Übung 6

Abgabetermin: 1. Dezember 2011 **vor** der Vorlesung

1. *Brute-Force Schlüsselsuche*

   Ein generischer Angriff auf Verschlüsselungsverfahren ist das systematische Durchsuchen des Schlüsselraumes, indem für einen bekannten Klartext jeder mögliche Schlüssel ausprobiert und mit dem abgehörten Chiffretext verglichen wird. Dieser Angriff ist auch als *Brute-Force Angriff* bekannt.
   Wie schnell der Angriff zum Erfolg führt, hängt im Einzelfall vom gewählten Schlüssel ab und an welcher Stelle er beim Durchsuchen probiert wird. Dennoch kann man allgemeine Aussagen über die Erfolgswahrscheinlichkeit des Angriffs bei Verschlüsselungsverfahren machen.

   (a) Gegeben sei ein Verschlüsselungsverfahren mit 56 Bit Schlüssellänge (DES). Wie viele Verschlüsselungen benötigt man für eine erfolgreiche Brute Force Attacke (I) im Durchschnitt *und* (II) im schlimmsten Fall, wenn der Schlüssel als allerletzes gefunden wird? (5 Pkt.)

   (b) Sie haben einen günstigen Computer für 350 EUR mit einem Core i7 Prozessor und $4 \cdot 3$ GHz zu Verfügung. Dieser Rechner schafft 10 Millionen DES-Verschlüsselungen bei 56 Bit Schlüssellänge pro Sekunde. Wie lange *(Jahre und Tage bzw. Tage und Stunden)* benötigt eine erfolgreiche Brute-Force Attacke mit diesem Rechner im Durchschnitt? (10 Pkt.)

   (c) Nehmen Sie an, sie haben insgesamt ein Budget von 17.500 EUR. Wenn Sie für dieses Geld Computer zu je 350 EUR kaufen, wie lange dauert dann eine parallele DES-Schlüsselsuche im Schnitt? (5 Pkt.)

   (d) Ein Spezialcluster mit 180 parallel arbeitenden Hardwarebausteinen (FPGAs) ist ebenfalls für 17.500 EUR zu realisieren. Ein einzelner Hardwarebaustein hat insgesamt 4 Rechenwerke, die jeweils 120 Millionen DES-Verschlüsselungen pro Sekunde schaffen. Wie lange dauert es im Durchschnitt, bis dieser Cluster einen DES-Schlüssel mit einer Brute-Force Attacke erfolgreich knacken kann? (10 Pkt.)

2. *DES-Entschlüsselung*

   In der Vorlesung wurde gezeigt, dass sich die Entschlüsselung nur geringfügig von der Verschlüsselung unterscheidet. Dies liegt an der besonderen Struktur, die nach dem Erfinder Horst Feistel benannt wurde.

   (a) Worin besteht der einzige Unterschied zwischen einer DES-Verschlüsselung und einer DES-Entschlüsselung? (5 Pkt.)

   (b) Zeige, warum dieser einzige Unterschied ausreicht, um aus einer Verschlüsselung eine Entschlüsselung zu erzeugen. Hinweis: Ein guter Start für den Beweis ist die 16. Runde der Verschlüsselung. (25 Pkt.)

3. *DES Bitkomplement*(Etwas kniffelige Aufgabe!)

   DES hat eine erstaunliche Eigenschaft bezüglich des bitweisen Komplements der Eingangs- und Ausgangsbits. Wir werden diese Eigenschaft in diesem Problem behandeln.

   Wir stellen das Komplement einer Zahl A (d.h. alle Bits dieser Zahl werden invertiert) mit A' da. (Bsp.: Wenn $A = 0110$ ist, dann ist $A' = 1001$.) "$\oplus$" entspricht dem bitweisen XOR. Wir wollen folgendes zeigen: Wenn

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

   dann gilt auch

   $$y' = \text{DES}_{k'}(x').$$

   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**. (Tipp: versuchen Sie diese Eigenschaft allgemein für jede beliebige Runde zu beweisen, anstelle alle 16 Runden durchzurechnen!) (25 Pkt.)