Kryptography Sheet 1

hhu Düsseldorf
Winter term 23/24

Hand in: until monday 16.10.2023, before the lecture starts

Website: `http://reh.math.uni-duesseldorf.de/~khalupczok/krypto/`

Exercise 1: Simple Decryption

Let be given the following encrypted text from a german plain text: (ß=ss, ä=ae, etc.)

> Lqghp glh Sulqchvvlq lq ghp Sulqchq yrq Shuvlhq glh Qhxjlhugh uhjh pdfkwh, ghq Nrhqljvsdodvw yrq Ehqjdohq cx vhkhq xqg gdulq ghq Nrhqlj, lkuhq Ydwhu, cx ehjuxhvvhq, vr kriiwh vlh, gdvv, zhqq hv lku jhodhqjh, lku Ydwhu ehlp Dqeolfn hlqhv vr zrko jheloghwhq, noxjhq, yroonrpphqhq xqg plw ghq yrucxhjolfkvwhq Hljhqvfkdiwhq dxvjhvwdwwhq Sulqchq vlfk ylhoohlfkw hqwvfkolhvvhq zxhugh, lkp hlqh Khludwvyhuelqgxqj dqcxwudjhq xqg lkp vlh vhoehu cxu Jhpdkolq yrucxvfkodjhq. Gd vlh dxvvhughp xhehuchxjw zdu, gdvv vlh ghp Sulqchq yrq Shuvlhq qlfkw johlfkjxhowlj vhl xqg gdvv glhvhu hlqh vrofkh Yhuelqgxqj qlfkw deohkqhq zxhugh, vr kriiwh vlh dxi glhvhp Zhj cxp Clho lkuhu Zxhqvfkh cx jhodqjhq, xqg gdehl cxjohlfk mhqhq Zrkovwdqg cx ehredfkwhq, ghu hlqhu Sulqchvvlq, glh lq doohp jdqc yrq ghp Zloohq lkuhv nrhqljolfkhq Ydwhuv dekdhqjlj huvfkhlqhq zroowh, cx ehredfkwhq jhclhpw. Grfk ghu Sulqc yrq Shuvlhq dqwzruwhwh lku xhehu glhvhq Sxqnw qlfkw jdqc vr, zlh vlh hv huzduwhw kdwwh.

Determine the distribution of the letters in the encrypted text. Try to encrypt the text with this information (by knowing that the plain text was in german), and in case of success, give the decrypted text completely. Which encryption (Caesar-encryption or permutation of letters) has been used?

Exercise 2: Viginère-encryption

We code the 26 letters of our alphabet by the numbers $0, \ldots, 25$. The Caesar-encryption $\mathrm{ROT}(i)$ for $0 \leq i < 26$ is described by $\mathrm{ROT}(i)(k) := k + i \mod 26$, if k stands for the letter to be encrypted.
For the Vigenère-encryption let $v_1, \ldots, v_\ell$ be a fixed given key word. Letter j on position number $n\ell + i$ ($1 \leq i \leq \ell$, $n \in \mathbb{N}_0$) in the plain text will be exchanged by the letter $\mathrm{ROT}(v_i)(j)$. Let p_j be the probability by which letter j appears in the plain text.

(a) Compute the probability by which a fixed letter k appears in the secret text.

(b) How could one determine the key length ℓ?

Exercise 3: Stancil-encryption

Let $m \in \mathbb{N}$ be the length of the plain text to be encrypted. We consider stancils, namely rectangled tables with quadratic equally sized fields with cutted holes in m many fields. The plain text will be written letter by letter through the holes (line by line) on a piece of paper, only one letter per hole. The stancil will be removed and the remaining fields will be filled by randomly chosen letters. The receiver of the secret text can decrypt easily, if he or she owns the same stancil.

(a) How many possible keys are there for this cryptography scheme?

(b) Under which conditions can the secret text be decrypted, even without knowing the stancil?