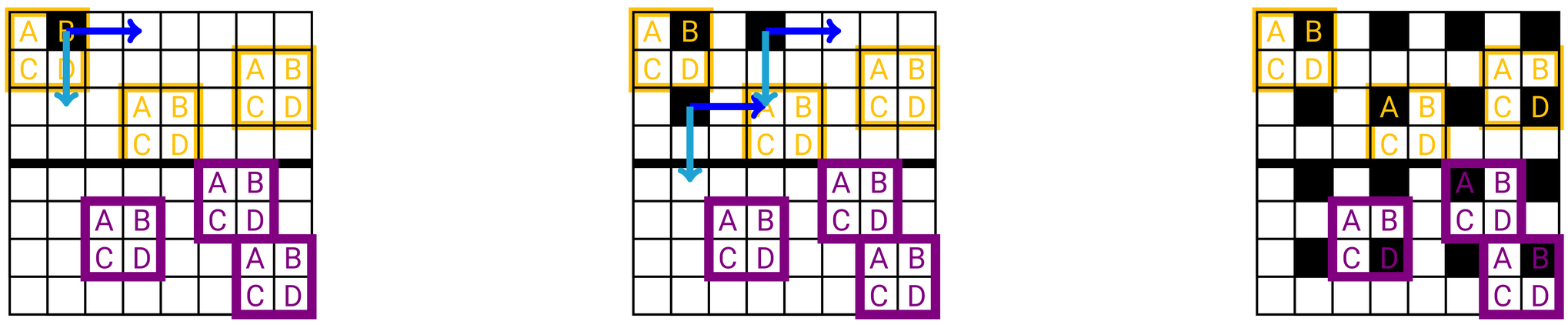
## Exemple d'algorithme de chiffrement

Plus récemment, les cryptographes essayent d'utiliser les réseaux euclidiens pour construire des algorithmes de chiffrements.
Montrons en un exemple, respectant les propriétés suivantes :

- le message clair est un mot de 3 lettres parmi A, B, C et D,
- le message chiffré sera le positionnement des boites (et oui le chiffré n'est pas toujours un message "traditionnel"), ainsi, cela permet de facilement chiffré énormément de message (si le damier est suffisamment grand),
- une case est coloriée par défaut, elle **initialise** notre réseau,
- la structure de répétition sera définie par les flèches bleues, elles seront nos clés de chiffrements symétriques (et de déchiffrements).

Voici un exemple, l'initialisation sera ici de colorier la deuxième case sur la gauche en haut. La clé est défini par les flèches bleues. L'exemple ci-dessous montre deux exemples de chiffrements de deux messages différents.

- On colorie en noir la deuxième case à gauche tout en haut **(étape 1)**,
- La coloration est définie par les flèches bleues. On propage en coloriant où pointe la flèche quand elle part d'une case coloriée **(étape 1)**,
- On repète le processus avec nos nouvelles cases coloriées (à notifier : on peut inverser le sens des flèches) **(étape 2)**,
- On remarque bien une fois le réseau complété (à droite) qu'il n'y a qu'une seule case coloriée dans chacune des boîtes, ici cela forme deux mots $BAD$ et $DAB$ qui était les clairs. **(étape 3)**.

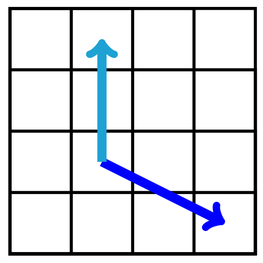



On vient ici de présenter le principe de déchiffrement d'un message : les boîtes étaient déjà placées et il ne vous restait plus qu'à colorier afin de retrouver le message.
Pour chiffrer, le principe est alors inversé, on colorie et on positionne nos boîtes de telle sorte à ce que la seule case coloriée soit la lettre de notre clair.

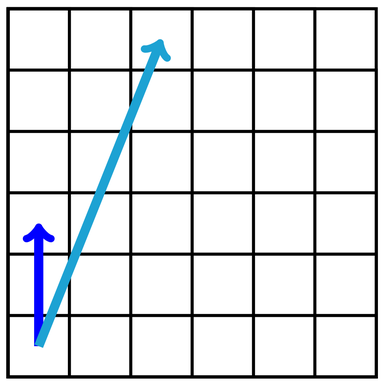
## Activité 3 : Chiffrement symétrique basé sur les réseaux euclidiens

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

**Niveau 1 :** Cette fois-ci, la case initialisée sera la première case en haut à gauche. Utiliser la clé partagée définie par

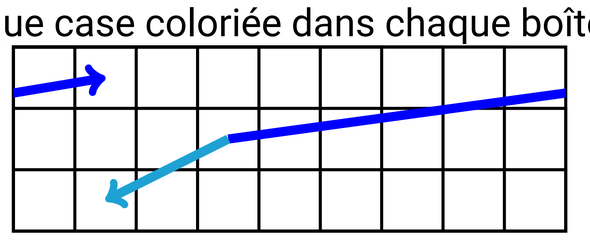


**Niveau 2 :** La case initialisée sera la première case en haut à gauche. Utiliser la clé partagée définie par



**Niveau 3 :** Cette fois-ci, vous ne connaissez pas l'initialisation, cependant vous savez plusieurs informations sur la coloration :

- la 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 avez-vous remarquez quelque chose entre ces 3 niveaux ?

