

7. Übung zur Vorlesung Kryptographie

Achtung 1: Nächste Woche gibt es 2 Übungsgruppentermine: **Montag**, 7. Juni, 10:15 wie gewohnt im HS F; **Mittwoch**, 9. Juni, 8:15 wie gewohnt in Raum A7-0-025.

ACHTUNG 2: In den drei Terminen der nächsten Woche können (**und sollen**) Sie sich in die Belegungsliste für das Modul eintragen!

Aufgabe 25: *SubBytes* und *MixColumns* **(2+2 Punkte)**

- (a) Verifizieren Sie die Einträge $\pi_S(02) = 77$ und $\pi_S(06) = 6F$ in Tabelle 4.2 algebraisch, indem Sie die Darstellung in Abschnitt 4.4 benutzen.
- (b) Beschreiben Sie ein Verfahren zur effizienten Berechnung von *MixColumns* mit Hilfe von Table-Lookups und XORs. Es ist aus Platzgründen nicht möglich, eine Tabelle für alle möglichen Inputwerte von *MixColumns* aufzustellen. Wieviele Tabellen benötigen Sie, und wie groß sind diese?

Aufgabe 26: Zahlen **(3+3+3+3(+10) Punkte)**

- (a) Chinesischer Restsatz: Finden Sie die kleinste natürliche Zahl, die Reste 1 (bzw. 2, 3, 4, 5) lässt, wenn man sie durch 3 (bzw. 5, 7, 9, 11) teilt.
- (b) Berechnen Sie mit der Methode der schnellen Exponentiation $3^{21} \bmod 7$ und $5^{18} \bmod 11$.
- (c) Kleiner Fermat: Geben Sie für $n = 1111$ einen Zeugen a an und zeigen Sie dadurch, dass 1111 nicht prim ist.
- (d) Wie viele Lösungen hat $x^2 \equiv 17 \pmod{19}$? Berechnen Sie diese Lösungen.
- (e) **Zusatzaufgabe:** Versuchen Sie, ausgehend von einer der Lösungen unter (d), je eine Lösung für $y^2 \equiv 17 \pmod{19^2}$ und $z^2 \equiv 17 \pmod{19^3}$ zu finden. Skizzieren Sie ein Verfahren, um generell Lösungen von $x^2 \equiv a \pmod{p^k}$ aus Lösungen von $x^2 \equiv a \pmod{p}$ zu bekommen (p prim).

Aufgabe 27: RSA **(2+2 Punkte)**

- (a) Es seien der RSA-Modul $n = 3599$ und der Verschlüsselungsexponent $e = 17$ gegeben. Verschlüsseln Sie $x = 7$. Die Zahl n ist sehr klein. Nutzen Sie dies, um n zu faktorisieren und d zu berechnen. Entschlüsseln Sie $y = 1901$.
- (b) Auf einer Webseite stehen die Schlüssel

$$\begin{array}{ll} n = 91, e = 61 & \text{für Alice,} \\ n = 143, e = 121 & \text{für Bob,} \\ n = 187, e = 133 & \text{für Charlie.} \end{array}$$

Sie erhalten eine Warnung, dass einer dieser Schlüssel gefälscht sein könnte. Welcher der dreien erweist sich als etwas merkwürdig?