Applied Cryptography: Homework 2

(Deadline: 10:00am, 2020/09/23)

Justify your answers with calculations, proofs, and programs.

1. (10 points, question 2.28, page 58 of the textbook)

   Decrypt the following ciphertext, obtained from the *Autokey Cipher*, by using exhaustive key search:

   ```
   MALVVMAFBHBUQPTSOXALTGVWWRG
   ```

2. (20 points, question 2.21(a), page 54 of the textbook)

   The task is to determine the plaintext.

   Give a clearly written description of the steps you followed to decrypt each ciphertext. This should include all statistical analysis and computations you performed.

   The plaintext was taken from *The Diary of Samuel Marchbanks*, by Robertson Davies, Clarke Irwin, 1947.

   Substitution Cipher:

   ```
   EMGLOSUDCGDNCUSWYSFHNSFCYKDPUMLWGYICOXYSIPJCK
   QPKUGKMGOLICGINCGACKSNISACYKZSCKXECJCKSHYSXCG
   OIDPKZCNKSHICGIWYGKKGKGOLDSILKGOIUSIGLEDSPWZU
   GFZCCNDGYYSFUSZCNXEOJNCGYEOWEUPXEZGACGNFGLKNS
   ACIGOIYCKXCJUCIUZCFZCCNDGYYSFEUEKUZCSOCFZCCNC
   IACZEJNCSHFZEJZEGMXCYHCJUMGKUCY
   ```

   HINT *F* decrypts to *w*.

3. (20 points, question 2.21(b), page 54 of the textbook)

   The task is to determine the plaintext.

   Give a clearly written description of the steps you followed to decrypt each ciphertext. This should include all statistical analysis and computations you performed.

   The plaintext was taken from *The Diary of Samuel Marchbanks*, by Robertson Davies, Clarke Irwin, 1947.

   Vigenère Cipher:

   ```
   KCCPKBGUFDPHQTYAVINRRTMVGRKDNBVFDETDGILTXRGUD
   DKOTFMBPVGEGLTGCKQRACQCWDNAWCRXIZAKFTLEWRPTYC
   QKYVXCHKFTPONCQQRHJVAJUWETMCMSPKQDYHJVDAHCTRL
   SVSKCGCZQQDZXGSFRLSWCWSJTBHAFSIASPRJAHKJRJUMV
   GKMITZHFPDISPZLVLGWTFPLKKEBDPGCEBSHCTJRWXBAFS
   PEZQNRWXCVYCGAONWDDKACKAWBBIKFTIOVKCGGHJVLNHI
   FFSQESVYCLACNVRWBBIREPBBVFEXOSCDYGZWPFDTKFQIY
   CWHJVLNHIQIBTKHJVNPIST
   ```

4. (10 points, question 2.24, page 55 of the textbook)

   An *Affine-Hill Cipher* is the following modification of a *Hill Cipher*: Let m be a positive integer, and define $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^m$. In this cryptosystem, a key K consists of a pair (L, b), where L is an $m \times m$ invertible matrix over $\mathbb{Z}_{26}$, and $b \in (\mathbb{Z}_{26})^m$. For $x = (x_1, \ldots, x_m) \in \mathcal{P}$ and $K = (L, b) \in \mathcal{K}$, we compute $y = e_K(x) = (y_1, \ldots, y_m)$ by means of the formula $y = xL + b$. Hence, if $L = (l_{i,j})$ and $b = (b_1, \ldots, b_m)$, then

$$(y_1, \ldots, y_m) = (x_1, \ldots, x_m) \begin{pmatrix} l_{1,1} & l_{1,2} & \ldots & l_{1,m} \\ l_{2,1} & l_{2,2} & \ldots & l_{2,m} \\ \vdots & \vdots & & \vdots \\ l_{m,1} & l_{m,2} & \ldots & l_{m,m} \end{pmatrix} + (b_1, \ldots, b_m).$$

   Suppose Oscar has learned that the plaintext

   `adisplayedequation`

   is encrypted to give the ciphertext

   `DSRMSIOPLXLJBZULLM`

   and Oscar also knows that $m = 3$. Determine the key, showing all computations.