**Les damiers sont identiques !** On dit que les flèches sont mauvaises quand elles sont grandes et pointant des directions relativement éloignées.

En réalité les réseaux euclidiens sont principalement utilisées dans des constructions cryptographiques asymétriques (**Voir l'activité 2.2**) :

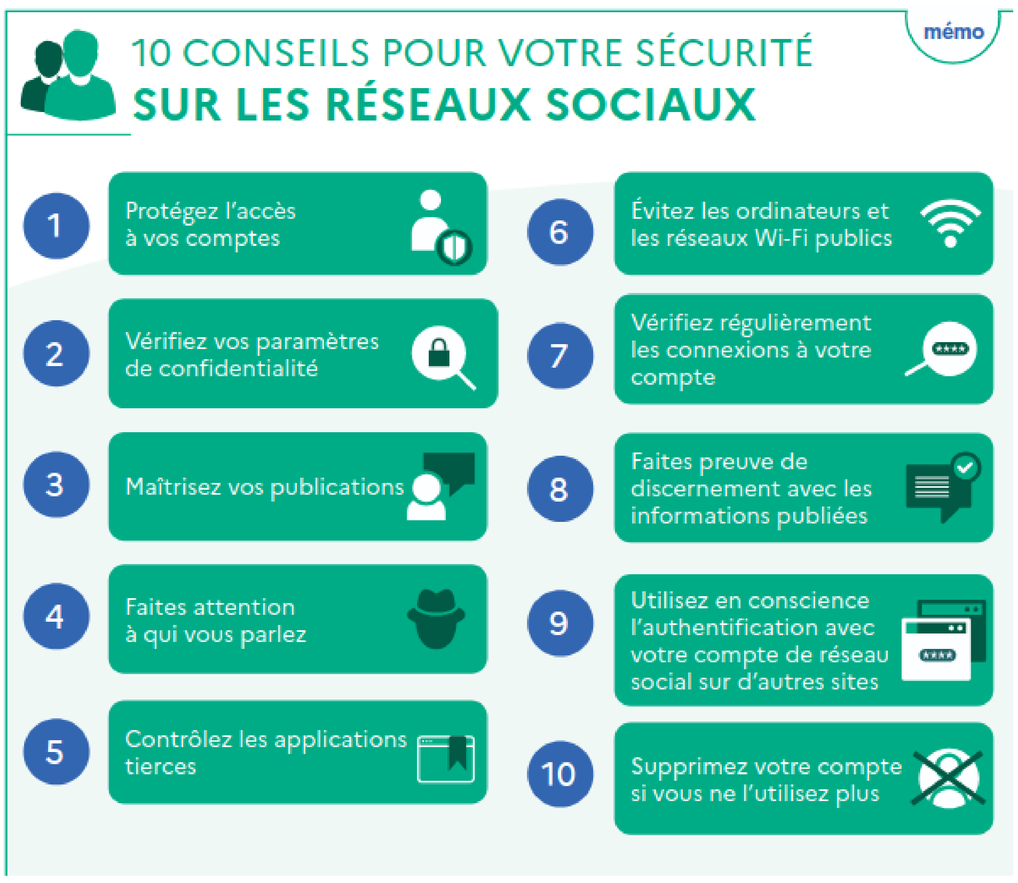
- On garde les petites flèches pour nous en tant que **clé privée**,
- On dévoile les grandes flèches en tant que **clé publique**.
- On ne considère plus que des damiers (cas en $2$ dimensions) mais des constructions dans de grandes dimensions $64, 256$ ou encore $1024$ non inimaginable pour un être humain.

## Contexte scientifique

Il n'est pas évident d'expliquer la pertinence des réseaux sans rigueur mathématique, ni informatiquen mais résumons en grande lignes.

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.
C'est-à-dire que même avec des ordinateurs très puissants exécutant une grande quantité de calculs à la seconde, il n'est pas possible de déchiffrer un message qui ne nous est pas destiné.

## Quelques conseils de cybersécurité :


Activité sur les réseaux inspiré par le `challenge AlKindi 2018`.

Initiation à la cryptographie