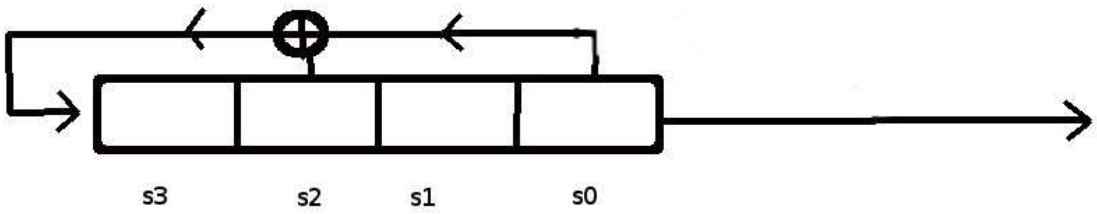
htw saar

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

Sicherheit und Kryptographie – Wiederholungsübung 2

Aufgabe 1 (LFSR)

Gegeben sei folgendes Linear–Feedback-Shift–Register:



Geben Sie eine Formel für den Programmierer an, der dieses LFSR in Programmcode umsetzen soll.

$$s_{i+1} = \ldots$$

Angenommen, der Angreifer beobachtet von diesem LFSR den Output

```
* * * * 1 1 1 1 ...
```

Berechnen Sie den Anfangszustand des Zufallsgenerators (hier als

```
* * * *
```

bezeichnet.

Aufgabe 2 (Modi der Blockchiffren)

Ein Blockchiffreverfahren sei benannt als Funktion $y = E_K(x)$ um den Klartext x mit dem Schlüssel K zu verschlüsseln.

Die Entschlüsselungsfunktion soll $x = D_K(y)$ heißen.

Im folgenden sind die Formeln der Modi genannt, die die Klartexte $P_1, P_2, \ldots, P_n$ in die Chiffretexte $C_0, C_1, C_2, \ldots, C_n$ transformieren:

CBC:

$$C_0 = IV, \qquad C_i = E_K(P_i \oplus C_{i-1}), 1 \leq i \leq n$$

CFB:

$$C_0 = IV, \qquad C_i = E_K(C_{i-1}) \oplus P_i, 1 \leq i \leq n$$

OFB:

$$Y_0 = IV, \qquad Y_i = E_K(Y_{i-1}), \quad C_i = P_i \oplus Y_i, 1 \leq i \leq n$$

(C_0 existiert in diesem Modus nicht)

CTR:

$$C_i = P_i \oplus E_K(\text{nonce}||i)$$

a) Geben Sie die entsprechenden Entschlüsselungsformeln an.

b) Wenn man den Initialization Vector IV an den Empfänger übermittelt, sollte man ihn nicht verschlüsseln, zumindest nicht mit dem Key K.

Zeigen Sie: wenn man im CFB– oder im OFB–Mode den IV separat als $E_K(IV)$ übermittelt, kann der Angreifer P_1 ausrechnen.

Aufgabe 3 (Hashfunktionen)

Sie haben die folgenden Eigenschaften von sicheren Hashfunktionen kennengelernt:

(I) preimage–resistance

(II) 2nd–preimage–resistance

(III) collision–resistance

Diese Eigenschaften sind nicht ganz unabhängig voneinander.

a) Gegeben sei die Hashfunktion $h : U \longrightarrow \{0, 1, 2, \ldots, 2^{256}\}$ mit

$$h(u) = 0$$

für alle $u \in U$. Welche Eigenschaft hat die Funktion h auf jeden Fall?

b) Gegeben sei die Hashfunktion $h : \{0, 1, 2, \ldots, 2^{256}\} \longrightarrow \{0, 1, 2, \ldots, 2^{256}\}$ mit

$$h(u) = u$$

für alle $u \in \{0, 1, 2, \ldots, 2^{256}\}$. Welche Eigenschaft hat die Funktion h auf jeden Fall?

c) Argumentieren Sie: (III) $\Longrightarrow$ (II)

(Hinweis: Kontraposition)

Aufgabe 4 (Differentielle und lineare Kryptoanalyse)

Gegeben sei folgende S–box (hexadezimal, 4 Bits)

```
          0 1 2 3 4 5 6 7 8 9 a b c d e f
sbox     : 6 4 c 5 0 7 2 e 1 f 3 d 8 a 9 b
```

a) Die zugehörige Difference–Distribution–Table ist

output	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
input 0 :	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
input 1 :	0	0	6	0	0	0	0	2	0	2	0	0	2	0	4	0
input 2 :	0	6	6	0	0	0	0	0	0	2	2	0	0	0	0	0
input 3 :	0	0	0	6	0	2	0	0	2	0	0	0	4	0	2	0
input 4 :	0	0	0	2	0	2	4	0	0	2	2	2	0	0	2	0
input 5 :	0	2	2	0	4	0	0	4	2	0	0	2	0	0	0	0
input 6 :	0	0	2	0	4	0	0	2	2	0	2	2	2	0	0	0
input 7 :	0	0	0	0	0	4	4	0	2	2	2	2	0	0	0	0
input 8 :	0	0	0	0	0	2	0	2	4	0	0	4	0	2	0	2
input 9 :	0	2	0	0	0	2	2	2	0	4	2	0	0	0	0	2
input a :	0	0	0	0	2	2	0	0	0	4	4	0	2	2	0	0
input b :	0	0	0	2	2	0	2	2	2	0	0	4	0	0	2	0
input c :	0	4	0	2	0	2	0	0	2	0	0	0	0	0	6	0
input d :	0	0	0	0	0	0	2	2	0	0	0	0	6	2	0	4
input e :	0	2	0	4	2	0	0	0	0	0	2	0	0	0	0	6
input f :	0	0	0	0	2	0	2	0	0	0	0	0	0	10	0	2

Was genau bedeutet der Eintrag 6 in Zeile e, Spalte f?

b) Die zugehörige Linear–Approximation–Table ist

output comb	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
input 0 :	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
input 1 :	0	2	2	0	4	-2	2	0	2	0	-4	-2	2	0	0	2
input 2 :	0	2	0	2	0	2	4	-2	2	0	2	0	-2	-4	2	0
input 3 :	0	0	2	-2	0	0	2	6	0	0	2	-2	0	0	2	-2
input 4 :	0	-2	2	0	-4	-2	-2	0	2	0	0	-2	2	-4	0	2
input 5 :	0	0	-4	0	0	-4	0	0	0	-4	0	0	0	0	4	0
input 6 :	0	0	-2	-2	0	-4	2	-2	0	4	2	-2	0	0	-2	-2
input 7 :	0	-2	0	-6	0	2	0	-2	2	0	-2	0	-2	0	2	0
input 8 :	0	4	0	0	-4	0	0	0	4	0	0	0	0	4	0	0
input 9 :	0	2	-2	0	0	2	-2	0	-2	4	0	-2	2	0	4	2
input a :	0	-2	0	2	0	-2	0	2	2	4	-2	4	-2	0	2	0
input b :	0	0	-2	-2	0	0	2	2	0	0	2	2	0	0	-2	6
input c :	0	2	2	0	0	-2	-2	0	-2	0	0	-2	-6	0	0	2
input d :	0	0	0	0	-4	0	4	0	-4	0	-4	0	0	0	0	0
input e :	0	4	-2	-2	0	0	-2	2	0	0	-2	2	0	-4	-2	-2
input f :	0	-2	-4	2	0	2	0	2	2	0	-2	-4	-2	0	-2	0

Was genau bedeutet der Eintrag 6 in Zeile b, Spalte f?