Kryptologie
Übungsblatt 6

Aufgabe 6.1

(a) Bei der Fermat-Faktorisierung startet man, bei Eingabe n, mit $x = \lceil n \rceil$ und $z = x^2 - n$ und testet in jedem Schleifendurchlauf, ob z eine Quadratzahl ist, also $z = y^2$. Ansonsten wird im nächsten Durchlauf x um 1 erhöht und dementsprechend z neu berechnet.
Führen Sie diesen Algorithmus durch, um $n = 2923$ zu faktorisieren.

(b) Die Fermat-Faktorisierung ist bei Eingabe $n = p \cdot q$ dann besonders effizient, wenn die Faktoren p und q sehr nahe beieinander liegen.
Bei RSA erzeugen wir (zum Beispiel) eine 1000-Bitzahl n mit Hilfe einer 499-Bit Primzahl p und einer 501-Bit Primzahl q. Kann man hier sagen, dass p und q „sehr nahe beieinander liegen", so dass man mit einer schnelleren Faktorisierung rechnen kann?

Aufgabe 6.2

Der $(p-1)$-Algorithmus von Pollard startet (zum Beispiel) mit $a = 2$ und berechnet in jedem Schritt a neu zu $a^B \mod n$, wobei B in jedem Schritt um 1 erhöht wird. Dabei wird jedesmal getestet, ob $\mathrm{ggT}(a-1, n)$ ein nicht-trivialer Teiler von n ist.
Führen Sie dies durch mit $a = 2$ und $n = 24823$.
Es gilt $24823 = 103 \cdot 241$. Sagen Sie voraus, welcher der beiden Faktoren hierbei zuerst gefunden wird.

Aufgabe 6.3

Der ρ-Algorithmus von Pollard mit Anwendung des Cycle Detection Tricks soll die Zahl 1219 faktorisieren. Man startet mit einer beliebigen Zahl, zum Beispiel $z_0 = 20$ und berechnet die Nachfolgerzahlen mittels $z_{i+1} = (z_i^2 + 1) \mod 1219$. Man testet dabei, ob $\mathrm{ggT}(z_k - z_{2k}, n)$ für $k = 1, 2, 3, ...$ einen nicht-trivialen Teiler von $n = 1219$ ergibt. Führen Sie dies durch.

Aufgabe 6.4

Bei der Babystep-Giantstep-Methode zur Bestimmung des Diskreten Logarithmus wird (bei Eingabe n, a, y) das gesuchte x mit $y = a^x \mod n$ zerlegt in x_1, x_2 so dass $x = x_1 \cdot \lceil \sqrt{n} \rceil + x_2$. Dementsprechend muss die Gleichung $\left(a^{\lceil \sqrt{n} \rceil}\right)^{x_1} = y \cdot \left(a^{-1}\right)^{x_2}$ gelöst werden.
Führen Sie dies durch für $n = 137$, $a = 3$ und $y = 11$.

Aufgabe 6.5

In einem RSA-System soll eine sogenannte blinde Signatur (also eine Signatur ohne den Nachrichteninhalt zu kennen) realisiert werden. Sei $n = 11 \cdot 13 = 143$ die öffentliche Modulgröße von Teilnehmer Bob. Bestimme den kleinstmöglichen öffentlichen Verschlüsselungsexponenten e sowie den dazu gehörigen (geheimen) Entschlüsselungsexponenten d.

Von Bob soll das Dokument $m = 9$ unterschrieben werden. Bestimmen Sie die Unterschrift u von Bob.
Die Teilnehmerin Alice verblendet nun zunächst das Dokument m mittels der Zufallszahl $z = 5$ zu $\tilde{m} = m \cdot z^e$. Bestimmen Sie $\tilde{m}$ sowie Bobs Unterschrift $\tilde{u}$ zu $\tilde{m}$.
Danach entfernt Alice wieder die Verblendung und erhält die Unterschrift u zu m. Rechnen Sie nach, dass Alice tatsächlich u erhält.