IV054 Coding, Cryptography and Cryptographic Protocols
2019 - Exercises IV.

1. *(4 points)* Decrypt the following cryptotexts:
   (a) 72 65 76 70 32 79 70 32 65 32 80 79 73 78 84 32 73 83 32 89 79 85 82 83
   (b) me e emm memm mmm eme mem
   (c) ATOM RUIN
   (d) 01110 01111 10010 10100 01000 10100 01111 10111 00101 10010
   (e) 97 11 71 71 23 13 47 73 43 7
   (f) IBBIKS INBMZ LQVVMZ
   (g) PRMT RM ZERTMLM
   (h) FWALOTNALHICLENKOMB

2. *(4 points)*
   (a) Using the affine cryptosystem with parameters $a = 11$ and $b = 16$ encrypt the message `CODING` and decrypt the message `MVUZRO`.
   (b) Using the Hill cryptosystem with
   $$M = \begin{bmatrix} 1 & 3 & 11 \\ 22 & 8 & 1 \\ 4 & 15 & 24 \end{bmatrix}$$
   encrypt the message `CODING` and decrypt the message `JTUYVC`.

3. *(4 points)* Find the unicity distance of the following ciphers. Suppose the keys are chosen uniformly at random.
   (a) the pigpen cipher;
   (b) Vigenère cipher with keylength 7;
   (c) transposition cipher with period 7;
   (d) the one-time pad.

4. *(5 points)* Consider a secret key cryptosystem with message space $P = \{0, 1, 2, 3\}$, key space $K = \{0, 1, 2, 3\}$ and encrypted message space $C = \{0, 1, 2, 3\}$. The encryption functions are given by the following table:

$m \backslash e_k$	e_0	e_1	e_2	e_3
0	3	1	2	1
1	2	0	3	3
2	1	3	0	2
3	0	2	1	0

   (a) Suppose K is distributed uniformly and P with a probability distribution $p_P(0) = p_P(1) = \frac{1}{6}, p_P(2) = p_P(3) = \frac{1}{3}$. Calculate $p_C(0), p_C(1), p_C(2)$ and $p_C(3)$.
   (b) Consider uniformly distributed keys K. Is the cryptosystem perfectly secure? If not, change one of the encryption functions e_i so that the cryptosystem becomes perfectly secure.

5. *(4 points)* To save resources used by sending the keys, the following simplified one-time pad cryptosystem was implemented. The cryptosystem uses a randomly generated key k_1 during its first use, but to encrypt i-th plaintext w_i, $i > 1$, instead of using new key k_i, the previous plaintext is used, i.e. $k_i = w_{i-1}$, $i > 1$. You managed to intercept all the cryptotexts c_i created by this cryptosystem and also the third plaintext w_3. Find the first plaintext w_1 and the original key k_1.

More on next page >>>

6. *(5 points)* For 26-letter alphabet, determine how many affine ciphers are there that leave

   (a) no characters fixed;

   (b) exactly one character fixed;

   (c) at least two characters fixed.

7. *(4 points)* Break the following cryptotext produced by the Vigenère cipher. Find the key length, the key and decipher the cryptotext. Explain your reasoning.

```
GBLZWW IVHUBS SHSXUO MKDMKO VQCYSF EJDZDR ISSGPY YSJLLH OCSHJH ZOPLUW XYUSUS JKSJLU
EPSQYZ OKSHVD ABYGHG KNWSEZ NDRWMC SVWBGH BLLSDB WHWKOF QYRTDO NWSJCQ LHZTIK BZKFOP
JYWNHZ GULHWC UGSFDC VHXBIP PJSMWC DGCWVS BUWVWB CQBGMY QHNSYZ CXMCSV WBMLBW SAKHWO
HIWXDS ICMBNK KSSNHG UVULAW NNRVSF YLBNOH WSVKHH KUSJKS JGBLQZ SHIOUD QDGWAO LJSVYQ
HLYNKS NSAHBW BYFWHR YUVWGL RHWDIW VWTIXF FKFRTL RYVCUS YWMGPU UHKGCW VLRYLB LOHWWG
XIIDSD YQHAXA KWKSXH OSZJDF WXNOMM XUZOJO NKOLRY ZOKCYY SJKFFS FDOUWW CNRCDK NHPSLV
DUWDIR KJYNHH GDBHGG MCHHQZ ILBLSH JCMDNK OLDBHQ QZBHFA CUYSJI IORGXY DBVDIE SXYOQR
AXGRGL LIRYKD BZOADY VKSCOQ OHYFRU WDCFOF NWKODV YQUWNV DPTKAH HGLLHO CRCVQA ZBHFOR
YWVWBI UBGDCW KSCVUS SUUEZW GUVWJB YOSNKH WHGGBH HZOLRF FYNLHO KMQSOL OWPSLV DUWCWX
FAYMLH QGUVGM PZLQAO HWZQKL RIKOXI CJRCPH GOGEOJ UIQOKO UUQZPI UOOOUN BWCMLB LRYYWY
OHHFWM CSVWBW UOUUCQ USNCIT AMOOHU SJKSJS MDYAXN RQDSGE WFQUVV WOLFZA PZIOUO NKSUBS
SHSXUO MKDCVG WOELBY KHBBGY ERFUBU QBQDBD HUYOOR HBIYWV ONKSKV CJVLOM WTGYNK CDNCQO
EYHROD ZBDPWD CFQAZB HFLRYF FQZNDB SVSVHO SFOZSD WKCFDI WVWPLH EMOHFM GPNKSD ONWSJC
VHQSEM HHZOWR AEYHHG LVYWHW BMVIUR UVSLKH GOOSFO GLKHGC MDHRAS DNHFZY QWVWIB DJWLYH
BVSMJI ACYGWF DBHDGV SDZHRU ESLSWY WYOHHF WMCSVW BNKSXB YTIWXW LSKKLH AMMBPC JOVDZS
XWHRTO WDIKON KSCOSZ CJNCVI KOXWCK GCWQZL YWKWOH FWHRYU ODZBDP WDMKSF MYDHXS LVHKSA
KHLRYU CUUZDQ WCYHAK ZYUTWM NOMKWI RHZCCP CFCCQU ZDBHQG NYECGU
```

8. *(Bonus, 2 points)*

   (a) I finished my second book. It was on the sixth day of Christmas. The manuscript was hidden on the bottom of the seventh drawer of my table. Fortunately, my friend called and said he can come over in three days. At first, I could not believe it. But my four-leg friend Hop greeted John in the door.

   (b)