

## TD 1 de cryptographie

### Entropie

On considère ce message utilisant 4 lettres : AAB C CDD DA  
Déterminez un encodage optimal.

### Codage de Huffman

Codez la phrase suivante : cryptographic hash function  
Le codage prend combien de bits ? Combien de bits par lettre en moyenne ?

### Chiffrement de César

Décryptez ce texte écrit en français :

Phvgdphv hw phvvlhxuv, mh qh yrvgudlv sdv yrsv diirohu, pdlv ghv irxv, lo b hq d ! Gdqv od uxh, rq hq frwrh... Uhfhpqhqw, mh uhqfrqwuh xq prqvlhxu. Lo srudlw vd yrlwxuh hq edqgrxolhuh !  
Lo ph glw : - Yrxv qh vdyhc sdv frpphqw rq ghwdfkf fhwwh fhqwxuh ? Mh oxlv glv : - Glwhv-prl !  
Oruvtxh yrsv o'dyhc erxfohh, hvw-fh txh yrsv dyhc hqwhqgx xq shwlv ghfolf ? Lo ph glw : -  
Rxl, gdqv pd whwh ! Mh ph glv : "Fh wbsh, lo hvw irx d olhu !" M'dl hx hqylh gh oh fhqwxuhu...  
Pdlv txdqg m'dl yx txh vd fhqwxuh hwdlw qrluh... Mh o'dl erxfohh !!

Quelle est la clé ?

Quel est l'auteur du texte ?

### Chiffrement de Vigenere

Question : qui est l'auteur du texte suivant ?

Informations : il s'agit d'un texte en anglais, la ponctuation est conservée.

Le chiffré :

S iz tyb htwaqajpcy zrig yyur up gba riik mwzk rmek ycg up oekkb gxiyy kvq zbqoavigoyvf. Yyur up gba riik mwzk pzryr neuw vnxbwj pkqy iotyy. Kvq yyur up gba riik mwzk pzbs kzrgc eukbm luez daoag -- wemfz pwe lbmrjyu ykpb lue jnzdmekn jl zrm fzyzzy yn ckbariebvx iaj cbnmqmekn jl zrm joxlf up xbrskr hbcggvqge. Iwh nkdr homa zrm ikdmegxa bl mzrgdqik ccslzvtq. Kbtqaaoo bb cyzx csbu zrm sgsbu zrig axmnnxmq yenskbqam sa eknmzvdqik. Qw ogms gu Wqfysafozxv, my jniu bb Gviogwi, tu lipq dw Fuebu Ikzbrsvn, my jniu bb Mowemsi, tu lipq dw Yueqfokvn, my jniu bb zrm freuf gxl tnobguc ws uez aubbukbv podqry, uvbcsvt zrig yyurnye gnsa fodcnzswa ikv ntn evrv jr iriamol. Ykd cf tyb jgvtbc sv gno dnrvml up lryzivx, S ane dw lue bbjkg, ze pzvkxlf. Gxl fu odrt dpbaqp jk pipk dpr jsnsomcyzsmf up bbjkg ntn bbsyzeug, Q fzsty nkdr g nzrgw. Qg oc i qxoiz jomcri zbudmq ox buk Kurxsknt nzrgw. Q ugfm n jbmns dpnz yvr jkg gnsa agdqbt gqyr bqfk ex ntn tvbo whz dpr zbcr soiaoxo bl sbf ibmrj: Gm uuvl gnoar zbcgnc bb ho arrp-mionmaz, dpnz kty sov nxo kekkbrj oyhgv. Q ugfm n jbmns dpnz yvr jkg bt dpr xol uovtf up Orubovg, dpr yyvf up nbxwme yviikc iaj dpr yyvf up nbxwme yviik yeakba jovt ok kjk dw fod lbcx bbmobukb ig zrm ggltr up jeudprxrbwj. S pnbo i qxoiz zrig uxm qgi mikx buk cbnzo ws Ssafocavvzq, n ydigk cerrdmeoxo jodp gno prgd ws oxrhydqp, cerrdmeoxo jodp gno prgd ws uzxeckavux, evrv jr zbiaypwesol vtdw nt yifoc ws lbmrjyu ntn rhydqpk. S pnbo i qxoiz zrig si nbab tvzdr irqyjbma csty uxm qgi tvbo qa g xigoyv jnozr zrml csty tyb ok tcqmol oe dpr iytbx yn gnoqe yuqa heb oe dpr iyvgkxb bl dprob kugbipzoz. V nkdr g nzrgw bbjkg!

