



Lösungsblatt 8

(Version 2)

Aufgabe 1 (RSA - Beschleunigung)

Wir berechnen zunächst den geheimen Exponenten $d = 65 = 257^{-1} \pmod{\varphi(n)}$.

(a) Zur schnellen Exponentiation berechnen wir

i	$c^{2^i} \pmod n$
0	74
1	308
2	225
3	237
4	290
5	120
6	188

Da $65 = 2^6 + 1$ gilt $m \equiv 188 \cdot 74 \equiv 23 \pmod{323}$. Wir haben 7 Multiplikationen modulo 323 benötigt und daher ca. $7 \cdot 8^2 = 448$ binäre Operationen.

(b) Wir berechnen zunächst $c \equiv 78 \equiv 10 \pmod{17}$ und $c \equiv 78 \equiv 2 \pmod{19}$. Zur Entschlüsselung berechnen wir $c^d \pmod{\varphi(p)} \equiv c^1 \pmod{p}$ und $c^d \pmod{\varphi(q)} \equiv c^{11} \pmod{q}$. Weiterhin berechnen wir die folgende Tabellen zur schnellen Exponentiation:

i	$c^{2^i} \pmod{17}$	und	i	$c^{2^i} \pmod{19}$
0	10		0	2
1			1	4
2			2	16
3			3	9

Wir wissen daher, daß $m \equiv 10 \pmod{17}$ und $m \equiv 2 \cdot 4 \cdot 9 \equiv -4 \pmod{19}$. Da $17 \cdot 9 - 8 \cdot 19 = 1$ gilt mit dem CRT: $m \equiv -4 \cdot (17 \cdot 9) + 10 \cdot (-8 \cdot 19) \equiv 129 \pmod{323}$. Wir haben hier 5 Multiplikationen modulo 19, sowie 4 Multiplikationen und eine Addition modulo 323 benötigt, was $5 \cdot 5^2 + 4 \cdot 8^2 + 8 = 389$ Binäroperationen entspricht. Da der Aufwand für den CRT nicht von dem Exponenten d abhängt, ist diese Variante, RSA mit CRT zu entschlüsseln meistens die schnellere. Je größer die Primzahlen werden, um so größer ist auch der Zeitvorteil.

Aufgabe 2 (Low Exponent Attack)

(a) Wir setzen $m_a = 55$, $m_b = 51$ und $m_c = 46$. Daraufhin berechnen wir $M_a = m_b \cdot m_c = 2346$, $M_b = m_a \cdot m_c = 2530$ und $M_c = m_a \cdot m_b = 2805$. es gilt $26 \cdot M_a \equiv 1 \pmod{m_a}$, $28 \cdot M_b \equiv 1 \pmod{m_b}$ und $45 \cdot M_c \equiv 1 \pmod{m_c}$. Daher können wir $m^3 \pmod{(m_a \cdot m_b \cdot m_c)}$ mit dem CRT bestimmen:

$$m^3 \equiv 13 \cdot 26 \cdot M_a + 37 \cdot 28 \cdot M_b + 21 \cdot 45 \cdot M_c \equiv 343 \pmod{129030}.$$

Es gilt: $\sqrt[3]{343} = 7$. Tatsächlich können wir feststellen, daß 7 die an Alice, Bob und Charlie gesendete Nachricht war, wenn wir die 7 mit dem jeweiligen Schlüssel verschlüsseln.

(b) Die Low Exponent Attacke funktioniert bei RSA, wenn eine Nachricht m an e viele Personen gesendet wurde, die verschiedene RSA-Schlüssel (n_i, e) , $i = 1, \dots, e$ haben, und deren öffentlicher Exponent jeweils e ist. In diesem Fall ist c eindeutig modulo $\prod_{i=1}^e n_i$ und kann mit dem CRT bestimmt werden. Wir nennen das Resultat \bar{c} . Da $m \leq n_i$ für alle $i = 1, \dots, e$ gelten muß, ist $m^3 = \bar{c} \leq \prod_{i=1}^e n_i$ und die Wurzel von \bar{c} über \mathbb{R} entspricht m .

