Vorlesung „Kryptographie für Lehramt“ (Wintersemester 2024/2025)

Aufgaben zur Klausurvorbereitung (5 ECTS)

Anmerkungen:

(1) Als Hilfsmittel ist nur ein Taschenrechner erlaubt.
(2) Zur Lösung einer Aufgabe gehören auch Darstellung des Lösungswegs und Begründungen.
(3) Großbuchstaben werden in der Klausur in folgender Weise mit Zahlen identifiziert:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	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

Aufgabe A1: Das Schlüsselwort „ERLANGEN“ liefert eine MASC-Verschlüsselungsabbildung f.

(1) Beschreibe f durch eine Tabelle.
(2) Gib ein längeres und ein kürzeres Schlüsselwort an, das die gleiche Abbildung f liefert.
(3) Ein Wort wurde mit dem angegebenen Schlüsselwort zu `BJQXNVWSQQN` MASC-verschlüsselt. Bestimme es.

Aufgabe A2: Die ALBC-2-Verschlüsselung mit dem Schlüssel $(1, 0, 4, 0, 1, 7)$ kann auch als VIGENERE-Verschlüsselung gedeutet werden. Welches VIGENERE-Schlüsselwort beschreibt diese Verschlüsselung?

Aufgabe A3: Der folgenden PLAYFAIR-Verschlüsselung liege das Schlüsselwort „ERLANGEN“ zugrunde.

(1) Stelle die zugehörige PLAYFAIR-Matrix auf.
(2) Erläutere die PLAYFAIR-Verschlüsselung an Hand der Verschlüsselung von „HENKELTASSE“.
(3) Entschlüssle den Chiffretext „RQ AU RL UK LZ ER“, der mit obigem Schlüsselwort PLAYFAIR-verschlüsselt wurde.

Aufgabe A4: Peter schickt an Michael folgende VIGENERE-verschlüsselte Nachricht:

```
HMPUAV XBYLLXH, MNA SMWE IMC XERPG JIFXJ JPKJWPAWTATNEE DWYQXJ. OLGJWE
WQ QTK RMPEHITVDX PBJ TLTN VLMOGSEWIRX CIMXJ, AZKWYQ BYL LVDXPG
OSWEPI? GBAPP ZNYPLOI AXPIC
```

(1) Bestimme das zugehörige VIGENERE-Schlüsselwort.
(2) Entschlüssle das achte Wort (`JPKJWPAWTATNEE`) der Nachricht.

Aufgabe A5: Der folgende Chiffretext `EDWSQEZXAUNNWXVVZB` ist STROM-verschlüsselt, wobei als Schlüsselstrom die Folge der Primzahlen benutzt wurde. Entschlüssle den Text.

Aufgabe A6: Ein Text wurde mit dem Schlüsselwort `ERLANGEN` TRANSSPA-verschlüsselt zu

Datei: ki_klausur_0_5ects.tex. Version vom 3.12.2024

`SEGNVESHLNIHURRSLECLOUGTESAM`

Entschlüssle den Text.

Aufgabe A7: Die Zahlen $m = 6015093799$ und $n = 10872069857$ haben die Primfaktorzerlegungen

$$m = 11^5 \cdot 13^3 \cdot 17 \quad \text{und} \quad n = 11^6 \cdot 17 \cdot 19^2.$$

Bestimme die Primfaktorzerlegungen von

$$\mathrm{ggT}(m, n), \quad \mathrm{kgV}(m, n) \quad \text{und} \quad m + n.$$

Aufgabe A8: Seien $a, b \in \mathbb{Z}$. Zeige: Genau dann ist $10a + b$ durch 19 teilbar, wenn $a + 2b$ durch 19 teilbar ist.

Aufgabe A9: Wende den erweiterten euklidischen Algorithmus auf 245 und 126 an und bestimme damit $\mathrm{ggT}(245, 126)$ und $x, y \in \mathbb{Z}$ mit $245x + 126y = \mathrm{ggT}(245, 126)$.

Aufgabe A10: Bestimme ein Inverses von a modulo n, das zwischen 0 und $n - 1$ liegt, falls ein solches existiert.

(1) $(a, n) = (10, 403)$,
(2) $(a, n) = (109, 4033)$.

