Übungen zur Kryptologie

Blatt 3 SoS 2024 — H. Kiechle

Präsenzaufgaben

7. Die LALL-Sprache benutzt das Alphabet $A := \{\texttt{A}, \texttt{L}\}$. In einem *sinnvollen* LALL-Wort muss der Anteil des Buchstaben `A` genau ein Viertel betragen.

(a) Bestimmen Sie den Friedman'schen Koinzidenzindex I_G für die Gleichverteilung auf A^*.

(b) Bestimmen Sie den Friedman'schen Koinzidenzindex I_L der LALL-Sprache.

(c) Bestimmen Sie $I(\texttt{LALLLLLA})$.

(d) Es sei $x \in A^*$ ein sinnvoller String der Länge n.

i. Bestimmen Sie $I(x)$ für die Fälle $n = 4$, $n = 40$, $n = 100$ und $n = 1000$.

ii. Was ergibt sich für allgemeines n?

iii. Untersuchen Sie $I(x)$ für $n \to \infty$. Was fällt auf?

Hausaufgaben

[je 8 Punkte pro Aufgabe]

Für die folgenden Aufgaben verwenden Sie bitte den mit der Vigenère-Chiffre verschlüsselten Text aus Aufgabe 6 einer anderen Gruppe. Der Tausch wird in den Übungsgruppen organisiert.

Bitte schreiben Sie bei den Lösungen so viel auf, dass Ihre Überlegungen nachvollziehbar sind.

8. Führen Sie den Kasiski-Test durch, und geben Sie die potentiellen Schlüssellängen an.

9. Führen Sie den Friedman-Test durch, und schätzen Sie die Schlüssellänge.

10. Geben Sie eine begründete Vermutung über die Schlüssellänge ab und entschlüsseln Sie den Text. Welches war das Schlüsselwort?