Aufgabe 3 (Common Modulus Attack)

- (a) Es gilt $53 \cdot 9 - 28 \cdot 17 = 1$. Daher gilt offensichtlich $(m^{53})^9 \cdot (m^{17})^{-28} \equiv m^{53 \cdot 9} \cdot m^{-17 \cdot 28} \equiv m \pmod{437}$. Wir berechnen: $354^9 \cdot 335^{-28} \equiv 8 \equiv m \pmod{437}$.
- (b) Eine „Common Modulus Attack“ ist möglich, wenn eine Nachricht m an s Personen gesendet wird, deren öffentliche RSA-Schlüssel (n_i, e_i) , $i = 1, \dots, s$ denselben Modulus $n_i = n$, $i = 1, \dots, s$ enthalten, und der größte gemeinsame Teiler aller Exponenten $\gcd(e_1, e_2, \dots, e_s) = 1$ ist. In diesem Fall existieren $x_i \in \mathbb{Z}$, $i = 1, \dots, s$, so daß $1 = \sum_{i=1}^s x_i e_i$ und daher ist $m = \prod_{i=1}^s c_i^{x_i} \pmod{n}$, wobei c_i der an Teilnehmer i gesendete Schlüsseltext ist.

Aufgabe 4 (Cycling-Attacke auf RSA)

- (a) Wir betrachten die von m^e erzeugte Untergruppe von \mathbb{Z}_n^\times bzw. die von e in $\mathbb{Z}_{\varphi(n)}^\times$ erzeugte Untergruppe. Da $\gcd(e, \varphi(n)) = 1$, ist das Erzeugnis von e in $\mathbb{Z}_{\varphi(n)}^\times$ eine Untergruppe und es gibt ein k , so daß $e^k \equiv 1 \pmod{\varphi(n)}$. Für dieses k gilt offensichtlich die gewünschte Eigenschaft.
- (b) Wir schließen

$$m = m^{e^k} \equiv (m^e)^{e^{k-1}} \equiv c^{e^{k-1}} \pmod{n}.$$

- (c) Es gilt $\varphi(n) = 16 \cdot 28$. Wir betrachten die Abbildung

$$\psi : \mathbb{Z}_n \rightarrow \mathbb{Z}_p \times \mathbb{Z}_q, x \mapsto (x \pmod{p}, x \pmod{q})$$

und stellen fest, daß das gesuchte k ein Vielfaches der Ordnung von 3 in \mathbb{Z}_{16}^\times und in \mathbb{Z}_{28}^\times sein muß. Wir bemerken daher, daß wir nicht das k aus Aufgabenteil (a) suchen:

$$\begin{aligned} e^k &\equiv 1 \pmod{\varphi(pq)} \\ &\Leftrightarrow \\ e^k &\equiv 1 \pmod{\varphi(p)} \text{ und } e^k \equiv 1 \pmod{\varphi(q)} \end{aligned}$$

Die Ordnung von 3 in \mathbb{Z}_{16}^\times ist 4, und Ordnung von 3 in \mathbb{Z}_{28}^\times ist 6. Damit ist das gesuchte k das kleinste gemeinsame Vielfache von 4 und 6, also 12.

- (d) Wir berechnen

i	c_i
1	99
2	23

Offensichtlich gilt $55^2 \equiv 1 \pmod{\varphi(17)}$ und $55^2 \equiv 1 \pmod{\varphi(19)}$.

