

Datenschutz und Datensicherheit / Systemsicherheit

1. Übung

1. Aufgabe:

Berechnen Sie

$$\begin{array}{l} 13 \bmod 5 \\ -12 \bmod 5 \end{array}$$

$$\begin{array}{l} 13 \operatorname{div} 5 \\ -12 \operatorname{div} 5 \end{array}$$

$$-12 \cdot 3 \equiv \dots \pmod{5}$$

$$121 \cdot 16 \equiv \dots \pmod{5}$$

2. Aufgabe:

Sei $a = D \cdot m + R$ mit $0 \leq R < m$. Zeigen oder widerlegen Sie:

$$a + b \equiv R + b \pmod{m}$$

$$a \cdot b \equiv R \cdot b \pmod{m}$$

$$a^k \equiv R^k \pmod{m}$$

$$b^a \equiv b^R \pmod{m}$$

3. Aufgabe:

Auf welche Ziffer endet $(12173)^{18}$?

4. Aufgabe:

Wir betrachten Nachrichten der Länge N über dem Alphabet $\Sigma = \{0, 1\}$.

a) Wieviele Verschlüsselungsfunktionen $E : \Sigma^N \rightarrow \Sigma^N$ gibt es?

b) Wieviel Speicher wird benötigt, wenn eine solche Verschlüsselungsfunktion als Tabelle abgelegt wird?