Leipzig University
Institute of Computer Science
Winter Term 2020/21

Prof. Dr. Andreas Maletti
Fabian Tronicke

Cryptography

Exercise Sheet 1

discussed on November 3, 2020

Exercise 1.1

Consider the following cipher technique:
Given an English word as a key we write the message row by row in a table under the key. The number of columns is given by the number of letters in the key. Empty spaces in the last row are possible. Now we rearrange the columns according to the alphabetical order of the letters in the key (Double letters are sorted by their occurrence). We read the ciphertext from the table column by column.

K	E	Y
P	L	A
I	N	T
E	X	T

$\rightarrow$

E	K	Y
L	P	A
N	I	T
X	E	T

Message: PLAINTEXT

Ciphertext: LNXPIEATT

(a) Specify the corresponding simplistic encryption scheme $(M, C, \text{enc}, \text{dec})$ and K. You can use numbers instead of letters.

(b) Do you have any approach to break this cipher?

Exercise 1.2

(a) Show $\lim_{|m|\to\infty} I(m) = I$ for all English messages m $\left(\text{i.e. } p_i = \frac{b_i^m}{|m|}\right)$.

(b) Why are we looking for the values of k where $\chi_k^2(c)$ is small?

(c) What does it mean, if the index of coincidence of a language is (close to) 1?

Exercise 1.3

Given a simplistic encryption scheme $(M, C, \text{enc}, \text{dec})$ for key space K. We know that $\text{dec}_k(\text{enc}_k(m)) = m$ for all $m \in M$. Must $\text{enc}_k(\text{dec}_k(c)) = c$ for all $c \in C$ also apply?