Crypto-analyse élémentaire

Les exercices qui suivent peuvent être résolus avec un papier et un crayon ou à l'aide d'un ordinateur. Votre rapport qui comprendra éventuellement une démonstration à l'ordinateur, doit être rendu le mercredi 16 novembre. Le travail est effectué en binôme. Dans votre rapport vous devez expliquer les méthodes de crypto-anlayse utilisée. Tous les fichiers utiles doivent être envoyés par mèl (avec une description de ces fichiers) à `coulbois@cmi.univ-mrs.fr`.

Dans les exercices 2, 3 et 5 les textes chiffrés sont en français, les accents, les espaces et la ponctuation ont été supprimés. Dans l'exercice 4 on a utilisé le texte codé avec le standard iso-8859-1.

On donne les tables des fréquences (en %) des caractères en français :

E	A	S	I	N	T	R	L	U	O	D	C	P
17,26	8,40	8,08	7,34	7,13	7,07	6,55	6,01	5,74	5,26	4,18	3,03	3,01
M	V	G	F	B	Q	H	X	J	Y	Z	K	W
2,96	1,32	1,27	1,12	1,06	0,99	0,92	0,45	0,31	0,30	0,12	0,05	0,04

Les bigrammes les plus fréquents sont dans l'ordre décroissant :

```
ES DE LE EN RE NT ON ER TE EL AN SE ET LA AI IT ME OU EM IE
```

Les fichiers des textes à déchiffrer sont disponibles à partir de la page :

`http://www.cmi.univ-mrs.fr/~coulbois/2006/crypto/index.html`

Exercice 1. Dans $\mathbb{Z}/26\mathbb{Z}$ on considère les substitutions $f : x \mapsto 5x-10$, $g : x \mapsto 9x+2$ et $h : x \mapsto x^5$.

1. Montrer que f, g et h sont des substitutions.

2. Coder le mot «SECRET» avec f , g et h.

3. Calculer $f \circ g$ et f^{-1}.

Exercice 2. Déchiffrer le texte suivant qui a été crypté par décalage.

```
UFIGV LYXYM DYOHY MZCFF YMYHZ FYOLM
```

Exercice 3. Déchiffrer le texte suivant qui a été chiffré par une substitution affine de l'alphabet. C'est à dire que si on identifie l'alphabet avec $\mathbb{Z}/26\mathbb{Z}$, la substitution est de la forme $x \mapsto ax + b$. On identifiera, a et b et on donnera la substitution affine inverse.

```
GLPKK NVAHR LBALY GRNAN LCLPO OFVWF VAHCN PKKNH VARFP LCNZV
YNGNK PZLON HHNOA FMOPR FANNM FVATV NWNYN ZAVHH NMLHT VNKNY
HNRSK NGNHZ IFHNH TVFYY NGFPO MLHUL PANNH OPYGP CPHPS KNNOT
VNGNH WNVYN HUPKK NHTVP RLYTV NYOGN ANHMN ZOLKL CPNPK KNHHN
UVHHN YOOFV OGVYZ FVMLA ANONN HMLAG NHHZA VMVKN HTVLY GPKHL
BPOGN MKLPH PAHMK VHONY OLONV AHTVN GNHLV ONAML AGNHH VHVYF
ZOFBN YLPAN
```

