Institut für Informatik
Prof. Dr. J. Rothe

Wintersemester 2023/24
Übungsblatt 6

Lösungsvorschläge

Kryptokomplexität 1

Bearbeitungszeit: 14. November bis 22-24. November
Verantwortlich: Roman Zorn

Aufgabe 1 : Chinesischer Restsatz

Lösen Sie die folgenden Kongruenzsysteme mit dem chinesischen Restsatz:

(a) ▶

$$\begin{aligned} 2x &\equiv 26 \mod 27 \\ 15x &\equiv 5 \mod 16 \end{aligned}$$

Lösungsvorschlag: ▶ Wir wollen zunächst das Kongruenzsystem umstellen, so dass es die gewünschte Form hat. Dazu berechnen wir mit dem erw. euklidischen Alg. $2^{-1} \equiv 14 \mod 27$ und $15^{-1} \equiv 15 \mod 16$. Wir erhalten

$$\begin{aligned} x &\equiv 14 \cdot 26 \equiv 13 \mod 27 \\ x &\equiv 15 \cdot 5 \equiv 11 \mod 16. \end{aligned}$$

Als nächstes benötigen wir $M = m_1 \cdot m_2 = 16 \cdot 27 = 432$ und können nun $q_1 = {}^{M}/_{m_1} = 16$ und $q_2 = {}^{M}/_{m_2} = 27$ berechnen. Für die Lösung laut chinesichem Restsatz brauchen wir nun noch $q_1^{-1} = 16^{-1} \equiv 22 \mod 27$ und $q_2^{-1} = 27^{-1} \equiv 3 \mod 16$, was wir erneut mit dem erw. euklidischen Alg. bestimmen können. Wir erhalten als Lösung $x \equiv a_1 \cdot q_1 \cdot q_1^{-1} + a_2 \cdot q_2 \cdot q_2^{-1} \equiv 13 \cdot 16 \cdot 22 + 11 \cdot 27 \cdot 3 \equiv 4576 + 891 \equiv 283 \mod 432$.

Als Probe können wir nun $x = 283$ oben einsetzen und überprüfen, ob die Lösung stimmt.

(b) ▶

$$\begin{aligned} 3x &\equiv 4 \mod 7 \\ x &\equiv 6 \mod 8 \\ 2x &\equiv 7 \mod 9 \end{aligned}$$

Lösungsvorschlag: ► Analog zu Aufgabenteil (a):

- $3^{-1} \equiv 5 \mod 7$ und $2^{-1} \equiv 5 \mod 9$
- $\Rightarrow$

$$\begin{aligned} x &\equiv 5 \cdot 4 \equiv 6 \mod 7 \\ x &\equiv 6 \mod 8 \\ x &\equiv 5 \cdot 7 \equiv 8 \mod 9 \end{aligned}$$

- $M = m_1 \cdot m_2 \cdot m_3 = 7 \cdot 8 \cdot 9 = 504$
- $q_1 = {}^{M}/_{m_1} = 72$, $q_2 = {}^{M}/_{m_2} = 63$ und $q_3 = {}^{M}/_{m_3} = 56$
- $q_1^{-1} = 72^{-1} \equiv 4 \mod 7$, $q_2^{-1} = 63^{-1} \equiv 7 \mod 8$ und $q_2^{-1} = 56^{-1} \equiv 5 \mod 9$
- $\Rightarrow x \equiv a_1 \cdot q_1 \cdot q_1^{-1} + a_2 \cdot q_2 \cdot q_2^{-1} + a_3 \cdot q_3 \cdot q_3^{-1} \equiv 6 \cdot 72 \cdot 4 + 6 \cdot 63 \cdot 7 + 8 \cdot 56 \cdot 5 \equiv 1728 + 2646 + 2240 \equiv 62 \mod 504$.

Aufgabe 2 : RSA Public-Key Kryptosystem

Betrachten Sie das RSA-Kryptosystem. Verwenden Sie beim Ver– und Entschlüsseln Square-and-Multiply und geben Sie Ihre Rechenschritte an.

(a) ▶ Wählen Sie $p = 53$, $q = 37$ und $e = 7$ und verschlüsseln Sie die Nachricht $m = \texttt{BROT}$ über dem kanonischen Alphabet $\Sigma = \{A, B, \ldots, Z\}$.

Lösungsvorschlag: ▶ Es wird $n = 53 \cdot 37 = 1961$ berechnet. Dann ist $\varphi(n) = 1872$. $e = 7$ ist valide, da ggT $(7, 1872) = 1$.

