Dr. Dirk Frettlöh 29.5.2019

Übungen zur Vorlesung Kryptographie

Blatt 8

Aufgabe 29: (RSA knacken IV: Wiener-Angriff)
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

$$c = (683, 3036, 6983, 1, 7847, 6983, 9057)$$

Dabei ist im Klartext a=0, b=1, c=2 ... z=25.
(Ihr Lösungsweg soll ein Wiener-Angriff sein. Andere Wege der Entschlüsselung sind hier möglich, zählen aber nicht als korrekte Lösung).

Aufgabe 30: (Schlechtes q bei RSA)
(a) Was geht bei RSA schief, falls p oder q keine Primzahlen sind? Genauer: angenommen, Alice wählt ein q, dass keine Primzahl ist, sondern zwei Primfaktoren r und s hat. Danach geht sie vor wie im Skript beschrieben. (Insbesondere berechnet sie "$\varphi(N)$" als $(p-1)(q-1)$). Ist das Verfahren weiterhin korrekt, effizient und sicher? Begründen Sie ihre Antwort.

(b) Was kann Alice tun, um das Problem aus (a) zu vermeiden?

Aufgabe 31: (Diffie-Hellman)
(a) In einem Diffie-Hellman-Schlüsseltausch sind $p = 19$ und $g = 2$ die öffentlichen Informationen. Eve erfährt, das Alice $3 \equiv g^a \bmod p$ an Bob gesendet hat, und Bob hat $9 \equiv g^b \bmod p$ an Alice gesendet. Was ist Alice' geheimer Exponent a? Was ist Bobs geheimer Exponent b? Was ist der gemeinsame Schlüssel $g^{ab} \bmod p$?

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

Aufgabe 32: (Diskrete Logarithmen)
(a) Berechnen Sie mit dem Baby-Step-Giant-Step-Algorithmus den diskreten Logarithmus $\mathrm{dlog}_7(11) \bmod 71$. Zeigen Sie Ihre Berechnung.

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

Falls Sie Programmcode abgeben, bitte (1) auch erklären, wie Sie vorgingen, (2) auch das Ergebnis aufschreiben, und (3) bitte den Code selbst (kein Foto) an den Tutor schicken.

Abgabe: Mittwoch 5.6.2019 bis 14 Uhr in Postfach 2183 in V3, oder per Email an den Tutor.
Bitte auf jeder Abgabe das Tutorium angeben! (Di oder Do)

Dienstag	Philipp Braukmann	pbraukmann@techfak.uni-bielefeld.de
Donnerstag	Oliver Tautz	otautz@techfak.uni-bielefeld.de