Wolfgang K. Seiler
Tel. 2515

A5, C201

27. September 2016

3. Übungsblatt Kryptologie

Aufgabe 1: *(5 Punkte)*

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:

a) Stellt man eine Zahl x zwischen 0 und 15 durch einen Vektor aus vier Bit dar, so ist $\overline{x}$ der Vektor zu $15 - x$.

b) Ist $s \in \mathbb{F}_2^{64}$ ein möglicher DES-Schlüssel, so auch $\overline{s}$.

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

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: *(5 Punkte)*

Für den Schlüsselstrom des DES wird der Schlüssel zerlegt in zwei Halbschlüssel; diese bestehen aus den Bitpositionen

$$57, 49, 41, 33, 25, 17, 9, 1, 58, 50, 42, 34, 26, 18, 10, 2, 59, 51, 43, 35, 27, 19, 11, 3, 60, 52, 44, 36$$

und

$$63, 55, 47, 39, 31, 23, 15, 7, 62, 54, 46, 38, 30, 22, 14, 6, 61, 53, 45, 37, 29, 21, 13, 5, 28, 20, 12, 4$$

des Originalschlüssels.

a) Schreiben Sie diese Bitpositionen jeweils in der Form $8a + b$ mit $0 \leq b \leq 7$!

b) Warum kommen keine Zahlen mit $b = 0$ vor?

c) Welche Bits der Schlüsselbytes gehen in welchen Halbschlüssel?

Abgabe bis zum Dienstag, dem 4. Oktober 2016, um 15.25 Uhr