Wolfgang K. Seiler
Tel. 2515

A5, C201

10. November 2004

3. Übungsblatt Kryptologie

Aufgabe 1: (*7 Punkte)*

a) Was passiert, wenn der Bayessche Gegner auf der Grundlage von Buchstabenhäufigkeiten allein versucht, eine Permutationschiffre zu entschlüsseln?

b) Lassen Sie ihn mit Hilfe von Kontaktwahrscheinlichkeiten Permutationschiffren der Blocklänge fünf entschlüsseln. Ab welcher Textlänge wird er erfolgreich?

c) Lassen Sie ihn mit Hilfe von Kontaktwahrscheinlichkeiten eine Permutationschiffre der Blocklänge drei entschlüsseln, von der er nur weiß, daß sie eine Blocklänge von höchstens sechs hat. Kann er die richtige Blocklänge bestimmen?

Aufgabe 2: (*8 Punkte)*

Der zu Zeiten zentraler Großrechner sehr populäre Zufallsgenerator RANDU geht aus von einem Startwert x_0 und generiert daraus die Folgewerte durch

$$x_{n+1} = (2^{16} + 3)x_n \bmod 2^{31} .$$

a) Erzeugen Sie eine Datei aus 10 000 Folgegliedern!

b) Betrachten Sie diese Datei als Folge von 40 000 Bytes und berechnen Sie deren Entropie sowohl auf der Basis einfacher Häufigkeiten als auch der von Kontakthäufigkeiten!

c) Testen Sie den Generator auf ein-, zwei- und dreidimensionale Gleichverteilung der Ergebnisse mit einer Auflösung von jeweils zwei, zehn und hundert Intervallen pro Dimension!

d) Erklären Sie das dreidimensionale Ergebnis, indem Sie zeigen, daß stets gilt

$$x_{n+2} - 6x_{n+1} + 9x_n = k \cdot 2^{31} \quad \text{mit} \quad -5 \le k \le 9 .$$

Aufgabe 3: (*5 Punkte)*

a) Verschaffen Sie sich eine Datei aus 4 096 „echten“ Zufallsbytes!
Hinweis: Unter LINUX dient dazu beispielsweise das Kommando

```
dd if=/dev/random of=Dateiname bs=1 count=4096;
```

wer kein Betriebssystem mit entsprechendem Generator hat, kann physikalisch erzeugte Zufallsbytes beispielsweise von `http://www.fourmilab.ch/hotbits/` beziehen.

b) Berechnen Sie auch hier die Entropie sowohl auf der Basis einfacher Häufigkeiten als auch der von Kontakthäufigkeiten!

c) Testen Sie wieder auf ein-, zwei- und dreidimensionale Gleichverteilung der Ergebnisse mit einer Auflösung von jeweils zwei, zehn und hundert Intervallen pro Dimension!