IV054 Coding, Cryptography and Cryptographic Protocols
2012 - Exercises I.

1. Let $d \geq d'$, q, $n \in \mathbb{N}$. Show that $A_q(n, d') \geq A_q(n, d)$.

2. Compute in detail code rate of the following binary codes:

   (a) $C_1 = \{1000, 1101, 0010, 0111\}$,

   (b) $C_2 = \{1000, 0110, 0111, 1101, 0010\}$,

   (c) a code with $n = 7$ and $M = 16$.

3. Every bit sent through a binary *erasure* channel is substituted with a special symbol e (e stands for erasure) with probability p.

   (a) Suppose n–bit codewords are used. How many different n–symbol strings can appear as the channel output?

   (b) For the binary erasure channel, derive an upper bound analogous to the sphere packing bound.

4. How many valid ISBN numbers start with $08493852x_9x_{10}$? Which of these books do you consider useful for study of cryptography?

5. (a) Construct a Huffman code for the letters A, B, C, D, E and F with the frequency of use given below.

Letter	Frequency
A	30%
B	22%
C	15%
D	13%
E	10%
F	10%

   (b) Find the average word length of the proposed Huffman code.

6. Suppose C is a binary optimal prefix code for a set of messages $S = \{x_1, \ldots, x_n\}$, where message x_i occurs with probability p_i. Prove the following statements.

   (a) If $p_j > p_k$, then $l_j \leq l_k$, where l_i is the length of codeword for the message x_i.

   (b) The two longest codewords have the same length.

   (c) The two longest codewords differ only in the last bit and correspond to the two least likely messages

   A prefix code is a code such that no codeword is a prefix of any other codeword.
   An optimal prefix code C is a prefix code with minimal average length, *ie.* if C' is another prefix code for S then

$$\sum_{i=1}^{n} l_i p_i \leq \sum_{i=1}^{n} l_i' p_i$$

   where l_i' is the length of codeword for the message x_i in C'.