# Travaux dirigés

18 septembre 2015

Vous trouverez toute la documentation nécessaire sur `http://www.sagemath.org/doc/`.

## 1 Démarrage et arithmétique de base

| | |
|---|---|
| Lancement | `sage` |
| Sortie | `quit` ou `Ctrl c` |
| Interface | `notebook()` |
| Dernier resultat | `_` |
| Chargement | `load` |
| Commentaire | `#` |
| Aide | `?` |

| | |
|---|---|
| `a=5` | `2^4` |
| `A` | S = `10%4` |
| `2==2` | L = `10/4` |
| `2<3` | L = `10//4` |
| `a==5` | T = `gcd(35,22)` |

## 2 Liste et branchement

| | |
|---|---|
| `S = [1,2,3,12]` | `S = [1..12]` |
| `len(S)` | S = `[1,3,..41]` |
| `S[0]` | L = `[1,5]+[3,4,5]` |
| `S[3]` | L = `[0]*12` |
| `S[2] = 5` | T = `range(5,10)` |
| `S.append(18)` | `type(T[0])` |
| `S` | `T[0].is_prime()` |
| `S.extend([4,3])` | `ZZ(T[0])._prime()` |
| `S` | `M = copy(S)` |
| `S[2:]` | `S[:-1]` |
| `18 in S` | `S.index(18)` |
| `S[2:4]` | |

| | |
|---|---|
| `if cond1:` | `while cond:` |
| `  inst1` | `  inst1` |
| `  inst2` | `  inst2` |
| `elif cond2:` | |
| `  inst3` | |
| `  inst4` | |
| `else:` | `for enumeration:` |
| `  inst5` | `  inst1` |
| `  inst6` | `  inst2` |

```
S = [i^2 for i in range(10)]
```

## 3 Types et Structures

| | |
|---|---|
| `QQ` | `factor(p)` |
| `PR.<x> = PolynomialRing(QQ)` | `p.roots(ring=RealField())` |
| `p = x^2-2 # Variante :` | `p(0)` |
| `p = PR([-2,0,1])` | `p.coeffs()` |
| `p.is_irreducible()` | `p[2]` |
| `p.roots()` | `p.degree()` |

| | |
|---|---|
| `A = IntegerModRing(8); A` | `euler_phi(8)` |
| `A.list()` | `a = A(5)` |
| `A.is_field()` | `a.multiplicative_order()` |
| `A.list_of_elements_of_multiplicative_group()` | `a.additive_order()` |

# 4 Cryptography

```
   A = AffineCryptosystem(AlphabeticStrings());
P = A.encoding("Vive le prof")
a, b = (9, 13)
C = A.enciphering(a, b, P); C
```

# 5 Attaque par recherche exhaustive

## 5.1 Vider l'océan avec un dé à coudre

La recherche exhaustive revient à "vider l'océan avec un dé à coudre". On considère qu'un dé à coudre est un cylindre de 1.5 cm de hauteur pour 1.5 cm de diamètre. Selon l'Institut Français des Mers, les océans couvrent 360 millions de $km^2$ avec une profondeur moyenne de 3800 m.

**Q.1** Encadrer entre deux puissances de 2 consécutives le nombre de dés à coudre d'eau que contiennent les océans.

## 5.2 Recherche exhaustive avec un ordinateur

Le facteur de travail d'un algorithme est le nombre d'instructions élémentaires nécessaire à son exécution. La puissance d'une machine est le nombre d'instructions qu'elle exécute par unité de temps. La puissance d'un PC actuel (Intel Core i7 Extreme 965EE) est d'environ 76383 Mips (millions d'instructions par secondes). Le facteur de travail d'un algorithme optimisée pour tester une clé de chiffrement moderne est d'environ 1200 instructions élémentaires pour $n = 128$. On dispose d'un couple clair/chiffrée connu et on désire retrouver la clé utilisée par recherche exhaustive, c'est-à-dire en testant toutes les clés les unes après les autres. Une clé est constituée de 128 bits. On suppose que toutes les clés sont équiprobables.

**Q.2** En combien de temps un Intel Core i7 Extreme 965EE teste-t-il une clé ?

**Q.3** Combien y a-t-il de clés possibles ? Quel est le nombre moyen de clées à tester avant de trouver la bonne ?

**Q.4** Quel est le facteur de travail moyen (en millions d'instructions) pour trouver la clé.

**Q.5** A quel temps moyen de calcul cela correspond-il si on suppose

**Q.5** Meme question que **Q.4** mais avec 100000 PCs.

### 5.3 En intégrant la loi de Moore

> [Gordon Moore 1965] The complexity for minimum component costs has increased at a rate of roughly a factor of two per year (see graph on next page). Certainly over the short term this rate can be expected to continue, if not to increase. Over the longer term, the rate of increase is a bit more uncertain, although there is no reason to believe it will not remain nearly constant for at least 10 years. That means by 1975, the number of components per integrated circuit for minimum cost will be 65,000.

