Universität Heidelberg
Mathematisches Institut

Dr. Rolf Busam
Andreas Riedel

Aufbau der Zahlsysteme

Sommersemester 2010

Aufgabenblatt 11 28. Juni 2010

Aufgabe 1. *(4 Punkte)*
Der folgende Text wurde mit einem Caesar-Coder verschlüsselt:

MRNBA CNGC RBC WRLQC VNQA PNQNRV.

Bestimmen Sie die Verschiebeziffer und entschlüsseln Sie den Text.

Aufgabe 2. *(4 Punkte)*
Erzeugen Sie zwei 8-Bit-Primzahlen p und q so, dass $n = pq$ eine 16-Bit-Zahl ist und der öffentliche Schlüssel $e = 5$ bei RSA-Verfahren verwendet werden kann. Berechnen Sie den privaten Schlüssel, der zum öffentlichen Schlüssel $e = 5$ gehört und verschlüsseln Sie die in der Binärdarstellung $N = (110100110110111)_2$ gegebene natürliche Zahl mit dem öffentlichen Schlüssel $e = 5$.

Aufgabe 3. *(4 Punkte)*
Ein Netzwerk bestehe aus drei Teilnehmern, die zum Verschlüsseln ihrer Kommunikation das RSA-Verfahren benutzen. Die öffentlichen Schlüssel der Teilnehmer seien $(n_1, 3), (n_2, 3), (n_3, 3)$ mit $n_1 = 205, n_2 = 319, n_3 = 391$. Ein Klartext N wird jeweils mit dem öffentlichen Schlüssel der drei Teilnehmer zu den Geheimtexten C_1, C_2, C_3 verschlüsselt. Einem Angreifer A fallen die Geheimtexte

$$C_1 = 102 + 205\mathbb{Z},\ C_2 = 193 + 319\mathbb{Z},\ C_3 = 121 + 391\mathbb{Z}$$

in die Hände. Kann A hieraus die ursprüngliche Nachricht N bestimmen?
Tipp: Chinesischer Restsatz.

Aufgabe 4. *(4 Punkte)*
Es gelten die Bezeichnungen wie beim RSA-Verfahren. Zeigen Sie: Sind n und $\varphi(n)$ bekannt, dann können die Primteiler p und q von n ermittelt werden: p und q sind die Nullstellen des Polynoms

$$P(X) = X^2 - (n - \varphi(n) + 1)X + n.$$

Tipp: Vieta'scher Wurzelsatz.

Homepage zur Vorlesung: `www.mathi.uni-heidelberg.de/~ariedel/zahlen`
Abgabe bis spätestens 5. Juli 2010, in der Vorlesung.