DÉPARTEMENT
Sciences Informatiques

Licence Pro R&S
2013–2014
Chiffrement et Authentification
T.T. Dang Ngoc
dntt@u-cergy.fr

TD1- Chiffrement ancien

1 Scytale

Vous interceptez le message suivant crypté à l'aide d'une scytale :
`lunlaessatsadueatebamtmeuiaalfsqieonuncrooaht`

1. Quel est le diamètre de la scytale ?
2. Quel est le message en clair ?

Chiffrez le message suivant en utilisant la même technique et la même clef (le diamètre (n'oubliez pas d'enlever les espaces) :
`repos pour demain`

2 Chiffre de César

Vous interceptez un légionnaire romain portant le message suivant de la part de Jules César à un de ses centurions :

```
ALCUF ATEPC YZFDG LTYNC ZYDNP DTCCP OFNET MWPDR LFWZT
DLGPN ZFDLY DAZET ZYXLR TBFP
```

1. Quel est la clef (le décalage) ?
2. Quel est le message en clair ?

Renvoyez le légionnaire à son expéditeur avec le message suivant chiffré avec la même clef.

`coucou cesar on a lu ton petit mot`

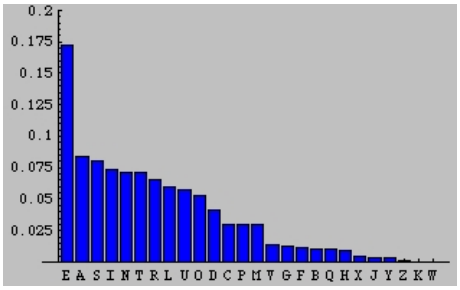
3 Substitution mono-alphabétique

```
ZPPZP PCILN FLBLI LNZFL IILHC LIPSC QLRLP JCNAS CQALS NLFZH JCQCL GLPQN

JSKLP LPRZF ZGLNJ IQFZU ZRZGL IJNGL QPLQC LIGNJ IQLIK JPCQC JIFZS QNLHJ

CQCLR JIQJS NILNZ FZOZP LLIIL HCLKZ NFLPS GLIUC IGLPF LSNNL PPLNJ IQGCP

KLNPL PFLPC BIZFG ZQQZM SLPLN ZGJII LKZNS ILUSP LLGLG LQNLP PLFZI RLLGL

KSCPF ZUJNL Q
```

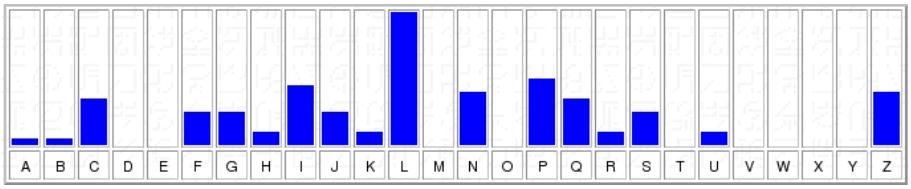
Correspondance d'alphabet

clair	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
chiffré																										

Fréquence sur les occurences des lettres en français



Fréquence sur les occurences des lettres dans le texte



- Quel est le message en clair ?
- Quel est le mot-clef ?

Maintenant que vous avez intercepté le mot-clef, chiffrez le message suivant pour tendre un piège :

```
Operations annulees. Repliez vous tous a la base.
```

4 Carré de Vigénère

Le mot-clef `TORTUE` a été intercepté ainsi que le message : `THKTK YXRVF UMGOC TOFX`

Codez le texte suivant pour tendre un piège à l'ennemi `operation annulee`

5 Chiffrement divers

Connectez-vous sur l'excellent site de Didier Müller sur :

`http://www.apprendre-en-ligne.net/crypto/menu/index.html`

et utilisez les applications en ligne pour résoudre les exercices suivants :

5.1 Scytale

```
diolrrsoseouartiwdmnrfieonuanpoemnsgierrrpeoenzeteinunalneLofseledrenalrasregfieauteseesslbrdsnra
feeoaeeanenpusprdtnnopsaaileesearlvetmisultecritptaarle
```

5.2 César

Avec un décalage de 14

```
XIZSG QGOFO RWHXS GIWGJ SBIXO WJISH XOWJO WBQIA OWGBS DOGMO ZZSFS HBSDO GJCWF QSGHZ SASWZ
ZSIFA CMSBR SBSDO GHFSJ OWBQI G
```

