Übung 5

Abgabetermin: 24. November 2011 **vor** der Vorlesung

1. *Bit-Lawineneffekte im DES (**Dieses Blatt ausgefüllt abgeben**)*

   Für eine gute Blockchiffre ist es wünschenswert, daß bei der Veränderung eines Eingangsbits möglichst viele Ausgangsbits verändert werden (Diffusion oder Avalanche-Effekt). Im folgenden werden wir versuchen, die Diffusionseigenschaft von DES zu überprüfen. Wir verwenden hierzu eine Eingangsbitfolge, bei der das Bit an der Position 57 gleich Eins ist ($x_{57} = 1$) und alle anderen Bits gleich Null sind. Die 56 Schlüsselbits sind ebenfalls alle gleich Null (das bedeutet auch, dass alle Rundenschlüssel Null sind). (Beachten Sie, daß die Eingangsbits als erstes die Eingangspermutation IP durchlaufen!)

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

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

   Eingangsbits:

   S-Box 1 | S-Box 2 | S-Box 3 | S-Box 4

   S-Box 5 | S-Box 6 | S-Box 7 | S-Box 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 Null sind (d.h. auch x_{57}). Wie viele Bits haben sich in L_1 und R_1 im vergleich zu Aufgabenteil b) verändert? (20 Pkt.).

   L_1

   R_1

   Anzahl geänderter Bits:

2. *Nichtlinearität der S-Boxen*

   Eine wichtige Eigenschaft des DES ist die Nichtlinearität der S-Boxen. In dieser Übungsaufgabe wollen wir diese Eigenschaft verifizieren, indem wir die Ausgangsbits für verschiedene Eingangsbits in einer S-Box S_i vergleichen. Zeigen Sie, daß für S_5 das folgende Entwurfkriterium gilt:

   $$S_i(x_1) \oplus S_i(x_2) \neq S_i(x_1 \oplus x_2).$$

   Benutzen Sie die folgenden Eingangsbits:

   (a) $x_1 = 010100$, $x_2 = 110001$ (10 Pkt.)

   (b) $x_1 = 111111$, $x_2 = 101000$ (10 Pkt.)

   (c) $x_1 = 100001$, $x_2 = 01110$ (10 Pkt.)

3. *Permutationen im DES*

   Wir möchten überprüfen, ob IP^{-1} die inverse Operation von IP ist. Wir betrachten den 64-bit Vektor $x = (x_1, x_2, \ldots, x_{64})$. Zeigen Sie für die Bits x_8, x_{22} und x_{58}, dass $\text{IP}^{-1}(\text{IP}(x_i)) = x_i$ gilt. (15 Pkt.)

4. *DES-Entschlüsselung*

   Ein Freund hat eine Nachricht für Sie mit dem DES verschlüsselt und hat Ihnen den zugehörigen Schlüssel auf einem kleinen Stück Papier in der Vorlesung zugesteckt. Da der Zettel von einer Ecke abgerissen wurde, ist leider die letzte Stelle des hexadezimalen 64-bit Schlüssels (=16 Hexzeichen) nicht vollständig lesbar. Erkennbar ist noch, dass das fehlende Symbol eine Zahl sein müsste.

   (a) Wie viele Möglichkeiten müssen Sie unter diesen Umständen im Durchschnitt *und* im schlimmsten Fall durchprobieren, um den korrekten Schlüssel durch Ausprobieren zu erraten? (Hinweis: DES verwendet 56-bit Schlüssel, aber es ist ein 64-bit Schlüssel angegeben. Die „überflüssigen“ Bit des 64-bit Schlüssels sind nicht willkürlich gewählt.) (10 Pkt.)

   (b) Im Übungsordner befindet sich die Nachricht `E-Mail_ciphertext.hex`. Gegeben sei der Schlüssel `B3 3A 89 2B A5 2B CC FX`, wobei **X** nur bedingt lesbar war (siehe Hinweis weiter oben). Verwenden Sie die im CrypTool vorhandene DES-Entschlüsselung, um

      i. den korrekten Schlüsselkandidaten herauszufinden (5 Pkt.)

      ii. die Nachricht Ihres Freundes zu entschlüsseln. (5 Pkt.)

      Hinweis: Beachten Sie, dass Sie die Entschlüsselung im ECB-Modus verwenden. Was sich hinter diesem Entschlüsselungsmodus verbirgt, werden Sie in den nächsten Vorlesungen kennenlernen.