Es ist $\lfloor \log_{26}(1961) \rfloor = 2$, also wird $m_1 = 1 \cdot 26 + 17$ als

$$c_1 = m_1^e \mod n \equiv (1 \cdot 26 + 17)^7 \equiv 43^7 \equiv 623 \mod 1961$$

und $m_2 = 14 \cdot 26 + 19$ als

$$c_2 = m_2^e \mod n \equiv (14 \cdot 26 + 19)^7 \equiv 383^7 \equiv 1105 \mod 1961$$

verschlüsselt.

Rechnungen mit square-and-multiply für die Verschlüsselung ($7 = 4 + 2 + 1 = 2^0 + 2^1 + 2^2$):

2^0	2^1	2^2
43	**1849**	**778**
383	**1575**	**1921**

$\implies$ $43^7 \equiv 43 \cdot 1849 \cdot 778 \equiv 623 \mod 1961$
$383^7 \equiv 383 \cdot 1575 \cdot 1921 \equiv 1105 \mod 1961$

(b) ▶ Berechnen Sie den passenden Entschlüsselungsschlüssel d und entschlüsseln Sie den Schlüsseltext, den Sie in Aufgabenteil (a) erhalten haben.

Lösungsvorschlag: ▶ Berechne d durch $d \equiv e^{-1} \mod \varphi(n) = 535 \mod 1872$.

Entschlüssele $c_1 = 623$ durch $m_1 \equiv c_1^d \equiv 623^{535} \equiv 43 \mod 1961$ und $c_2 = 1105$ durch $m_2 \equiv c_2^d \equiv 1105^{535} \equiv 383 \mod 1961$

Rechnungen mit square-and-multiply für die Entschlüsselung ($535 = 512 + 16 + 4 + 2 + 1 = 2^0 + 2^1 + 2^2 + 2^4 + 2^9$):

2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9
623	**1812**	**630**	778	**1296**	1000	1851	334	1740	**1777**
1105	**1283**	**810**	1126	**1070**	1637	1043	1455	1106	**1533**

$\Longrightarrow \quad 623^{535} \equiv 623 \cdot 1812 \cdot 630 \cdot 1296 \cdot 1777 \equiv 43 \mod 1961$
$1105^{535} \equiv 1105 \cdot 1283 \cdot 810 \cdot 1070 \cdot 1533 \equiv 383 \mod 1961$

(c) ▶ Nehmen Sie wie in der Vorlesung an, dass Alice verschlüsselt und Bob entschüsselt. Welche Informationen würden in den Aufgabenteilen (a) und (b) zwischen den beiden ausgetauscht werden?

Lösungsvorschlag: ▶ Bob berechnet n aus p und q und wählt e. Dann schickt er (n, e), den Public-Key, zu Alice. Alice verschlüsselt daraufhin die Nachricht und schickt die beiden Schlüsseltexte zurück an Bob.

Aufgabe 3 : RSA Schema für digitale Signaturen

▶ Simulieren Sie das RSA Schema für digitale Signaturen aus der Vorlesung, indem Sie Alice' öffentlichen und privaten Schlüssel auf Basis von $p = 11$, $q = 89$ und e als kleinster gültiger Exponent berechnen, ihre Nachricht $m = \texttt{LAMA}$ über dem kanonischen Alphabet $\Sigma = \{A, B, \ldots, Z\}$ signieren und anschließend die so entstandene Signatur mit Alice' öffentlichen Schlüssel verifizieren. Verwenden Sie dabei Square-and-Multiply und geben Sie Ihre Rechenschritte *als Tabelle wie in der Vorlesung* an.

Lösungsvorschlag: ▶

Schritt	Alice	Erich	Bob
1	Alice wählt $p = 11$, $q = 89$. Sie berechnet $n = 11 \cdot 89 = 979$. Dann ist $\varphi(n) = 880$. Außerdem wählt sie $e = 3$ (da $\text{ggT}(3, 880) = 1$) und berechnet d durch $d \equiv e^{-1} \mod \varphi(n) = 587 \mod 880$.		
2		$(n{=}979, e{=}3)\rightarrow$	
3	Es ist $\lfloor \log_{26}(979) \rfloor = 2$, also signiert Alice $m_1 = 11 \cdot 26 + 0$ durch $\text{sig}(m_1) = m_1^d \mod n \equiv (11 \cdot 26 + 0)^{587} \equiv 286^{587} \equiv 946 \mod 979$ und $m_2 = 12 \cdot 26 + 0$ durch $\text{sig}(m_2) = m_2^d \mod n \equiv (12 \cdot 26 + 0)^{587} \equiv 312^{587} \equiv 929 \mod 979$.		
4		$\langle m_1{=}286, \text{sig}(m_1){=}946, m_2{=}312, \text{sig}(m_2){=}929\rangle\rightarrow$	
5			Bob verifiziert m durch $m_1 \equiv \text{sig}(m_1)^e \mod n$ und $m_2 \equiv c_2^e \mod n$ $\Rightarrow m_1 = 946^3 \equiv 286 \mod 979$ und $m_1 = 929^3 \equiv 312 \mod 979$.

