IV054 Coding, Cryptography and Cryptographic Protocols
2015 - Exercises V.

1. (a) Consider a code with minimum distance d. What is the maximum number of erased bits you can always correct with this code? An erased bit is a bit that cannot be read.

   (b) Consider the binary $[7, 4]$ Hamming code with parity-check matrix

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

   Decode the codeword 0110???, where ? represents erased bits. Explain why this does not contradict the previous result.

2. Find the relation between the codes meeting the Singleton bound and the codes meeting the Hamming bound.

3. Find all prime numbers q such that the linear code over $\mathbb{F}_q$ with generating matrix

$$G = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}$$

   is cyclic.

4. Suppose the following cryptotext[1] is a result of applying the Vigenère cryptosystem on an English text:

```
WZHIC VSUUL BDNDA WWWJC WARJL BAMWN RTDLY UQKEH JTDSU XKDBI QYSUR WKZHY HSRYY
ULNQH DDXPY ZASXN KWGUF SGEIN DLHIN LUZBG HLGEX VKTSB DKJQM LKJYM PWSXI GSKII
GARSI YWQUX EQBXU UDDIV DTAQA HAMJB LKDNY UUHIY BGTQL HKTFJ RKDTN RMRUZ UADTG
DFLUN KGCJB RMFXN KARCY WZNTC VNDHS VEZHN LFCUY GFDLY ULGUF HKRTI HKMEN KACUM
WSSYM WABII ILGUJ OSHDN HPSOI XUZDU OKNIY HLGYM EQSXY ISBJN KSSJB HJDQL HUHFB
HJSUR WHKQC QLDNN SSHHZ RJVXC FZMEM XASQV OWJUS HPHIN VXNKL
```

   (a) Use the Friedman method to determine the key length.

   (b) Decrypt the message.

5. Suppose you have intercepted three cryptotexts

$$c_1 = 1010010110,\ c_2 = 0101101110,\ c_3 = 1001101010$$

   encrypted with the one-time pad cryptosystem. You also managed to find out that, out of laziness, the sender used the same key for all three plaintexts and that the corresponding binary plaintexts w_1, w_2, w_3 have weights 2, 5 and 8, respectively. Can you recover the plaintexts and the key?

6. Decrypt the following cryptotext[1] using the hint 0077095030:

37, 13, 14	39, 3, 39	307, 6, 25	129, 1, 38	269, 21, 35	148, 17, 31	5, 10, 46	88, 9, 56
9, 28, 27	207, 11, 38	342, 13, 4	39, 7, 29	75, 5, 74	390, 2, 46	208, 6, 17	9, 15, 44
306, 3, 1	77, 31, 64	65, 4, 66	6, 28, 55	385, 1, 55	249, 5, 49	183, 14, 29	41, 9, 73
152, 9, 58	307, 7, 17	360, 10, 5	125, 3, 57	15, 21, 30	77, 35, 6	10, 39, 9	307, 2, 10
342, 16, 30	245, 8, 26	86, 3, 28	10, 5, 10	15, 14, 48	77, 3, 23	307, 3, 6	

[1] Available as text file in the Study Materials in IS MU.