WOLFGANG K. SEILER B6, B4.18
Tel. 2515

October 1, 2018

Mathematics and Information, Exercise sheet 4

Problem 1: (*6 points*)

The following cipher texts are english words encoded by a Caesar cipher. Find them!

a) bcjkun *b)* htzwxj *c)* iylepa *d)* jfkfpqbo

Problem 2: (*6 points*)

a) For an arbitrary monoaphabetic substition, the 26 letters of the alphabet are permuted. Compute the entropy of the key under the assumption that all permutations are chosen with the same likelyhood!

b) How can a cryptanalyst find out that a cipher text was encoded using such a monoalphabetic substitution?

c) A permutation cipher writes the plain text as a sequence of blocks of a given length r and applies a permutation from $\mathfrak{S}_r$, the full permutation group on the r positions. If r is chosen as an integer from 10 to 30, what's the entropy of the key?

d) How can a cryptanalyst find our that a permutation cipher was used?

Problem 3: (*3 points*)

In the first half of the twentieth century, so called rotor machines were popular in cryptography. A rotor was a cylinder with 26 contacts on each of its two disks; the internal wiring gave a permutation from $\mathfrak{S}_{26}$. On top of the barrel, there was a ring with the 26 letters of the alphabet; this ring was movable, so that the user could freely decide, which contact corresponded to the letter A. For the german Enigma, five rotors existed, of which three were put into the machine. For encryption, a letter was given into the first rotor, whose output went into the second rotor and from there to the third. The output of the third rotor was subjected to a fixed permutation and then went back through rotors three, two and one, giving a letter of the cipher text. After each letter, the first rotor, and sometimes also the second or third, moved by one position, so that the cipher text also depended on the initial positions of the rotors. Compute the key entropy of this machine!

Problem 4: (*5 points*)

A given source produces sequences of zeroes and ones, but the probability for a one is only 1/200.

a) Compute the entropy of this source!

b) The sequences produced by this source are divided into blocks of length one hundred. For each sequence containing at most three ones, a code word is chosen, and there is also one singe word for all sequences containing more than three ones. All code words have the same length, Determine the smallest possible length of these code words and the probability of the word for sequences with more than three ones!

Can be submittel till Thursday, October 4, 2018 at 11.55h