TD1 : Ère pré-informatique de la cryptographie

Tous les cryptogrammes de cette feuille d'exercices (sauf le défi) ont été obtenus à partir de textes français écrits par R. Queneau et sont présentés par paquets de cinq lettres, pour plus de lisibilité. L'alphabet utilisé est réduit aux 26 lettres latines, les lettres accentuées étant converties en leurs équivalentes non accentuées, les espaces et signes de ponctuation ayant été supprimés.

1 Transpositions

Le principe d'une transposition est de modifier l'ordre des lettres du texte clair, pour obtenir le texte chiffré. Il existe de nombreuses manières d'effectuer ce genre de manipulations.

Exercice 1. *Un exemple de transposition simple*

Une transposition simple opérant par remplissage d'un rectangle en lignes et relèvement par colonnes fonctionne comme suit : la clé est une suite de lettres, mot ou phrase, comme par exemple `ECRITURE`. Chacune des lettres de la clé est numérotée, à partir de `A`, et suivant l'ordre alphabétique. Sur notre exemple, cela donne :

```
E  C  R  I  T  U  R  E
2  1  5  4  7  8  6  3
```

Lors du chiffrement, le texte clair est écrit sur des lignes de même longueur que la clé, ces lignes étant disposées l'une au-dessus de l'autre pour former un rectangle :

```
E  C  R  I  T  U  R  E
2  1  5  4  7  8  6  3

R  A  Y  M  O  N  D  Q
U  E  N  E  A  U  E  S
T  U  N  A  U  T  E  U
R  F  A  N  T  A  S  T
I  Q  U  E
```

On relève ensuite les colonnes dans l'ordre déterminé par les nombres associés aux lettres de la clé :
`AEUFQ RUTRI QSUTM EANEY NNAUD EESOA UTNUT A`

Question 1. Le cryptogramme suivant

```
PVSNO  UPNOR  AYREA  VDNLQ  SNDEE
AUEUC  AEUEI  TOLDG  EEENU  EAEMS
ALLAA  UNFDE  LNUCL  ETGED  UITLN
LIEMC  QEERE  IE
```

a été construit suivant ce procédé avec le mot–clé `"QUENEAU"`. Retrouvez le texte clair.

Question 2. Que pourrait-on faire si on ne disposait pas de la clé, mais seulement de sa longueur ? Et si on ne savait rien de la clé ?

2 Substitutions

Pour vous aider à percer les cryptogrammes dont la clé n'est pas donnée, voici par ordre décroissant des fréquences la répartition des lettres en français [1] :

E	17,76	S	8,23	A	7,68	N	7,61	T	7,30	I	7,23
R	6,81	U	6,05	L	5,89	O	5,34	D	3,60	C	3,32
P	3,24	M	2,72	Q	1,34	V	1,27	G	1,10	F	1,06
B	0,80	H	0,64	X	0,54	Y	0,21	J	0,19	Z	0,07
K	0,01	W	0,00								

1. source : *Manuel de cryptographie*, L. Sacco, Payot, 1947

et celle des bigrammes :

es	305	te	163	ou	118	ec	100	eu	89	ep	92
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	139	is	103	ra	92	ue	85	sa	75
on	164	ne	124	la	101	in	90	ta	85	ss	73
er	163										

On utilisera dans les exercices suivants une représentation numérique des lettres de l'alphabet :

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
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

Exercice 2. *Jules César*

Le système le plus ancien est attribué à Jules César. Il consiste en un décalage de l'alphabet (dans le système original `A` était remplacé par `C`, `B` par `D`, `C` par `E`, ...).

Question 1. Voici un texte chiffré obtenu avec la clé `H` :

```
QLZBP  ZHSVU  KYLZK  HUZBU  LKLZY
BLZSL  ZWSBZ  TPZLY  HISLZ  KLSHC
PSSLQ  LTHYJ  OLLUT  LKLTH  UKHUA
JVTTL  UAZLK  PABYP  UVPYL  UZSHU
N
```

Retrouvez le texte clair.

Question 2. Voici un autre texte chiffré ; on ne connait pas ici la clé utilisée.

```
FYPYQ  LYELO  TEUPD  LTDOP  DAZPX
PDFYP  YQLYE  LOTEN  SDLTD  OPDAZ
PDTPD
```

Retrouvez le texte clair.

Exercice 3. *Chiffrement affine*

Le chiffrement affine consiste à chiffrer toute lettre claire m en une lettre c égale à

$$c = (am + b) \pmod{26},$$

où a et b sont deux entiers compris entre 0 et 25 fixés. Le couple (a, b) est la clé de chiffrement.

Pour le choix de la clé tous les couples (a, b) ne conviennent pas. Il est nécessaire que a soit inversible modulo 26, ce qui est le cas si a et 26 sont premiers entre eux.

