Übung zur Vorlesung
Kryptokomplexität IIBearbeitungszeit: 16. April bis 26. April
Verantwortlich: Roman Zorn

Begründen Sie Ihre Antworten und bereiten Sie sie so vor, dass Sie sie in der Übung präsentieren können.

Aufgabe 1: Wiederholung RSA

Gegeben seien der RSA-Modul $n = 403$ und das Alphabet $\Sigma = \{D, E, G, I, N, R, U\}$ kodiert über $\mathbb{Z}_7$:

0	1	2	3	4	5	6
<hr/>						
D	E	G	I	N	R	U

Bob wählt als öffentlichen Exponenten $e = 149$, schickt den Schlüssel (n, e) an Alice und erhält von ihr folgende verschlüsselte Nachricht

DGIG DENN DUEG DGGR DEDG.

► Bestimmen Sie Bobs privaten Schlüssel d und entschlüsseln Sie die Nachricht. Verwenden Sie dabei Square-and-Multiply und geben Sie alle benötigten Zwischenschritte an.

Aufgabe 2: Angriffe auf RSA

- Gegeben sei der RSA-Modul $n = 95$.
 - Welche Auswirkungen hat die Wahl des öffentlichen Exponenten $e = 17$ auf das Kryptosystem?
- Welche Maßnahmen können ergriffen werden, um einen Angriff auf kleine Nachrichten (*Small-Message Attack*) zu verhindern?
- Gegeben seien der RSA-Modul $n = 14803 = 113 \cdot 131$ sowie der öffentliche Exponent $e = 9707$.
 - Ist es möglich, Wieners Angriff auszuführen?

Aufgabe 3: *Low-Exponent-Angriff* auf RSA

Drei Parteien verwenden das RSA-Kryptosystem, um dieselbe Nachricht m zu verschlüsseln. Sie fangen die dabei verschickten öffentlichen Schlüssel $(n_1, e) = (85, 3)$, $(n_2, e) = (87, 3)$ und $(n_3, e) = (253, 3)$ sowie die entsprechenden verschlüsselten Texte $c_1 = 56$, $c_2 = 26$ und $c_3 = 66$ ab.

► Verwenden Sie einen *Low-Exponent-Angriff*, um die Originalnachricht m zu ermitteln.