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

Sommersemester 2019

Übungsaufgaben Kryptographie, Serie 2

Aufgabe 1

Es seien $Q_1 = (X_1, p_1)$ und $Q_2 = (X_2, p_2)$ zwei Quellen, und es sei $Q = (X, p)$ die Produktquelle mit $X = X_1 \times X_2$ und $p(x_1x_2) = p(x_1)p(x_2)$ für $x_1x_2 \in X$. Man zeige, dass für die Entropie zur Basis $r = 2$ gilt $H(Q) = H(Q_1) + H(Q_2)$.

Aufgabe 2

Der nachfolgende Geheimtext ist aus einem deutschsprachigen Text durch eine Vigenere-Chiffrierung entstanden. Versuchen Sie die Schlüsselwortlänge durch den Kassiski Test und dann das Schlüsselwort zu bestimmen.

KWCSS GXYUT ZBZMU CMRFY JZZNZ HMEBS WMEXA ZMZAW IATBS ABUUK NMZHT ZAKCE HBVLY ZPVCE OMONT PKYML VJVGW CZRFK ZQEYF FTRLL ZFKVM XPJNS WMEXS MAKYD GMEES IVRVW MURHV VZWHA XPKPW MOVMK ZVUUK NLVLY ZPVCE OMONV ZVBFS MBVRL ZQEXW PBZAT ZAKCE HMEGM NAQOE WMZMH DMCCK OMJHA XPKGG ZOICU CLRMK DMVCF ZURFY JZZNZ HCJXW MOVBW DUKYP OJLWZ NBRVW IQDED VZKYP OMZHE VTVOF YMZHS ILVLW NURFK ZVKMH MQTBL JPEYV VAJYK YIWOW MMZHW MMXYD BQSNV DMUYE ZUGZS ZVXYJ BMEUM NIXNO VVEYJ ZCEXO VVEYJ NMENK KZZWZ OMJCK OMENK XPVCV ZVUXS NARHB ZLVLK OMCFW YMJEJ TXKIY MIDGK YMIMU CTLYK NMCYA ILVOL DOUYF FTRLL ZFKVM XPJNS WMETM EMUYE BMYYA HBVRL WCTBK OISYF AMJND ZOK

Aufgabe 2

Mit Hilfe des Kryptoprogramms ilmcrypt versuche man die Texte ueb 1 bis ueb 8 zu entschlsseln.

Aufgabe 3

Es sei $L \in \mathbb{N}^{(n,n)}$ eine lateinisches Quadrat der Ordnung n (d.h., in jeder Zeile und Spalte von L treten die Zahlen $1, 2, \ldots, n$ genau einmal auf. Ferner sein $(\mathcal{K}, \mathcal{G}, \mathcal{S}, k, d)$ ein symmetrisches Kryptosystem mit $\mathcal{K} = \mathcal{G} = \mathcal{S} = \{1, 2, \ldots, n\}$ und $k_s(T) = L_{(s,T)}$ für $s \in \mathcal{S}$ und $T \in \mathcal{K}$. Man zeige, dass dieses Kryptosystem perfekte Sicherheit bietet, wenn die Schlüssel zufällig und gleichverteilt benutzt werden.

Aufgabe 4

Wir betrachten folgendes Chiffriersystem $(\mathcal{K}, \mathcal{G}, \mathcal{S}, k, d)$ mit $\mathcal{K} = \{0, 1\}$, $\mathcal{G} = \{a, b\}$, $\mathcal{S} = \{s, t\}$, sowie

$$k_s(0) = a, k_s(1) = b, k_t(0) = b, k_t(1) = a.$$

Die Wahrscheinlichkeiten für das Auftreten von $T \in \mathcal{K}$ seien $p_{\mathcal{K}}(0) = 1/4$ und $p_{\mathcal{K}}(1) = 3/4$. Die Schlüssel treten mit folgenden Wahrscheinlichkeiten auf $p_{\mathcal{S}}(s) = 1/4$ und $p_{\mathcal{S}}(t) = 3/4$. Untersuchen Sie die Sicherheit des Systems. Ist das Chiffriersystem perfekt sicher?

Aufgabe 5

Im Jahre 1929 erfand der Mathematiker Lester Hill eine Blockchiffre mit variabler Blocklänge für das natürliche Alphabet $A = \{a = 0, b = 1, \ldots, z = 26\}$ Für die Blocklänge $m = 2$ besteht der Schlüssel aus eine Matrix $S \in \mathbb{Z}_{27}^{(2,2)}$. Jeder Klartextblock x in Form eines Vektors aus $\mathbb{Z}_{27}^2$ wird chiffriert in $y = Sx$, wobei alle Additionen und Multiplikationen modulo 27 zu berechnen sind.

(a) Berechnen Sie mit einem Known-Plaintext-Angriff die Hill-Chiffre: Der Geheimtext zum Klartect $T = turing$ ist $C = ubixgt$. Findenn Sie die Schlüsselmatrix S und den Klartext T zum Geheimtext $C = enerhlnhahrm$

(b) Warum wurde hier das Alphabet künstlich um ein Zeichen erweitert, so dass mit dem Modul 27 statt 26 gerechnet wird.