Einführung in die Zahlentheorie
Blatt 12

hhu Düsseldorf
WiSe 2021/22

Abgabe: bis Montag 17.1.2022

Vorlesungswebseite: `http://reh.math.uni-duesseldorf.de/~khalupczok/EZ/`
Die folgenden Aufgaben sind schriftlich zu bearbeiten und abzugeben. Wie üblich sind dabei alle Behauptungen zu beweisen. Resultate aus der Vorlesung dürfen verwendet werden, die zugehörigen Referenznummern können Sie zur Klarstellung dann mit angeben.

Aufgabe 1 (7 Punkte):

Eine zusammengesetzte Zahl $n \in \mathbb{N}_{>2}$ heißt Carmichaelzahl, wenn sie für alle $a \in \mathbb{Z}$ mit $(a, n) = 1$ die Kongruenz $a^{n-1} \equiv 1\ (n)$ erfüllt.

(1) Zeigen Sie, dass eine zusammengesetzte Zahl $n \in \mathbb{N}_{>2}$ genau dann eine Carmichaelzahl ist, wenn n ungerade, quadratfrei ist und außerdem $(p-1) \mid (n-1)$ für alle $p \in \mathbb{P}$ mit $p \mid n$ erfüllt. (Arbeiten Sie mit Primitivwurzeln und dem chinesischen Restsatz.)

(2) Zeigen Sie, dass 561 eine Carmichaelzahl ist.

(3) Zeigen Sie, dass jede Carmichaelzahl mindestens drei Primfaktoren besitzt.

Aufgabe 2 (13 Punkte):

Seien $K := \{n \in \mathbb{N}_0; n < 31\}$ und $V := \{n \in \mathbb{N}_0; n < 32\}$. Gemäß der folgenden Tabelle soll den Zahlen aus V bijektiv ein Alphabet zugeordnet werden.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P

16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Q	R	S	T	U	V	W	X	Y	Z	Ä	Ö	Ü	ß	␣	.

Klartexte werden zu Dreierblöcken und zugehörigen Zahlentripeln aus je drei Zahlen in K zusammengefasst, also z. B. "KLARTEXT␣"= 10,11,0/17,19,4/23,19,30. Jedem Tripel k_1, k_2, k_3 wird die Zahl $k = k_1 \cdot 31^2 + k_2 \cdot 31 + k_3$ zugeordnet, die beim RSA-Verfahren gemäß $v(k) = k^t\ (N)$ verschlüsselt wird. Die Zahl $v(k)$ wird durch $v(k) = v_1 \cdot 32^2 + v_2 \cdot 32 + v_3$ mit einen Geheimtextblock aus drei Zeichen $v_1, v_2, v_3 \in V$ beschrieben. Seien $N := 32399$ und $t := 1463$.

(1) Verschlüsseln Sie den Klartext "SEI␣EPSILON␣" wie beschrieben.

(2) Geben Sie die Primfaktorzerlegung von N an und finden Sie ein $s \in \mathbb{N}$ mit $st \equiv 1\ (\varphi(N))$.

(3) Entschlüsseln Sie den verschlüsselten Text "GF.SPCAAXÖOM"

(4) Warum ist das angegebene N – abgesehen davon, dass N sehr klein gewählt ist – eine besonders schlechte Wahl für N? Welche N sind generell eher ungeeignet?

Zur schnellen Potenzierung mod N können Sie einen PC zur Hilfe nehmen, z. B. "bc" im Terminal unter Linux.