Institut für Informatik
Algorithmen und Komplexität II
Prof. Dr. Johannes Köbler

Sommersemester 2000
31. Mai 2000

Übungen zur Kryptologie

7. Übung

Abgabe am 14. Juni 2000

Aufgabe 26 (*schriftlich zu bearbeiten,* 12 Punkte)

a) Beweisen Sie, dass die vier Schlüssel

`0101010101010101`, `FEFEFEFEFEFEFEFE`,
`1F1F1F1F0E0E0E0E`, `E0E0E0E0F1F1F1F1`

(jeweils in Hexadezimaldarstellung) die einzigen schwachen Schlüssel für den DES-Algorithmus sind.

b) Begründen Sie, dass für schwache Schlüssel k gilt:

$$\mathrm{DES}(\mathrm{DES}(x,k),k) = x.$$

(Hinweis: Verwenden Sie Teil c) der nächsten Aufgabe).

c) Ein Schlüssel k heißt semi-schwach, falls es genau zwei verschiedene Schlüssel in den Schlüsselauswahlen $k_1, \ldots, k_{16}$ gibt (d.h. falls gilt $\|\{k_1,\ldots, k_{16}\}\|=2$).

Geben Sie einen semi-schwachen Schlüssel k an.

d) Geben Sie einen weiteren semi-schwachen Schlüssel k' an mit

$$\mathrm{DES}(\mathrm{DES}(x,k),k') = x.$$

Aufgabe 27 (*schriftlich zu bearbeiten,* 8 Punkte)

a) Ermitteln Sie den 64-Bit-Schlüsselblock, der (bei ungerader Parität) zum 56-Bit-DES-Schlüssel `01 23 45 67 89 AB CD` (Hexadezimaldarstellung) gehört.

b) Zeigen Sie: $\mathrm{DES}(\overline{x},\overline{k}) = \overline{\mathrm{DES}(x,k)}$. ($\overline{x}$ ist die bitweise Negation von x.)

c) Zeigen Sie: $\mathrm{DES}^{-1}(x,k) = \mathrm{IP}^{-1} \circ g \circ h_{k_1} \circ g \circ h_{k_2} \circ \cdots \circ g \circ h_{k_{16}} \circ g \circ \mathrm{IP}(X).$

d) Zeichnen Sie das Berechnungsdiagramm der Schlüsselauswahlfunktion, die die internen Schlüssel $k_1, \ldots, k_{16}$ in umgekehrter Reihenfolge generiert.

Aufgabe 28 (*schriftlich zu bearbeiten,* 8 Punkte)

a) Bei der Übertragung einer mit DES kodierten Nachricht tritt genau bei einem Bit ein Fehler auf. Wie viele Bits des entschlüsselten Kryptotextes können hierduch maximal verfälscht werden.

– unter ECB-Mode	– unter CFB-Mode
– unter CBC-Mode	– unter OFB-Mode

b) Beschreiben Sie wieviele der nachfolgenden Bits maximal verfälscht werden, falls ein Block des Kryptotextes bei der Übertragung verlorengeht.

– unter ECB-Mode	– unter CFB-Mode
– unter CBC-Mode	– unter OFB-Mode