

Diskrete Mathematik für Informatiker

Tutorium WS 14/15

Übungsblatt 5

Aufgabe 1

Gegeben sind die öffentlichen Schlüssel $n = 21$ und $k = 13$ für eine RSA-Kodierung.

- Kodieren Sie die Nachrichten 7 und 14.
- Bestimmen Sie die privaten Schlüssel $\varphi(n), l$ und dekodieren Sie die Nachricht 9.

Aufgabe 2

Bestimmen Sie $x \in \mathbb{Z}_{910}$ mit

$$1 \equiv x \pmod{2}$$

$$4 \equiv x \pmod{5}$$

$$2 \equiv x \pmod{7}$$

$$11 \equiv x \pmod{13}$$

Aufgabe 3

Bestimmen Sie die folgenden Werte der eulerschen φ -Funktion:

- $\varphi(8)$
- $\varphi(167)$
- $\varphi(121)$
- $\varphi(221)$