Double Blind Permutation

Seconde permutation

- Étant donné un tableau de chiffré partiellement ordonné

$$T = [0,0,2,3,0,5,0,7]$$

- Pour chaque position, on compte le nombre de zéros vus

$$Z = [1,2,2,2,3,3,4,4]$$

- On construit $\sigma = T - Z \pmod{n}$

$$\sigma = (7,6,0,1,5,2,4,3)$$

Double Blind Permutation

Seconde permutation

$$R = [0,\ldots,0];\ Z = 0$$

Pour i de 0 à n:

$$Z = Z + Eq(T_i,0)$$

$$R_i = T_i - Z$$

Retourner R