TU Ilmenau
Institut für Mathematik, Diskrete Mathematik
Prof. Michael Stiebitz/Dr. Axel Wolf

Sommersemester 2019

Übungsaufgaben Kryptographie, Serie 1

Aufgabe 1 (Entropie)

Für eine Wahrscheinlichkeitsverteilung $(p_1, \ldots, p_n)$ und eine ganze Zahl $r \geq 2$, sei

$$H_r(p_1, \ldots, p_n) = -\sum_{i=1}^{n} p_i \log_r p_i = \sum_{i=1}^{n} p_i \log_r \frac{1}{p_i}$$

die Entropiefunktion zur Basis $r \geq 2$. Man beachte die Konvention, dass $0 \log_b 0 = 0$ gesetzt wird. Man zeige folgende Aussagen:

(a) Für alle rellen Zahlen $x > 0$ gilt: $\ln x \leq x - 1$, wobei die Gleicheheit nur für $x = 1$ gilt.

(b) Sind $(p_1, \ldots, p_n)$ und $(q_1, \ldots, q_n)$ zwei Wahrscheinlichkeitsverteilungen mit $q_1, \ldots, q_n > 0$, so gilt:

$$\sum_{i=1}^{n} p_i \ln \frac{1}{p_i} \leq \sum_{i=1}^{n} p_i \ln \frac{1}{q_i},$$

wobei die Gleichheit nur gilt, wenn $p_i = q_i$ für alle $i = 1, \ldots, n$ ist

(c) Für jede Wahrscheinlichkeitsverteilung $(p_1, \ldots, p_n)$ gilt $H_r(p_1, \ldots, p_n) \leq \log_r n$, wobei die Gleihheit nur für die Gleichverteilung gilt, also nur für $p_i = \frac{1}{n}$ $(i = 1, \ldots, n)$:

(d) Man gebe den kleinsten Wert an, den die Entropiefunktion $H_r(p_1, \ldots, p_n)$ annehmen kann.

Aufgabe 2

Nicht immer ist e der häufigste Buchstabe und oft sind die Nachrichten veraltet. Man dechiffriere

$$C = nmxpuefzuwaxmgemnqzppm$$

wenn man weiß, dass eine Verschiebechiffre (mit festem Schlüssel) benutzt wurde und es sich um einen deutschsprachigen Text handelt.

Aufgabe 3

Wir betrachten die monoalphabetische Tauschchiffre mit $A = B = \mathbb{Z}_p$ und $p \geq 2$. Der Schlüssel ist ein Paar (s, t) mit $0 \leq s, t \leq p - 1$ und die zugehörige Abbildung

$\sigma : A \to B$ mit $\sigma(\alpha) = t(\alpha + s)$ Mod 26. Dann wird der Klartetxt $T = \alpha_1\alpha_2 \dots \alpha_n$ durch den Geheimtext $C = k_\sigma(T) = \sigma(\alpha_1)\sigma(\alpha_2) \dots \sigma(\alpha_n)$ ersetzt. Man zeige, dass die Abbildung σ genau dann bijektiv ist, wenn $\mathrm{ggT}(s, t) = 1$ ist.

Aufgabe 4

Wir betrachten die monoalphabetische Tauschchiffre, d.h., $A = B = \{a = 1, b = 2, \dots, y = 25, z = 0\} = \mathbb{Z}_{26}$. Der Schlüssel ist ein Paar (s, t) mit $0 \leq s, t \leq 25$ und $\mathrm{ggT}(s, t) = 1$ und die zugehörige Abbildung $\sigma : A \to B$ mit $\sigma(\alpha) = t(\alpha + s)$ Mod 26. Dann wird der Klartetxt $T = \alpha_1\alpha_2 \dots \alpha_n$ durch den Geheimtext $C = k_\sigma(T) = \sigma(\alpha_1)\sigma(\alpha_2) \dots \sigma(\alpha_n)$ ersetzt.

(a) Man dechiffriere $C = vfabln$, wenn man weiß dass eine Tauschchiffre der Form $(7, t)$ benutzt wurde und der Klartext T ein deutscher Mädchenname ist

(b) Analog zu (a) mit $C = hnkvbx$, wobei eine Tauschchiffre der Form $(s, 3)$ benutzt wurde.

(c) Durch wieviel korrespondierende Paare von Klartext/Geheimtextbuchstaben ist eine Tauschchiffre eindeutig festgelegt.

(d) Man zeige, dass bei einer Tauschchiffre der Form $(0, t)$ stets m in m und z in z übergehen.

Aufgabe 5

$BDWZDIZVIORJMOVPAYDZAMVBZRVIINVBOZXVZNVMQZIDQDYDQDXD$

Über den obigen Geheimtext C weiß man, dass er aus einem deutschsprachigen Klartext T durch eine Verschiebechiffre entstanden ist. Wie lautet der Klartext T.

Aufgabe 6

$FWJNKYICW\ CAFFL\ NGXJMHGTK\ IWLLG\ FGMTG$
$KYIPMGHGJFNLLGJ\ PMGZGJ\ FWR\ FMHJWGTG$
$FGMTG\ CWLVGT\ IWXG\ MYI\ HGHGT\ VRALU\ GMTHGLWNKYIL$
$ZGTGT\ HMTH\ GK\ KAPMGKA\ TMYIL\ XGKATZGJK\ PWK$
$FWYIL\ ZGMT\ INTZ\ JWNYIL\ GJ\ MFFGJ\ TAYI\ KA\ OMGR$

Über den obigen Geheimtext C weiß man, dass er aus einem deutschsprachigen Klartext T durch eine monoalphabetische Chifrrierung, also eine Permutationschiffre entstanden ist. Wie lautet der Klartext T.