14. Aufgabenblatt

KRYPTOGRAPHIE (für GHRG) (SS 2011)

Bearbeitung zum 14.7.2011, keine Abgabe mehr!

Internet: http://math-www.uni-paderborn.de/~chris

39. Aufgabe: a) Bei einem RSA–Verfahren ist $(1147, 29)$ der öffentliche Schlüssel eines Teilnehmers A. Ein an ihn gesendeter Geheimtext lautet

222

Versuche, den Geheimtext zu entschlüsseln.

b) Diegleiche Aufgabe wie in a), wobei A den öffentlichen Schlüssel

$$(345678910111213141683814774943373125204 11, 56789101112147)$$

hat und der Geheimtext

3126164303657176958375974575680342921 7563

lautet.

40. Aufgabe: Zwei Teilnehmer A und B an einem RSA–Verschlüsselungsverfahren haben die folgenden Schlüssel;

Teilnehmer	öffentlicher Schlüssel	geheimer Schlüssel
A	$(1517, 7)$	$(1517, 823)$
B	$(2021, 55)$	$(2021, 1651)$

A schickt an B ein Schlüsselwort w für eine Vigenère–Chiffre in verschlüsselter und signierter Form, d.h. A verschlüsselt zuerst w mit dem öffentlichen Schlüssel von B und dann mit seinem geheimen Schlüssel. Das Ergebnis ist

1047 68

Finde dieses Wort heraus (jeder Block muss einzeln behandelt werden) und entschlüssele damit den folgenden Geheimtext:

H V H W M F W H M R O I X M W I E H I K E O H M R Q H V

O E B X S T U E T U L I A N V J Y R U I M A J P Y R F O

Hinweis: Folgende Ergebnisse dürfen ohne Beweis benutzt werden:

$1047^3 \bmod 1517 = 480$, $68^3 \bmod 1517 = 413$

$1225^{825} \bmod 2021 = 1417$, $1227^{825} \bmod 2021 = 1595$, $1338^{825} \bmod 2021 = 414$

$11^{1650} \bmod 2021 = 1048$, $13^{1650} \bmod 2021 = 815$, $17^{1650} \bmod 2021 = 1870$