Institut für Informatik
Prof. Dr. J. Rothe

Sommersemester 2024
Übungsblatt 3

Lösungsvorschläge

Kryptokomplexität II

Bearbeitungszeit: 23. April bis 3. Mai
Verantwortlich: Roman Zorn

Aufgabe 1 (10 Punkte): 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 $p + q = -a_1$ und $p \cdot q = a_0$ gilt.

(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:

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

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

$$\begin{aligned} p &= \frac{72487 - 71896 + 1}{2} - \sqrt{\left(\frac{72487 - 71896 + 1}{2}\right)^2 - 72487} \\ &= 296 - \sqrt{15129} = 196 - 123 = 173, \\ q &= 296 + 123 = 419. \end{aligned}$$

(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 2 (10 Punkte): Fälschung von RSA-Signaturen
Erich fängt die folgenden RSA-signierten Nachrichten $(m_i, \mathrm{sig}_A(m_i))$ von Alice ab:

$$\langle 576, 102\rangle, \langle 215, 1595\rangle, \langle 338, 764\rangle, \langle 59, 1130\rangle, \langle 512, 339\rangle, \langle 26, 988\rangle, \langle 532, 1392\rangle.$$

Der öffentliche Schlüssel ist $(n, e) = (1961, 7)$.

(a) ▶ Führen Sie den *Chosen-Plaintext*-Angriff aus der Vorlesung für alle $r \in \{1, 2, 3\}$ durch und wählen Sie $e_i = 1$ für alle i.

(b) Nehmen Sie an, alle Nachrichten seien mit Blocklänge 2 über dem kanonischen Alphabet $\Sigma = \{A, B, \ldots, Z\}$ kodiert.
▶ Ergeben die Nachrichten von Alice und/oder die gefälschte Nachricht von Erich aus Aufgabenteil (a) Sinn?

Lösungsvorschlag:

(a) Benutze die Formeln aus der Vorlesung:

$$m = r^e \prod_{i=1}^{k} m_i^{e_i} \mod n \quad \text{und}$$

$$\mathrm{sig}_A(m) = r \prod_{i=1}^{k} (\mathrm{sig}_A(m_i))^{e_i} \mod n.$$

$r = 1$**:** Wir berechnen $m_1 = 1^7 \cdot 576 \cdot 215 \cdot 338 \cdot 59 \cdot 512 \cdot 26 \cdot 532 \equiv 1333 \mod 1961$
und $\mathrm{sig}_A(m_1) = 1 \cdot 102 \cdot 1595 \cdot 764 \cdot 1130 \cdot 339 \cdot 988 \cdot 1392 \equiv 889 \mod 1961$

$r = 2$**:** Wir berechnen $m_2 = 2^7 \cdot 576 \cdot 215 \cdot 338 \cdot 59 \cdot 512 \cdot 26 \cdot 532 \equiv 17 \mod 1961$
und $\mathrm{sig}_A(m_2) = 2 \cdot 102 \cdot 1595 \cdot 764 \cdot 1130 \cdot 339 \cdot 988 \cdot 1392 \equiv 1778 \mod 1961$

$r = 3$**:** Wir berechnen $m_2 = 3^7 \cdot 576 \cdot 215 \cdot 338 \cdot 59 \cdot 512 \cdot 26 \cdot 532 \equiv 1225 \mod 1961$
und $\text{sig}_A(m_3) = 3 \cdot 102 \cdot 1595 \cdot 764 \cdot 1130 \cdot 339 \cdot 988 \cdot 1392 \equiv 706 \mod 1961$

(b) Die Nachrichten von Alice ergeben dekodiert: 22, 4, 8, 7, 13, 0, 2, 7, 19, 18, 1, 0, 20, 12, was dem deutschen Wort "Weihnachtsbaum" entspricht. Die Nachricht von Erich ergibt keinen Sinn, da 1333 und 1225 nicht über dem kanonischen Alphabet mit Blocklänge 2 dekodiert werden können.

Aufgabe 3 (10 Punkte): Primitive Elemente I

(a) ▶ Bestimmen Sie alle primitiven Elemente in $\mathbb{Z}_{19}^*$ und $\mathbb{Z}_{65}^*$.

(b) ▶ Bestimmen Sie das kleinste primitive Element in $\mathbb{Z}_{89}^*$.
▶ Wie viele primitive Elemente gibt es in $\mathbb{Z}_{89}^*$?

Lösungsvorschlag:

(a) (i) Wir bestimmen alle primitiven Elemente in $\mathbb{Z}_{19}^*$: Da 19 eine Primzahl ist, gilt laut Vorlesung, dass $\mathbb{Z}_{19}^*$ genau $\varphi(19-1) = \varphi(18) = \varphi(2) \cdot \varphi(3^2) = 6$ primitive Elemente hat. Die Zahl 2 generiert $\mathbb{Z}_{19}^*$ und ist damit gem. Vorlesung ein primitives Element in $\mathbb{Z}_{19}^*$.

