MATHEMATISCHES INSTITUT
DER UNIVERSITÄT MÜNCHEN
Prof. Otto Forster

SS 2005
April 14, 2005

Cryptography

Problem Sheet #1

Problem 1 The following cipher text was obtained from an English plaintext using a Caesar shift σ_d with offset $d \in \mathbb{Z}_{26}$:

```
TVSFP IQWLI IXRYQ FIVSR I
```

a) Find the plaintext and the offset d.

b) Apply σ_d repeatedly to the cipher text. What happens? Formulate a theorem that explains the phenomenon and prove it.

Problem 2 You can define a permutation of the alphabet by using a *keyword* and an *offset* (given by a character) in the following way: Write down the characters of the keyword in the order of their appearance in the word (each character only once). We obtain a string of all characters of the alphabet by appending all the remaining characters in their alphabetic order. The permutation will send the offset to the first character of the string, the alphabetic successor of the offset to the second character of the string and so on (where `A` is the alphabetic successor of `Z`). An example may illustrate this. The keyword `CRYPTOGRAPHY` with offset `D` yields the following permutation:

```
a b c D E F G H I J K L M N O P Q R S T U V W X Y Z A B C d e f ...
    C R Y P T O G A H B D E F I J K L M N Q S U V W X Z
```

a) Encipher the first sentence of this problem until the colon ':', using the permutation given by the keyword `SUMMERTIME` with offset `F`.

b) The following cipher text was created by encoding an English plaintext, using a permutation as described above:

```
MRIKG JFWCZ DKRZZ MIKYN ZMRNJ KYVTV GJICM QZEMT FEZ
```

Find the plaintext, the keyword and the offset.

Problem 3 Let $n \geq 1$ and σ a permutation of the set $\{1, 2, \ldots, n\}$. We define a transposition cipher $T = T_{n,\sigma}$: The text is divided into blocks of n^2 letters. These letters are written as the n rows $(x_{i1}x_{i2}\ldots x_{in})$, $i = 1, 2, \ldots, n$, of an $n \times n$-matrix. The transformed block is the sequence of columns $(x_{1\sigma(j)}x_{2\sigma(j)}\ldots x_{n\sigma(j)})$, $j = 1, 2, \ldots, n$, in the permuted order. (If the last block is shorter than n^2 letters, only the upper part of the matrix is filled, and the columns become shorter.)

---

p.t.o.

The following text was obtained from an English plaintext using a transposition cipher as described above with $n = 5$:

```
UBEPA PCRGY EICOH IUKYR SLYTP
```

a) Find the plaintext and the permutation σ.

b) Show that there is an integer $N > 0$ such that $T_{5,\sigma}^N$ is the identity map.

c) Determine the smallest such N (the order of $T_{5,\sigma}$).

Problem 4 For fixed n, let G be the set of all transpositions $T_{n,\sigma}$ as described in the previous problem. Decide whether G is a group (with respect to composition of maps). Give a proof for your answer.

Due: Thursday, April 21, 2005, 14:10 h