Aufgabe A11:

(1) Bestimme die kleinste natürliche Zahl, die das folgende Kongruenzgleichungssystem löst:

$$x \equiv 2 \bmod 25, \quad x \equiv 5 \bmod 52.$$

(2) Warum besitzt das folgende Kongruenzgleichungssystem keine Lösung?

$$x \equiv 4 \bmod 45, \quad x \equiv 5 \bmod 54.$$

Aufgabe A12: Erläutere die square-and-multiply-Methode an der Berechnung von

$$3^{97} \bmod 100.$$

Aufgabe A13:

(1) Wie kann man $\varphi(n)$ berechnen, wenn man die Primfaktorzerlegung von n kennt?
(2) Berechne $\varphi(100)$.
(3) Was besagt der Satz von Euler über die Eulersche φ-Funktion?
(4) Was sind die letzten beiden Dezimalstellen von 3^{123}?
(5) Was ist $7^{5001} \bmod 11$?

Aufgabe A14:

(1) Gib zwei Varianten des kleinen Satzes von Fermat an.
(2) Zeige: Ist p eine von 2 und 5 verschiedene Primzahl und n eine natürliche Zahl mit $p-1 \mid n$, so gilt $10^n \equiv 1 \bmod p$.
(3) Gib mindestens 6 verschiedene Primteiler der 60-stelligen Zahl

$$\underbrace{999\ldots999}_{60\,\text{Einsen}} = 10^{60} - 1.$$

Aufgabe A15:

(1) Was ist eine Carmichael-Zahl?
(2) Was besagt das Korselt-Kriterium?
(3) Zeige, dass 561 eine Carmichael-Zahl ist.
(4) Warum kann eine RSA-Zahl $N = pq$ keine Carmichael-Zahl sein? (Hinweis: $pq - 1 = p(q-1) + (p-1)$)

Aufgabe A16:

(1) Beschreibe den Miller-Rabin-Test (zur Basis 2). Welche Ergebnisse sind möglich?
(2) Teste $n = 21$ mit dem Miller-Rabin-Test (zur Basis 2).
(3) Zeige: Ist n eine natürliche Zahl $\equiv 1 \bmod 4$ und gilt $4^{\frac{n-1}{4}} \equiv -1 \bmod n$, so erfüllt n den Miller-Rabin-Test zur Basis 2.

Aufgabe A17:

(1) Ist 25 eine Fermat-Pseudoprimzahl zur Basis 7?
(2) Ist 25 eine Miller-Rabin-Pseudoprimzahl zur Basis 7?

Aufgabe A18: $(N, e) = (55, 27)$ ist ein öffentlicher RSA-Schlüssel.

(1) Bestimme einen zu $(55, 27)$ passenden privaten RSA-Schlüssel $(55, d)$.
(2) Ein aus vier Großbuchstaben bestehendes Wort wurde nach dem Schema der Vorbemerkungen in eine Zahlenfolge a_1, a_2, a_3, a_4 umgewandelt, dann mit dem Schlüssel $(55, 27)$ zur Zahlenfolge 33,9,8,24 RSA-verschlüsselt. Entschlüssle es.

Aufgabe A19: $N = 89425157$ ist eine RSA-Zahl.

(1) Faktorisiere N mit der Fermatschen Faktorisierungsmethode.
(2) Bestimme die kleinste natürliche Zahl $e > 1$, sodass (N, e) ein gültiger (öffentlicher) RSA-Schlüssel ist.

Aufgabe A20: Von der RSA-Zahl $N = 848731787$ kennt man $\varphi(N) = 848673456$. Faktorisiere N.

Aufgabe A21: $N = 2699773523$ ist eine RSA-Zahl. Für $w = 20427359$ gilt $w^2 \equiv 1 \bmod N$.

(1) Bestimme alle $x \in \{0, 1, \ldots, N-1\}$ mit $x^2 \equiv 1 \bmod N$.
(2) Faktorisiere N.

Aufgabe A22: Für $N \in \mathbb{N}$ sei $Q_N = \{a \in \mathbb{Z} : 0 \leq a \leq N-1, a^2 \equiv 1 \bmod N\}$ die Menge der Quadratwurzeln von 1 modulo N. $N = 11592649$ hat die Primfaktorzerlegung $N = pq$ mit $p = 2713$ und $q = 4273$. Bestimme Q_N.

Aufgabe A23: Bestimme die Kettenbruchentwicklung von $\frac{1234}{4321}$ und die zugehörigen Näherungsbrüche.

Aufgabe A24: $(N, e) = (57174151, 3291863)$ ist ein öffentlicher RSA-Schlüssel. Der private Exponent d kommt im 5. Näherungsbruch von $\frac{e}{N}$ vor.
(1) Bestimme den 0., 1., 2., 3., 4., und 5. Näherungsbruch von $\frac{e}{N}$.
(2) Bestimme den privaten Exponenten d.
(3) Bestimme $\varphi(N)$.