Institut für Informatik
Prof. Dr. J. Rothe

Sommersemester 2024
Übungsblatt 1

Lösungsvorschläge

Kryptokomplexität II

Bearbeitungszeit: 9. April bis 26. April
Verantwortlich: Roman Zorn

Aufgabe 1: Wiederholung: Chinesischer Restsatz

▶ Lösen Sie das folgende Kongruenzsystem für x, $0 \leq x \leq 27$,

$$\begin{aligned} x &\equiv 3 \mod 4, \\ x &\equiv 1 \mod 7. \end{aligned}$$

Lösungsvorschlag: Mit dem Chinesischen Restsatz lässt sich das Kongruenzsystem

$$\begin{aligned} x &\equiv 3 \mod 4, \\ x &\equiv 1 \mod 7, \end{aligned}$$

wie folgt lösen. Es gilt $M = 4 \cdot 7 = 28$, $q_1 = M/m_1 = 7$, und $q_2 = M/m_2 = 4$. Wir berechnen mit dem erweiterten Euklidischen Algorithmus die Inversen von q_1 und q_2 modulo 4 bzw. 7 ($xm + yn = 1$)

m	n	$\lfloor \frac{m}{n} \rfloor$	$m \bmod n$	x	y
7	4	1	3	-1	2
4	3	1	1	1	-1
3	1	3	0	0	1
1	0			1	0

und erhalten

$$q_1^{-1} \equiv 7^{-1} \equiv -1 \equiv 3 \mod 4 \quad \text{und} \quad q_2^{-1} \equiv 4^{-1} \equiv 2 \mod 7.$$

Daraus ergibt sich die gesuchte Lösung modulo 28 als

$$x \equiv 3 \cdot 7 \cdot (-1) + 1 \cdot 4 \cdot 2 \equiv -13 \equiv 15 \mod 28.$$

Aufgabe 2: Wiederholung: RSA

(a) Gegeben sei der RSA-Modul $n = 91$.
► Sind $e_1 = 1, e_2 = 3$, und $e_3 = 13$ jeweils gültige öffentliche Exponenten? Begründen Sie Ihre Antwort.

(b) ► Berechnen Sie für jeden gültigen Exponenten aus Aufgabenteil (a) den zugehörigen privaten Exponenten d. Verwenden Sie den erweiterten Euklidischen Algorithmus.

(c) ► Berechnen Sie mit Hilfe von Fermats kleinem Satz

$$127^{247} \mod 83.$$

(d) ► Wie viele gültige öffentliche Exponenten gibt es für den RSA-Modul $n = 4141$?

Lösungsvorschlag:

(a) Für $n = 91 = 7 \cdot 13$ gilt $\varphi(91) = \varphi(7) \cdot \varphi(13) = 6 \cdot 12 = 72$. Dann gilt für die Kandidaten:

(i) $e_1 = 1$ ist kein gültiger Exponent da $e_1 > 1$ gelten muss.

(ii) $e_2 = 3$ ist kein gültiger Exponent da $\mathrm{ggT}(e_2, \varphi(n)) = 1$ gelten muss. Mit $\varphi(n) = 2^3 \cdot 3^2$ gilt aber $\mathrm{ggT}(3, 72) = 3$.

(iii) $e_3 = 13$ ist ein gültiger Exponent, da sowohl $1 < 13 < 72$ als auch $\mathrm{ggT}(13, 72) = 1$ erfüllt sind.

(b) Der einzige gültige Exponent aus Aufgabenteil a) ist $e_3 = 13$. Berechne für diesen den privaten Exponenten $d = e^{-1} \mod \varphi(n)$:

m	n	$\lfloor \frac{m}{n} \rfloor$	$m \mod n$	x	y
72	13	5	7	2	−11
13	7	1	6	−1	2
7	6	1	1	1	−1
6	1	0	0	0	1
1	0			1	0

Mit $-11 \equiv 61 \mod 72$ folgt, dass der private Exponent $1 < d = 61 < 72$ ist.

(c) Wir berechnen $127^{247} \mod 83$. Da $\mathrm{ggT}(127, 83) = 1$ gilt, folgt mit Fermats kleinem Satz

$$127^{83-1} \equiv 1 \mod 83.$$

Folglich können wir schreiben

$$127^{247} \equiv 127^{3 \cdot 82+1} \equiv 127^{3 \cdot 82} \cdot 127 \equiv 1 \cdot 127 \equiv 44 \mod 83.$$

(d) Ein öffentlicher Exponent e muss $1 < e < \varphi(n)$ und $\text{ggT}\,(e, \varphi(n)) = 1$ erfüllen. Es gilt $n = 4141 = 41 \cdot 101$. Damit lässt sich berechnen, dass

$$\varphi(4141) = 40 \cdot 100 = 2^5 \cdot 5^3 = 4000$$

gilt. Wir berechnen die Anzahl der Zahlen die kleiner als 4000 und zusätzlich teilerfremd zu 4000 sind. Es gilt

$$\begin{aligned}\varphi(4000) = \varphi(2^5 \cdot 5^3) = \varphi(2^5) \cdot \varphi(5^3) = (2^5 - 2^4) \cdot (5^3 - 5^2) \\ = 2^4 \cdot (4 \cdot 5^2) = 16 \cdot 4 \cdot 25 = 1600.\end{aligned}$$

Mit $\varphi(\varphi(4141)) = 1600$ wissen wir, dass es 1600 zu 4000 teilerfremde Zahlen gibt, die kleiner als 4000 sind. Das bezieht die Zahl 1 mit ein, die nicht erlaubt ist. Folglich gibt es ingesamt $1600 - 1 = 1599$ gültige öffentliche Exponenen für den RSA-Modul $n = 4141$.

Aufgabe 3: Wiederholung: Zahlentheoretische Grundlagen

► Beweisen Sie, dass es unendlich viele Primzahlen gibt.

Lösungsvorschlag: Wir beweisen die Aussage per Widerspruch. Angenommen es gibt nur die Primzahlen $p_1, \ldots, p_n$ für ein festes $n \in \mathbb{N}$. Dann definieren wir

$$p = \left(\prod_{i=1}^{n} p_i\right) + 1$$

und betrachten zwei Fälle.

(i) p ist eine Primzahl.
Da $p \neq p_j$ für alle $1 \leq j \leq n$ gilt, ist dies ein Widerspruch zur Annahme, dass $p_1, \ldots, p_n$ die einzigen Primzahlen sind. Dieser Fall kann also nicht eintreten.

(ii) p ist keine Primzahl.
Da $p \neq p_j$ gilt und jedes p_j den Wert $p - 1$ teilt für $1 \leq j \leq n$, folgt

$$p \equiv 1 \mod p_j,$$

also $p_j \nmid p$. Da p keine Primzahl ist, muss eine Primzahl q mit $q \neq p_j$ für $1 \leq j \leq n$ existieren, die p teilt. Das ist ein Widerspruch zu unserer Annahme, dass $p_1, \ldots, p_n$ die einzigen Primzahlen sind.

Da beide Fälle im Widerspruch enden, ergibt sich daraus, dass unsere Annahme falsch ist und folglich die Anzahl der Primzahlen unendlich ist.