*IV054 Coding, Cryptography and Cryptographic Protocols*
**2016 - Exercises I.**

1. (a) Determine $A_2(4,3)$ and $A_2(5,4)$.
   (b) Prove that $A_2(n,2d) \leq 4A_2(n-3,2d-1)$.

2. Alice and Bob are communicating with each other. Since their communication channel is noisy, they use the following code:

$$\begin{aligned} 00 &\rightarrow 010010 \\ 01 &\rightarrow 000101 \\ 10 &\rightarrow 101000 \\ 11 &\rightarrow 111111 \end{aligned}$$

   Bob receives the message 001101. Assume that the probability of a bit error is $p = 0.01$.

   (a) What is Bob's decoding of the message?
   (b) What is the probability that Bob's interpretation of the message is the same as Alice intended?
   (c) What is the probability that Alice actually wanted to send the message 11?

3. Prove the two following properties of the entropy function

$$S(p_1, p_2, \dots p_n) = -\sum_{i=1}^{n} p_i \log p_i.$$

   (a) For any two probability distribution $\sum_{i=1}^{n} p_i = 1$ and $\sum_{i=1}^{n} q_i = 1$ it holds

$$S(p_1, p_2, \dots p_n) \leq -\sum_{i=1}^{n} p_i \log q_i.$$

   (b) The entropy function reaches its maximum for uniform distribution, i.e. for any probability distribution $\sum_{i=1}^{n} p_i = 1$ it holds

$$S(p_1, p_2, \dots p_n) \leq S\left(\frac{1}{n}, \frac{1}{n}, \dots \frac{1}{n}\right).$$

4. Consider a binary symmetric channel with physical capacity of transmitting 900 bits per second. Assume that this channel can transmit 500 bits per second with arbitrarily low error probability. How can we bound the error probability of this channel?

5. Determine $x$ in ISBN 0345272$x$52.

6. Consider a channel characterized by the following conditional probabilities, where X and Y are the probability distributions of the input and output, respectively.

$$\begin{aligned} P(Y = 0|X = 0) &= 1 \\ P(Y = 0|X = 1) &= p \\ P(Y = 1|X = 0) &= 0 \\ P(Y = 1|X = 1) &= 1 - p, \end{aligned}$$

   for some $0 < p < 1$.

   (a) Calculate the probability of $t$ errors in $n$ received bits if the input distribution is $P(X = 0) = q$ and $P(X = 1) = 1 - q$, $0 \leq q \leq 1$, independently for every bit.
   (b) For which $q$ will this value be minimal?

7. Consider a source is producing symbols with the following probabilities: A = 0.20, B = 0.22, C = 0.22, D = 0.18, E = 0.10, F = 0.04, G = 0.04.

   (a) Construct a Huffman tree.
   (b) Calculate the average bit length of the code constructed in (a).