Travaux Dirigés n°3 – *Chiffre à clés secrètes*
RSX112 – Sécurité et Réseaux - Correction

Remarque :
L'ensemble des exercices peuvent se faire à la main, mais un programme ou même un simple tableur peut vous rendre bien des services ! (vous pouvez donc programmer ou utiliser un tableur pour vous aider).

Exercice 1 – Cryptogramme 1.
Cassez le cryptogramme suivant qui utilise une substitution monoalphabétique. Le texte en clair ne contient que des lettres et des espaces. C'est un extrait d'une fable de La Fontaine.

```
gcxob wryvn ibnog xntbn syiib
ypsyx gnibn ogxnt bvnqm gzev
thcpb nwgqr pnwro xnqys yib
gntbv nobiy bwvnt hroxr igpv
vconc pnxge yvntb nxcoj cyb
ibnqr csbox nvbnx orcsg nzyv
abnig yvvbn gnebp vboni gnsyb
jcbnw yobpx nqbvn tbcdn gzyv
ibnob fginw cxnwr oxnmr ppbxb
oybpn pbnzg pjcgy xngcn wbvxyp
```

Solution :
Compter les fréquences :

a	*1*	*i*	*12*	*q*	*5*	*y*	*17*
b	*32*	*j*	*3*	*r*	*9*	*z*	*4*
c	*13*	*k*	*0*	*s*	*6*		
d	*1*	*l*	*0*	*t*	*7*		
e	*3*	*m*	*2*	*u*	*0*		
f	*1*	*n*	*39*	*v*	*16*		
g	*18*	*o*	*15*	*w*	*8*		
h	*2*	*p*	*13*	*x*	*16*		

Le n est sûrement l'espace.
Le b est le e.
Ensuite, regarder sur les mots de 2 ou 3 lettres avec les lettres fréquentes : S, A, R, I, N, T, U, L, O.

a	J	i	L	q	C	y	I
b	E	j	Q	r	O	z	M
c	U	k	k	s	V		
d	X	l	l	t	D		
e	P	m	H	u	u		
f	G	n		v	S		
g	A	o	R	w	F		
h	'	p	N	x	T		

```
A U T R E F O I S   L E   R A T   D E   V I L L E
I N V I T A   L E   R A T   D E S   C H A M P S
D ' U N E   F A C O N   F O R T   C I V I L E
A   D E S   R E L I E F S   D ' O R T O L A N S
S U R   U N   T A P I S   D E   T U R Q U I E
L E   C O U V E R T   S E   T R O U V A   M I S
J E   L A I S S E   A   P E N S E R   L A   V I E
Q U E   F I R E N T   C E S   D E U X   A M I S
L E   R E G A L   F U T   F O R T   H O N N E T E
R I E N   N E   M A N Q U A I T   A U   F E S T I N
```

Exercice 2 – Cryptogramme 2.
Casser le cryptogramme suivant qui utilise une transposition par colonnes. Le texte en clair est issu d'un ouvrage classique sur l'informatique ; on peut donc supposer que le mot "ordinateur" y figure. Le texte ne contient que des lettres (sans espace). Il est découpé en blocs de 5 caractères pour plus de lisibilité.

```
ntsus ueire eibps etsio ootuu rpmrn eaicq iunps cnlog
euern lndur raose xnntu dnaeo eseue clton nretd trels
```

Solution :
Prendre des mots de 15 caractères :

```
1 n t s u s u e i r e e i b p s
2 e t s i o o o t u u r p m r n
3 e a i c q i u n p s c n l o g
4 e u e r n l n d u r r a o s e
5 x n n t u d n a e o e s e u e
6 c l t o n n r e t d t r e l s
```

Puis, réordonner pour trouver :

```
4 e u e r n -l n d u -r r a o s e
1 n t s u s u e i r e e i b -p s
3 -e a -i c -q i -u n -p s -c n l o -g
5 x n n t u -d n a e o e s e u e
2 e t s i o o -o t u u r -p m r n
6 c -l t o n n r e t d t r e -l s
```

Exercice 3 – Chiffre de Vigenère.

1) Chiffrer avec le chiffre de Vigenère le texte suivant "textesecretadecoder" en utilisant comme clef le mot crypto.

Correction :

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
MSG :	t	e	x	t	e	s	e	c	r	e	t	a	d	e	c	o	d	e	r
CLE :	c	r	y	p	t	o	c	r	y	p	t	o	c	r	y	p	t	o	c
CRYPTOGRAMME :	v	v	v	i	x	g	g	t	p	t	m	o	f	v	a	d	w	s	t

2) Pour le même texte en clair on obtient le texte chiffré suivant "brqksmzcspxiqxtcxzr". Quel est la clef ?

Correction :

MSG :	t	e	x	t	e	s	e	c	r	e	t	a	d	e	c	o	d	e	r
CRYPTOGRAMME :	b	r	q	k	s	m	z	c	s	p	x	i	q	x	t	c	x	z	r
CLE :	i	n	t	r	o	u	v	a	b	l	e								

3) Imaginez des stratégies de cryptanalyse dans le cas ou la clef est un mot français et dans le cas ou c'est une suite aléatoire de lettres. Comment distinguer à priori ces deux cas ?

Correction :
Si la clé est répétitive, qu'elle soit claire ou aléatoire, le décryptement peut se faire par la méthode classique.
C'est un peu plus facile si la clé est un mot clair car dès que l'on a identifié quelques lettres, on peut deviner le mot.
Si la clé est aléatoire et non répétitive, c'est à dire aussi longue que le texte clair, c'est « MATHEMATIQUEMENT » indécryptable. Une exception toutefois : si cette clé a servi pour plusieurs messages, toute hypothèse basée sur le premier cryptogramme devra donner aussi du clair dans le deuxième.

4) Attaque par mot probable
On sait que le message suivant contient le mot PLUIE. Décryptez-le.
PIFEW ZTEYW QWNVH AYMIZ MJKEB OI

Solution :
Texte clair : "Demain pluie sur toute la France"
Mot clé : METEO

Exercice 4 – Chiffre de Vigenère.

1) Dans la substitution à masque jetable 'One Time Pad', on utilise un XOR pour chiffrer. Chiffre le message 309 à l'aide de la clé 173. Déchiffrer ensuite pour vérifier.

Correction :
MSG : 100110101 (309)
CLE : 010101101 (173)
CRY : 110011000 (408)
MSG : 100110101 (309)