Institut für Informatik
Prof. Dr. J. Rothe

Sommersemester 2024
Übungsblatt 2

Lösungsvorschläge

Kryptokomplexität II

Bearbeitungszeit: 16. April bis 26. April
Verantwortlich: Roman Zorn

Aufgabe 1: Wiederholung RSA
Gegeben seien der RSA-Modul $n = 403$ und das Alphabet $\Sigma = \{\mathrm{D}, \mathrm{E}, \mathrm{G}, \mathrm{I}, \mathrm{N}, \mathrm{R}, \mathrm{U}\}$ kodiert über $\mathbb{Z}_7$:

0	1	2	3	4	5	6
D	E	G	I	N	R	U

Bob wählt als öffentlichen Exponenten $e = 149$, schickt den Schlüssel (n, e) an Alice und erhält von ihr folgende verschlüsselte Nachricht

DGIG DENN DUEG DGGR DEDG.

► Bestimmen Sie Bobs privaten Schlüssel d und entschlüsseln Sie die Nachricht. Verwenden Sie dabei Square-and-Multiply und geben Sie alle benötigten Zwischenschritte an.

Lösungsvorschlag: Es gilt $n = 403 = 31 \cdot 13$, also $\varphi(n) = 30 \cdot 12 = 360$. Der öffentliche Exponent $e = 149$ ist gültig, da $\mathrm{ggT}\,(e, \varphi(n)) = 1$ und $1 < e < \varphi(n)$ gilt. Wir berechnen nun $d \equiv 149^{-1} \mod 360$:

m	n	$\lfloor \frac{m}{n} \rfloor$	$m \mod n$	x	y
360	149	2	62	−12	29
149	62	2	25	5	−12
62	25	2	12	−2	5
25	12	2	1	1	−2
12	1	12	0	0	1
1	0			1	0

Damit ergibt sich Bobs privater Schlüssel als $d = 29 \mod 360$. Die Blocklänge zum Verschlüsseln ist $l = \lfloor \log_7(403) \rfloor = 3$. Also ist die verschlüsselte Nachricht in Blöcke der Länge $l + 1 = 4$ eingeteilt. In $\mathbb{Z}_{403}$ gilt:

Block 1: DGIG $\widehat{=}\ c_b = 0 \cdot 7^3 + 2 \cdot 7^2 + 3 \cdot 7^1 + 2 \cdot 7^0 = 121$,
$m_b = c_b^d = 121^{29} = 121^{16+8+4+1} = 10$
(mit *Square-and-Multiply*: 121, 133, 360, 237, 152)
$= 0 \cdot 7^2 + 1 \cdot 7^1 + 3 \cdot 7^0 \widehat{=}$ DEI

Block 2: DENN $\widehat{=}\ c_b = 0 \cdot 7^3 + 1 \cdot 7^2 + 4 \cdot 7^1 + 4 \cdot 7^0 = 81$,
$m_b = c_b^d = 81^{29} = 81^{16+8+4+1} = 204$
(mit *Square-and-Multiply*: 81, 113, 276, 9, 81)
$= 4 \cdot 7^2 + 1 \cdot 7^1 + 1 \cdot 7^0 \widehat{=}$ NEE

Block 3: DUEG $\widehat{=}\ c_b = 0 \cdot 7^3 + 6 \cdot 7^2 + 1 \cdot 7^1 + 2 \cdot 7^0 = 303$,
$m_b = c_b^d = 303^{29} = 303^{16+8+4+1} = 270$
(mit *Square-and-Multiply*: 303, 328, 386, 289, 100)
$= 5 \cdot 7^2 + 3 \cdot 7^1 + 4 \cdot 7^0 \widehat{=}$ RIN

Block 4: DGGR $\widehat{=}\ c_b = 0 \cdot 7^3 + 2 \cdot 7^2 + 2 \cdot 7^1 + 5 \cdot 7^0 = 117$,
$m_b = c_b^d = 117^{29} = 117^{16+8+4+1} = 208$
(mit *Square-and-Multiply*: 117, 390, 169, 351, 286)
$= 4 \cdot 7^2 + 1 \cdot 7^1 + 5 \cdot 7^0 \widehat{=}$ NER

Block 5: DEDG $\widehat{=}\ c_b = 0 \cdot 7^3 + 1 \cdot 7^2 + 0 \cdot 7^1 + 2 \cdot 7^0 = 51$,
$m_b = c_b^d = 51^{29} = 51^{16+8+4+1} = 324$
(mit *Square-and-Multiply*: 51, 183, 40, 391, 144)
$= 6 \cdot 7^2 + 4 \cdot 7^1 + 2 \cdot 7^0 \widehat{=}$ UNG

Die entschlüsselte Nachricht lautet also

DEINEERINNERUNG.

Aufgabe 2: Angriffe auf RSA

(a) Gegeben sei der RSA-Modul $n = 95$.
► Welche Auswirkungen hat die Wahl des öffentlichen Exponenten $e = 17$ auf das Kryptosystem?

