IV054 Coding, Cryptography and Cryptographic Protocols
2011 - Exercises IV.

1. Decrypt the following cryptotexts:
   (a) 
   (b) CJ CI CF EI AG BI DJ DH DH DF DJ AF DG AJ
   (c) AQ HP NT NQ UN

2. (a) Show that if the shift cipher is used to encrypt a single character, it is perfectly secure.
   (b) Determine the largest cardinality of the plaintext space for which a monoalphabetic substitution cipher can be perfectly secure.
   (c) Suppose that the Vigenère cipher is used to encrypt plaintexts of length n. Show that this encryption can be perfectly secure.

3. Let $f \in \{0, ..., 7\}$. Consider the following cryptosystem $S_f = \{\mathbb{Z}_8, \mathbb{Z}_8, \mathbb{Z}_8, e_k, d_k\}$, where $e_k(m) = m + k^f$ and $d_k(c) = c - k^f$.
   For which f is the cryptosystem S_f perfectly secure given that each key $k \in K$ is used with the same probability.

4. Decrypt the following cryptotext. Show your reasoning.

```
ECVNK VDUTL CNZCC DAVUN RCEVK FHLDH DQKEN FVDGE VIENF VCDAV
RNAVQ FVQVL ZBPID RVEBG DZVUN GVZCV VIGPU UHCDA VOVVQ JNQKQ
VTTOV DPEHD QKEIP ECECV EINEV TPOYV ZETBG CPFDQ VGGBI ETMBT
TVTTN BQTBP ELDIK TPZZV TTUPW PIHCD AVDUL DHTTV VFVKE BFVZB
QEVFM ENOUV
```

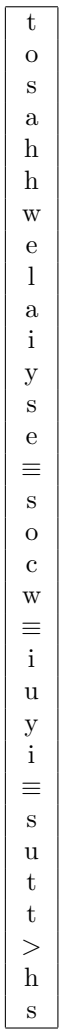
5. Consider the following cryptosystem. $P = C = \mathbb{Z}_{26}^2$, $K = M_2(26)^* \times \mathbb{Z}_{26}^2$, where $M_2(26)^*$ is the set of invertible matrices modulo 26 of degree 2.
   Encryption using a key $k = (M, v)$ is defined as $e_k(p) = Mp + v$.
   The cryptotext $c = \begin{pmatrix} 24 \\ 15 \end{pmatrix}$ was obtained using the key $(\begin{pmatrix} 11 & 4 \\ 1 & 17 \end{pmatrix}, \begin{pmatrix} 5 \\ 9 \end{pmatrix})$. Determine the plaintext. Justify your answer.

6. You have found an old cryptotext encrypted with the Vigenère cryptosystem. You have noticed that at positions 91, 1423 and 1819 the same cryptotext sequence of length 7 is repeated. What can you deduce from that?

More on next page >>

7. *(Bonus)* Decrypt the folowing cryptotexts:

(a)



(b) (Hint: 1984)

```
2,2,7,1 3,11,1,2 3,11,26,1 6,3,1,11 4,2,9,1 1,1,3,4 1,1,1,1
8,1,20,5 15,1,9,5 4,4,3,2 10,2,26,5 10,12,1,7 10,12,11,4
12,2,22,1 1,3,1,9 1,3,2,3 16,8,2,1 1,25,30,14 1,25,6,2
15,2,7,3 3,9,8,4 9,3,15,3 5,1,3,1 1,49,2,2 1,18,3,1 9,1,9,1
9,1,12,2 9,1,12,3 15,5,8,5 15,5,12,14 15,5,13,7 17,2,1,2
16,2,6,11 1,1,27,8
```

(c) 7777332228877744489998447776668844466622777722288777444899 9

(d) (Hint: plaintext is related to cryptography)

```
THSSTMMSTBPRCTCLL,FNTMTHMTCLLNDCPHRBL;
TMSTNTBRQRDTBSCRT,NDTMSTBBLTFLLNTTHHNDSFTHNMWTHTNCNVNNC;
TSKMSTBCMMNCBLNDRTNBLWTHTTHHLPFWRTTNNTS,NDCHNGBLRMDFBLTTHWLLFTHCRRSPNDNTS;
TMSTBPPLCBLTTLGRPHCCRRSPNDNC;
TMSTBPRTBL,NDTSSGNDFNCTNMSTNTRQRTHCNCRSFSRVLPPL;
FNLL,TSNCSSR,GVNTHCRCMSTNCSTHTCMMNDTSPPLCTN,THTTHSSTMBSTS,
RQRNGNTHRMNTLSTRNNRTHKNWLDGFLNGSRSFRLSTBSRV.
```