

Übungen zur Vorlesung Kryptographie

Blatt 7

Aufgabe 25: (RSA knacken IV)

Führen Sie einen Wiener-Angriff auf folgende Situation durch: Es ist $N = 10807$, $e = 7067$ und d ist fahrlässigerweise klein. Berechnen Sie mittels Satz 5.1 im Skript Kandidaten für d . Probieren Sie diese Kandidaten nacheinander aus zum Entschlüsseln der verschlüsselten Botschaft

$$c = (1, 3036, 3965, 6151, 3645, 8123, 6983, 112, 9057)$$

Dabei ist im Klartext $a=0$, $b=1$, $c=2 \dots z=25$.

(Ihr Lösungsweg soll ein Wiener-Angriff sein. Andere Wege der Entschlüsselung sind hier möglich, zählen aber nicht als korrekte Lösung.)

Aufgabe 26: (Diffie-Hellman)

(a) In einem Diffie-Hellman-Schlüsseltausch sind $G = Z_{19}^*$ und $g = 2$ die öffentlichen Informationen. Eve erfährt, dass Alice $3 \equiv g^a \pmod{p}$ an Bob gesendet hat, und Bob hat $9 \equiv g^b \pmod{p}$ an Alice gesendet. Was ist Alice' geheimer Exponent a ? Was ist Bobs geheimer Exponent b ? Was ist der gemeinsame Schlüssel $g^{ab} \pmod{p}$?

(b) Was ist falsch an folgendem Argument: "Eve kennt g^a und g^b , kann also $g^{ab} = g^a \cdot g^b \pmod{p}$ effizient berechnen und kennt damit den gemeinsamen Schlüssel."

Aufgabe 27: (Baby steps)

Berechnen Sie mit dem Baby-Step-Giant-Step-Algorithmus die folgenden diskreten Logarithmen: $\text{dlog}_7(11) \pmod{101}$ und $\text{dlog}_{71}(101) \pmod{1009}$. Zeigen Sie Ihre Berechnung.

Aufgabe 28: (Wieviele dlogs?)

(a) Finden Sie drei Primzahlen $a, b, p \in \mathbb{N}$ mit $1 < a < p$, $1 < b < p$, $a \neq b$, so dass $\text{dlog}_a(b)$ modulo p nicht existiert.

(b) Sei g ein Erzeuger von G . Zeigen Sie, dass für jedes $a \in G$ der diskrete Logarithmus $\text{dlog}_g(a)$ existiert.

(c) Sei nun $|G|$ gerade und g kein Erzeuger von G , sondern g habe die Ordnung $|G|/2$. Wieviel Werte kann der diskrete Logarithmus $\text{dlog}_g(a)$ für ein $a \in G$ annehmen? Begründen Sie Ihre Antwort.

Abgabe bis Mittwoch 27.5.2020 bis 14 Uhr per Email an den Tutor.

Philipp Braukmann pbraukmann@techfak.de
Jonas Friemel jfriemel+krypto@techfak.de