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 29 novembre. Le travail est effectué en binôme. Dans votre rapport vous devez expliquer les méthodes de crypto-anlayse utilisées. 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 4 les textes sont en anglais, les espaces et la ponctuation ont été supprimés. Dans l'exercice 5 le texte est en anglais en code ASCII.

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

E	T	A	O	I	N	S	H	R	D	L	C	U
12.702	9.056	8.167	7.507	6.966	6.749	6.327	6.094	5.987	4.253	4.025	2.782	2.758
M	W	F	G	Y	P	B	V	K	J	X	Q	Z
2.406	2.360	2.228	2.015	1.974	1.929	1.492	0.978	0.772	0.153	0.150	0.095	0.074

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

`TH HE IN EN NT RE ER AN TI ES ON AT`

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

`http://www.cmi.univ-mrs.fr/~coulbois/2007/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. Décrire les substitutions $f \circ g$ et f^{-1}.

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

`XEDDYIEYJGKYCQBOFUDIU`

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.

```
ONCHF GAXBR DJFZG GAXNA HGAFS GFCCJ FDQYB AFSFM XSFGA FXSRA
DSYBD CCZDS FAHTA DQYAD SYGXR CHJKD QYGAF ECDRF YFDGA RXQZH
YFSHQ TBAXG AXNDS GHMDQ PXMJP VHQZJ FQMHQ YGAFF AFSFS XJFXB
HGACX UFZCH TAGBH QTZYH YHXFS EFSRA GAFZF BDCCZ MXSZG XQPCH
JHGZR DQQXG AXCYC XUFXN GDQYB ADGCX UFRDQ YXGAD GYDSF ZCXUF
DGGFJ EGGAF SFMXS FGAPV HQZJF QDSFQ XCFGG XJF
```

Exercice 4. Déchiffrer le texte suivant qui a été chiffré par une substitution sur l'alphabet.

```
BVBFM NOHXN CIEXB MEIQM WOZBH EOGBI FYKIF ROCYI FYZIK OHWWM
IMBWN IVBZI CCBFO EKIRZ ICCPF MOMNB XEPGO ZMNBX BWMIG OIFYI
CCMNB OYPOH WIGGI EIMHW OZFIJ PEHCB UBWNI CCFOM ZCIXO EZIPC
UBWNI CCXOO FMOMN BBFYU BWNIC CZPXN MPFZE IFQBU BWNIC CZPXN
MOFMN BWBIW IFYOQ BIFWU BWNIC CZPXN MUPMN XEOUP FXQOF ZPYBF
QBIFY XEOUP FXWME BFXMN PFMNB IPEUB WNICC YBZBF YOHEP WCIFY
UNIMB VBEMN BQOWM KIRLB UBWNI CCZPX NMOFM NBLBI QNBWU BWNIC
CZPXN MOFMN BCIFY PFXXE OHFYW UBWNI CCZPX NMPFM NBZPB CYWIF
YPFMN BWMEB BMWUB WNICC ZPXNM PFMNB NPCCW UBWNI CCFBV BEWHE
EBFYB EIFYB VBFPZ UNPQN PYOFO MZOEI KOKBF MLBCP BVBMN PWPWC
IFYOE ICIEX BGIEM OZPMU BEBWH LAHXI MBYIF YWMIE VPFXM NBFOH
EBKGP EBLBR OFYMN BWBIW IEKBY IFYXH IEYBY LRMNB LEPMP WNZCB
BMUOH CYQIE EROFM NBWME HXXCB HFMPC PFXOY WXOOY MPKBM NBFBU
UOECY UPMNI CCPMW GOUBE IFYKP XNMWM BGWZO EMNMO MNBEB WQHBI
FYMNB CPLBE IMPOF OZMNB OCY
```

Exercice 5. 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.

```
12 0b 05 59 01 64 58 69 25 0b 07 4b 2c 2b 23 0a
38 0b 1a 13 2c 2b 5b 73 61 1e 0c 50 51 4d 4b 20
20 1c 0c 1f 4b 54 5d 74 61 1e 06 5a 4c 52 23 0a
36 0b 4e 4d 44 01 17 30 64 4e 04 5a 55 40 5e 68
2e 1c 64 35 56 48 5a 68 61 0f 49 53 44 40 40 6e
24 1d 1a 1f 4e 47 0e 6d 24 0f 07 56 4f 46 23 0a
20 1e 19 4d 4e 40 4d 68 28 00 0e 1f 49 58 5e 65
33 43 0d 56 52 55 47 6c 2d 0f 1d 56 4e 4f 23 0a
20 00 0d 1f 4e 4f 4d 65 61 1b 19 50 4f 01 4f 20
35 07 04 5a 2c 2b 59 65 61 19 0c 4d 44 01 43 6f
2e 00 1a 57 48 4f 4b 0d 4b 1c 1c 4c 49 48 40 67
61 0a 06 48 4f 01 5a 68 24 4e 1d 57 53 4e 4f 74
61 01 0f 1f 40 01 49 69 33 0f 0f 59 44 2c 24 79
24 1d 45 1f 53 54 5d 68 28 00 0e 1f 45 4e 59 6e
61 1a 01 5a 01 4d 41 6e 26 4e 01 5e 4d 4d 59 61
38 63 63 5b 44 52 5e 69 35 0b 49 48 49 40 5a 20
35 06 0c 1f 51 0f 4f 2e 61 0f 07 51 4e 54 40 63
24 03 0c 51 55 01 5d 61 38 1d 64 35 58 44 5d 2c
61 1c 1c 4c 49 48 40 67 61 0a 06 48 4f 01 5a 68
24 4e 05 50 4f 46 0e 73 35 0f 00 4d 52 2c 24 77
28 1a 01 1f 55 49 4b 20 36 06 00 4c 4a 44 57 20
2e 08 49 5a 55 44 5c 6e 28 1a 10 32 2b 47 4b 72
2c 0b 07 4b 44 45 0e 61 2f 0a 49 5b 48 52 5a 69
2d 02 0c 5b 2c 2b 5a 6f 61 0b 00 58 49 55 4b 65
2f 4e 04 56 4f 54 5a 65 32 63 63 5d 54 53 40 69
2f 09 49 5b 4e 56 40 20 2e 1b 1b 1f 55 49 5c 6f
20 1a 1a 32 2b 45 41 77 2f 4e 1d 57 44 01 46 61
2d 02 64 35 45 4e 59 6e 61 1a 01 5a 01 52 5a 61
28 1c 1a 32 2b 48 40 20 20 4e 0b 4a 48 4d 4a 69
2f 09 49 4c 4e 01 5a 61 2d 02 64 35 55 49 4f 74
61 07 1d 1f 56 48 42 6c 61 0f 05 48 40 58 5d 20
```