WOLFGANG K. SEILER
Tel. 2515

A5, C201

17. November 2004

4. Übungsblatt Kryptologie

Aufgabe 1: (*7 Punkte*)
Eine HILLS-Chiffre auf Bytebasis ordnet einem Byte, aufgefaßt als Element $\vec{v} \in \mathbb{F}_2^8$, den Chiffretext $A\vec{v} + \vec{b}$ zu mit einer festen Matrix $A \in \mathbb{F}_2^{8\times 8}$ und einem festen Vektor $\vec{b} \in \mathbb{F}_2^8$. Der Text „Dagobert Duck" werde dabei verschlüsselt durch die Bytefolge `253, 149, 16, 40, 204, 44, 47, 170, 68, 253, 207, 169, 145`. Bestimmen Sie A und $\vec{b}$!

Aufgabe 2: (*2 Punkte*)
Ein DES-Schlüssel kann auch dadurch spezifiziert werden, daß man eine Folge von acht Buchstaben und Ziffern nimmt, deren ASCII-Codes (mit Prüfbit) dann als Schlüssel verwendet werden.

a) Welche Entropie hat ein solcher Schlüssel im Vergleich zu einem allgemeinen?

b) Um welchen Faktor erleichtert es die Arbeit eines Gegners, wenn er an Stelle der Menge aller Schlüssel nur die so erhaltenen Schlüssel durchsuchen muß?

Aufgabe 3: (*7 Punkte*)
Ein wesentlicher Designfaktor für iterierte Blockchiffren wie DES ist der sogenannte Lawineneffekt: Änderung eines einzigen Bits in Schlüssel *oder* Klartext soll über die Runden hinweg immer mehr Bits der Ausgabe verändern, bis am Ende etwa die Hälfte aller Bits betroffen ist.

a) Warum beschränkt man sich auf die Forderung, daß nur etwa die Hälfte der Bits betroffen sein soll?

b) Wählen Sie einen festen Schlüssel sowie einen Klartext, und berechnen Sie die Ausgaben der 16 Runden! Vergleichen Sie mit den Resultaten, die bei Änderung eines Bits im Klartext entstehen, und zählen Sie jeweils, wie viele Bits sich nach k Runden, $k \leq 16$, geändert haben!

c) Dasselbe bei Änderung eines Schlüsselbits.

Aufgabe 4: (*4 Punkte*)
Verschlüsseln Sie einen längeren ASCII-Klartext mit DES und vergleichen Sie die Entropie pro Byte des Klartexts mit der beim Chiffretext sowohl auf der Basis von Zeichen- als auch auf der Basis von Kontakthäufigkeiten! Interpretieren Sie Ihr Ergebnis!