Wolfgang K. Seiler
Tel. 2515

B6, B4.08

28. September 2022

4. Übungsblatt Kryptologie

Aufgabe 1:
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 2:

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 3:

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 4:

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.

Aufgabe 5:
Zeigen Sie: Für zwei zueinander teilerfremde Zahlen n, m ist die Abbildung von $\mathbb{Z}/mn$ nach $\mathbb{Z}/m \times \mathbb{Z}/n$, die jeder Restklasse $x \bmod mn$ das Paar $(x \bmod m, x \bmod n)$ zuordnet, bijektiv!

Aufgabe 6:

a) Zeigen Sie: $N = 2^{2n} - 1$ ist genau dann eine Primzahl, wenn $n = 1$ ist.

b) Zeigen Sie: $2^n - 1$ ist genau dann durch drei teilbar, wenn n gerade ist.
Hinweis: $2 \equiv -1 \bmod 3$

c) Die Zahl $N = \frac{1}{3}(2^{122} - 1)$ ist Produkt zweier Primzahlen. Finden Sie diese!

Besprechung am Mittwoch, dem 4. Oktober 2022, um 15.30 Uhr