Wolfgang K. Seiler
Tel. 2515

B6, B4.18

20. September 2019

3. Übungsblatt Kryptologie

Aufgabe 1: *(5 Punkte)*

a) Für eine allgemeine monoalphabetische Substitution können wir die Permutation dadurch angeben, daß wir von einem längeren Wort ausgehen, das zweite und jedes weitere Vorkommen eines jeden Buchstabens streichen, und die so erhaltene Buchstabenfolge als Chiffre für die ersten Buchstaben des Alphabets verwenden. Der Rest wird durch die verbleibenden Buchstaben aufgefüllt. Wird die Sicherheit des Verfahrens dadurch beeinträchtigt?

b) 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?

Aufgabe 2: *(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 3: *(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?

Aufgabe 4: *(5 Punkte)*

Zeigen Sie:

a) Wenn bei DES alle sechzehn Rundenschlüssel identisch sind, ist die Entschlüsselung gleichbedeutend mit der Verschlüsselung.

b) Die ist insbesondere dann der Fall, wenn jeder der beiden anfangs aus dem Schlüssel extrahierten Teilschlüssel entweder nur aus Nullen oder nur aus Einsen besteht.

c) Finden Sie vier Schlüssel, bei denen dies der Fall ist!

Abgabe bis zum Freitag, dem 27. September 2019, um 11.55 Uhr