(b) ► Welche Maßnahmen können ergriffen werden, um einen Angriff auf kleine Nachrichten (*Small-Message Attack*) zu verhindern?

(c) Gegeben seien der RSA-Modul $n = 14803 = 113 \cdot 131$ sowie der öffentliche Exponent $e = 9707$.
► Ist es möglich, Wieners Angriff auszuführen?

Lösungsvorschlag:

(a) Mit $n = 95 = 19 \cdot 5$ gilt $\varphi(n) = 18 \cdot 4 = 72 = 2^3 \cdot 3^2$. Bestimme mit dem erweiterten Euklidischen Algorithmus den privaten Exponenten d:

m	n	$\lfloor \frac{m}{n} \rfloor$	$m \bmod n$	x	y
72	17	4	4	-4	17
17	4	4	1	1	-4
4	1	4	0	0	1
1	0			1	0

Demnach gilt $d = e = 17$. Das Kryptosystem wird somit symmetrisch. Außerdem kann eine dritte Person den öffentlichen Schlüssel und die verschlüsselte Nachricht abfangen und mit $m \equiv c^e \mod n$ den Klartext herausfinden.

(b) Um eine Small-Message Attack zu verhindern, sollte der öffentliche Exponent möglichst groß sein. Besser ist, wenn die zu verschlüsselnde Nachricht immer sehr groß ist, denn in der Regel präferiert man einen kleinen öffentlichen Exponent, um ein effizientes Verschlüsseln zu ermöglichen sowie Wieners Angriff zu verhindern.

(c) Laut Vorlesung funktioniert Wieners Angriff genau dann, wenn

(i) $3d < \sqrt[4]{n}$ und

(ii) $q < p < 2q$

erfüllt sind. Mit $n = 14803 = 113 \cdot 131$ folgt $\varphi(n) = 14560 = 2^5 \cdot 5 \cdot 7 \cdot 13$. Der öffentliche Exponent $e = 9707$ ist gültig, da sowohl $1 < 9707 < 14560$ als auch $\text{ggT}(9707, 14560) = 1$ gelten. Der private Exponent kann beispielsweise über den erweiterten Euklidischen Algorithmus ermittelt werden. Es folgt $d = 3$, da $e \cdot d = 9707 \cdot 3 \equiv 1 \mod 14560$ gilt. Eingesetzt in die obigen Bedingungen

erhalten wir $3 \cdot 3 = 9 < \sqrt[4]{14803}$ sowie $113 < 131 < 226$. Damit sind (i) und (ii) erfüllt und Wieners Angriff ist möglich.

Aufgabe 3: *Low-Exponent*-Angriff auf RSA
Drei Parteien verwenden das RSA-Kryptosystem, um dieselbe Nachricht m zu verschlüsseln. Sie fangen die dabei verschickten öffentlichen Schlüssel $(n_1, e) = (85, 3)$, $(n_2, e) = (87, 3)$ und $(n_3, e) = (253, 3)$ sowie die entsprechenden verschlüsselten Texte $c_1 = 56$, $c_2 = 26$ und $c_3 = 66$ ab.
► Verwenden Sie einen *Low-Exponent*-Angriff, um die Originalnachricht m zu ermitteln.

Lösungsvorschlag: Löse das folgende Kongruenzsystem

$$\begin{aligned} m^3 &\equiv 56 \mod 85, \\ m^3 &\equiv 26 \mod 87, \\ m^3 &\equiv 66 \mod 253, \end{aligned}$$

mit dem chinesischen Restesatz. Dazu berechnen wir

$$\begin{aligned} M &= 85 \cdot 87 \cdot 253 = 1870935, \\ q_1 &= 87 \cdot 253 = 22011, \\ q_2 &= 85 \cdot 253 = 21505, \\ q_3 &= 85 \cdot 87 = 7395 \end{aligned}$$

sowie die drei Inversen für q_i, $1 \leq i \leq 3$, mit dem erweiterten Euklidischen Algorithmus als

$$\begin{aligned} q_1^{-1} &\equiv 22011^{-1} \equiv 81^{-1} \equiv 21 \mod 85, \\ q_2^{-1} &\equiv 21505^{-1} \equiv 16^{-1} \equiv -38 \equiv 49 \mod 87 \quad \text{und} \\ q_3^{-1} &\equiv 7395^{-1} \equiv 58^{-1} \equiv 48 \mod 253. \end{aligned}$$

Insgesamt ist die gesuchte Lösung modulo 1870935 also gegeben durch

$$m^3 \equiv 56 \cdot 22011 \cdot 21 + 26 \cdot 21505 \cdot 49 + 66 \cdot 7395 \cdot 48 \equiv 1331 \mod 1870935.$$

Der eindeutige Repräsentant $0 \leq m^3 < n_1 \cdot n_2 \cdot n_3$ ist demnach $m^3 = 1331$ und damit ist die Originalnachricht $m = \sqrt[3]{1331} = 11$.