Wolfgang K. Seiler
Tel. 2515

B6, B4.08

5. März 2025

3. Übungsblatt Kryptologie

Aufgabe 1:

In einem Feistel-Netzwerk wird ein Nachrichtenblock $(L_0, R_0) \in \mathbb{F}_2^N \times \mathbb{F}_2^N$ in r Schritten transformiert zu einem Block (R_r, L_r), wobei gilt $L_i = R_{i-1}$ und $R_i = f(s_i, R_{i-1}) \oplus L_{i-1}$ für $i \geq 1$ mit der Feistel-Funktion $f\colon \mathbb{F}_2^k \times \mathbb{F}_2^N \to \mathbb{F}_2^N$ und dem i-ten Rundenschlüssel s_i.

a) Wie kann man aus (R_r, L_r) und den s_i die Nachricht (L_0, R_0) rekonstruieren?

b) Angenommen, $k = N$, alle Rundenschlüssel s_i sind gleich einem festen Schlüssel $s \in \mathbb{F}_2^N$ und $f(s, R_{i-1}) = s \oplus R_{i-1}$, wobei $\oplus$ die Addition im Vektorraum $\mathbb{F}_2^n$ bezeichnet. Ist das (für hinreichend große N) ein sicheres Kryptoverfahren?

c) Welcher Bedingung muß f mindestens genügen, damit Shannons Forderungen nach Konfusion und Diffusion erfüllt sind?

Aufgabe 2:

a) Zeigen Sie: Ersetzt man im einem DES-Schlüssel s alle Nullen durch Einsen und umgekehrt, so entsteht wieder ein gültiger DES-Schlüssel s'. Ist c die Verschlüsselung eines Blocks m mit s, so entsteht die Verschlüsselung c' mit s' aus c durch Vertauschen aller Nullen und Einsen.

b) Die erste S-Box von DES ist durch die folgende Wertetabelle gegeben:

a	e	$m=0$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
1	0	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
1	1	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Wenden Sie diese S-Box an auf die Eingaben 010101 und 101010, und vergleichen Sie die Binärdarstellungen der Ergebnisse!

c) Welche der Anfangs- und Endpermutationen von DES und DES^{-1} heben sich weg bei Triple-DES in der Form $m \mapsto \mathrm{DES}(s_1, \mathrm{DES}(s_2, \mathrm{DES}(s_3, m)))$ und bei Triple-DES in der „ublichen“ Form $m \mapsto \mathrm{DES}(s_1, \mathrm{DES}^{-1}(s_2, \mathrm{DES}(s_1, m)))$?

Aufgabe 3:

Für den Schlüsselstrom des DES wird der Schlüssel zerlegt in zwei Halbschlüssel. Diese bestehen aus den Bitpositionen

$$57, 49, 41, 33, 25, 17, 9, 1, 58, 50, 42, 34, 26, 18, 10, 2, 59, 51, 43, 35, 27, 19, 11, 3, 60, 52, 44, 36$$

und

$$63, 55, 47, 39, 31, 23, 15, 7, 62, 54, 46, 38, 30, 22, 14, 6, 61, 53, 45, 37, 29, 21, 13, 5, 28, 20, 12, 4$$

des Originalschlüssels.

a) Schreiben Sie diese Bitpositionen jeweils in der Form $8a + b$ mit $0 \leq b \leq 7$!

b) Warum kommen keine Zahlen mit $b = 0$ vor?

c) Welche Bits der Schlüsselbytes gehen in welchen Halbschlüssel?

Aufgabe 4:

a) Zeigen Sie: Sind a und b teilerfremde natürliche Zahlen, so gibt es eindeutig bestimmte ganze Zahlen α, β mit $0 \leq \alpha < b$ und $0 \leq \beta < a$, so daß $\alpha a - \beta b = 1$ ist.

b) Damit gibt es auch ganze Zahlen α', β' mit $0 \leq \alpha' < b$ und $0 \leq \beta' < a$, so daß $\beta' b - \alpha' a = 1$ ist. Wie hängen α, β, α' und β' zusammen?

c) Bestimmen Sie diese vier Zahlen für $a = 12345$ und $b = 67891$!

Aufgabe 5:

a) Finden Sie die Umkehrabbildung zu φ: $\begin{cases} \mathbb{F}_p \to \mathbb{F}_p \\ x \mapsto x^e \end{cases}$ für die Primzahl $p = 123\,456\,791$ und den Exponenten $e = 3$!

b) Zeigen Sie, daß es für $e = 2$ keine Umkehrabbildung gibt!

c) Bestimmen Sie alle $e \leq 10$, für die φ eine Umkehrabbildung hat!

Aufgabe 6:

a) Zeigen Sie: Zu einem Element $x \in \mathbb{Z}/N$ gibt es genau dann $y \in \mathbb{Z}/N$ mit $xy = 1$, wenn x teilerfremd zu N ist!

b) $\mathbb{Z}/N$ ist genau dann ein Körper, wenn N eine Primzahl ist.

Abgabe und Besprechung am Mittwoch, dem 12. März 2025, um 15.30 Uhr