Übungsblatt 8

Sommersemester 2016 — Abgabe vor der Übung am 13.06.2016

Aufgabe 8.1 (2 Pkt.)

Alice verwendet für das RSA-Verfahren den Modul n mit öffentlichem Schlüssel e und geheimem Schlüssel d. Bob verschlüsselt und versendet damit eine Nachricht m an Alice mit $\mathrm{ggT}(m, n) > 1$. Zeigen Sie, dass Alice beim Entschlüsseln tatsächlich m erhält, obwohl $m \notin \mathbb{Z}_n^*$.

Aufgabe 8.2 (2+2+1+1 Pkt.)

Eine zusammengesetzte Zahl n habe die Primfaktorzerlegung $p_1^{t_1} \cdots p_k^{t_k}$, p_i ungerade. Zeigen Sie:

a) n ist genau dann eine Carmichael-Zahl, wenn $\varphi(p_i^{t_i}) \mid (n-1),\ 1 \le i \le k$.

   Tipp: Es gibt eine Zahl g, die für alle $i \in \{1, \ldots, k\}$ modulo $p_i^{t_i}$ kongruent ist zu einem Erzeuger von $\mathbb{Z}^*_{p_i^{t_i}}$.

b) Jede Carmichael-Zahl ist quadratfrei, d. h. $t_1 = t_2 = \ldots = t_k = 1$.

c) Jede Carmichael-Zahl besteht aus mindestens 3 unterschiedlichen Primfaktoren.

d) $1729 = 7 \cdot 13 \cdot 19$ ist eine Carmichael-Zahl.

Aufgabe 8.3 (2 Pkt.)

Angenommen bei der verschlüsselten Kommunikation per RSA-Verfahren benutzen Alice und Bob das gleiche n und verschiedene teilerfremde e_1 und e_2, d. h. die öffentlichen Schlüssel (n, e_1) und (n, e_2) werden verwendet. Charlie verschlüsselt dieselbe Nachricht m mit diesen Schlüsseln zu Chiffretexten c_1 bzw. c_2 und schickt diese an Alice bzw. Bob.

Zeigen Sie, dass dann jeder, der die beiden Chiffretexte c_1 und c_2 abfängt, den Klartext m berechnen kann.

Aufgabe 8.4 (2 Pkt.)

Ein weiteres in der Vorlesung vorgestelltes Verschlüsselungsverfahren ist das ElGamal-Verfahren. Alice hat den öffentlichen Schlüssel $(n = 53, a = 5, k_A = 43)$ und Bob schickt Alice die Nachricht $(\tilde{z} = 32, c = 42)$. Entschlüsseln Sie die Nachricht.

Aufgabe 8.5 (4 Pkt.)

Lösen Sie SPOX-Aufgabe „Miller-Rabin-Test“.