

Aufgabe 40. (a) Beschreibe und berechne einen Diffie-Hellman-Schlüsselaustausch mit den Parametern $p = 31$, $g = 5$, $a = 13$, $b = 11$.

(b) Zu einem Diffie-Hellman-Schlüsselaustausch seien folgende Daten bekannt:

$$\begin{array}{ll} g = 11 & p = 29 \\ m = 17 & n = 12 \end{array}$$

Bestimme die geheimen Parameter a , b und den Schlüssel r !

Hinweis: Computer erlaubt (z.B. sage)!

Aufgabe 41. Welche der folgenden Zahlen g , m , n , p sind für eine Schlüsselvereinbarung nach Diffie-Hellman-Merkle geeignet? Berechne gegebenenfalls die geheimen Parameter a und b sowie den Schlüssel s . (Für die Zwischenrechnungen ist ein Computer erlaubt.)

- (a) $g = 17$, $m = 29$, $n = 59$, $p = 201$
- (b) $g = 10$, $m = 29$, $n = 45$, $p = 199$
- (c) $g = 10$, $m = 24$, $n = 6$, $p = 101$

Aufgabe 42. Gegeben sei $m = 1363$.

(a) Welche der folgenden Zahlen sind als öffentliche RSA-Schlüssel geeignet (Begründung!)?

$$r = 21 \qquad r = 23 \qquad r = 25$$

Berechne ggf. die zugehörigen inversen Schlüssel.

(b) Wähle einen geeigneten Schlüssel und verschlüssele die Botschaft

“OKAY”

mit der Konvention “ $i \cdot 26 + j$ ” aus Aufgabe 39.

(c) Die folgende Nachricht wurde mit dem Schlüssel $r = 17$, $m = 1363$ verschlüsselt.

[1143, 499]

Finde den inversen Schlüssel s und entschlüssele die Botschaft.

Hinweis: Für die Zwischenrechnungen ist ein Computer erlaubt.

Aufgabe 43. In diesem Beispiel soll gezeigt werden, dass die Verwendung kleiner Exponenten in öffentlichen Schlüsseln (z.B. aus Effizienzgründen) problematisch sein kann.

Sei $r = 3$ und es sei bekannt, dass die gleiche Nachricht x mit den öffentlichen Schlüsseln $(m_1, r) = (143, 3)$, $(m_2, r) = (391, 3)$ und $(m_3, r_3) = (899, 3)$ zu folgenden Werten verschlüsselt wurde:

$$x^3 \equiv 129 \pmod{143}$$

$$x^3 \equiv 281 \pmod{391}$$

$$x^3 \equiv 380 \pmod{899}$$

Bestimme x , ohne die Schlüssel m_i zu faktorisieren. Wie groß darf x sein, damit diese Methode funktioniert?