Pour déchiffrer, on calcule la lettre claire m par l'équation

$$m = a^{-1}(c - b) \pmod{26},$$

où a^{-1} est l'inverse de a modulo 26, c'est à dire l'unique entier x compris entre 0 et 25 tel que

$$ax \pmod{26} = 1.$$

Question 1. Combien y a-t-il de clés ?

Question 2. Le cryptogramme qui suit a été chiffré avec la clé $(a, b) = (11, 17)$. Déchiffrez-le.

```
YREHI HRDEJ QJDWJ YRUUI DJENJ
DESVA JYREH IJHOB EFSHB KREHN
QRAJR DTPDR OJNNP WYPEW JTAIR
NRESI JWDCR ENPDS WPAIP EFNPT
TJHBP EIDBR ORBSS BWJYJ HHDHI
JHFJE HYJHN JEYJE SIJSV AJJEL
DJHSB PEHBW WBSJN PESWJ DEOPB
HBEBI IDBWJ AWPNQ JYJIJ CPDHN
DIJWN QRLDJ UPBHL DBIAR HHJLD
JILDD ESPEA IJDWE BNQRW YLDBH
JOJDS TJNQR ES
```

Question 3. Retrouvez la clé utilisée pour obtenir le cryptogramme ci-dessous.

```
UJWXN WMJCJ GGPGP MVMPU PCPZS
JWFGP XPUPM GJZJW SGPGR WFUNW
PGVFW PUCRV SPNWA RBRVU PJMCP
XPWSJ WSNWP ZJGRS SPXMA PCVHN
PPWSR NCPPU PUPNY XVWNX RVUPX
JNUPX XNXUN WPMJC SVPZT GVWUC
VHNPU PGRWF NPNCX NMPCV PNCPJ
WMCPX PWSPN WMRVW SUPZR WSJZS
JIPZN WARBR VUPSC VIVJG EUPBR
WSCPC HNPZP MRVWS UPZRW SJZSP
XSNWM RVWSU PCPEC RNXXP BPWS
```

Exercice 4. *Chiffrement de Vigenère*

Question 1. Ce cryptogramme a été obtenu par chiffrement de Vigenère avec le mot–clé "RAYMOND"

```
RILEW  FRETJ  QGZRV  UPERR  VDAJQ
GRWUE  QRSZH  CLCER  NQJLC  DSTQV
ALUAN  OUEDM  QBQGR  MHWQH  ETGQZ
YH
```

Question 2. Décryptez maintenant ce cryptogramme sans connaître la clé

```
LFODV  BSGSS  USNDG  IEGHW  TVPHJ  RJCQH  ITGSS  USERR  SPOPI  RVPWL
EQWLW  DFUSI  TJVVK  AUGDY  XMCGI  CPWYI  RUGDP  OSUYS  IMCTY  IUTDY
MBVLW  ERWLW  AJVVM  LFTHU  UJPES  UMQWX  EMGVX  USDRX  SFVSS  USVDR
TDGWE  IUNXM  LFHUI  RFFHJ  EJPWM  SFSXM  CMQFL  ASFGI  VFPDR  TKGWE
IUUHW  OSKSI  AVZOY  NFVOE  UUTHS  NUTDM  SPPQS  NMCIS  UMGLQ  PSGFM
SFNRV  SRWRR  VPADM  TBWOS  IOHOE  MCGUP  ETCUF  RJUVI  AVZOI  SQTLX
SPWIJ  LFGWV  ETQXJ  FMGDY  DFUVY  SEGOE  BPVWI  LFVRY  RJUWI  AGNRV
EOEHM  GOQEP  EDJDV  ICQWX  EMQUW  QVQQF  OJVGY  MBVHP  OOFHZ  IFPWE
RHGQX  IOUDW  CVNSX  USGHW  TJNOY  SUTHI  TECQW  LFHRR  DEGVG  ORWHW
CPOSX  AOVWI  SBDDX  TJUOI  CUGXV  TVVHH  ITNRU  UFUVM  LFWUS  PFNHZ
EVVOI  USQSI  OVURR  DFUWM  N
```

Q 2–1. Comment peut-on justifier que la clé a une longueur très probablement égale à 5 ?

Q 2–2. En tenant compte des dénombrements des occurrences des 26 lettres dans le cryptogramme rassemblées dans le tableau ci-dessous, déterminez la clé la plus vraisemblable.

