WOLFGANG K. SEILER
Tel. 2515

A5, C201

24. November 2004

5. Übungsblatt Kryptologie

Aufgabe 1: (*8 Punkte*)

a) Zeigen Sie: Bezeichnet $\overline{x}$ das 1-Komplement eines Bitvektors, jenen Vektor also, bei dem alle Nullen durch Einsen und alle Einsen durch Nullen ersetzt sind, so ist

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

b) In welcher Weise läßt sich dies ausnutzen, um die Arbeit von DES-Cracker zu optimieren?

c) Hat auch AES diese Eigenschaft?

Aufgabe 2: (*8 Punkte*)

DES hat einige sogenannte schwache Schlüssel; dabei handelt es sich um Schlüssel s, für die

$$\mathrm{DES}\bigl(s, \mathrm{DES}(s,x)\bigr) = x \qquad \text{für alle Blöcke } x\,.$$

Sie bestehen alle aus jeweils acht identischen Bytes.

a) Wie viele Schlüssel müssen Sie durchprobieren, um (mit dieser Information) alle schwachen Schlüssel zu finden?

b) Finden Sie die vier schwachen Schlüssel!

c) Wie groß ist die Wahrscheinlichkeit, bei zufälliger Schlüsselwahl auf einen von ihnen zu stoßen?

d) Welche Folgen hat der Einsatz eines schwachen Schlüssels in den verschiedenen Operationsmodi?

Aufgabe 3: (*4 Punkte*)

a) Zeigen Sie: Hat a die Eigenschaft, daß jedes von Null verschiedene Element von $\mathbb{F}_{256}$ als Potenz von a dargestellt werden kann, so hat a^n genau dann ebenfalls diese Eigenschaft, wenn $\mathrm{ggT}(n, 255) = 1$ ist.

b) Wie viele Elemente $a \in \mathbb{F}_{256}$ haben die Eigenschaft, daß sich jedes von Null verschiedene Element als a-Potenz schreiben läßt?