MATHEMATISCHES INSTITUT
DER UNIVERSITÄT MÜNCHEN
Prof. Otto Forster

SS 2007
April 20, 2007

Cryptography
Problem Sheet #1

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

BPMZWBWZUIKPQVMMVQOUIEIACAMLQVEEBEW

a) Find the plaintext and the offset d.

b) Prove that $\sigma_d^{-1} = \sigma_d^k$ for some positive integer k and determine the (smallest) value of k in the present case.

Problem 2 A permutation of the alphabet can be constructed 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) and append the remaining characters of the alphabet 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 TAKEITEASY with offset S.

b) The following ciphertext was created by encrypting an English plaintext, using a permutation as described above:

PQOAJ TCYEW MRERL UTXLN QCYOB DNBCY CDCYR EBYBQ LBJ

Find the plaintext, the keyword and the offset.

Problem 3 Let π be a permutation of the alphabet $\mathfrak{A} = \{\mathtt{A}, \mathtt{B}, \ldots, \mathtt{Z}\} \mathrel{\widehat{=}} \mathbb{Z}_{26}$. Encryption using monoalphabetic substitution by π can be enhanced by different modes of operation (CBC, CFB, OFB). All modes use an initial element $v_0 \in \mathbb{Z}_{26}$. The ciphertext $z = (z_1, \ldots, z_N) \in \mathfrak{A}^N$ corresponding to a plaintext $x = (x_1, \ldots, x_N) \in \mathfrak{A}^N$ is calculated as follows:

(CBC)	$z_0 := v_0,$	$y_i := x_i + z_{i-1},$	$z_i := \pi(y_i)$	for $i \geq 1$,
(CFB)	$z_0 := v_0,$	$y_i := \pi(z_{i-1}),$	$z_i := x_i + y_i$	for $i \geq 1$,
(OFB)	$y_0 := v_0,$	$y_i := \pi(y_{i-1}),$	$z_i := x_i + y_i$	for $i \geq 1$.

Here + denotes addition modulo 26.

a) Derive formulas for the decryption of the different modes.

b) Prove that if π is a Caesar shift, then CBC and CFB modes coincide.

c) Let π be the permutation defined by the keyword `OPERATION` and offset `M` $\widehat{=}$ 12 as in problem 2. Encrypt the text

`FISCHERSFRITZEFISCHTFRISCHEFISCHE`

in the three modes with permutation π and initial element $v_0 =$ `R` $\widehat{=}$ 17.

Problem 4 The following ciphertext was obtained from an English plaintext by an encryption in CBC mode as described in problem 3.

`MZVBC COHPG OZSEY PIROK BVYLQ EGYCU ERPFF EMILB KUNDW JRFEL RH`

The first word of the plaintext was `SUETONIUS`, the last word `CAESAR`. Decrypt the ciphertext and determine the initial element v_0 and the permutation π as complete as possible.

Due: Friday, April 27, 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.