Pour pouvoir faire une analyse sur les espaces de répétition, j'enlève les espaces et ponctuations :

SiztybhtwqajpcyzrigyyurupgbariikmwzkrmekycgupoekkbgsxiyykvqzbqoavigoyvfYurupgbariikm  
wzkipzryneuwnxbwjpkqyiotyyKvqyyurupgbariikmwzkipzbskzrgceukbmluezdaoagwemfzpwelbmr  
jyuykplbluejnzdmeknjlrzfzyzyynckbariebvxiajcbnmqmeknjlrzmxjoxlfupxbrskrhhbcggvqgeIwhnkd  
rhomazrmikdmegxablmzrgdqikccslozvtqKbtdqaobbcyzxcsbuzrmsgsbuzrigaxmnnxmnyenskbqams  
aeknmzvdqikQwogmsguWqfysafozxvmyjniubbGviogwitulipqdwFuebulkzbrsvnmyjniubbMowemsi  
tulipqdwYueqfokvnmyjniubbzrmfreufgxltnobgucwsuezaubbukbvpodqryuvbcsvtzrigyyurnyegnsafo  
dcnzswaikvntnevrjririamolYkdcftybjgvtbcsvgnodnrvmplryzivxSanedwluebbjkgzepzvklfGxlfuo  
drtdpbaqppjkpipkdprjsnsomcyzsmfupbbjkgntnbbsyzeugQfzstynkdrgnzrgwQgocixozjomcrizbudmq  
oxbukKurxskntnrgwQugfmnjbmnsdpnyvrjkggnsaagdqbgtqyrbqfkecntntvbowhzdprzbcsoiaoxobl  
sbfibmrjGmuuvlgnoarzbcbgncbbhoarrpmionmazdpnzkysovnxokekbrjoyhgvQugfmnjbmnsdpnyvrj  
kgbtdprxoluovtupOrubovgdpryvfupnbxwmevyiikciajdpnyvfupnbxwmevyiikyeakbajovtokkkykd  
wfdlbcxbmobukbigzrmggltrupjeudprxrbjSpnboiqxoizzriguxmqgimikxbukcbnzowsSsafocavvzq  
nydigkcerrdmeoxojodpnoprgdwsorhydqpkcerrdmeoxojodpnoprgdwsuzxekcavuxevrvjrzbaiypwe  
solvtwntyifocwslbmrjyuntnrhydqpKSpnboiqxoizzriginbabbtvzdrirqyjbmacstyuxmqgitvboqagxigo  
yvjnozrzmrcstytyboktcqmoloedpriybtxyngnoqeyuqaheboedpriyvgkxbbldprobkugbipzozVnkdrgnzr  
gwbjkg!

Analyse :

**Séquence répétée      Espace de répétition**

S	564, 408, 164
iz	664
tyb	532

Cette analyse permet-elle de retrouver la longueur de la clé ?

Quelle est la longueur L de la clé ?

J'aurais pu prendre d'autres séquences et le résultat aurait été le même. Il faut noter qu'ici j'ai utilisé la ponctuation pour simplifier (j'ai choisi S majucule suivi d'un espace).

Maintenant, il faut faire une analyse statistique sur les apparition des lettres pour  $i, i+L, i+2L, \dots$  et comparer avec les statistique d'un texte en anglais. Pour  $i=1, 2, 3$  et  $4$ . Si cela ne suffit pas on peut essayer des bigrammes, des trigrammes,...

Pourquoi le chiffrement de Vigenere n'est-il pas sûr ?

Que faudrait-il faire pour le rendre sûr et quels en seraient les inconvénients ?

Voici la grille de Vigenere qui permet de chiffrer et déchiffrer rapidement :

	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