ENSEIGNER PAR LA MAGIE...

Aimé LACHAL
aime.lachal@insa-lyon.fr
http://math.univ-lyon1.fr/~alachal

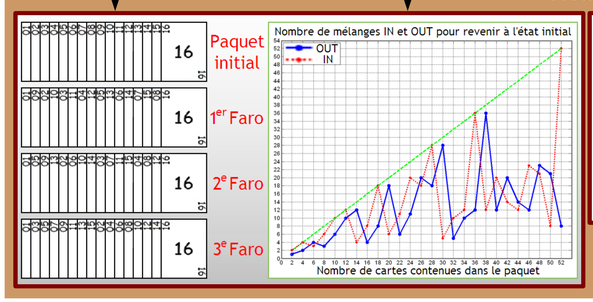
Pierre SCHOTT
magie.carte@laposte.net
http://magiealacarte.free.fr

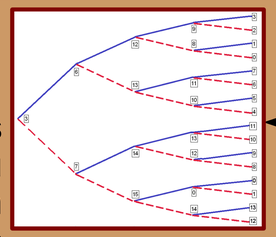
Utilisation du mélange américain (nommé aussi « *riffle shuffle* »)

En réitérant les mélanges FAROs, le jeu reviendra toujours à sa configuration initiale

4 mélanges FAROs OUT pour revenir au jeu initial de 16 cartes

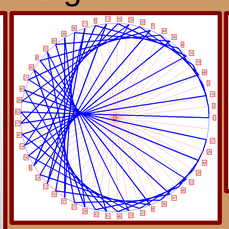
Nombre de mélanges à faire pour revenir au jeu initial en fonction du nombre de cartes



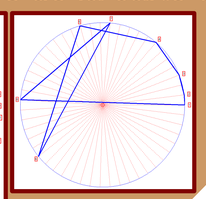


Quelle séquence de mélanges FAROs IN (rouge) et OUT (bleu) pour déplacer la carte de position 3 à une position voulue ?

Positions successives au cours des mélanges FAROs de la carte en position 2



FARO IN



FARO OUT

MATHÉMATIQUES

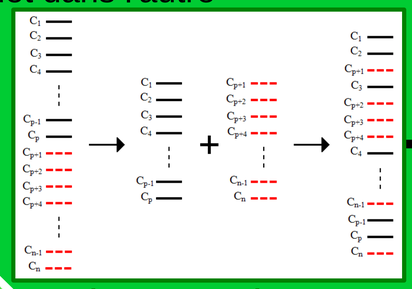
CARTOGRAMIE

INFORMATIQUE

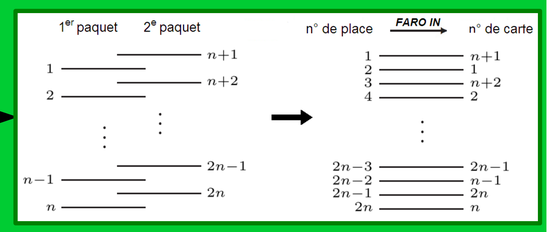
CRYPTOGRAPHIE

Mélanges FAROs « IN » et « OUT »

- Couper le paquet en 2
- Effeuiller chaque paquet pour intercaler de manière aléatoire les cartes d'un paquet dans l'autre



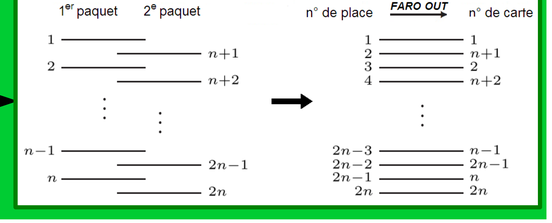
MÉLANGE AMÉRICAIN



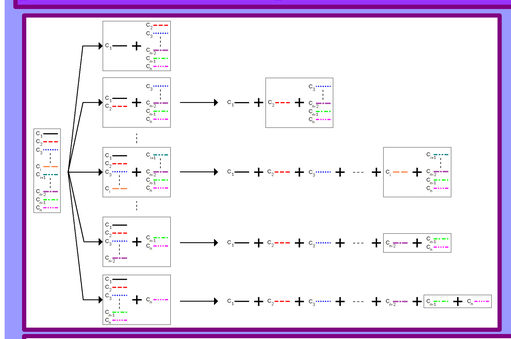
FARO IN

Si chaque carte d'un paquet est insérée entre 2 cartes successives de l'autre, le mélange est appelé FARO

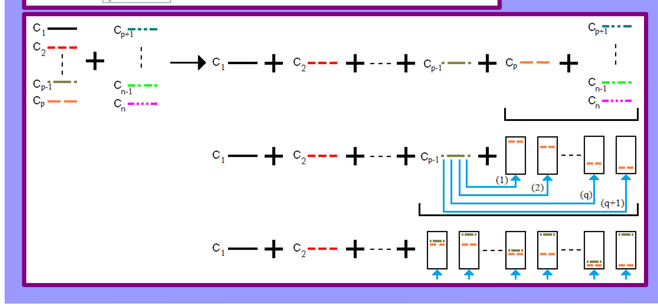
FARO OUT



Trouver tous les paquets mélangés possibles par un mélange américain (ou « riffle shuffle »)

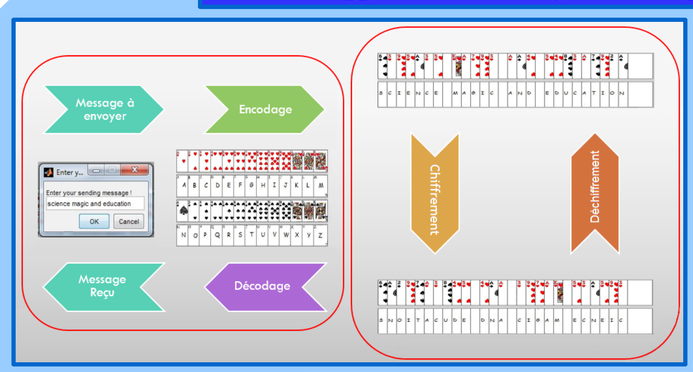


Toutes les coupes possibles.
Pour chaque cas,
appliquer l'algorithme récursif



- **Initialisation :** « décomposer » un des paquets
- **Cœur de la récursivité :** trouver tous les paquets possibles entre une carte et un paquet de *p* cartes
- **Récursivité :** recommencer pour chaque carte le cœur de la récursivité

Chiffrer avec p mélanges FAROs et déchiffrer avec q mélanges FAROs



Procédé simpliste de chiffrement ne reposant que sur l'algorithme des FAROs

Pour améliorer et être plus réaliste, il suffit de partager une clé secrète entre l'émetteur et le récepteur qui définit le nombre de sous-paquets qui seront chiffrés puis réassemblés