Logik und diskrete Strukturen
Wintersemester 2022/2023

Abgabe: 23.01.23, 10:00
Besprechung: KW5

UNIVERSITÄT BONN

PD Dr. Elmar Langetepe
Christine Dahn
Joshua Könen
Institut für Informatik

Übungszettel 12

Aufgabe 12.1: Chinesischer Restsatz

(4+4 Punkte)

a) Bestimmen Sie mit Hilfe des chinesischen Restsatzes eine Zahl $x \in \mathbb{Z}$ mit $x \equiv 4 \mod 14$ und $x \equiv 3 \mod 9$. Geben Sie dazu ihre Zwischenschritte und das finale Ergebnis an.

b) Ein Kartenspiel, bestehend aus 56 unterschiedlichen Karten, wird in 7 Zeilen mit je 8 Spalten offen ausgelegt (siehe Abbildung 1a). Nun wird ein Zuschauer gebeten, sich eine der Karten zu merken und zu verraten, in welcher Spalte seine Karte liegt. Anschließend werden die Karten wieder eingesammelt, sodass sie sich wieder in derselben Reihenfolge befinden wie vor dem Auslegen. Nun wird das Kartenspiel in 8 Zeilen mit je 7 Spalten ausgelegt (siehe Abbildung 1b) und der Zuschauer soll wieder angeben, in welcher Spalte sich seine Karte befindet.

   Rekonstruieren Sie aus diesen beiden Informationen, welche Karte sich der Zuschauer gemerkt hat.

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56

(a) 7 Zeilen mit je 8 Spalten

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	32	33	34	35
36	37	38	39	40	41	42
43	44	45	46	47	48	49
50	51	52	53	54	55	56

(b) 8 Zeilen mit je 7 Spalten

Abbildung 1: Anordnung der ausgelegten Karten

Aufgabe 12.2: RSA Verschlüsselung

(8 Punkte)

Verschlüsseln Sie den Begriff *REST* mittels RSA mit den Parametern $p = 3$ und $q = 7$. Verwenden Sie dabei die Zeichenkodierung aus dem Beispiel am Ende von Abschnitt 4.3.5 des Vorlesungsskriptes und geben Sie alle durchgeführten Rechenschritte sowie das öffentliche und das private Schlüsselpaar an.