▶ **MP1 – Maple**
Quatrième TD de maple
Vendredi 11 janvier 2013

Cryptographie et codes correcteurs

1 Codes correcteurs

```
Un code correcteur est une technique de
codage basée sur la redondance. Elle est
destinée à corriger les erreurs de transmission
d'une information (plus souvent appelée
message) sur une voie de communication peu
fiable.                                  -Wikipedia
```

Un premier exemple

Le premier code que nous allons voir est très simple. Il s'agit simplement de tripler chaque bit. 1001 devient 111000000111.

▶ **Question 1** *Sachant que dans le canal de transmission chaque bit transmis a une probabilité ϵ d'être inversé, en utilisant notre code quelle est la probabilité que notre code inverse des bits ?*

▶ **Question 2**
Écrire une fonction code qui prend une liste de 0 et de 1 et code de la façon décrite ci-dessus.

▶ **Question 3** *Écrire une procédure qui prend une liste de 0 et de 1 (de taille divisible par 3) et la décode.*

Code de Hamming (7,4)

Ici, on code les bits 4 par 4. À chaque bloc de 4 bits, on ajoute 3 bits dits de parités. Si les bits sont (x_1, x_2, x_3, x_4) les bits de parités sont (les calculs sont dans $\mathbb{Z}/2\mathbb{Z}$) : $p_1 = x_1 + x_2 + x_4$
$p_2 = x_1 + x_3 + x_4$
$p_3 = x_2 + x_3 + x_4$
Ce code permet de corriger une erreur ou d'en détecter deux.

▶ **Question 4** *Il est facile de trouver une matrice H qui envoie les vecteurs (x_1, x_2, x_3, x_4) sur $(x_1, x_2, x_3, x_4, p_1, p_2, p_3)$. Calculer une telle matrice G.*

▶ **Question 5** *Écrire une procédure qui détermine si 7 bits sont de la forme d'un code de Hamming.*

▶ **Question 6** *On cherche maintenant à décoder. Il existe plusieurs façons mais une simple (bien que jamais employée en pratique) consiste à tester toutes les erreurs possibles. Écrire une telle procédure.*

2 Cryptographie

Création de clés RSA

Alice choisit deux entiers premiers très grands p et q. Elle pose ensuite $n = p \times q$ et $\phi(n) = (p-1)(q-1)$. Dorénavant tous les calculs sont exprimés dans $\mathbb{Z}/n\mathbb{Z}$, n est donc public. Alice choisit e pas trop grand co-premier avec $\phi(n)$, e est appelé **clé publique** de Alice, $d = e^{-1}$ est appelé sa **clé privé**.

Chiffrement

Pour chiffrer un entier $m < n$ que seule Alice peut lire, il suffit de calculer $c \equiv m^e\ [n]$.

Déchiffrement

Pour déchiffrer, il suffit de calculer $m = c^d\ [n]$. En effet $c^d \equiv m^{(de)} \equiv m\ [n]$

▶ **Question 7** *Créer une paire de clés et communiquer, avec un voisin, un message chiffré avec sa clé.*

▶ **Question 8** *Casser ce chiffre revient essentiellement à factoriser le n. À partir de quelles tailles pour n, maple ne réussit pas à factoriser rapidement l'entier ?*

▶ **Question 9** *Comment signer un message avec RSA ?*

2.1 Partage d'information à plusieurs tiers

Voici un algorithme pour diffuser un message à n personnes de sorte que k d'entre elles puissent mais que $k-1$ personnes n'aient aucune information à son propos.
Soit m le message, on choisit $p > m$ premier et $f_1, \ldots, f_{k-1}$ des entiers inférieurs à p. On note alors $F(X) = m + \sum_{i=1}^{k-1} f_i X^i$. On distribue à la personne i le couple $(i+1, F(i+1))$. Par interpolation, k personnes peuvent retrouver le polynôme mais $k-1$ personnes ne peuvent pas car toutes les valeurs pour m sont encore possibles.

▶ **Question 10** *Implémenter un tel crypto-système.*