Diskrete Mathematik für Lehramt Informatik
Sommersemester 2021

12. Übungsblatt (24.6.2021)

Beispiel 12.1. Welche der folgenden Zahlen g, m, n, p können bei einer Schlüsselvereinbarung nach Diffie-Hellman vorkommen? Berechnen Sie gegebenenfalls die geheimen Parameter a und b sowie den Schlüssel s. (Für diese Rechnungen ist Computerhilfe erlaubt, Sie sollten die nötigen Schritte und Überlegungen aber in der Übung zeigen können.)

(a) $g = 17$, $m = 1$, $n = 100$, $p = 201$.

(b) $g = 10$, $m = 29$, $n = 45$, $p = 199$.

(c) $g = 10$, $m = 24$, $n = 6$, $p = 101$.

Beispiel 12.2. Welche der folgenden Zahlenpaare (m, r) können als öffentliche Schlüssel für eine RSA-Verschlüsselung mit Verschlüsselungsfunktion $f(k) = k^r \bmod m$ verwendet werden?

(a) $(m, r) = (229, 149)$ (b) $(m, r) = (319, 39)$

(c) $(m, r) = (299, 189)$ (d) $(m, r) = (399, 109)$

Beispiel 12.3. Die Zahlenfolge $(28, 56, 3)$ wurde per RSA-Verfahren mit dem öffentlichen Schlüssel $m = 779$ und $r = 103$ verschlüsselt. Ermitteln Sie den privaten Schlüssel s und entschlüsseln Sie die Nachricht.

Rechnen Sie beim Entschlüsseln modulo m (und nicht modulo p und q wie in Beispiel 12.4).

Beispiel 12.4. Die Entschlüsselung beim RSA-Verfahren kann effizienter gestaltet werden, wenn man $g(k) = k^s \bmod m$ nicht direkt berechnet, sondern zunächst $g_p(k) = k^s \bmod p$ und $g_q(k) = k^s \bmod q$ ausrechnet und dann $g(k)$ mit Hilfe des chinesischen Restsatzes aus $g_p(k)$ und $g_q(k)$ bestimmt.

Berechnen Sie sämtliche Schlüssel für $p = 11$, $q = 41$ und $r = 9$ und führen Sie danach obiges Prinzip aus, um die verschlüsselte Nachricht $(409, 166)$ zu entschlüsseln.

Erinnerung: Die entschlüsselte Nachricht sollte aus natürlichen Zahlen kleiner als m bestehen.