TP1-CRYPTOGRAPHIE CLASSIQUE

EXERCICE 1 : CHIFFREMENT DE CESAR

Décrypter le texte suivant qui a été obtenu en appliquant le chiffrement de César sur un texte en langue française dans lequel les espaces ont été supprimées :

```
Aeysaeo mo nodksv xo dyemro ox kemexo wkxsobo ke pyxn wowo no mo aeo xyec
kfyxc k bkmyxdob, sv x'ocd zoed-odbo zkc sxedsvo, xo ped-mo aeo zyeb odbo
ohkmd ox dyed, n'sxnsaeob sms voc lbesdc od voc zbyzyc aes kfksoxd myebe
ceb cyx mywzdo ke wywoxd ye sv odksd kbbsfo nkxc vo nsymoco.
```

Remarque : voici la fréquence des lettres en langue française :

a	b	c	d	e	f	g	h	i	j	k	l	m
8,46	1,02	3,21	3,78	17,60	1,11	1,12	1,07	7,40	0,48	0	6,05	2,70
n	o	p	q	r	s	t	u	v	w	x	y	z
6,38	5,19	2,68	1,21	6,56	7,56	7,26	6,63	1,65	0	0,03	0,03	0,01

EXERCICE 2 : ENIGMA

1. De quel type de chiffrement est la machine Enigma ?
2. Calculer le nombre de clés possibles dans une machine Enigma avec choix parmi cinq rotors et qui utilise six fiches.
3. Quelles sont les techniques de cryptanalyse qui ont permis de casser le chiffrement d'Enigma.

EXERCICE 3 : CRYPTANALYSE DU CHIFFRE DE VIGENERE

Le chiffrement de Vigenère est un système de substitution poly-alphabétique élaboré par B. de Vigenère en 1586. Ce procédé de chiffrement repose sur l'utilisation périodique de plusieurs alphabets de substitution déterminés par la clé (en général un mot). Pour pouvoir chiffrer un texte clair, à chaque caractère nous associons une lettre de la clé pour effectuer le décalage correspondant comme dans le chiffrement de César. Exemple :

Clair	C	H	I	F	F	R	E	D	E	V	I	G	E	N	E	R	E
Clef	B	A	C	H	E	L	I	E	R	B	A	C	H	E	L	I	E
Décalage	1	0	2	7	4	11	8	4	17	1	0	2	7	4	11	8	4
Chiffré	D	H	K	M	J	C	M	H	V	W	I	I	L	R	P	Z	I

1. Chiffrez le texte suivant avec le chiffre de Vigenère en utilisant le mot-clef "SECURITE":

```
« Introduction a la cryptographie appliquee »
```

Si la longueur de la clé est connue, retrouver le texte clair à partir du texte chiffré peut se faire en appliquant une cryptanalyse du chiffrement de César. La difficulté pour le cryptanalyste consiste donc à retrouver la longueur de la clé.

La première méthode pour déterminer la longueur de la clé est connue sous le nom de test de Kasiski (d'après F.W. Kasiski). Elle repose sur le fait que si deux groupes de lettres (ou polygrammes) du chiffré sont égaux alors il s'agit probablement du même polygramme dans le texte clair chiffré avec la même partie de la clé. La taille de l'intervalle qui sépare ces deux polygrammes identiques dans le chiffré sera donc, dans la majorité des cas, un multiple du nombre de la longueur de la clé. S'il y a plusieurs répétitions de polygrammes, le plus grand diviseur commun des distances les séparant est très probablement la taille de clé.

2. Le texte suivant a été obtenu en appliquant le chiffrement de Vigenère sur un texte en langue française dans lequel les espaces ont été supprimées :

```
ZBPUEVPUQSDLZGLLKSOUSVPASFPDDGGAQWPTDGPTZWEEMQZRDJTDDEFEKEFERDPRRCYNDGLUAOW
CNBPTZZZRBVPSSFPASHPNCOTEMHAEQRFERDLRLWWERTLUSSFIKGOEUSWOTFDGQSYASRLNRZPPDH
TTICFRCIWURHCEZRPMHTPUWIYENAMRDBZYZWELZUCAMRPTZQSEQCFGDRFRHRPATSEPZGFNAFFIS
BPVDBLISRPLZGNEMSWAQOXPDSEEHBEEKSDPTDTTQSDDDGXURWNIDBDDDPLNCSD
```

- Utiliser le test de Kasiski pour déterminer la longueur de la clé utilisée et décrypter ce texte.

3. Le texte suivant a été obtenu en appliquant le chiffrement de Vigenère sur un texte en langue française dans lequel les espaces ont été supprimées :

```
gmyxzoocxziancxktanmyolupjrztgxwshctzluibuic
yzwxyqtvqxzukibkotuxkagbknmimmzzyajvjzampqyz
loinoiqknaumbknknvkaiakgwtnilvvzvqydmvjcximr
vzkilxzqtomrgqmdjrzyazvzmmyjgkoaknkuiaivknvvy
```

Expliquer ce qu'est l'indice de coïncidence. Utiliser l'indice de coïncidence pour déterminer la longueur de la clé utilisée et décrypter ce texte.

EXERCICE 4 : CHIFFREMENT AFFINE

Le chiffre affine est un chiffre de substitution simple. L'idée est d'utiliser comme fonction de chiffrement une fonction affine du type y = (**a**x + **b**) mod26, où a et b sont des constantes, et où x et y sont des nombres correspondant aux lettres de l'alphabet selon le tableau ci-dessous :

Lettre	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Nombre	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Décrypter le texte suivant qui a été obtenu en appliquant le chiffrement affine sur un texte en langue française dans lequel les espaces ont été supprimées :

```
ntjmpumgxpqtstgqpgtxpnchumtputgfsftgthnngxnchumwx
ootrtumhpyctgktjqtjchfooxujqhgztumxpotjxotfoqtohr
xumhzutwftgtopfmntjmpuatmfmshodpfrxpjjtqtghbxuj
```

EXERCICE 5 : MASQUE JETABLE

Un utilisateur a chiffré deux mots (non accentués) de la langue française de sept lettres avec le chiffrement one-time pad mais il a été imprudent et a utilisé deux fois la même clé pour chiffrer ces deux messages. Sachant que les chiffrés obtenus sont les mots HQQYAJT et RJAJPWG, écrire un programme informatique qui recherche dans un corpus tous les couples de textes clairs du français susceptibles de produire ces chiffrés.