Übungen zur Vorlesung Kryptographie

Blatt 7

Aufgabe 25: (RSA knacken mit Wienern)
Führen Sie einen Wiener-Angriff auf folgende Situation durch: Es ist $N = 1005973$, $e = 602381$ 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

$$c = (830057, 614316, 0, 871795, 737805, 830057, 876283, 614316, 293606, 961198, 614316)$$

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 26: (Diffie-Hellman in $(Z_N^*, \cdot \bmod N)$)
(a) In einem Diffie-Hellman-Schlüsseltausch sind $G = Z_{23}^*$ und $g = 5$ die öffentlichen Informationen. Eve erfährt, das Alice $9 \equiv g^a \bmod 23$ an Bob gesendet hat, und Bob hat $6 \equiv g^b \bmod 23$ an Alice gesendet. Was ist Alice' geheimer Exponent a? Was ist Bobs geheimer Exponent b? Was ist der gemeinsame Schlüssel $g^{ab} \bmod 23$?

(b) Berechnen Sie $\mathrm{dlog}_2(6)$ und $\mathrm{dlog}_2(7)$ in Z_{23}^* (falls möglich).

(c) Warum nehmen Alice und Bob in (a) nicht $g = 2$?

Aufgabe 27: (Diffie-Hellman in $(Z_N, + \bmod N)$)
Diese Aufgabe zeigt, warum es keine gute Idee ist, den Diffie-Hellman-Schlüsseltausch mit der Gruppe $(Z_N, + \bmod N)$ zu nutzen.

(a) Was heißt g^a in der Restklassengruppe $(Z_N, +)$? Was ist also 2^5 in $(Z_{11}, +)$?
(Erinnerung: $g^a := \underbrace{g \oplus g \oplus \cdots \oplus g}_{a \text{ mal}}$, wobei $\oplus$ die Gruppenoperation ist.)

(b) Was heißt also $\mathrm{dlog}_g(a)$ in $(Z_N, +)$? Was ist also $\mathrm{dlog}_2(3)$ in $(Z_{11}, +)$? Wieso ist dieser dlog auch für hohe N effizient berechenbar?

(c) Zeigen Sie, dass 2 ein Erzeuger von $(Z_{101}, +)$ ist.

(d) Alice und Bob benutzen leichtfertigerweise Diffie-Hellman mit $G = (Z_{101}, +)$ und $g = 2$. Alice schickt $g^a \equiv 54 \bmod 101$ an Bob. Bob schickt $g^b \equiv 56 \bmod 101$ an Alice. Was ist ihr gemeinsamer Schlüssel?

Aufgabe 28: (Geburtstage und Baby Steps)
(a) Berechnen Sie $\mathrm{dlog}_7(20) \bmod 71$, einmal mit dem Baby-Step-Giant-Step-Algorithmus, einmal mit dem Geburtstagsangriff-Algorithmus.

(b) Sie lösen nun das Geburtstagsparadox für Tage im Monat. Ab welcher Anzahl n von versammelten Personen ist die Wahrscheinlichkeit größer als 50%, dass mindestens zwei Personen am gleichen Tag im Monat Geburtstag haben? *(Wir nehmen der Einfachheit halber an, dass jeder der 31 Tage im Monat gleich wahrscheinlich ist. Diese Annahme ist unrealistisch, liefert aber dennoch einen recht genauen Wert.)*

Abgabe bis Mittwoch 2.6.2021 bis 14 Uhr per Email an den Tutor.

Jan Jan-Philipp Brünger jbruenger@techfak.de
Leonard Simon Ellinghaus lellinghaus+krypto@techfak.de
Kallias Stoupas kstoupas+krypto@techfak.de