Wolfgang K. Seiler
Tel. 2515

A5, C201

1. März 2013

3. Übungsblatt Kryptologie

Aufgabe 1: *(6 Punkte)*

a) Ein DES-Schlüssel kann auch dadurch spezifiziert werden, daß man eine Folge von acht (Groß- oder Klein-)Buchstaben oder Ziffern nimmt, deren ASCII-Codes (mit Prüfbit) dann als Schlüssel verwendet werden. Um welchen Faktor erleichtert es die Arbeit eines Gegners, wenn er an Stelle der Menge aller Schlüssel nur die der so darstellbaren Schlüssel durchsuchen muß?

b) Das 1-Komplement $\overline{x}$ eines Bitvektors x ist jener Vektor $\overline{x}$, bei dem alle Nullen durch Einsen und alle Einsen durch Nullen ersetzt sind. Zeigen Sie: Stellt man eine Zahl x zwischen 0 und 15 durch einen Vektor aus vier Bit dar, so ist $\overline{x}$ der Vektor zu $15 - x$.

c) Zeigen Sie, daß für DES gilt: $\mathrm{DES}(\overline{s}, \overline{x}) = \overline{\mathrm{DES}(s, x)}$.

Aufgabe 2: *(6 Punkte)*

Geben Sie für die Operationsmodi CBC, OFB und CTR jeweils einen konkreten Algorithmus an, wie der Empfänger aus der Folge $c_1 c_2 \ldots c_r$ der Chiffretextblöcke die Folge $m_1 m_2 \ldots m_r$ der Nachrichtenblöcke rekonstruiert! Über welche Informationen muß er jeweils verfügen?

Aufgabe 3: *(4 Punkte)*

Sie verschlüsseln eine Datei via Triple-DES (oder einer anderen Blockchiffre) im OFB-Modus mit einem Schlüssel und Anfangsblock, den Sie vorher mit Ihren Kollegen vereinbart haben; danach stellen Sie die verschlüsselte Datei ins Netz. Plötzlich bemerkt Ihre Sekretärin, daß der Name des Generaldirektors falsch geschrieben ist: Herrmann statt Hermann. In der Hoffnung, daß erst wenige Kollegen den Text heruntergeladen haben, verbessern Sie den Fehler, verschlüsseln das Ergebnis mit den vereinbarten Parametern und ersetzen die fehlerhafte Datei durch die neue. Welche Informationen kann ein Gegner gewinnen, der sich beide Versionen verschafft hat, und wie geht er vor?

Aufgabe 4: *(4 Punkte)*

a) Eine Folge von Blöcken $x_1, \ldots, x_N$ wird im CBC-Modus einer Blockchiffre verschlüsselt zu $c_1, \ldots, c_N$. Zeigen Sie: Falls für zwei Indizes i, j gilt $c_i = c_j$, so ist $x_i + x_j = c_{i-1} + c_{j-1}$.

b) Läßt sich dies kryptanalytisch ausnutzen?

Abgabe bis zum Freitag, dem 8. März 2013, um 11.55 Uhr