Martin-Luther Universität Halle-Wittenberg
Fachbereich Mathematik und Informatik
Institut für Informatik

4. Übung zur Vorlesung „Datensicherheit“

Sommersemester 2005 2. Mai 2005

Abgabe: 09.05.2004 in der Übung

Aufgabe 4.1: (3 Punkte)

Modifizieren Sie Ihr Programm aus der Aufgabe 3.2 zur Berechnung der Koinzidenz der beiden Texte *lit.txt* und *gnu.txt*.
Wie verhalten sich Ihre Ergebnisse zu den in der Vorlesung gennanten Werten für die deutsche und englische Sprache ?

Aufgabe 4.2: (3 + 2 + 3 Punkte)

Unter der Homepage finden Sie den Text *vigenere.txt*, von dem man weiß, daß er mit der VIGENÈRE-Verschlüsselung chiffriert wurde.

(a) Versuchen Sie mit Hilfe des KASISKI-Tests Aufschluß über die vermeintliche Länge des Schlüsselwortes zu gewinnen.

(b) Führen Sie eine Textanalyse durch, und bestimmen Sie mit Hilfe von FRIEDMANNs Formel die vermeintliche Länge des Schlüsselwortes. Benutzen Sie Aufgabe 3.1 als Hilfsmittel.

(c) Begründen Sie eventuelle Unterschiede. Bestimmen Sie damit den Klartext der Mitteilung.

Aufgabe 4.3: (3 Punkte)

Betrachten Sie die linearen Rekursionsfolgen, die durch

$$s_{n+5} = s_{n+1} + s_n \bmod 2,\ n \geq 1,$$

gegeben sind. Zeigen Sie daß sich solche Folgen durch ein Schieberegister mit 5 Registern erzeugen lassen. Finden Sie Anfangswerte, aus denen sich Folgen der Periode 1, 3, 7, 21 ergeben. Zeigen Sie daß es sich um die einzigen möglichen Perioden handelt. Simulieren Sie die Schieberegister auf dem Rechner.

e-mail: {schenzel,pries}@informatik.uni-halle.de Web: http://www.informatik.uni-halle.de/∼{schenzel,pries}