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$2^i \mod 19$	1	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10

Die restlichen primitiven Elemente $2^i \mod 19$ erfüllen nun nach Vorlesung $\text{ggT}(18, i) = 1$. Überprüfen der obigen Tabelle ergibt damit die primitiven Elemente $\{2, 13, 14, 15, 3, 10\}$ in $\mathbb{Z}_{19}^*$.

(ii) Wir bestimmen alle primitiven Elemente in $\mathbb{Z}_{65}^*$: Nach Vorlesung besitzt die Gruppe $\mathbb{Z}_{65}^*$ nur dann primitiven Elemente, wenn $65 \in \{1, 2, 4\}$ gilt oder $65 = q^k$ bzw. $65 = 2q^k$ für eine Primzahl $q > 2$ erfüllt ist. Mit $65 = 5 \cdot 13$ erfüllt 65 keine der Bedingungen, so dass es keine primitiven Elemente in $\mathbb{Z}_{65}^*$ gibt.

(b) Da 89 eine Primzahl ist, existieren primitiven Elemente in $\mathbb{Z}_{89}^*$. Wir bestimmen zuerst die Anzahl der primitiven Elemente in $\mathbb{Z}_{89}^*$. Mit $\varphi(89-1) = \varphi(88) = \varphi(2^3) \cdot \varphi(11) = 40$ folgt, dass es 40 primitive Elemente in $\mathbb{Z}_{89}^*$ gibt.

Um nun das kleinste primitive Element in $\mathbb{Z}_{89}^*$ zu bestimmen, nutzen wir die Aussage aus der Vorlesung, dass ein Element $\gamma \in \mathbb{Z}_p^*$ für eine Primzahl p genau dann ein primitives Element in $\mathbb{Z}_p^*$ ist, wenn $\gamma^{(p-1)/q} \not\equiv 1 \mod p$ für alle Primzahlen q, die $p-1$ teilen, gilt. Alle Primzahlen, die $89 - 1 = 88$ teilen, sind 2 und 11. Wir betrachten das Element $2 \in \mathbb{Z}_{89}^*$. Es gilt

$$2^{88/2} = 2^{32+8+4} \equiv 45 \cdot 78 \cdot 16 \equiv 1 \mod 89,$$

und folglich kann 2 kein primitives Element in $\mathbb{Z}_{89}^*$ sein. Als nächstes betrachten

wir das Element $3 \in \mathbb{Z}_{89}^*$. Es gilt

$$3^{88/2} = 3^{32+8+4} \equiv 4 \cdot 64 \cdot 81 \equiv 88 \mod 89 \quad \text{und}$$
$$3^{88/11} = 3^8 \equiv 64 \mod 89,$$

so dass folgt, dass 3 das kleinste, primitive Element in $\mathbb{Z}_{89}^*$ ist.

Aufgabe 4 (10 Punkte): Primitive Elemente II
Sei p eine Primzahl mit $p \equiv 1 \mod 4$.
► Zeigen Sie:

Wenn γ ein primitives Element in $\mathbb{Z}_p^*$ ist,
dann ist auch $p - \gamma$ ein primitives Element in $\mathbb{Z}_p^*$.

Lösungsvorschlag: Sei $\gamma \in \mathbb{Z}_p^*$ ein primitives Element. Dann wissen wir mit der Aussage aus der Vorlesung, dass für alle Primzahlen q, die $p-1$ teilen, gilt $\gamma^{(p-1)/q} \not\equiv 1 \mod p$. Um zu beweisen, dass auch $p - \gamma$ ein primitives Element ist, genügt es die gleiche Eigenschaft nachzuweisen, also, dass für alle Primzahlen q, die $p - 1$ teilen, gilt $(p - \gamma)^{(p-1)/q} \not\equiv 1 \mod p$.
Mit $p \equiv 1 \mod 4$ folgt, dass $p-1$ ein Vielfaches von 4 ist, d.h. wir können $p-1 = 4k$ für passendes $k \in \mathbb{N}$ schreiben.
Sei nun q eine Primzahl die $p - 1$ teilt. Wenn q gerade ist, dann gilt $q = 2$ und es folgt, dass $(p - 1)/q = 2k$ gerade ist. Wenn q ungerade ist, so folgt ebenfalls, dass $(p - 1)/q = 2 \cdot 2k/q$ gerade ist. Folglich ist $(p - 1)/q$ für alle Primzahlen q, die $p - 1$ teilen, gerade. Mit dieser Erkenntnis ergibt sich für eine Primzahl q, die $p - 1$ teilt,

$$(p - \gamma)^{(p-1)/q} \equiv (-\gamma)^{(p-1)/q} = (-1)^{(p-1)/q}\gamma^{(p-1)/q} = \gamma^{(p-1)/q} \not\equiv 1 \mod p.$$

Dabei folgt die letzte Gleichheit aus der Tatsache, dass γ ein primitives Element in $\mathbb{Z}_p^*$ ist. Also erfüllt auch $p-\gamma$ die Voraussetzungen und ist somit ein primitives Element in $\mathbb{Z}_p^*$.