Diskrete Mathematik für Informatikstudien
Sommersemester 2022

6. Übungsblatt (26.4.2022)

Auf diesem Blatt müssen an mehreren Stellen die Werte von Schlüsseln/Parametern berechnet werden. Falls mehrere Werte in Frage kommen, wählen Sie jeweils den kleinsten positiven Wert für Ihr Ergebnis.

Beispiel 6.1. Alice und Bob führen einen Diffie-Hellman-Schlüsselaustausch durch. Dazu vereinbaren Sie zuerst eine Primzahl p und eine natürliche Zahl $k < p$. Dann wählt Alice eine natürliche Zahl $a < p$ und übermittelt $A = k^a \bmod p$ an Bob. Analog wählt Bob eine natürliche Zahl $b < p$ und übermittelt $B = k^b \bmod p$ an Alice. Aus diesen Werten berechnen sie den Schlüssel

$$s \equiv A^b \bmod p \equiv B^a \bmod p.$$

Eve hört die übermittelten Zahlen p, k, A und B ab. Welche der folgenden Zahlen können dabei vorkommen? Berechnen Sie gegebenenfalls die Parameter a, b und den Schlüssel s.

(a) $p = 189$, $k = 11$, $A = 5$, $B = 4$;

(b) $p = 197$, $k = 14$, $A = 183$, $B = 42$;

(c) $p = 199$, $k = 10$, $A = 70$, $B = 28$.

Beispiel 6.2. Welche der folgenden Zahlenpaare (m, r) können als öffentliche Schlüssel für eine RSA-Verschlüsselung mit Verschlüsselungsfunktion $f(k) = k^r \bmod m$ verwendet werden? Berechnen Sie gegebenenfalls den privaten Schlüssel s, der für die Entschlüsselungsfunktion $g(k) = k^s \bmod m$ benötigt wird.

(a) $(m, r) = (219, 153)$ (b) $(m, r) = (239, 163)$

(c) $(m, r) = (259, 173)$ (d) $(m, r) = (279, 193)$

Beispiel 6.3. Die Zahlenfolge $(60, 2, 118, 178)$ wurde per RSA-Verfahren mit dem öffentlichen Schlüssel $m = 767$ und $r = 443$ 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 6.4).

Beispiel 6.4. 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.

Führen Sie obiges Prinzip für den Schlüssel $m = 473 = 11 \cdot 43$ und $s = 89$ aus, um die Nachricht $(89, 303, 42, 83)$ zu entschlüsseln.

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

Beispiel 6.5. Für den RSA-Algorithmus wurde der öffentliche Schlüssel $m = 259$ und $r = 7$ bekannt gegeben.

(a) Verschlüsseln Sie die Nachricht $(26, 4)$.

(b) Berechnen Sie den Geheimschlüssel s.

(c) Entschlüsseln Sie die Nachricht $(36, 63)$.