UNIVERSITÄT DES SAARLANDES

Fachrichtung Mathematik
Prof. Dr. Simon Brandhorst
Dr. Tobias Columbus

Elementare Zahlentheorie

Übungsblatt 13

Aufgabe 1 (2 Punkte)
Berechnen Sie 5^{26} und 7^{23} modulo 29 mittels schneller Exponentiation.

Aufgabe 2 (3 Punkte)

(a) Erzeugen Sie einen öffentlichen RSA-Schlüssel (N, e) für die beiden Primzahlen $p = 7$ und $q = 11$.

(b) Verschlüsseln Sie mit dem öffentlichen Schlüssel aus Teil (a) eine Nachricht $m \in (\mathbb{Z}/N\mathbb{Z})^\times$.

Aufgabe 3 (3 Punkte)
Sie haben den öffentlichen RSA-Schlüssel $N = 55$ und $e = 3$. Entschlüsseln Sie das Chiffrat $c = 8$.

Aufgabe 4 (4 Punkte)
Alice, Bob und Carrol kommunizieren mit dem RSA-Algorithmus aus der Vorlesung. Weil Alice ein bisschen faul ist und nicht soviel rechnen möchte, hat sie Bob und Carrol gebeten, denselben Modulus zu benutzen. Die beiden haben zugestimmt und gemeinsam Primzahlen p, q und den Modulus $N = pq$ gewählt. Schließlich haben sie voreinander geheimgehaltene private Schlüssel d_1 und d_2 sowie öffentliche Schlüssel (N, e_1) bzw. (N, e_2) mit $\mathrm{ggT}(e_1, e_2) = 1$ gewählt.

(a) Alice verschickt eine Nachricht m an Bob. Warum kann Carrol diese Nachricht leicht entschlüsseln?

(b) Alice verschickt nun dieselbe Nachricht $m \in (\mathbb{Z}/N\mathbb{Z})^\times$ an Bob und Carrol. Eva fängt beide Chiffrate ab. Wie kann Eva die Nachricht entschlüsseln?

Aufgabe 5 (4 Punkte)
Alice und ihre Freunde Bob, Carrol und Dieter kommunizieren wieder mit dem RSA-Algorithmus aus der Vorlesung. Weil Alice so faul ist und nicht soviele Multiplikationen durchführen wollte, bat sie Bob, Carrol und Dieter einen kleinen Exponenten e zu wählen. Daraufhin haben die drei die öffentlichen Schlüssel $(N_1, 3)$, $(N_2, 3)$ und $(N_3, 3)$ mit paarweise teilerfremden Moduli N_1, N_2 und N_3 gewählt.

(a) Warum kann Eva nun Chiffrate von Nachrichten $[m] \in (\mathbb{Z}/N\mathbb{Z})^\times$ für Bob mit „kleinem“ $m \in \mathbb{N}$ durch ganzzahlige Rechenoperationen entschlüsseln?

(b) Alice schickt die Chiffrate $m^3 \mod N_1$, $m^3 \mod N_2$ und $m^3 \mod N_3$ derselben Nachricht $m \in \mathbb{N}$ mit $m < \min\{N_1, N_2, N_3\}$ und $\mathrm{ggT}(m, N_i) = 1$ an Alice, Carrol und Dieter. Eva fängt alle drei Chiffrate ab. Wie kann Eva die Nachrichten einfach entschlüsseln?

Abgabe bis spätestens Montag, den 08. 07. 2019, um 12:00 Uhr. Werfen Sie Ihre Lösungsvorschläge in die dafür vorgesehenen Einwurfkästen vor dem Zeichensaal in Gebäude E 2 5. Abgabe zu zweit ist möglich. Bitte geben Sie Ihren Namen, Ihre Matrikelnummer und Ihre Übungsgruppe and!