Diskrete Mathematik für Informatikstudien
Sommersemester 2020

6. Übungsblatt (28.4.2020)

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

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

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

(a) $p = 101$, $k = 10$, $A = 28$, $B = 4$;

(b) $p = 199$, $k = 10$, $A = 7$, $B = 81$;

(c) $p = 201$, $k = 17$, $A = 1$, $B = 100$.

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) $(m, r) = (229, 149)$ (b) $(m, r) = (319, 219)$

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

Beispiel 6.3. 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 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.

Bekannt sind der öffentliche Schlüssel $m = 451$ und $r = 9$. Berechnen Sie den privaten Schlüssel s und führen Sie obiges Prinzip aus, um die Nachricht $(222, 21, 123, 97)$ zu entschlüsseln. *Erinnerung:* Die entschlüsselte Nachricht sollte aus natürlichen Zahlen kleiner als m bestehen.

Beispiel 6.5. Für den RSA-Algorithmus wurde der öffentliche Schlüssel $m = 119$ und $r = 17$ bekannt gegeben.

(a) Verschlüsseln Sie die Nachricht $(50, 35)$.

(b) Berechnen Sie den Geheimschlüssel s.

(c) Entschlüsseln Sie die Nachricht $(18, 11)$.