Master 1ère année
Initiation à la Cryptographie

Travaux Dirigés

Cryptanalyse des Chiffrements « antiques »

Exercice 1 : Décrypter le message suivant :
« OJQEFJGZJMXBTMNQFJPQOMXQ »
(indications : méthode de César mais pas la même clé, caractère espace mal codé)

Exercice 2 : Décrypter le chiffré suivant, obtenu par substitution monoalphabétique, sachant que le caractère espace n'est pas chiffré ni la ponctuation :

FSCALS WLOFCKLTW OL VAUULSATV WLBTL O'ASBLDKANFKAZSD DZCAFULD LK LCZSZ-
VAJTLD VARFLU GUZVRBADK LDK CZSKFCKL PFW ILSWAR BFSNLW PFKWAFWCIL O'TS
PTADDFSK NWZTPL ASOTDKWALU YFVAUAFU PZTW WLUFSCLW TSL LSJTLKL FGFS-
OZSSLL OLPTAD 40 FSD DTW UF OADPFWAKAZS OL DF SALCL IFWWALK.

Les fréquences d'apparition des lettres sont les suivantes (en pourcentage):

=13.483	L=12.360	A=8.614	F=7.865	S=7.865	W=6.367	D=5.618	K=5.243
T=4.869	U=3.745	Z=3.745	C=3.371	O=3.371	P=2.622	V=2.247	B=1.498
I=1.124	N=1.124	R=1.124	'=0.749	G=0.749	J=0.749	Y=0.375	.=0.375
4=0.375	0=0.375						

Exercice 3 : [Indice de coïncidence]

1. Calculer l'indice de coïncidence théorique d'un texte en français selon la répartition des lettres donnée au verso de cette feuille.
2. Calculer l'indice de coïncidence théorique du texte de l'exercice précédent.
3. Calculer l'indice de coïncidence mutuelle entre un message théorique (dont les occurences d'apparition des lettres sont conformes à la répartition théorique) et
   a) d'un message clair : « il est rapide meme tres rapide »
   b) du message précédent chiffré par César.

   Déterminer ainsi une méthode de déchiffrement automatique du chiffrement par décalage.

Exercice 4 : Décrypter le message suivant (Chiffrement de Vigenère).

```
VIQLPCCILMSPOZCBXQVIQCIGQPCCHCTEZVSLNWYMGSOMJVEGOR
RVLGBSLNIJVICXPCEVNYXNKGGPMOEISXXYCHCFSGHHMSWCKYVM
VGKMRFIPCPCCWGVPMXWQSHMEGCWILDUSSPLOJYEXNKWBKYRBIQ
WYQSUSOW
```

Calculer la longueur de la clé utilisée.
Calculer les différents décalages entre les alphabets ou le décalage de chaque alphabet.
Quel est le message? Quelle est la clé utilisée?

Exercice 5 : On suppose que l'on connaît l'algorithme utilisé : il s'agit d'un chiffrement par transposition.

1. Quel principe la phrase précédente illustre-t-il?
2. Que pensez-vous d'une attaque par analyse fréquentielle?
3. Décrypter le message suivant : `NVPUEEOASIRNSOLESAL`

Référence : Extrait de `http://pedroiy.free.fr/alphabets/frequence.htm`

Fréquence des lettres dans la langue française
exprimé en pourcentage du nombre total de lettres

E	17.76	O	5.34	B	0.80
S	8.23	D	3.60	H	0.64
A	7.68	C	3.32	X	0.54
N	7.61	P	3.24	Y	0.21
T	7.30	M	2.72	J	0.19
I	7.23	Q	1.34	Z	0.07
R	6.81	V	1.27	K	0.00
U	6.05	G	1.10	W	0.00
L	5.89	F	1.06		

Dans la langue française, hormis la fréquence des lettres, l'espace entre les mots dans un texte compte pour 17,4 %. Le pourcentage de voyelles est de 44 %.

Fréquence des bigrammes de lettres doublées dans la langue française
fréquence d'apparition sur 10.000 bigrammes (sur un texte à chiffrer sans espaces et ponctuation)

SS	73	MM	20	AA	3
EE	66	RR	17	UU	3
LL	66	PP	16	II	2
TT	29	FF	10	GG	1
NN	24	CC	8		

Ces bigrammes sont toujours précédés d'un voyelle. Ils sont toujours suivis d'une voyelle ou des consommes R ou L.

Fréquence des bigrammes de lettres non-doublées dans la langue française
fréquence d'apparition sur 10.000 bigrammes

ES	305	TE	163	OU	118	EC	100	EU	89	EP	82
LE	246	SE	155	AI	117	TI	98	UR	88	ND	80
EN	242	ET	143	EM	113	CE	98	CO	87	NS	79
DE	215	EL	141	IT	112	ED	96	AR	86	PA	78
RE	209	QU	134	ME	104	IE	94	TR	86	US	76
NT	197	AN	30	IS	103	RA	92	UE	85	SA	75
ON	164	NE	124	LA	101	IN	90	TA	85	SS	73
ER	163										

A noter, que les bigrammes, constitués par deux consommes, les plus fréquents sont : NT (197) TR(86) NS(79) ST(61).

Ceux constitués de deux voyelles fréquentes sont : OU(118) AI(117) IE(94) EU(89) UE(85) UI(68) AU(64) OI(52) IO(49)