Exercise sheet 1, 12 November 2020

There are several nice tools online for cryptanalysis of classical systems, e.g. http://www.cryptool-online.org

There are more challenges online at https://www.mysterytwisterc3.org/en/

The raw data for the texts is also at http://www.hyperelliptic.org/tanja/teaching/CS15/data1.html. 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 ddoba nyocx ydkzz okbyp doxex voccs xaekb dobae kbkxd sxoae
oloma ekbdj ybaek cskbd spsms kvaeo 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 fhdww 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 fxpzw ngtdc bwuka gdgev oehyw gafkl cjlii
gfywg ktrka jokup nkhkg zwxof uedyh gtzwq bzwho xldsg opifl alkdg
ejwwf idcgw vebrg xfxwn sewpn vmoir oayim ehvfd mhdal fusej tqhkk
tufap gkktm kwhjv vprwd atkxc czsju vgqyu gjhid htafw gleht alqhz
rccah dsiww emfeh jrutz wlzrl ctwpp oihge lsebv gxnlz agrpt swiqs
eftif ldstl ehwjp sowqu lldsl qxtkl dsdvt lnwoo ihpll wnsuw wejww
fvdcu etaff isixx afvqi tqhag fihut kpwkx iigfy wgktr axpvv fxpzw
ncghg alwoc evxny dazvw iejke hzvie jearr vxmhd agleh talqh zrcca
hdsid rihza fkkpt ghafr wtsgf hoijt ryjki gvdfd wphvu hikla fdhsp
gduui dehau wafqd adhdo shiiu uedyh gukwo tzatd kmxgk liula kbfyt
```

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

5. The Playfair cipher uses a keyword. Encryption/decryption uses a 5×5 grid of letters. To turn the keyword into this grid, start filling in the letters of the keyword row-wise from the top left corner. The grid contains each letter once, with I and J identified; so when you reach a letter in the keyword that has been used already, you skip it.

   After the end of the keyword, the remainng letters of the alphabet are inserted, again in the order they appear.

   If the keyword is SECRET then the grid looks as follows:

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

   Note the skipped second E in the keyword. This fills up the grid completely – if you have any letters left, something went wrong earlier.

   To encrypt a message, split it up into pairs of letters, starting from the beginning. If one pair consists of two equal letters, insert an X; this shifts the second letter into the next pair. If there is a single character at the end, append an X. There are three cases for encrypting a pair of letters:

   (a) If the two letters appear in the same row, encrypt each of the two letters to the letter to the right of it.

   (b) If the two letters appear in the same column, encrypt each of the two letters to the letter below it.

   (c) If the two letters span a rectangle in the grid, encrypt each of them to the letter in the same row and opposite corner.

   To decrypt, reverse the procedure.

   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 $(a_1, a_2, \ldots, a_n) \in (\mathbb{Z}/26\mathbb{Z})^n$. The corresponding ciphertext is $c^T = Ma^T$. To decrypt compute $a^T = M^{-1}c^T$.

(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				