Aufgabe 5 (Rabin Faktorisierung)

Wir berechnen zunächst $\gcd(187 - 95, n) = 23$ und erhalten $n = 47 \cdot 23$. Jetzt können wir $m_p = 8^{48/4} \pmod{47} = 14$ und $m_q = 8^{24/4} \pmod{23} = 13$ berechnen. Mit dem erweiterten euklidischen Algorithmus erhalten wir $45 \cdot 23 \equiv 1 \pmod{47}$ und $1 \cdot 47 \equiv 1 \pmod{23}$. Daher können wir mit dem CRT eine der möglichen Nachrichten berechnen:

$$m \equiv (14 \cdot 45 \cdot 23 - 13 \cdot 1 \cdot 47) \equiv 907 \pmod{n}.$$

Aufgabe 6 (Elementordnungen)

- (a) Um ein Element der Ordnung 4 zu finden, nutzen wir, wie in den folgenden Teilaufgaben auch die folgende Tatsache, die sich mittels des kleinen Satz von Fermat beweisen lässt:

Sei $a \cdot b$ mit $a, b \in \mathbb{N}$ die Ordnung der Gruppe (G, \cdot) , dann gilt für alle $x \in G$: Die Ordnung von x^b teilt a .

Wählen wir zufällig ein Element x aus \mathbb{Z}_{35}^\times und berechnen $e = x^{24/4} \pmod{35}$. Damit gilt: $\text{ord}(e) \mid 4$. Falls $e \not\equiv 1 \pmod{35}$, dann ist $\text{ord}(e) > 1$, also 2 oder 4. Folglich ist e oder $x^{24/8}$ das gesuchte Element, da die Ordnung von $x^{24/8}$ das doppelte der Ordnung von e ist, oder $\text{ord}(e) = 1$ gilt. Wir fangen an mit $2^6 \equiv 64 \equiv -6 \pmod{35}$. Das ist nicht das gesuchte Element, dafür ist aber $2^3 \equiv 8$ das gesuchte Element.

- (b) Es kann kein Element der Ordnung 5 geben, da 5 nicht $\varphi(149) = 148$ teilt.
(c) Mögliche Elementordnungen sind Teiler von 148. Mögliche Elementordnungen sind daher 2, 4, 37, 74 und 148.
(d) Wir nehmen wieder ein beliebiges Element aus \mathbb{Z}_{149}^\times , z.B. 44. Da $44^4 \equiv 1 \pmod{149}$, ist weder 44 noch $44^2 \pmod{149}$ noch $44^4 \pmod{149}$ ein Element der gewünschten Ordnung. Wir raten also weiter. Diesmal versuchen wir es mit der 2. Da $2^4 = 16$ und $2^{4 \cdot 37} \equiv 1 \pmod{149}$, ist 16 das gesuchte Element.

Aufgabe 7 (RSA-Faktorisierung mit geheimen Exponenten)

Wir bestimmen zunächst $s = \max \{i \in \mathbb{N} : 2^i \mid (ed - 1)\} = 3$ und $k = (ed - 1)/(2^s) = 3213$. Wir wählen nun zufällig $a \in \mathbb{Z}_n$ und berechnen $\text{gcd}(a^{k2^i} - 1, n)$ für $i = 1, \dots, s$: $a = 2$, $2^{3213 \cdot 2} \equiv 115 \pmod{551}$, $\text{gcd}(115 - 1, 551) = 19$. Damit haben wir schon einen Primfaktor von n gefunden. Der andere ist $n/19 = 29$.

Aufgabe 8 (Cycling-Attacke auf RSA)

Um diese Aufgabe zu beantworten, zeigen wir folgenden Sachverhalt für einen RSA-Modulus n , der Produkt der Primzahlen p und q ist:

Ein Tripel (n, e, k) hat die Eigenschaft, daß

$$(1) \quad \text{für alle } m \text{ mit } \text{gcd}(m, n) = 1 \text{ gilt } m^{e^k} \equiv m \pmod{n}$$

genau dann, wenn

$$(2) \quad \text{für alle Primzahlpotenzen } r \text{ mit } r \mid (p - 1) \text{ oder } r \mid (q - 1) \text{ gilt } e^k \equiv 1 \pmod{r}.$$

Sei $n = pq$ das Produkt der zwei Primzahlen p und q . Für jedes m mit $\text{gcd}(m, n) = 1$ gilt

$$(3) \quad m^{e^k} \equiv m \pmod{n} \implies m^{e^k - 1} \equiv 1 \pmod{p} \text{ und } m^{e^k - 1} \equiv 1 \pmod{q}.$$