	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
0	7	2	5	4	10	1	1	0	11	0	0	7	3	4	6	2	1	7	11	9	11	2	0	1	0	0
1	0	4	2	2	4	19	1	1	0	10	1	0	9	0	6	7	2	3	11	4	9	9	0	0	0	0
2	1	0	6	2	2	3	18	3	0	1	1	0	0	8	3	7	8	0	1	6	11	13	8	0	0	2
3	0	0	0	13	2	2	3	14	2	0	0	5	0	0	9	1	5	9	8	1	5	7	12	4	2	0
4	0	0	0	0	6	2	2	2	16	4	1	2	10	0	0	4	1	6	10	0	2	6	10	9	9	2

Exercice 5. *Le masque jetable*

La technique du masque jetable a été élaborée en 1926 par G. Vernam sous le nom de "one-time pad", et consiste en l'ajout au texte clair d'une suite de symboles aléatoire de même longueur que le texte clair, et qui sera jetée après usage. Il faudra considérer une nouvelle suite aléatoire pour un chiffrement ultérieur. C. Shannon, fondateur de la théorie de l'information, a démontré en 1949 que ce système est inconditionnellement sûr (c'est le seul système inconditionnellement sûr à l'heure actuelle).

Question 1. Le cryptogramme suivant

```
QCFPP  WXAZS  POUIH  QHHCF  VVFGT
GFDAS  VSKUE  BSYYD  QESWV  OEHDB
```

a été chiffré par une technique du masque jetable. Expliquez pourquoi vous ne pouvez pas le décrypter.

Question 2. Discutez des avantages et inconvénients de ce système.

Un défi

Voici un cryptogramme. Décryptez-le sans aucune autre indication qu'il s'agit d'un texte en français.

```
NLYMKSSDPNAAA JLLLLLLAMZAPNAAA J JUU'ALWJRGCPPKVVVA
QBQSSDRGTTEEJLWJRRA,
JUUA LLLMKMZA QBQALLLPNAAAARR J QBQJRGQBQRGPNAAA AQBQRR :
KKBODQQQHITOMZZUUFFFVVGTWWUXXVI.
```

Pour se familiariser avec les ordres de grandeur

Exercice 6. *Vider l'océan avec un dé à coudre*

La recherche d'une clé par force brute 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. Encadrer entre deux puissances de 2 consécutives le nombre de dés à coudre d'eau que contiennent les océans.

Exercice 7. *La force brute*

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 (en 2004) est d'environ 1800 Mips. (millions d'instructions par secondes).

Le facteur de travail d'un algorithme optimisé pour tester une clé de 128 bits de l'algorithme AES est d'environ 1200 instructions élémentaires.

On dispose d'un couple clair/chiffré connu et on désire retrouver la clé utilisée par force brute, c'est-à-dire en testant toutes les clés les unes après les autres. Une clé est constituée d'un mot de 128 symboles binaires. On suppose que toutes les clés sont équiprobables.

Question 1. En combien de temps une machine de 1800 Mips teste-t-elle une clé ?

Question 2. Combien y a-t-il de clés possibles ? Quel est le nombre moyen de clés à tester avant de trouver la bonne ?

Question 3. Quel est le facteur de travail moyen pour trouver la clé ?

Question 4. À quel temps moyen de calcul cela correspond-il si on suppose que les 300 millions de PC de l'internet sont mobilisés à cette tâche ?

Exercice 8. *La loi de* Moore

Il est admis que, grâce aux progrès 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 1800 Mips. Pour tout entier n, on note W_n le nombre d'instructions exécutées par la machine du mois n.

Question 1. Quel est le facteur d'amélioration a de la puissance des machines d'un mois à l'autre ?

Question 2. Calculer W_0, puis W_n en fonction de W_0, de a et de n.

Question 3. Quel est le temps moyen nécessaire pour trouver la clé ?

Ordres de grandeurs [2]

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 (par an, aux États-Unis)	2^{-12}
Probabilité d'être tué dans un accident d'automobile	1 chance sur 75 (sur une vie, aux États-Unis)	2^{-6}
Temps d'ici à la prochaine glaciation	14 000 ans	2^{14}
Temps d'ici à la transformation du soleil en nova	14 000 ans	2^{14}
Âge de la terre	10^{9} années	2^{30}
Âge de l'univers	10^{10} années	2^{34}
	Si l'univers est fermé :	
sa durée de vie est	10^{11} années	2^{37}
	10^{18} secondes	2^{61}
	Si l'univers est ouvert :	
Temps d'ici au refroidissement des étoiles peu massives	10^{14} années	2^{47}
Temps d'ici à ce que les planètes quittent leur étoile	10^{15} années	2^{50}
Temps d'ici à ce que les étoiles quittent leur galaxies	10^{19} années	2^{64}
Temps d'ici à la disparition des orbites par radiation gravitationnelle	10^{20} années	2^{67}
Temps d'évaporation complète des trous noirs	10^{64} années	2^{213}
Temps d'ici à la liquéfaction à $0K^{\circ}$ de la matière	10^{65} années	
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}
Volume de l'univers	10^{84} cm^3	2^{280}

FIGURE 1 – Ordre de grandeur

2. source : *Cryptographie appliquée*, Bruce Schneier

Le carré de Vigenère

	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**
A	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
B	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	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

TABLE 1 – Le carré de Vigenère