

6. Übungsblatt

Kryptographie I (SS 2006)

Stefan Lucks, Emin Islam Tatli

Besprechung: Mittwoch, 7. Juni 2006

P3-P4 Generatoren

Aufgabe 1 Auf der Internetseite

<http://th.informatik.uni-mannheim.de/teach/Krypto-06/uebungen/Interaktiv2/>
findet ihr die erste interaktive Aufgabe.

Data Encryption Standard (DES)

Aufgabe 2 In der Vorlesung wurde behauptet, dass der DES eine Komplement-Eigenschaft aufweist. Wir wollen dies nun beweisen.

a) Zeige zunächst, dass für jede Runde des DES gilt:

$$f_i(\bar{k}_i, \bar{x}) = f_i(k_i, x)$$

b) Zeige, dass daraus für den gesamten DES folgt:

$$\overline{DES(k, x)} = DES(\bar{k}, \bar{x})$$

Differentielle Kryptanalyse

Aufgabe 3 Auf der Internetseite

<http://th.informatik.uni-mannheim.de/teach/Krypto-06/uebungen/Interaktiv3/>
findet ihr die nächste interaktive Aufgabe.

Aufgabe 4 In der Vorlesung wurde die Technik der Differentiellen Kryptanalyse vorgestellt. Wir betrachten nun eine Charakteristik, die zur Kryptanalyse des DES besonders geeignet ist. Sie betrifft die S-Boxen S_1, S_2 und S_3 , wobei gilt:

$$\Pr(S_1(x) \oplus S_1(x') = 0000 \mid x \oplus x' = 000011) = 14/64$$

$$\Pr(S_2(x) \oplus S_2(x') = 0000 \mid x \oplus x' = 110010) = 8/64$$

$$\Pr(S_3(x) \oplus S_3(x') = 0000 \mid x \oplus x' = 101100) = 10/64 .$$

Alle übrigen S-Boxen werden ignoriert, d.h. wir benutzen für $i = 4, \dots, 8$ die Eigenschaft

$$\Pr(S_i(x) \oplus S_i(x') = 0000 \mid x \oplus x' = 000000) = 1 .$$

Konstruiere nun schrittweise einen differentiellen Angriff gegen den DES!

- a) Welche Runden-Charakteristik $(\Delta x, \Delta f(x))$ ergibt sich aus der obigen S-Boxen-Charakteristik? Wie groß ist die Wahrscheinlichkeit, dass sie (für zufällig gewähltes x und zugehöriges $x' := x \oplus \Delta x$) erfüllt ist¹?
- b) Welche Input-Differenz $(\Delta L, \Delta R)$ muss man wählen, um diese Charakteristik ausnutzen zu können?
- c) Welche Gestalt besitzen die Output-Differenzen $(\Delta X_i, \Delta Y_i)$ nach der i -ten Runde, wenn die obige Charakteristik in jeder Runde erfüllt wird? Mit welcher Wahrscheinlichkeit ist für i Runden der Fall?
- d) Wie viele Klartextpaare (R, L) und (R', L') müssen im Mittel getestet werden, damit die Charakteristik bei einem i -Runden-DES im Mittel mindestens einmal erfüllt ist?
- e) Betrachte eine DES-Variante mit gerader Rundenzahl i . Angenommen, es sei gelungen, ein Klartextpaar (R, L) und (R', L') mit der korrekten Input-Differenz $(\Delta L, \Delta R)$ zu finden, das nach i Runden die durch die Charakteristik "vorhergesagte" Output-Differenz $(\Delta X_i, \Delta Y_i)$ aufweist. Wie kann dann der DES-Schlüssel k rekonstruiert werden?

¹Zum Vergleich: Für die Runden-Charakteristik

$$\begin{aligned}\Delta x &= 04\ 00\ 00\ 00 \\ \Delta f(x) &= 40\ 08\ 00\ 00\end{aligned}$$

war in der Vorlesung die Wahrscheinlichkeit 1/4 angegeben worden.