Cryptography

Priv.-Doz. Dr. Adrian Spalka, Konstantin Ziegler

2 Assignment

(Due: Thursday, 11 November 2010, 12^{00})

Exercise 2.1. (6 points) From now on, we will identify the 26 letters of the english alphabet A, B, ..., Z with the integers 0, 1, ..., 25. (For any integer n, we denote the set $\{0, 1, \ldots, n-1\}$ by $\mathbb{Z}_n$.)

(i) We consider for encryption the function

$$\mathrm{enc}(m, (a, b, c)) = am^2 + bm + c \mod 26.$$

An english text is encrypted with this function letter-by-letter and you find that the three most common letters in the ciphertext are Z, V and B (in that order). Can you recover the key, i.e. the triple (a, b, c)?

(ii) A very simple encryption function is given by

$$\mathrm{enc}(m, b) = m + b \mod 26. \tag{2.2}$$

A first generalization of (2.2) is

$$\mathrm{enc}(m, (a, b)) = a \cdot m + b \mod 26 \tag{2.3}$$

with $a, b \in \mathbb{Z}_{26}$. What are requirements on a and b to make decryption possible? How would you break a cryptosystem that encrypts a long text letter-by-letter with (2.3).

(iii) A further generalization makes (2.3) "multi-dimensional". Pick a positive integer ℓ and let

$$\mathrm{enc}(\vec{m}, (A, \vec{b})) = A \cdot \vec{m} + \vec{b} \mod 26, \tag{2.4}$$

where $A \in \mathrm{GL}_\ell(\mathbb{Z}_{26})$ is an invertible $\ell \times \ell$-matrix, $m, b \in \mathbb{Z}_{26}^\ell$ are ℓ-dimensional vectors and the modulus 26 is taken in each component. A long text is now divided into blocks of size ℓ and each block is encrypted with (2.4). How could an attacker find the block size ℓ given a sufficiently long ciphertext?

Exercise 2.5. (8 points) Consider a graphics format of your choice, e.g. BMP.

- Write a program which takes as input a graphics file and a string and outputs a graphics file with the string encoded in the pixels.
- Which fraction of a graphics's information can you substitute, before a human can tell the difference from the original?

Exercise 2.6. (8 points) Collect several CPPs (certification practice statements), compare and evaluate them in detail.

Exercise 2.7 (mathematical bonus)**.** (+2 points)

$$\sin 3x + \cos 3x = \sqrt{2}$$