

Exercise sheet 1, 12 November 2015

There are several nice tools online for cryptanalysis of classical systems, e.g.

<http://www.braingle.com/brainteasers/codes/index.php>

<http://www.cryptool-online.org>

<http://axion.physics.ubc.ca/cbw.html>

Once upon a time I helped to make <https://www.mysterytwisterc3.org/en/old-mystery-twister-games/> where you can find many more examples

See below for some frequency distribution.

1. The following text was encrypted using the Caesar cipher. Find the plaintext.

aopza leapz huleh twslv muvyt hsale azvao lbzbh skpza ypiba pvuzv
mjohy hjaly zmvyl unspz oalea zovbs kovsk

2. The following text was encrypted using the Caesar cipher. Find the plaintext.

drovo ddoaba nyocx ydkzz okbyp doxex voccs xaekb dobae kbxkd sxoae
oloma ekbdj ybaek cskbd spsms kvaao cdsyx c

3. The following text was encrypted using the Viginère cipher. Find the plaintext.

evtdw dlgsz fepll xdwpk tevlg scjgs zfevs jecdp sszkp yqcjd etcyl
boosn cmaew zykzc ypgsy hvpyc yprzp gyzhs ljpev pvsj

4. The following text was encrypted using the Vigenère cipher. Find the plaintext.

xnuju dkrvr shdmr vjbkl ehlwx ofued yhgik siskk ddgxa btrsi fyxmn
kxczm jwkvd fhdw ewtxl snsih elsua rnlih ualvv uiepl wqtrg dafch
fdgey mhoiv nslwi hyhjn aloar bqeka jucha ellaf jwwee gohtr bmgfl
ozuho xdahk hgslj edchi sgxhs kwtrk eelkx gekgb hyhpb gnaoe ghoxg
nhyww ejwys zytrv wywgk trkld skhmt tqlsi idrea jurqx nnwng vvjbk
lehlw xofkq pjwxt mlece fpxzw ngtdc bwuka gdgev oehyw gafkl cjlii
gfywg ktrka jokup nkhhg zwxof uedyh gtzwq bzwho xldsg opifl alkdg
ejwwf idcgw vebg xfxwn sewpn vmoir oayim ehvfd mhdal fusej tqhkk
tufap gkktm kwhjv vprwd atkxc czsju vgqyu gjhid htafw gleht alqhz
rccah dsiw emfeh jrutz wlzrl ctwpp oihge lsebv gxnlg agrpt swiqs
eftif ldstl ehwjv sowqu lldsl qxtkl dsdvt lnwoo ihpll wnsuw wejww
fvdcu etaff isixx afvqi tqhag fihut kpwx iigfy wgktr axpvv fpxzw
ncghg alwoc evxny dazvw iejke hzvie jearr vxmhd agleh talqh zrcca
hdsid rihza fkkpt ghafz wtsgf hoijt ryjki gvdfd wphvu hikla fdhsp
gduui dehau wafqd adhdo shiiu uedyh gukwo tzatd kmxgk liula kbfiy

rlzas ewxrw eagjd veoza fvdha hghmr oehst ahzfr ihzaf lvtss fqash
 goxkq pjwxt mlece vptva btvut nlhkg zwxof kebkk tmwko oxhhl wjaol
 qxtxj kakkt pdseb khmta kiogs tdlgk bvrus wnafr oeokk epzox tawow
 ewweu alvvu ieplw buyxc wnafr d

5. The following text was encrypted using the Playfair cipher with keyword MATHEMATICS. Decrypt the message.

gc lz po nt au tc ad uh st

6. The Hill cipher is a secret-key system based on matrices. It takes a message in the English alphabet (26 characters), translates the characters into numbers as given below, and then encrypts the message by encrypting n numbers at a time as follows:

Let the secret key M be an $n \times n$ matrix over $\mathbb{Z}/26\mathbb{Z}$ which is invertible and let the plaintext a be the vector $(a_1, a_2, \dots, a_n) \in (\mathbb{Z}/26\mathbb{Z})^n$. The corresponding ciphertext is $c^T = Ma^T$. To decrypt compute $a^T = M^{-1}c^T$. Note, this is the other way round from what I said on Monday, sorry! (... and for the second year in a row, updating notes now!)

- (a) Let

$$M = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 3 & 2 \\ 1 & 3 & 1 \end{pmatrix}.$$

Encrypt the text CRY PTO

- (b) Let M be a 2×2 matrix. You know that $(1, 3)^T$ was encrypted as $(-9, -2)^T$ and that $(7, 2)^T$ was encrypted as $(-2, 9)^T$. Find the secret key M .

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

Probability distributions of 1-grams in English, from Henk van Tilborg “Fundamentals of cryptology”, page 5. Boldfacing of values larger than 0.06 by me. Note the probabilities of e and the triple r,s, and t.

a	0.0804	b	0.0154	c	0.0306	d	0.0399
e	0.1251	f	0.0230	g	0.0196	h	0.0549
i	0.0726	j	0.0016	k	0.0067	l	0.0414
m	0.0253	n	0.0709	o	0.0760	p	0.0200
q	0.0011	r	0.0612	s	0.0654	t	0.0925
u	0.0271	v	0.0099	w	0.0192	x	0.0019
y	0.0173	z	0.0009				