Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Stefan Hoffmann, Ilya Ozerov

Hausübungen zur Vorlesung

Kryptographie

WS 2013/14

Blatt 9 / 9. Dezember 2013

Abgabe: 17. Dezember 2013, 14.00 Uhr (vor der Vorlesung), Kasten NA/02

AUFGABE 1 (7 Punkte)**:**

Der DES-Algorithmus besitzt eine Komplement-Eigenschaft, das heißt es gilt

$$DES_k(m) = \overline{DES_{\overline{k}}(\overline{m})}.$$

Der Wert $\overline{x}$ stellt hier (und im folgenden Text) die bitweise Invertierung (also das Komplement) des Vektors x dar.

Weisen Sie die Komplement-Eigenschaft von DES nach. Gehen Sie dazu nach folgenden Schritten vor.

(a) Die Erweiterungsfunktion $E : \{0,1\}^{32} \to \{0,1\}^{48}$ im Algorithmus der Rundenfunktion auf Folie 163 (Schritt 1) erweitert die 32-Bit-Eingabe auf einen 48-Bitstring. Dazu werden 16 Bits der Eingabe verdoppelt. Die dadurch entstehenden 48 Bits werden auf die 48-Bit-Ausgabe von E permutiert. Zeigen Sie, dass E linear ist, dass also $E(x \oplus y) = E(x) \oplus E(y)$ mit $x, y \in \{0,1\}^{32}$ gilt.

(b) Zeigen Sie, dass $E(x) = \overline{E(\overline{x})}$ gilt, da E linear ist.

(c) Betrachten Sie nun die S-Boxen $S_j : \{0,1\}^6 \to \{0,1\}^4$. In der Rundenfunktion wird vor Eingabe des 6-Bit-Blocks y_j auf diesen der 6-Bit-Block $(k_i)_j$ mit XOR addiert (siehe Folie 163). Zeigen Sie, dass $S_j(y_j \oplus (k_i)_j) = S_j(\overline{y_j} \oplus \overline{(k_i)_j})$ mit $y_j, (k_i)_j \in \{0,1\}^6$.

(d) Zeigen Sie nun mithilfe der in (a), (b) und (c) bewiesenen Aussagen die Komplement-Eigenschaft. Betrachten Sie hierzu, wie sich die Invertierung der Eingabe und die Invertierung des Rundenschlüssels jeder einzelnen Runde auf die Ausgabe der Runde auswirkt.

Hinweis: Zur Lösung dieser Aufgabe genügen die Beschreibungen des DES-Algorithmus auf den Folien 162 (Feistelnetzwerk) und 163 (Rundenfunktion). Gehen Sie zusätzlich davon aus, dass eine Invertierung des Hauptschlüssels k auch zu einer Invertierung der Rundenschlüssel k_i führt. (Seien $k_1, \ldots, k_r$ die aus k abgeleiteten Rundenschlüssel, dann sind also $\overline{k_1}, \ldots, \overline{k_r}$ die aus $\overline{k}$ abgeleiteten.)

AUFGABE 2 (7 Punkte)**:**

Wir betrachten eine DES-Variante $c = DES_k^{R3}(m))$ mit drei Runden. Es gilt also

$$\begin{aligned}(L_0||R_0) &:= IP(m)\\ L_1 &:= R_0\\ R_1 &:= L_0 \oplus f_1(R_0)\\ L_2 &:= R_1\\ R_2 &:= L_1 \oplus f_2(R_1)\\ L_3 &:= R_2\\ R_3 &:= L_2 \oplus f_3(R_2)\\ c &:= FP(L_3||R_3).\end{aligned}$$

Skizzieren Sie einen Key-Recovery-Angriff auf diese Variante. Nach welcher Strategie und mit welcher Laufzeit (Größenordnung) lässt sich der Hauptschlüssel k berechnen?

Hinweis: Bei dieser Variante ist offensichtlich von keiner der drei Rundenfunktionen f_1, f_2 und f_3 sowohl der Eingangs- als auch der Ausgangswert bekannt. Dafür ist (beispielsweise) die XOR-Verknüpfung der beiden Ausgangswerte von f_1 und f_3 bekannt.

Schlüsselableitung: Vor der Schlüsselableitung wird der Hauptschlüssel $k \in \{0,1\}^{56}$ in zwei Hälften $k_L, k_R \in \{0,1\}^{28}$ mit $k = (k_L||k_R)$ aufgeteilt. Aus jeder der beiden Hälften werden jeweils 24 Bits für jede Hälfte des jeweiligen Rundenschlüssels entnommen. Das bedeutet unter anderem, dass sich k_L nur auf die Eingänge der S-Boxen $S_1, \ldots, S_4$ auswirkt. k_R wirkt sich dementsprechend nur auf die S-Boxen $S_5, \ldots, S_8$ aus.

AUFGABE 3 (6 Punkte)**:**

Gegeben sei eine fehlerhafte Variante des DES-Algorithmus $FDES_k^{R8}(m)$ mit acht Runden. Die Rundenfunktionen $f_1, \ldots f_8 : \{0,1\}^{32} \to \{0,1\}^{32}$ seien definiert als

$$f_i(x) = x \oplus k_i,$$

wobei $k_1, \ldots k_8 \in \{0,1\}^{32}$ die acht Rundenschlüssel sind, die aus dem Hauptschlüssel k abgeleitet werden.

Der Ausgabewert $(L_i||R_i)$ einer einzelnen Runde wird also wie folgt berechnet.

$$\begin{aligned}L_i &:= R_{i-1}\\ R_i &:= L_{i-1} \oplus f_i(R_{i-1}) = L_{i-1} \oplus R_{i-1} \oplus k_i\end{aligned}$$

Zeigen Sie, wie man mit lediglich einem gültigen Paar Klartext/Chiffretext einen (alternativen) Schlüssel berechnen kann, mit dem man wiederum beliebige andere Chiffrate entschlüsseln kann.