Übungen zur Kryptologie

Blatt 5 SoS 2024 — H. Kiechle

Präsenzaufgaben

14. Es sei $(G,+)$ eine kommutative Gruppe. Wir definieren ein Kryptosystem (Q,G,K,f) mit $Q=K=G$ durch $f: Q\times K\to G; (x,k)\mapsto x+k$.

(a) Zeigen Sie, dass (Q,G,K,f) tatsächlich ein Kryptosystem ist, indem Sie eine Entschlüsselungs-Abbildung angeben.

(b) Es sei ein Geheimtext $c\in G$ beliebig gewählt. Zeigen Sie, dass es zu jedem Klartext $m\in Q$ genau einen Schlüssel $k\in K$ gibt mit $f(m,k)=c$.

Hausaufgaben

15. *Fortsetzung von Aufgabe 14.*

Wir nehmen nun an, dass auf Q und K Wahrscheinlichkeitsfunktionen p_Q bzw. p_K gegeben sind, und dadurch — wie in der Vorlesung — eine Wahrscheinlichkeitsfunktion p auf $Q\times K$ erklärt ist. Für jedes $c\in G$ (Geheimtext) sei $D_c := \{(x,k)\in Q\times K\,;\ f(x,k)=c\}\subseteq Q\times K$ die Menge aller Paare aus Klartext x und Schlüssel k, die auf c chiffriert werden (ebenfalls wie in der Vorlesung).

(a) Damit (Q,G,K,f) perfekt ist, müssen nach dem Satz von Shannon gewisse Bedingungen erfüllt sein. Untersuchen Sie welche dieser Bedingungen sowieso schon erfüllt sind, und welche man zusätzlich fordern muss.

(b) Bestimmen Sie unter diesen Voraussetzungen und mit $|G|=n$

i. $p_K(k)$ für alle $k\in K$; ii. $P(D_c)$ für alle $c\in G$.

(c) `Ersatzlos gestrichen`

16. Es sei $c\in\mathbb{Z}_{26}^*$ ein mit der Vigenère-Chiffre verschlüsselter Geheimtext der Länge n und $I(c)$ der zugehörige Friedman'schen Koinzidenzindex. Dann gilt für die Schlüssellänge ℓ nach Vorlesung

$$\ell \approx \frac{n(I_D - I_G)}{(n-1)I(c) + I_D - nI_G} \tag{1}$$

Begründen Sie:

(a) Aus $I(c)=I_G$ folgt $\ell\approx n$.

(b) Wenn die rechte Seite von (1) gleich n ist, dann folgt $I(c)=I_G$.

(c) Interpretieren Sie die Ergebnisse.

bitte wenden!

Der QR-Code für die Evaluation. Bitte nutzen Sie den QR-Code oder den Link in STiNE um die Veranstaltung zu evaluieren.