Kryptographie Blatt 1

hhu Düsseldorf
WiSe 2023/24

Abgabe: bis Montag 16.10.2023, vor der Vorlesung

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

Aufgabe 1: Einfache Verschlüsselung

Gegeben sei dieser verschlüsselte Text: (ß=ss, ä=ae, usw.)

> 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.

Bestimmen Sie die Verteilung der Buchstaben in dem verschlüsselten Text. Versuchen Sie, so den Text zu entschlüsseln, und geben Sie im Erfolgsfall den entschlüsselten Text an. Welche Verschlüsselung (Cäsar-Verschlüsselung bzw. Buchstabenpermutation) wurde verwendet?

Aufgabe 2: Viginère-Verschlüsselung

Die 26 Buchstaben des Alphabets seien durch $0, \ldots, 25$ kodiert. Die Cäsar-Verschlüsselung $\mathrm{ROT}(i)$ für $0 \leq i < 26$ lässt sich dann durch $\mathrm{ROT}(i)(k) := k + i \mod 26$ beschreiben, wenn k der zu verschlüsselnde Buchstabe bezeichnet. Für die Vigenère-Verschlüsselung sei ein Schlüsselwort $v_1, \ldots, v_\ell$ gegeben. Der Buchstabe j, der an Stelle $n\ell + i$ ($1 \leq i \leq \ell$, $n \in \mathbb{N}_0$) im Klartext steht, wird dabei durch $\mathrm{ROT}(v_i)(j)$ ersetzt. Sei p_j die Wahrscheinlichkeit, mit der der Buchstabe j im Klartext vorkommt.

(a) Berechnen Sie die Wahrscheinlichkeit, mit der ein fester Buchstabe k im Geheimtext vorkommt.

(b) Wie könnte man die Schlüssellänge ℓ bestimmen?

Aufgabe 3: Schablonen-Verschlüsselung

Sei $m \in \mathbb{N}$ die Länge des zu verschlüsselnden Klartextes. Wir betrachten Schablonen, nämlich Rechtecke mit quadratischen, gleichgroßen Feldern, wobei in m der Felder Löcher ausgeschnitten werden. Der Klartext wird zeilenweise der Reihe nach durch die Löcher auf ein Blatt Papier geschrieben, pro Loch immer ein Buchstabe. Die Schablone wird dann entfernt und die restlichen Felder mit zufällig gewählten Buchstaben aufgefüllt. Der Empfänger des Geheimtextes kann diesen nun leicht entschlüsseln, wenn er oder sie dieselbe Schablone besitzt.

(a) Wie viele mögliche Schlüssel gibt es bei diesem Verfahren?

(b) Unter welchen Bedingungen könnte man den Geheimtext auch ohne Schablone entschlüsseln?