

# Muster-Klausur

**Aufgabe 1.** Mit Hilfe des Pohlig-Hellman Algorithmus finden Sie alle Lösungen der Kongruenz

$$3 \equiv 7^x \pmod{71}.$$

**Aufgabe 2** (über das RSA Kryptosystem).

Sei  $(p, q, d) = (11, 19, 151)$  der private Schlüssel von Bob.

- (a) Berechnen Sie seinen öffentlichen Schlüssel  $(n, e)$ .
- (b) Alice will Klartext  $t = 2$  mit RSA-Verfahren chiffrieren und an Bob schicken. Wie sieht der Chiffretext  $s = s(t)$  aus.
- (c) Bob erhält den Chiffretext  $s = 3$  von Claudia. Wie sieht ihr Klartext  $t$  aus?

**Aufgabe 3.** Faktorisieren Sie die Zahl 1769 mit der Pollard  $\rho$ -Methode.

**Aufgabe 4.** Berechnen Sie die erste drei Näherungsbrüche der Zahl  $\sqrt{1769}$ .