5.3 Chiffre de Porta

Avec le mot clef CORBEAU

```
XXUBG OUZBW GWRBQ HSEOZ QHLWP DERQT CFJEE BTMOG RMQLU UIRKZ OBRCF LBUWP JAVFI
RNRRP ZAMRG RKZLV CYEOC WWHGN OXVZY JVDUH BCPHM FMURW NKSTY RSOLB PJHGZ LBMNR
JETIV JEZRQ IKCRK BEGAW FUBOU KCRKB EGSWF PZRXX HOPNE GTIFX RKHOM FTILH LWEYZ
QSXAR GNMDI MGPIL HLWCW HPZZW IDHCH XAYPC XBOFQ PFXHX AQPPU GUJVH NSQMR BIFOQ
VJEZR QIHWF PFUBA KNHQU VINRP GMCBM ZDADF XMFYO UXRWI DVHUR JHKEU IHQNG TUNXU
YYVCG XBBXO UFMSC GBYQR WEPAQ FWARC FQUMN GPGTU ARBCO LBSJA HVUIL SCEEU BXHDJ
RDCBB SWNDH XCEKV DZBFQ ERKGW WPPYE UKCVW PLIAW PPGDQ RWBCI QIATV PAEBY MBXNW
QMSAH QLIAW YPPLF UWNJU LBAWH MRDOI ISJFZ ILSZY VCIHK RJGQF WLHDA KQRGC GRKPL
SVICO IM
```

5.4 Carré de Polybe

Avec le mot-clef FOURMI

```
412224 213222 413131 514122 111213 141521 412224 213222 413122 542242 512433
224251 511213 514151 453151 141213 522211 121451 254312 131452 133144 132242
254122 232145 311113 515231 421331 432245 134245 311341 433151 215115 121424
312213 253115 121324 333112 132531 523114 152145 453122 133141 413122 414122
241421 311411 221521 423124 333155 412211 121314 152145 225212 214521 423141
224314 212242 512531 411321 431451 311444 133141 441331 321422 214243 121314
451323 452145 513114 341345 441341 224522 214512 424212 135231 414131 343152
121345 432221 311422 214113 212521 513141 413122 522242 514112 511112 212522
422115 224121 425114 513151 431421 422421 432241 412211 121314 152142 314551
432245 431451 311345 312431 455141 451242 151221 422514 312511 221351 441331
112221 452131 555212 134522 135131 154345 243322 132525 215131 414131 243151
513131 154314 134251 311345 314213 215131 513412 131451 121351 523142 224251
343124 332242 512221 454231 521213 452543 412221 453152 121345 243322 425121
315534 314245 132145 111214 512221 453131 332321 314225 224245 315515 222142
513142 224251
```

5.5 Carré de Vigénère

Avec le mot-clef "cyrano".

```
OYZSP VCLKE EFXCI RVFGN RSFST RIEFS WJKRR ZKZIE NJQGI LBSKJ HUVFG ERRQS DGVNY
OXMZX DIKTZ BESOC KTESS SRNQW NTFUF DNYKS BBHCL TESFC KRNJG PJPBI TSEOH WRMLR
HBPME SRPCR KRRCW DRIES WLMEE G
\end{verbatimii}
%MAISCHANTERRVERRIREPASSERTRESEULTRELIBREAVOIRLOEILQUIREGARDEBIENLAVOIXQUIVIBREMETTREQUANDILVOUSPLATSONFEUTRE


\subsection {Cylindre de Jefferson}
(utilisation de celui du site uniquement)
Mot-clef : CRYPTO
\begin{verbatim}
YOVVF BWQBC DAMBJ XIHHX
```

5.6 Enigma

(utilisation de celui du site uniquement)
- Position des trois rotors : 2 - 1 - 3
- Orientations des rotors : 7 - 2 - 11
- Branchements des connexions : A/L - P/R - T/D - B/W - K/F - O/Y
- Indicateurs : G - B - K

Déchiffrez le message :

```
YSJNG XVBZJ YQTVX PMFQX ZYHIO NHUER XCBME FA
```

Annexe

Carré de Vigénère :

	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