IV054 Coding, Cryptography and Cryptographic Protocols
2018 - Exercises IV.

1. Decode the following cryptotexts:
   (a) NRIILI XRKSVI
   (b) DWWDFN DW GDZQ
   (c) DIBHAJ AGCFAFAHBJ AHBHAFCGAGAJDG
   (d) ⊐□⊐□⊡>⊏ ⊐⊏⌜·⌜
   (e) SLHOIPCEEMEAYCRANRTIFNTTAPRCSA
   (f) GO HAPPILY ERA
   (g) HUMANITIES HORN JETS
   (h) aaab a ba aa aaab aa baa aa aaab aa baba aa

2. Consider the Hill cryptosystem with the following plaintext-cryptotext pairs:

$$\left(\begin{bmatrix}9\\2\\8\end{bmatrix}, \begin{bmatrix}17\\19\\11\end{bmatrix}\right), \left(\begin{bmatrix}16\\7\\14\end{bmatrix}, \begin{bmatrix}4\\11\\23\end{bmatrix}\right), \left(\begin{bmatrix}12\\16\\9\end{bmatrix}, \begin{bmatrix}21\\11\\2\end{bmatrix}\right).$$

   (a) Without determining the key, decrypt the cryptotext

$$\begin{bmatrix}12\\4\\13\end{bmatrix}.$$

   (b) Find the key.

3. Consider the Polybius cryptosystem where the keys are all the unique 5×5 inner squares with 25 English letters with uniform distribution over keys.

   Calculate the unicity distance for this cryptosystem, assuming that English without the letter J has the same redundancy as normal English.

4. Decrypt the following ciphertext:

```
111000 101010 101001 010100 011100 110000 111010 100000 010100 111000 111000 100010
```

5. Consider a secret key cryptosystem with message space $P = \{0, 1, 2, 3\}$, key space $K = \{0, 1, 2, 3\}$ and ciphertext 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	0	1	2	1
1	1	2	3	3
2	2	3	0	2
3	3	0	1	0

   (a) Suppose both P and K are distributed uniformly. Calculate $p_C(0)$, $p_C(1)$, $p_C(2)$ and $p_C(3)$.
   (b) Is the cryptosystem with uniformly distributed keys K perfectly secure?
   (c) Change one of the encryption functions e_i so that the cryptosystem becomes perfectly secure with uniform distribution of keys K.

More on next page >>>

6. Consider a variant of the Playfair cryptosystem, in which for each digram an encoding table is chosen uniformly at random.

   (a) How many possible encryption tables exist?

   (b) What is the probability that a digram ij gets encrypted as xy, where i, j, x and y are different letters?

   (c) What is the probability that a digram ij gets encrypted as jx, where i, j and x are different letters?

   (d) Is this cryptosystem perfectly secure?

7. Consider a p-ary alphabet where p is prime. What is the size of the keyspace in

   (a) the Affine cryptosystem?

   (b) the Hill cryptosystem?

(Bonus) What is the keyspace size of the Hill cryptosystem over the 26-ary alphabet?

8. Find the key length, the key and decipher the following cryptotext produced by the Vigenère cryptosystem. Explain your reasoning.

```
DOSSE IXUGL TGGLU TLCGT RRHRE ENRUW JFJVA GJZXI PXTST ZTJXT KRJTT HDOSC CCVJW VMIFB
PSZXL VXGBW ZJVRH CLIWQ HPOWK ITAKG JGEVP KHYKL YTKHV JFWMJ WJUMU VQJVI CYXPH TFQRE
GHVCC WGTST FKPBB SUSIE TWGVY IPXXS IGYDE KGYVH KMVVV UMUVQ JVICE TOSKF PKZJH FEPAB
PHYVX YXPHZ VXJVG BKLVA PJSEJ GJHNO IJIZT OWEVH DTDPR XIUXZ HVEWK OGBFK IUBPH YVQGT
PHZDI JBUHV TLPBS IVNEU BPRVG IPWGB KCCFB UQFMI TXFPP WVKXF FZTLY BNVVC QMTUW JBMCK
GHZII FITIJ JMCGC FDPSH YKQVI IXXTG ZEGGX KUYKI GGUWO KCVAT SVNLG GJSGL FNBUV VULKL
EFPGX CGCZP KMEUT SRBXJ KQIXY MPWKS XVLGB OGTYV KYVSE LRFWK SUVGJ BHTIZ VMNPG KJIEK
GHNIM VBPUR EHVAG OIKSH WGQZG LGKKB XKLGM GQYEM SNGVR JFGXP YEFAP TUHYV OCLKG BZXGL
VOEUF CUDOX VWEHP HIZFW MKCEY EUUGS ECETZ GZPZK PHTSU RRFPJ MUZHD TDPRX IHTKZ KFTWU
NWTZD GAKGT IEEDK BXFJU NEVRM MVTNQ ZGLGK JSTVV VTKBC PLCWC VRSMV HHBFK JKGKG YZRII
TCAVG VLCBU ESVIW PCZWJ BPUYZ WFBUQ FMITB GGNYM EAOWX YXUNI UVJXV ACHKY MUBUX LJXQG
GAFII GQCAG CIQYJ WJCEE DCRRZ WKVCZ RKXKM WRVYS YXXSI KLGKG WJRRC EVSIE EVXGL GCEPT
VWFEJ QKJWJ RRQGA AZKCJ BURZJ GQOGF PFGEN TFVUW QHPOW KITMJ SFLXD KGOBF JVAGQ IZQGT
PKRIE PWQBV KLGHT MZJXJ TVWKX EXXVV VSVKM KGYRG NXCFR UZCGV OXVSX XTHYV MTKWG JZEPX
PSDPM VBUEL ZXGIQ GJZFN XVVRK XJXDF ZKMUA OWCZX CKARV DEPWG RKYEV UCPSR KGDGS GYMUP
QFBJI EKGHK YYUIT CMZHK GIHYV QYBVV REMPX ASRIL GTFGK RVVHX SIKLG KGGKF JVAGK FIPFB
HHYZW YTUHY VGCLG HYVRK MYCLC HHBVW ENMVA VVVCS PZUHR EHKGI HIRHK MKCEF JJNUV ZEKWI
ECUVF TXCYZ EKCVJ WVMIO XPHJZ RVAGW EKITX UHJFJ PTVWF EENLG QLIMV RCDIR GVBES KYEVA
CGTFR VBPIV UMPMQ HYVXY XPHZV XJVGB KLVAL KAFEW KGIVK YIEHF SSFSM
```