Il est admis que, grâce aux progr'es technologiques permanents, la puissance des machines double en moyenne tous les 18 mois (loi de Moore). On suppose maintenant que l'on change les machines tous les mois (30 jours) en commençant avec une machine d'une puissance de 76383 Mips. Pour tout entier $n$, on note $W_n$ le nombre d'instructions exécutées par la machine du mois $n$.

**Q.5** Quel est le facteur d'amélioration $a$ de la puissance des machines d'un mois à l'autre ?

**Q.6** Calculer $W_0$, puis $W_n$ en fonction de $W_0$, de $a$ et de $n$.

**Q.7** Quel est le temps moyen nécessaire pour trouver la clé ?

## Ordre de Grandeur

| | | |
|---|---|---|
| Masse de l'atome | $10^{-26}$ kilogramme | $2^{-86}$ |
| Diamètre de l'atome | $10^{-10}$ mètre | $2^{-33}$ |
| | | |
| Probabilité de se noyer | 1 chance sur 59 000 | $2^{-16}$ |
| Probabilité d'être tué dans un accident d'automobile | 1 chance sur 5 600 | $2^{-12}$ |
| Âge de la terre | $10^9$ années | $2^{30}$ |
| Âge de l'univers | $10^{10}$ années | $2^{34}$ |
| | | |
| | si l'univers est fermé | |
| duré de vie de l'univers | $10^{11}$ années | $2^{37}$ |
| | $10^{18}$ secondes | $2^{61}$ |
| | | |
| | si l'univers est ouvert | |
| Temps d'ici à la transformation de toute la matière en fer | $10^{500}$ années | $2^{216}$ |
| Temps d'ici à l'absorption complète de toute matière par des trous noirs | $10^{10^{76}}$ années | |
| | | |
| Nombre d'atomes constituant la terre | $10^{31}$ | $2^{170}$ |
| Nombre d'atomes constituant le soleil | $10^{37}$ | $2^{190}$ |
| Nombre d'atomes constituant la galaxie | $10^{67}$ | $2^{223}$ |
| Nombre d'atomes constituant l'univers | $10^{80}$ | $2^{263}$ |

# 6 Cryptographie dans SAGE

Sage dispose de module pour la cryptographie ! Vous allez utiliser la documentation de ce module pour resoudre un certain nombre de challenges :

`http://doc.sagemath.org/pdf/en/reference/cryptography/cryptography.pdf`

Ne vous inquiétez pas non n'avons pas besoin de tout le document : seulement des pages 7 à 47.

## 6.1 Challenge 1

Le texte suivant a été chiffré avec un chiffrement affine. A vous de suivre la documentation pour retrouver le texte clair :

`GOEESJKGWNKOJNFQODMOVIQGDQGMIMINQEIGZWSLQIFWJJOJ`

## 6.2 Challenge 2

Le texte suivant a été chiffré avec une permutation choisit au hasard. A vous de jouer avec sage pour retrouver le texte clair. Pour vous aider, vous risquer d'avoir besoin de comprendre :

— `frequency_distribution()`
— `characteristic_frequency(table_name="beker_piper")`
— ne pas oublier la méthode `replace` des `strings` de `python`.

UGPDLVRSPKXVMYLEDUVWLFDGEFZNXPYLPYEXEXUPKXMJLZBXGFZBZUPLPXUBZWFDDSBYFUBV
ZVMYVKKJZBYFUBVZUGPVLEBZUGBXDFDPLFUGPVLEVMXPYLPYEXEXUPKXBXNPAPSVDPNUGPFD
DLVFYGBXVZFUGPVLPUBYFSSPAPSFZNBXBZUPZNPNUVYVKDSPKPZUUGPULPFUKPZUMVJZNBZX
UFZNFLNTVLQXVZYLEDUVWLFDGEUGPLPFNPUFBSPNXUJNEBXKFNPVMUGPKFZEXUFZNFLNUEDP
XVMYVNPXFZNYBDGPLXFZNVMUGPTFEXVMRLPFQBZWUGPKTPTBSSRPKVLPYVZYPLZPNTBUGUGP
WPZPLFSKFUGPKFUBYFSXULJYUJLPFZNDLVDPLUBPXVMXPYLPYEXEXUPKX