11. Übungsblatt

Abgabe: Freitag, 29. Juni 2018, bis 10.00

Aufgabe 1 Es seien $p = 123456791$, $q = 987654323$, $n = p \cdot q$ und $e = 3$. Der Klartext sei

$$a = 14152019010605 \in \mathbb{Z}_n.$$

Berechnen Sie $a^e \bmod p$ und $a^e \bmod q$. Berechnen Sie hieraus mithilfe des chinesischen Restsatzes $c \equiv a^e \bmod n$.
Hinweis. Der chinesischen Restsatz für zwei Primzahlen wurde in Blatt 6 , 2. Aufgabe von Ihnen bewiesen.

Aufgabe 2 Um eine Textnachricht mit RSA zu verschlüsseln, wandeln wir sie zunächst wie folgt in eine Zahlenfolge um: Der Klartext wird so eingeteilt, dass je zwei Buchstaben einen Block von vier Ziffern bilden:

$$a = 00, b = 01, c = 02 \text{ usw..}$$

Zum Beispiel wird die Nachricht "klar" zu 1011 0017. Diese Ziffernblöcke können dann mit RSA verschlüsselt werden.

Es sei $(n, e) = (3149, 563)$ der öffentliche Schlüssel beim RSA Verfahren. Hiermit wurde der folgende Geheimtext erzeugt:

$$1263\ 0996\ 1102\ 3039\ 2177\ 2311.$$

Wie lautet der geheime Schlüssel d? Bestimmen Sie den Klartext.

Aufgabe 3 Sei $n = p \cdot q$ für zwei verschiedene Primzahlen p und q. Angenommen, Sie kennen n und $\varphi(n)$. Zeigen Sie, dass Sie dann p und q bestimmen können.
Hinweis: Betrachten Sie das Polynom $x^2 - (n - \varphi(n) + 1)x + n$.

Aufgabe 4 Zeigen Sie

$$\binom{n}{i} = \frac{n(n-1)\cdots(n-i+1)}{1 \cdot 2 \cdots i}$$

(a) mit Hilfe eines Urnenmodels;
(b) algebraisch.