## Cryptography Problem Sheet #2

**Problem 5** A monoalphabetic substitution  $\pi : \{A, B, C, \ldots, Z\} \to \mathfrak{B}$ , where

has been applied to an English plaintext, which was taken from a detective story by Agatha Christie. The resulting cipher text is

The plaintext contained the words MISSMARPLE. Decrypt the cipher text.

Problem 6 (CBC mode for monoalphabetic ciphers)

Let  $\mathfrak{A} = \{A, B, \ldots, Z\} \cong \mathbb{Z}_{26}$  and  $\sigma : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$  be a permutation. The CBC mode for the monoalphabetic cipher given by  $\sigma$  is defined as follows: Let

$$x = (x_1, x_2, \dots, x_N) \in \mathbb{Z}_{26}^N$$

be the plaintext and  $y_0 \in \mathbb{Z}_{26}$  an arbitrary initial element. Then the encrypted text  $y = (y_1, \ldots, y_N)$  is defined by

$$y_i := \sigma(x_i + y_{i-1})$$
 for  $i = 1, ..., N$ .

a) Show that if  $\sigma$  is a Caesar shift, then the decryption of the CBC mode for  $\sigma$  can be reduced to the decryption of an ordinary Caesar shift. Why does this method not work for a general permutation  $\sigma$ ?

b) Decrypt the following cipher text which has been obtained from an English plaintext using the CBC mode of a Caesar shift:

## ALBILFKVNXEYTWQXEHCDZQUOVYL

**Problem 7** An element  $\sigma$  of a group is called an involution if  $\sigma \neq e$ , but  $\sigma^2 = e$ , where e is the unit element of the group. Determine the number of all involutions  $\sigma \in \text{Aff}(1, \mathbb{Z}_{26})$ .

**Problem 8** In the following, the elements  $\varphi$  of the group  $\text{Aff}(2, \mathbb{Z}_{26})$  are used as bigram substitutions (Hill ciphers of order 2).

a) Determine, if possible, an element  $\varphi \in Aff(2, \mathbb{Z}_{26})$  that transforms MUNICH into LONDON and an element  $\psi \in Aff(2, \mathbb{Z}_{26})$  that transforms MUNICH into VIENNA.

b) How many elements  $\varphi \in Aff(2, \mathbb{Z}_{26})$  transform JUNE into JULY ?

Due: Friday, April 29, 2005, 14:10 h