# Homework 2 in Advanced Methods of Cryptography - Proposal for Solution -

Prof. Dr. Rudolf Mathar, Michael Reyer, Henning Maier
08.11.2013

## Solution to Exercise 5(b).

(b) Frequency analysis:

| B | C | D | E | F | G | K | M | N | O | P | R | S | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4 | 8 | 12 | 3 | 2 | 4 | 3 | 4 | 1 | 11 | 2 | 3 | 8 | 3 | 2 | 3 | 6 | 2 |

Map the most frequent letters to ETAOIN and derive the key.

First attempt, try D → E:

$$\begin{aligned} \mathrm{D} &= e(\mathrm{E}) \\ \mathrm{D} &\equiv \mathrm{E} + k \pmod{26} \\ 3 &\equiv 4 + k \pmod{26} \\ k &\equiv 3 - 4 \equiv -1 \equiv 25 \pmod{26}. \end{aligned}$$

Decoding the first few letters of the ciphertext yields: TETDE...
⇒ This result is meaningless in English, try another key.

Second attempt, try D → T:

$$\Rightarrow k \equiv -16 \equiv 10 \pmod{26}.$$

The deciphered ciphertext yields:
IT IS INSUFFICIENT TO PROTECT OURSELVES WITH LAWS.
WE NEED TO PROTECT OURSELVES WITH MATHEMATICS.

**Remark**: Feel free to program tools for encryption, decryption, frequency analysis, etc.

## Solution to Exercise 6.

(a) The $l$-th encryption, $2 \le l \le n$, depends on the previous one:

$$\begin{aligned} e_{k_1}: \ c^{(1)} &= (m + k_1) \mod 26, \\ e_{k_2}: \ c^{(2)} &= (c^{(1)} + k_2) \mod 26, \\ &\vdots \\ e_{k_l}: \ c^{(l)} &= (c^{(l-1)} + k_l) \mod 26, \\ &\vdots \\ e_{k_n}: \ c^{(n)} &= (c^{(n-1)} + k_n) \mod 26. \end{aligned}$$

By iterative substitution, we obtain $e_k$ in terms of the plaintext $m$:

$$e_k : \; c^{(n)} = (m + \sum\nolimits_{i=1}^{n} k_i) \mod 26.$$

The effective key is: $k \equiv \sum_{i=1}^{n} k_i \pmod{26}$, such that we get:

$$e_k : \; c = (m + k) \mod 26.$$

(b) The order of keys does not matter since addition in a ring is commutative.

**Remark**: Feel free to apply this problem to other classical ciphers, e.g., the permutation cipher.