Rechnungen mit square-and-multiply für die Signierung ($587 = 512+64+8+2+1 = 2^0 + 2^1 + 2^3 + 2^6 + 2^9$):

2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9
286	**539**	737	**803**	627	550	**968**	121	935	**957**
312	**423**	751	**97**	598	269	**894**	372	345	**566**

$\Longrightarrow \quad 286^{587} \equiv 286 \cdot 539 \cdot 803 \cdot 968 \cdot 957 \equiv 946 \mod 979$

$312^{587} \equiv 312 \cdot 423 \cdot 97 \cdot 894 \cdot 566 \equiv 929 \mod 979$

Rechnungen mit square-and-multiply für die Entschlüsselung ($3 = 2 + 1 = 2^0 + 2^1$):

	2^0	2^1
	946	**110**
	929	**542**

$\Longrightarrow$ $946^3 \equiv 946 \cdot 110 \equiv 286 \mod 979$
$929^3 \equiv 929 \cdot 542 \equiv 312 \mod 979$

Aufgabe 4 : Eigenschaften der RSA-Funktion

Betrachten Sie erneut das RSA-Kryptosystem aus der Vorlesung. Es erfüllt die Eigenschaft $\star$, wenn für alle Schlüssel (n, e) und Klartexte $m_1, m_2 < n$,

$$E_{(n,e)}(m_1) \star E_{(n,e)}(m_2) = E_{(n,e)}(m_1 \star m_2)$$

gilt. Die RSA-Funktion E ist *multiplikativ*, falls sie die Eigenschaft $\star$ mit $\star$ = 'Multiplikation über $\mathbb{Z}_n$' erfüllt. Sie ist *additiv*, falls sie die Eigenschaft $\star$ mit $\star$ = 'Addition über $\mathbb{Z}_n$' erfüllt.

(a) ▶ Zeigen Sie, dass die RSA-Funktion multiplikativ ist.

Lösungsvorschlag: ▶ Sei (n, e) eine Schlüssel und $m_1, m_2 < n$ Klartexte. Dann ist

$E_{(n,e)}(m_1 \star m_2) = (m_1 \star m_2)^e \equiv (m_1 \cdot m_2 \mod n)^e \equiv ((m_1 \mod n) \cdot (m_2 \mod n))^e \equiv (m_1 \cdot m_2)^e \equiv m_1^e \cdot m_2^e \equiv (m_1^e \mod n) \cdot (m_2^e \mod n) \mod n = E_{(n,e)}(m_1) \cdot E_{(n,e)}(m_2) \mod n = E_{(n,e)}(m_1) \star E_{(n,e)}(m_2)$.

(b) ▶ Überprüfen Sie die multiplikative Eigenschaft explizit mit $n = 11 \cdot 13 = 143, e = 3, m_1 = 7$ und $m_2 = 5$.

Lösungsvorschlag: ▶ Es gilt

$$E_{(143,3)}(m_1 \star m_2) = (7 \cdot 5 \mod 143)^3 \equiv (35)^3 \equiv 118 \mod 143 \quad (1)$$

$$E_{(143,3)}(m_1) \star E_{(143,3)}(m_2) = (7^3 \mod 143) \cdot (5^3 \mod 143) \equiv 57 \cdot 125 \equiv 118 \mod 143 \quad (2)$$

und somit (1) = (2).

(c) ▶ Ist die RSA-Funktion auch additiv? Beweisen oder widerlegen Sie.

Lösungsvorschlag: ▶ Gegenbeispiel mit den Werten aus (b):

$$E_{(143,3)}(m_1 \star m_2) = (7 + 5 \mod 143)^3 \equiv (12)^3 \equiv 12 \mod 143 \quad (3)$$

$$E_{(143,3)}(m_1) \star E_{(143,3)}(m_2) = (7^3 \mod 143) + (5^3 \mod 143) \equiv 57 + 125 \equiv 39 \mod 143 \quad (4)$$

Es folgt, dass (3) $\neq$ (4) und somit ist die RSA-Funktion nicht additiv.