Institut für Informatik
Prof. Dr. J. Rothe

Wintersemester 2023/24
Übungsblatt 8

Lösungsvorschläge

Kryptokomplexität 1

Bearbeitungszeit: 28. November bis 6-8. Dezember
Verantwortlich: Roman Zorn

Aufgabe 1 : Fermat- und Miller-Rabin-Lügner
Sei $n \in \mathbb{N}$ eine ungerade, zusammengesetzte Zahl. Zeigen Sie, dass für jeden Fermat-Lügner $a \in \mathbb{Z}_n$ für n auch $n - a$ ein Fermat-Lügner für n ist. Gilt diese Aussage auch für Miller-Rabin-Lügner?
Hinweis: Benutzen Sie den binomischen Lehrsatz für den ersten Teil der Aufgabe.

Lösungsvorschlag:
Fermat:
Sei $n \in \mathbb{N}$ eine ungerade, zusammengesetzte Zahl. Sei a ein Fermat-Lügner für n. Also gilt $a^{n-1} \equiv 1 \mod n$. Es gilt

$$(n-a)^{n-1} \equiv \sum_{k=0}^{n-1} \binom{n-1}{k} n^k \cdot (-a)^{n-1-k} \equiv (-a)^{n-1} + \underbrace{\sum_{k=1}^{n-1} \binom{n-1}{k} n^k \cdot (-a)^{n-1-k}}_{\equiv 0 \mod n}$$

$$\equiv (-a)^{n-1} \equiv (-1)^{n-1} \cdot a^{n-1} \equiv (-1)^{n-1} \cdot 1 \equiv 1 \mod n,$$

da $n-1$ gerade und somit $(-1)^{n-1} = 1$ ist. Also ist $n-a$ auch ein Fermat-Lügner für n.

Miller-Rabin:
Für Miller-Rabin-Lügner gilt die Aussage auch.
Beweis: Sei $n \in \mathbb{N}$ eine ungerade, zusammengesetzte Zahl, d. h., $n - 1 = 2^k \cdot m$ mit m ungerade und $k > 0$. Sei a ein MR-Lügner von n, d. h., es gibt drei Fälle:

Fall 1: $a^m \equiv 1 \mod n$. Es gilt

$$(n-a)^m \equiv (-a)^m \mod n \equiv -1 \mod n,$$

da m ungerade ist. Dann ist $n - a$ im ersten Schritt wegen $(n-a)^{m \cdot 2^0} \equiv -1 \mod n$ ein MR-Lügner für n. Dieser Schritt wird ausgeführt, da $k > 0$ ist.

Fall 2: $a^{m \cdot 2^0} \equiv -1 \mod n$. Hier gilt

$$(n-a)^m \equiv (-a)^m \equiv (-1) \cdot (a^m) \equiv (-1) \cdot (-1) \equiv 1 \mod n.$$

Also ist $(n-a)$ ein MR-Lügner von n.

Fall 3: $a^{m\cdot 2^i} \equiv -1 \mod n$ für ein i mit $0 < i < k$.

$$(n-a)^{m\cdot 2^i} \equiv (-a)^{m\cdot 2^i} \equiv a^{m\cdot 2^i} \equiv -1 \mod n.$$

Also ist auch hier $n-a$ ein MR-Lügner für n.

Aufgabe 2 : Faktorisierungsangriffe auf RSA

(a) Sei $x^2 + a_1 x + a_0 = 0$ eine quadratische Gleichung mit den Koeffizienten a_0 und a_1, und den Lösungen p und q.

► Zeigen Sie, dass

$$p + q = -a_1 \qquad \text{und}$$
$$p \cdot q = a_0$$

Lösungsvorschlag: ► Da p und q die Lösungen von $x^2+a_1x+a_0 = 0$ sind, gilt $x^2+a_1x+a_0 = (x-p)\cdot(x-q) = x^2-(p+q)\cdot x+p\cdot q$. Per Koeffizientenvergleich gilt dann $a_1 = -(p+q)$ und $a_0 = p\cdot q$.

(b) Gegeben seien jeweils ein RSA-Modul $n \in \mathbb{N}$ und die zugehörige Zahl $\varphi(n)$, wobei φ die Euler-Funktion ist. Faktorisieren Sie jeweils n.

(i) $n = 72487$, $\varphi(n) = 71896$,

(ii) $n = 81061$, $\varphi(n) = 80172$.

Lösungsvorschlag: ► Laut Vorlesung müssen die folgenden Gleichungen gelöst werden:

$$p = \frac{n-\varphi(n)+1}{2} - \sqrt{\left(\frac{n-\varphi(n)+1}{2}\right)^2 - n}$$

und

$$q = \frac{n-\varphi(n)+1}{2} + \sqrt{\left(\frac{n-\varphi(n)+1}{2}\right)^2 - n}.$$

Für die gegebenen Zahlen bedeutet das:

(i) $n = 72487$, $\varphi(n) = 71896$:

$$\begin{aligned} p &= \frac{71896 - 71896 + 1}{2} - \sqrt{\left(\frac{71896 - 71896 + 1}{2}\right)^2 - 71896} \\ &= 296 - \sqrt{15129} = 196 - 123 = 173, \\ q &= 296 + 123 = 419. \end{aligned}$$

(ii) $n = 81061$, $\varphi(n) = 80172$:

$$\begin{aligned} p &= \frac{81061 - 80172 + 1}{2} - \sqrt{\left(\frac{81061 - 80172 + 1}{2}\right)^2 - 81061} \\ &= 445 - \sqrt{116964} = 445 - 342 = 103, \\ q &= 445 - 342 = 787. \end{aligned}$$

Aufgabe 3 : Wieners Angriff auf RSA
Sei $(n, e) = (50413813, 30239297)$ der öffentliche Schlüssel.
► Führen Sie Wieners Angriff auf RSA durch, um n zu faktorisieren. Berechnen Sie zunächst die Kettenbruch Erweiterung von $\frac{e}{n}$ und geben Sie dann $\mathbf{C}_i$ und, falls möglich, das berechnete $\varphi(n)$ für jeden durchgeführten Test an.
Hinweis: Wie in der Vorlesung muss nur so lange gerechnet werden, bis ein Test erfolgreich ist.

Lösungsvorschlag: Die Kettenbruch Erweiterung ist

$$(0, 1, 1, 2, 223, 1, 8, 6, 1, 5, 10, 1, 2, 1, 2).$$

Die folgenden Test werden dann ausgeführt.

i	0	1	2	3	4
r_i	30239297	50413813	30239297	20174516	10064781
c_i		0	1	1	2
$\mathbf{C}_i$	$\frac{1}{0}$	$\frac{0}{1}$	$\frac{1}{1}$	$\frac{1}{2}$	$\frac{3}{5}$
$\varphi(n)$ Kandidaten			30239296	60478593	50398828

Der Test für $\phi(n) = 50398828$ ergibt die Primfaktoren $q = 5099, p = 9887$. Die vorherigen Tests ergeben entweder kein $\varphi(n)$ oder keine ganzzahligen Primfaktoren und schlagen somit fehl.