IV054 Coding, Cryptography and Cryptographic Protocols
2014 - Exercises IV.

1. Decrypt the following ciphertexts:

   (a) `CHICKEN'S FLIPPER FORK`

   (b)
   ```
   DLCCC QDIKW YQDFC ZVYMX GMEJV CGPRM DQYDL CWERS GYVPW SRBOG GZLCB EZVI
   SXKEW RXSRL IPOUS SVCNX MLIQO GPOXY XHGDQ SCXZO EZVIR YJYVP GXXMD LCREL NWMPX FOILO
   QWGMR RSSDM LMSLF ILSIL MI
   SXQUI WWYQD FCMSK WYLSG YLPCK RBBIR KMLKF JOAGD LMEXR RIFOP NYJUB MRDIL XSROW YXHAR
   ELQIY LPCYV KYHGP MYLPC KXRRI USPJY JRRIA YVPOW NYRBO RRC SXKEW RLIYZ TJSGY LPCDS
   ROPCQ VYZLG MGMBV CCTMX HCXGC
   SXKEW RLINY VRKFJ OELNM RCYQK KCKRB PYLMX GYRKE WRXSR BIOEM POXFO GMXGM EVQOS DCITO
   VYVTC YTJO
   PMLKP JIMRS WLOGC CWYBC ESZCX XFOGG BGSWW RKRAO WRRER MSKWE LNMRC ENZPG MERSS LDLYD
   XFOWW CXCWF COEQI XMEWC BIOEM PSREX IGDLC BQCXX YVWRB EGXRM BXFOO LYAJO HEOSD KPMXK
   QOVGO WMPVS VIQDS MLWCB ZC
   ```

   (c) `YLJHQHUH`

2. Consider the following variation of the one time-pad cryptosystem. Let $P = K = \{00, 01, 10\}^\ell$. Encryption and decryption work the same way as in the one time pad.

   (a) Is this cryptosystem perfectly secure?

   (b) Is it secure if $P = K = \{00, 01, 10, 11\}^\ell$?

3. Consider using a double encryption in order to increase security of a cryptosystem. The double encryption works as follows:

   (i) Generate and share two secret keys key_1 and key_2.

   (ii) Encrypt message m with key_1 and obtain ciphertext c_1.

   (iii) Encrypt c_1 with key_2 and obtain ciphertext c_2.

   (iv) Send c_2.

   (v) Receiver decrypts c_2 with key_2 to obtain c_1.

   (vi) Receiver decrypts c_1 with key_1 to obtain m.

   For the following cryptosystems, show that the proposed encryption has actually the same effect as a single encryption with a different key key_3 ans describe how to obtain key_3 from key_1 and key_2.

   (a) the Caesar cryptosystem,

   (b) the Hill cryptosystem,

   (c) the Vigenère cryptosystem.

4. Consider a binary one time pad encryption with a key of length five. You have intercepted the following cryptotexts:

   ```
   10100 10001 00101 11101 10111
   ```

   You have the following information: the same key was used for all five words and the plaintexts are cyclic shifts of each other. Find the plaintexts and the key.

5. Consider the following modified Hill cryptosystem: $c_c = Mc_w + v \bmod 26$, where v is a column vector of length n. You are leading a known-plaintexts attack against such system. The known pairs [plaintext, cryptotext] are

   $$\left[\begin{pmatrix}4\\20\end{pmatrix}, \begin{pmatrix}0\\16\end{pmatrix}\right], \left[\begin{pmatrix}13\\6\end{pmatrix}, \begin{pmatrix}14\\11\end{pmatrix}\right], \left[\begin{pmatrix}6\\23\end{pmatrix}, \begin{pmatrix}9\\19\end{pmatrix}\right].$$

   Find M and v.

6. Consider the Affine cryptosystem. Explain why one can not use a such that $\gcd(a, 26) > 1$.