MATHEMATISCHES INSTITUT
DER UNIVERSITÄT MÜNCHEN
Prof. Otto Forster

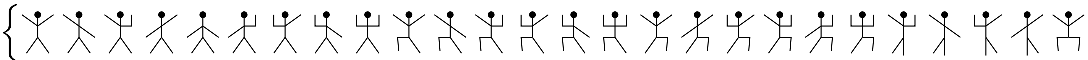
SS 2007
April 27, 2007

Cryptography

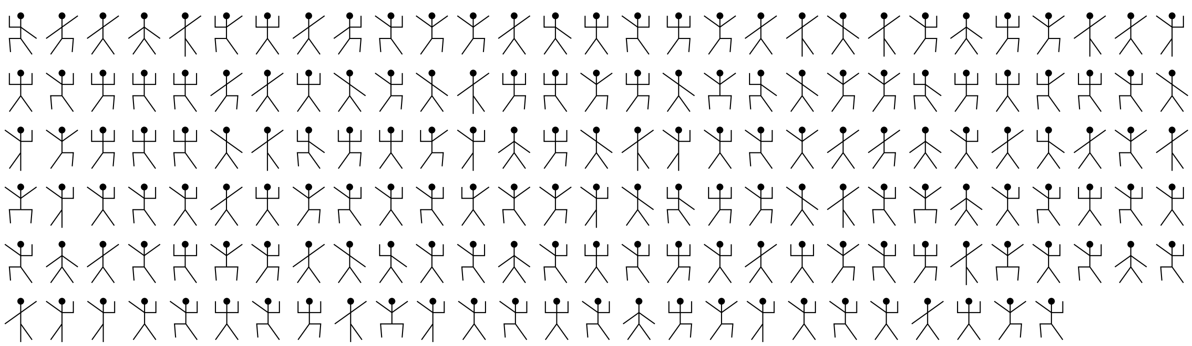
Problem Sheet #2

Problem 5

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

$\mathfrak{B} = \Big\{$  $\Big\}$,

has been applied to an English plaintext, which was taken from a detective story by Agatha Christie.



Decrypt the ciphertext.

Hint. The plaintext contains the words `MISSMARPLE`. Remember also that `THE` is the most frequent trigram in English.

Problem 6

a) Using the extended Euclidean algorithm, calculate the inverse of 55 modulo 89.

b) Calculate integers λ, μ with

$$101\lambda + 211\mu = 1.$$

Problem 7

In this problem, the elements of $\mathrm{GL}(2, \mathbb{Z}_{26})$ are interpreted as Hill bigram substitutions.

a) Determine an element $\psi \in \mathrm{GL}(2, \mathbb{Z}_{26})$ that transforms `BERT` into `HERB`. Is ψ uniquely determined?

b) Same problem with `PETE` and `ALEX`.

c) Prove that there is no $\psi \in \mathrm{GL}(2, \mathbb{Z}_{26})$ that transforms `KAIN` into `ABEL`.

Problem 8

A bijective map $\sigma : X \to X$ is called an *involution*, if $\sigma \circ \sigma = \mathrm{id}_X$, but $\sigma \neq \mathrm{id}_X$. An example is

$$\texttt{rot13} : \mathbb{Z}_{26} \to \mathbb{Z}_{26}, \quad x \mapsto x + 13.$$

a) Determine all involutions in $\mathrm{Aff}(1, \mathbb{Z}_{26})$, which is the group of all maps

$$\sigma : \mathbb{Z}_{26} \to \mathbb{Z}_{26}, \quad x \mapsto \sigma(x) = ax + b, \quad a \in \mathbb{Z}_{26}^*,\ b \in \mathbb{Z}_{26}.$$

b) Determine the number of involutions in $\mathrm{GL}(2, \mathbb{Z}_{26})$.

Hint. Use $\mathrm{GL}(2, \mathbb{Z}_{26}) \cong \mathrm{GL}(2, \mathbb{F}_2) \times \mathrm{GL}(2, \mathbb{F}_{13})$. Consider the possible eigenvalues of involutions.

Due: Friday, May 4, 2007, 14:10 h

Solutions should be returned in the Cryptography letter box in the first floor of the Institute in front of the library.