

# Maple et cryptographie

T.P. n°8

1. Implémenter le système de **permutation par colonne** ; clef : un entier qui indique le nombre de caractères par colonne. Cryptage et décryptage. Test : déchiffrez le message ‘ *Nesevaveyer r*’.



## 2. Chiffrage par ou exclusif

a) écrire une procédure `xor(a, b)` à deux éléments 0 ou 1 qui renvoi  $a \text{ xor } b$

b) écrire une procédure *ToBinaire* qui prend un caractère et qui renvoie l'écriture en binaire de *ToNum* sur 8 bits dans une liste. Exemple  $ToBinaire(a) = [0, 0, 0, 1, 1, 0, 1, 1]$  car

$$\text{ToNum}(a) = 27$$

c) implémenter le codage XOR de la façon suivante :

- entrée : le message (chaîne et la clef (chaîne))
- sortie : liste d'octets en base 10 (entre 0 et 255)
- test : déchiffrer le message [23, 54, 49, 54, 44, 7, 61, 51, 7, 51, 44, 49, 63, 5, 52, 4, 57, 29], clef="Secret"

d) implémenter la version fichier du codage XOR qui chiffre un fichier avec la clef fournie et écrit le résultat dans un fichier de sortie (utiliser la fonction `readbytes`)



### 3. Chiffre linéaire 1-1

a) implémenter le chiffrement linéaire 1-1 lettre par lettre : décoder ' ?'

b) on veut implémenter le chiffrement linéaire 1-1 par blocs de 10 lettres :

- chaque bloc est codé sur 10 x 8 bits : un entier compris entre 0 et  $2^{80}-1$
- la clef doit être inversible modulo  $2^{80}$
- le résultat est une liste de nombre entre 0 et  $2^{80}-1$

Ecrivez une fonction `bloc10` qui prend dix lettres et à l'aide de `ToNum` renvoie un nombre entre 0 et  $2^{80}-1$ .

[illegible]

c) chiffrez 'Ca va bien" avec la clef

```
> k:=nextprime(10^16);
```

```
k := 10000000000000061
```

Par exemple 'TRANQUILLE' donne

[ > 90038561500629239008004 \* k mod (2^80);  
35541504215080681971700

d) Décryptez [538441979703758413314952, 388061783782591839059762] chiffré avec la même clef. Par exemple pour retrouver 'TRANQUILLE' on fait

[ > 35541504215080681971700 / k mod (2^80);  
90038561500629239008004

Mais ensuite il faut écrire ce nombre en binaire sur 80 bits, découper en paquets de 8 bits et retrouver les 10 lettres.

