Übung 5

Abgabe: 29.11.2018 **bis** 12:15 Uhr

1. Fragen zur DES-Historie 20 Punkte

Bemerkung: Bitte antworten Sie in max. 2-3 Sätzen.

a) Wie heißt die Behörde, die die Entwickelung des DES ausgeschrieben hat? (2 Pkt.)

b) In welchem Jahr wurde der DES standardisiert? (2 Pkt.)

c) Welche Behörde soll außerdem mit auf die Entwicklung des DES eingewirkt haben? (2 Pkt.)

d) Welcher Firma gehörten die Kryptographen an, die den Kandidaten eingereicht haben? (2 Pkt.)

e) Auf welcher allgemeinen Struktur basiert die Chiffre Lucifer[1]? (2 Pkt.)

f) Welche Schlüssellänge wurde für Lucfier ursprünglich vorgeschlagen? (2 Pkt.)

g) Wie lang ist ein DES-Schlüssel? Welches Sicherheitsniveau bietet der DES? (2 Pkt.)

h) Wie viele Klartextbits können mit einer DES-Operation verschlüsselt werden? (2 Pkt.)

i) Zeichnen Sie das Schaubild der allgemeinen Struktur, die Sie in e) bestimmt haben. (4 Pkt.)

2. Die S-Box S_4 20 Punkte

Die DES-S-Box S_4 hat einige besondere Eigenschaften:

a) Zeigen Sie, dass die 1. Zeile mithilfe der folgenden Abbildung aus der 0. Zeile („Zeile“ bezieht sich hier auf die Standarddarstellung der S-Boxen wie z.B. im Lehrbuch verwendet) abgeleitet werden kann:

$$(y_1, y_2, y_3, y_4) \rightarrow (y_2, y_1, y_4, y_3) \oplus (0, 1, 1, 0),$$

wobei (y_1, y_2, y_3, y_4) die binäre Ausgabe der S-Box darstellt.
Hinweis: Es reicht, diese Abbildung exemplarisch für 5 Einträge zu überprüfen. (10 Pkt.)

b) Kann eine ähnliche Aussage auch für die Zeilen 2 und 3 gemacht werden? (10 Pkt.)

[1] siehe Kapitel 3.1

3. Bit-Lawineneffekte im DES 30 Punkte

Für eine gute Blockchiffre ist es wünschenswert, dass bei der Veränderung eines einzelnen Eingangsbits möglichst viele Ausgangsbits verändert werden (Diffusion oder Avalanche-Effekt). Im Folgenden überprüfen wir die Diffusionseigenschaft des DES. Wir verwenden hierzu eine Eingangsbitfolge, bei der das Bit an der Stelle $x_{57} = 0$ ist (Zählung von x_1 bis x_{64}) und alle anderen Bits gleich Eins sind. Die 56 Schlüsselbits sind ebenfalls alle gleich Eins (das bedeutet auch, dass alle Rundenschlüssel gleich Eins sind).
Bemerkung: Beachten Sie, dass die Eingangsbits zunächst die Eingangspermutation IP durchlaufen.

a) Auf welche S-Boxen wirkt sich dieses Bit in der ersten Runde des DES aus bzw. wie sehen die Eingangsbits aller S-Boxen aus? (10 Pkt.)

Auswirkungen auf (bitte ankreuzen):
S_1 ☐ S_2 ☐ S_3 ☐ S_4 ☐ S_5 ☐ S_6 ☐ S_7 ☐ S_8 ☐

Eingangsbits:

S-Box S_1 | S-Box S_2 | S-Box S_3 | S-Box S_4

S-Box S_5 | S-Box S_6 | S-Box S_7 | S-Box S_8

b) Geben Sie das Ergebnis nach der ersten Runde an. (L_1 und R_1) (10 Pkt.)

L_1

R_1

c) Ermitteln Sie das Ergebnis nach der ersten Runde für den Fall, dass *alle* Eingangsbits gleich Eins sind (d.h. auch x_{57}). Wie viele Bits haben sich in L_1 und R_1 im Vergleich zu Aufgabenteil b) verändert? (10 Pkt.).

L_1

R_1

Anzahl geänderter Bits:

4. Das DES-Bitkomplement 30 Punkte

Der DES hat eine erstaunliche Eigenschaft bezüglich des bitweisen Komplements der Eingangs- und Ausgangsbits. Wir werden diese Eigenschaft in dieser Aufgabe behandeln.
Wir stellen das Komplement einer Zahl A (d.h. alle Bits dieser Zahl werden invertiert) mit $\overline{A}$ da. (z.B.: wenn $A = 0110$ ist, dann ist $\overline{A} = 1001$.) "$\oplus$" entspricht dem bitweisen XOR. Wir wollen folgendes zeigen:
Wenn

$$y = \mathrm{DES}_k(x)$$

dann gilt auch

$$\overline{y} = \mathrm{DES}_{\overline{k}}(\overline{x}).$$

Das bedeutet, wenn wir das Komplement des Klartexts und des Schlüssels bilden, dann werden die Ausgangsbits auch das Komplement des orginalen Geheimtexts sein. Ihre Aufgabe ist es diese Eigenschaft zu **beweisen**.
Hinweis: Beweisen Sie diese Eigenschaft allgemein für jede beliebige Runde, anstatt alle 16 Runden durchzurechnen.