htw saar

Studiengang Kommunikationsinformatik (Master)
Prof. Dr.–Ing. Damian Weber

Sicherheit und Kryptographie
Praktische Übung 5

Die folgenden Aufgaben können Sie auf Ihrem eigenen Laptop oder auf ISL–/STL–Rechnern in einer beliebigen Programmiersprache lösen, die sowohl XOR (exklusiv–oder) als auch die Ausgabe von hexadezimalen Werten unterstützt.

Aufgabe 1 (Symmetrisches Verschlüsselungsverfahren ZERO)

Diese Aufgabe entwickelt den Prototyp, der in den folgenden Aufgaben erweitert werden wird.

Schreiben Sie einen Chiffre ZERO, der 4-bit-Nachrichten m mit einem 4-bit-Schlüssel k verschlüsseln kann:

$$E_k(m) = m \oplus k$$

a) Verschlüsseln Sie alle möglichen 4-bit-Nachrichten m für einen gegebenen Schlüssel k.

b) Stellen Sie theoretisch wie praktisch fest, wenn zwei Nachrichten die gleiche Differenz d haben $(m_1 \oplus m_1) = d$, dann haben auch die Differenz d:

$$E_k(m_0) \oplus E_k(m_1) = d.$$

Aufgabe 2 (Symmetrisches Verschlüsselungsverfahren ONE)

Ergänzen Sie das Verschlüsselungsverfahren ZERO um eine nicht–lineare Komponente, eine S–box. Hier die Wertetabelle der S–box.

```
           00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
SBox     : 06 04 0c 05 00 07 02 0e 01 0f 03 0d 08 0a 09 0b

           00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
SBox^{-1}: 04 08 06 0a 01 03 00 05 0c 0e 0d 0f 02 0b 07 09
```

Zum Beispiel gilt, wenn man S als Funktion und S^{-1} als ihre Umkehrfunktion schreibt

$$S(0x5) = 0x7 \qquad S^{-1}(0x7) = 0x5$$

Eine S–Box muss wegen der Umkehreigenschaft eine bijektive Funktion darstellen.

Die Ver– und Entschlüsselung beim Chiffreverfahren ONE benutzt einen 8–bit Schlüssel k (und nach wie vor 4–bit Nachrichten). Der Schlüssel $k = (k_0, k_1)$ besteht aus zwei 4–bit Teilen k_1 und k_2.

Implementieren Sie die folgenden Funktionen zur Ver– und Entschlüsselung

- $E_k(m)$
  a) $u = m \oplus k_0$
  b) $v = S(u)$
  c) $c = v \oplus k_1$
  d) return c
- $D_k(c)$
  a) $v = c \oplus k_1$
  b) $u = S^{-1}(v)$
  c) $m = u \oplus k_0$
  d) return m

Testen Sie Ihre Implementierung am Beispiel: $E_{0x97}(0xd) = 0x7$

Erklären Sie, wie man aus der Verschlüsselungsfunktion die Entschlüsselungsfunktion herleiten kann.

Aufgabe 3 (Symmetrisches Verschlüsselungsverfahren TWO)

Wir nehmen die Chiffre ONE als Grundlage, um für die Chiffre TWO einen S–Box–Aufruf und einen weiteren Teilschlüssel k_2 hinzuzunehmen.

Implementieren Sie den Chiffre TWO:

- $E_k(m)$
  a) $u = m \oplus k_0$
  b) $v = S(u)$
  c) $w = v \oplus k_1$
  d) $x = S(w)$
  e) $c = x \oplus k_2$
  f) return c
- $D_k(c)$
  a) $x = c \oplus k_2$
  b) $w = S^{-1}(x)$
  c) $v = w \oplus k_1$
  d) $u = S^{-1}(v)$
  e) $m = u \oplus k_0$
  f) return m

Überprüfen Sie Ihre Implementierung: die Nachricht $m = 0xd$ wird mit dem Schlüssel $k = 0x959$ zu $0xe$ verschlüsselt.

Aufgabe 4 (Difference Distribution Table der S–Box)

Berechnen Sie das zweidimensionale Array der *Difference Distribution Table* T.

Eine Schleife läuft über alle Paare x, x' von Eingabewerten für S.

Für jedes Auftreten der Inputdifferenz $i = x \oplus x'$ in den Eingabewerten von $S()$ wird die Outputdifferenz $j = S(x) \oplus S(x')$ berechnet. Dann wird der Zähler t_{ij} erhöht.