Aufgaben zum Mathematik-Propädeutikum

WiSe 2020, Teil 3

Im zugehörigen Lehrvideo gibt es zwei Sorten von Aufgaben: Kleinere Aufgaben, für die Sie das Video anhalten sollen, und die dann im Video gelöst werden – und andererseits größere Aufgaben, die etwas mehr Nachdenken und Rechnen erfordern. Bitte lösen Sie die kleineren Aufgaben, wenn Sie das Video sehen. Am Ende des Videos können Sie über die Knobelaufgaben nachdenken.

Kleinere Aufgaben

Minute 20:45: Hier ist ein Beispiel für eine Verschlüsselung und Entschlüsselung mit RSA:

$$\begin{aligned} \text{Öffentlicher Schlüssel:} \quad & n = 13 \cdot 17 = 221 \\ & e = 35 \\ \text{Privater Schlüssel:} \quad & d = 11 \quad (\text{denn } \phi = 12 \cdot 16 = 192 \text{ und } e \cdot d = 385 \equiv 1 \ (\phi)) \end{aligned}$$

Jetzt soll die Nachricht $M = 14$ verschlüsselt werden. Dazu berechnet Bob

$$C = M^e \% n = 14^{35} \,\%\, 221$$

Beispielsweise mit Hilfe einer Tabellenkalkulation findet er $C = 92$. (Später im gleichen Video werden wir eine schnellere Methode zum Potenzieren kennenlernen.) Alice muss nun $92^{11} \,\%\, 221$ berechnen, mit dem Ergebnis $C^d \,\%\, n = 14$, also genau der von Bob versendeten Nachricht.

Versuchen Sie jetzt, die Nachricht $M = 15$ mit dem öffentlichen Schlüssel $n = 77$ und $e = 13$ zu verschlüsseln. Prüfen Sie, dass $\phi = 60$ und $13 \cdot 37 \equiv 1 \ (\phi)$ gelten und versuchen Sie anschließend, das Chiffrat mit $d = 37$ wieder zu entschlüsseln.

Minute 38:28: Prüfen Sie $1 = 3 \cdot 40 - 7 \cdot 17$.

Minute 42:10: Prüfen Sie $33 \cdot 17 \equiv 1 \pmod{40}$.

Minute 45:05:
Satz: Seien $r, s \in \mathbb{N}$ mit $r \equiv s \pmod{\phi}$ und $a \in \mathbb{N}$ teilerfremd zu n. Dann ist $a^r \equiv a^s \pmod{n}$.

Beweis: Nach Voraussetzung gibt es ein $k \in \mathbb{Z}$ mit $r = s + k \cdot \phi$. Damit ist ...

Versuchen Sie, den Beweis zu vervollständigen, indem Sie r in a^r einsetzen.

Minute 48:15: Wo ist die Lücke in dem Argument, dass $M^{e \cdot d} \,\%\, n \;=\; M$ ist?

Aufgaben zum Knobeln und Ausarbeiten

(1.1): Seien p und q Primzahlen. Gibt es tatsächlich genau $(p-1)(q-1)$ Zahlen zwischen 1 und pq, die zu pq teilerfremd sind?

(2.1): Berechnen Sie 3^{19} mit der schnellen Methode aus dem Video.

(3.1): Kann man ein Verschlüsselungsverfahren wie RSA auch verwenden, um sich zu identifizieren? Nehmen wir an, Alice hat, wie zuvor, Primzahlen p und q gewählt und $n = p \cdot q$ zusammen mit einem passenden e veröffentlicht. Bob nimmt jetzt Kontakt auf, kann sich aber nicht sicher sein, ob er tatsächlich mit Alice kommuniziert, oder mit jemandem, der sich nur als Alice ausgibt (denn Alice's öffentlicher Schlüssel (n und e) ist ja jedem bekannt). Wie kann Alice gegenüber Bob beweisen, tatsächlich Alice zu sein, ohne dabei ihren privaten Schlüssel (die Zahl d, oder alternativ die Primzahlen p und q) preiszugeben?