Exercice 4. le texte suivant a été chiffré par un masque et un ou exclusif. Trouver la longueur de la clé, la clé et déchiffrer le texte.

```
02 0b 52 05 80 10 c8 16 6e 2e 0a 00 06 c9 15 9d 12 74 3f 00
52 0c 9c 44 8b 1a 6e 3c 45 02 02 9a 44 8d 1d 20 20 0a 1c 17
88 0a 9c 53 74 22 10 18 0c 9c 16 9b 5f 20 3d 10 1b 10 c9 20
89 1d 74 a5 16 52 10 8c 0a 9c 1a 74 6d 14 07 44 86 0a c8 1f
65 6d 15 00 06 87 05 81 07 20 3d 04 00 43 85 05 c8 07 ea 39
00 52 06 9d 44 98 12 72 6d 09 17 10 c9 14 81 16 64 3e 45 17
17 c9 15 9d 54 6f 23 45 1e 06 c9 06 89 1f 61 23 82 13 0a 9d
4a e5 79 ab 6d 30 1c 06 c5 44 8c 1a 72 28 0b 06 43 85 01 9b
53 66 22 16 01 0c 90 01 9d 01 73 63 68 78 4e c9 20 8d 06 78
63 68 78 4e c9 30 9a 1c 69 3e 45 53 43 52 69 e2 36 6e 6d 08
98 0e 8c 44 9c 16 6d 3d 16 5e 43 ad 05 86 07 e8 3e 45 01 06
c9 17 8d 1d 74 24 11 52 0f 88 0a 8b 9a 2c 6d 00 1c 43 8c 02
8e 16 74 61 45 16 02 87 17 c8 06 6e 6d 13 1b 07 8c 44 01 1d
6f 3f 08 17 4f c9 10 9a 12 76 28 17 01 02 87 10 c8 1f 65 3e
45 13 0a 9b 17 c8 10 6f 20 08 17 43 9c 0a c8 1c 69 3e 00 13
16 c9 06 84 16 73 3e 8c 5e 43 9d 0b 85 11 61 23 11 5e 43 9d
0b 85 11 61 23 11 52 17 86 11 82 1c 75 3f 16 52 02 9f 01 8b
53 75 23 00 52 8a 99 0b 9d 05 61 23 11 17 43 98 11 81 53 6c
38 0c 52 04 85 05 0f 12 69 39 45 1e 06 c9 07 87 16 75 3f 4b
```

Exercice 5. Déchiffrer le texte suivant qui a été chiffré par une substitution sur l'alphabet.

```
OFHAY GFYGF GQOSR ZAGFL IPAYL FOSPU FIEKS MQSDF FRSMR ZSRIY
KFYGF FYFQM FGUHU FYKAI MJIVI FRFIE PFPFV IUGAY QOFGK OIGLU
BBURU OFGSR AYQFY QFMFY QAIQF SIQMF RZAGF YAYQK AUYQR AIQIP
FLFYL FGUMF MKOIG VIUOG FYAYQ FYVIA UUOYF GQKSG JMSUG FPHOS
HOFVI FQAIG GFQMA PKFYQ PSUGK OIQAQ RFOSQ FPAUD YFVIF OSKIU
GGSYR FLFHU FYXID FMFQL UGQUY DIFMO FJMSU LSJFR OFBSI EVIUF
GQKMA KMFPF YQRFV IAYYA PPFOF HAYGF YGAIO SMSUG AYFGQ YSQIM
FOOFP FYQFD SOFFY QAIGO FGZAP PFGFQ SUYGU VIFOS LUJFM GUQFL
FYAGA KUYUA YGYFJ UFYQK SGLFR FVIFO FGIYG GAYQK OIGMS UGAYY
SHOFG VIFOF GSIQM FGPSU GGFIO FPFYQ LFRFV IFYAI GRAYL IUGAY
GYAGK FYGFF GKSML UJFMG FGJAU FGFQY FRAYG ULFMA YGKSG OFGPF
PFGRZ AGFGR SMRFY FGQKS GSGGF CLSJA UMOFG KMUQH AYPSU GOFKM
UYRUK SOFGQ LFOSK KOUVI FMHUF YOFGK OIGDM SYLFG SPFGG AYQRS
KSHOF GLFGK OIGDM SYLGJ URFGS IGGUH UFYVI FLFGK OIGDM SYLFG
JFMQI GFQRF IEVIU YFPSM RZFYQ VIFBA MQOFY QFPFY QKFIJ FYQSJ
SYRFM HFSIR AIKLS JSYQS DFGUO GGIUJ FYQQA IXAIM GOFLM AUQRZ
FPUYV IFYFB AYQRF IEVIU RAIMF YQFQV IUGFY FOAUD YFYQ
```