TMA4155 — Exercise 1

Kristian Gjøsteen

2006-08-31

Task 1 — Encryption and decryption

a. Encrypt `caesar` using the Cæsar cipher with 3 as the key.

b. Find the decryption of `DQKBWZG` when it was encrypted using the Cæsar cipher with 8 as the key.

c. Encrypt `victory` using the affine cipher with $(3,3)$ as the key.

d. Decrypt `WDKDBE` when it was encrypted using the affine cipher with $(7,1)$ as the key.

e. If m is the number corresponding to the plaintext letter, c is the number corresponding to the ciphertext letter, and (k_1,k_2) is the key, then c is determined by the equation

$$c \equiv k_1 m + k_2 \pmod{26}.$$

Find the corresponding equation determining m from c and (k_1,k_2). What must k_1 satisfy to obtain a decryption?

f. Encrypt `unbreakable cipher` using the Vigenère cipher with `weak` as the key word.

g. Decrypt `VOQMFXMSYS` using the Vigenère cipher with `dubious` as the key word.

Task 2 — Simple cryptanalysis

The following ciphertexts have been encrypted using either the Cæsar cipher or the affine cipher. Find the plaintext and the keys.

Hint: One or more of the plaintexts start with `hi`.

Note: Spaces and punctuation has been removed from the plaintext and the ciphertexts have been split into groups of five letters.

a. `YBKBV YI`

b. `WFBWT LIVTH JWVIV`

c. `HSPCP LCPJZ EZXZC CZH`

Task 3 — Cryptanalysis

The following ciphertext has been encrypted using a substitution cipher. You know that the six most common letters in the plaintext are `e`, `t`, `s`, `o`, `a`, `i` (the last three with roughly the same frequency). The six most common letters in the ciphertext are `c`, `k`, `j`, `w`, `o`, `n`.

Note: Spaces and punctuation from the plaintext has been retained unchanged.

```
ltncr wfoip ktcjc foknqcj uwj ktc oqchutcefnip nycw or ktc phcwk
utwec tnfjcer.  jmlt w bohkcikomj wiy fxjkchnomj foijkch homjcy
wee fx lmhnojnkx.  ktci ktc uney wiy ynjkwik jcwj utchc tc hoeecy
tnj njewiy amed; ktc miycenqchwaec, iwfcecjj bchnej or ktc utwec;
ktcjc, unkt wee ktc wkkciynip fwhqcej or w ktomjwiy bwkwpoinwi
jnptkj wiy jomiyj, tcebcy ko juwx fc ko fx unjt.  unkt oktch
fci, bchtwbj, jmlt ktnipj uomey iok twqc acci niymlcfcikj; amk
wj roh fc, n wf kohfcikcy unkt wi cqchewjknip nklt roh ktnipj
hcfokc.  n eoqc ko jwne rohanyyci jcwj, wiy ewiy oi awhawhomj
lowjkj.  iok npiohnip utwk nj pooy, n wf gmnld ko bchlcnqc w
tohhoh, wiy lomey jknee ac jolnwe unkt nk - uomey ktcx eck fc
- jnilc nk nj amk ucee ko ac oi rhnciyex kchfj unkt wee ktc
nifwkcj or ktc bewlc oic eoypcj ni.
```

Task 4 — Advanced cryptanalysis

a. Find the plaintext and the key word of the following Vigenère ciphertext when you know the key word has length four.

```
cwppt ikxtv ztvmw bcizk timvx dbeli kmtam bcopa tbaxg bativ
tmxwg hgigr cimbd vlhrw gvtqo xsigw hwwxs qvtim wvpve hcoxg
sckxl matgm fxiwg tvzxt ijtmi txyxm ewdnm apbpt gexap dxvdu
xmdlx wxktm tiihg bbhcw ymwim yxmew patyx vtegm lmxvz iaivx
uwkmw wlxlp hatzx zpdxm wmbka qoxhb atiba tivtm xwgfx oamaq
oxxbb lptmh vmmat zybii gwezh itzma pbpxh phnal whipb l
```

b. The following has been encrypted with the Vigenère cipher. Find a plausible candidate for the key length.

```
owmwr ulphl kwsyx jksfo zyias yvvxr gexlo slpxs zlhis znsyv
jsimx zymwd nrxlk bzrkx urhia arxiu tfapo jxisp zyifo efrhs
jfrsd viiwe svxlk zzlef kzxfe zfrid nzrks jfory crrhd nrxmc
zyexd uusmx plwxs ivsvd airqi hrgoy tklil kkxib ojeps qvero
bzpex jrhmc miego gehro bvvwr gcpmp krvez ujwml rvksy jiexr
kixlk trzss jrgib zrmro bzpmp efywk eksqo yfgvk zvwex ekywp
gzpwd utsrf oegie ynipo zpsyq ufrgy tumxs uexlk zpsyx ucsrq
kiwto tucse xcmjo oexls yjieb iyern zyexi ulkmf klttr ocswy
vycfe zzjcy ayevm glkld gkmxk mrmri ulqyc zumiw eiitv ezwqo
tfjed nvrws nfrse xrrhv umicy asyxs yyepv usicq uuved nvvxr
gecse gehar ociml xvexr krrhr gmixr kjxvo txxls yyepv tvzib
zlvrp xfqtr ocswy vycry xwvsw crvrs txern guqsx ojlmx mrrcy
lpsys ifqik iiswc tfxxy jzwkb gticy aigmd oqirc nztsp gxvik
ztmxi xvrsg tvhjy xzxwg ojhsw gehwd kekxr hpkmf oekcy aixly
axlxd uiiez oekxr kcevq kjxty yjmfv kyevf kjxsp cvepd nrrhr
uesyb gehkv uicex jxmzs txris zyivd nfykr zesvm giixr gkcse
srcvo gtlxr ksiwd oenyn mvqix zkvyd nrrhd nvwse r
```

Task 5 — Number theory

a. What is the remainder of 117 divided by 7? 110 by 7? -2 by 7?

b. Find an inverse for 3, 7 and 28 modulo 29.