Sei m derart gewählt, daß $m \equiv g_p \pmod{p}$ für eine Primitivwurzel g_p von p , und $m \equiv g_q \pmod{q}$ für eine Primitivwurzel g_q von q . Dies ist nach dem Chinesischen Restsatz möglich. Da g_p die Ordnung $p - 1$ zum Modul p hat, und g_q die Ordnung $q - 1$ zum Modul q , ziehen die Kongruenzen auf der rechten Seite von (3) nach sich, daß

$$(p - 1) \mid e^k - 1 \quad \text{und} \quad (q - 1) \mid e^k - 1, \quad \text{also} \quad \text{lcm}((p - 1), (q - 1)) \mid e^k - 1.$$

Somit muß für jede Primzahlpotenz r , die $p - 1$ oder $q - 1$ teilt, gelten, daß $e^k \equiv 1 \pmod{r}$.

Umgekehrt: gilt für jede Primzahlpotenz r , die $p - 1$ oder $q - 1$ teilt, daß $e^k \equiv 1 \pmod{r}$, dann gilt auch $e^k \equiv 1 \pmod{p - 1}$ und $e^k \equiv 1 \pmod{q - 1}$. Somit gilt für jedes m mit $\text{gcd}(m, n) = 1$ (und damit $\text{gcd}(m, p) = 1$ und $\text{gcd}(m, q) = 1$)

$$m^{e^k} \equiv m \pmod{p} \quad \text{und} \quad m^{e^k} \equiv m \pmod{q},$$

so daß Eigenschaft (1) erfüllt ist.

- (a) Wir fixieren $n = pq$ mit der Eigenschaft, daß $p - 1 = 2r$ und $q - 1 = 2s$ mit primen r, s derart, daß $(r - 1)/2$ und $(s - 1)/2$ selbst prim sind. Sei ferner $k \leq 2^{80}$. In dem vorangegangenen Lösungsblatt, Aufgabe 3, haben wir gezeigt, daß für ein e die Aussage

$$\text{für alle } m \text{ mit } \text{gcd}(m, n) = 1 \text{ gilt } m^{e^k} \equiv m \pmod{n},$$

genau dann gilt, wenn

$$(4) \quad e^k \equiv 1 \pmod{r}, \quad e^k \equiv 1 \pmod{s}, \quad e^k \equiv 1 \pmod{2}$$

Wir sehen sofort, daß e ungerade sein muß.

Seien g_r und g_s Primitivwurzeln für r bzw. s . Dann existieren a_r und a_s derart, daß

$$e \equiv g_r^{a_r} \pmod{r} \quad \text{und} \quad e \equiv g_s^{a_s} \pmod{s}.$$

Die Ordnung von e zum Modul r ist $(r-1)/\gcd(a_r, r-1)$. Da $e^k \equiv 1 \pmod{r}$ und $k \leq 2^{80}$, ist die Ordnung von e zum Modul r auch kleiner gleich 2^{80} . Da $(r-1)/2$ prim und $r > 2^{500}$ ist, sind die einzigen Teiler von $r-1$ kleiner als 2^{80} die Zahlen 1 und 2. Damit muß a_r entweder $(r-1)/2$ oder $r-1$ sein. Dies zieht für e nach sich, daß $e \equiv \pm 1 \pmod{r}$. Gleiches gilt zum Modul s .

Nach dem Chinesischen Restsatz existieren genau 4 Zahlen in dem Intervall $[0, 2rs-1]$, für die

$$(5) \quad e \equiv \pm 1 \pmod{r}, \quad e \equiv \pm 1 \pmod{s}, \quad e \equiv 1 \pmod{2}$$

Es gibt demnach höchstens 8 Zahlen e im Intervall $[1, 4rs-1]$, welche die Kongruenzen (4) erfüllen können.

Ist umgekehrt e eine dieser Zahlen, für die (5) erfüllt ist, und $k=2$, dann gilt auch (4), so daß die Cycling-Attacke mit $k=2$ zum Erfolg führt.

Die Wahrscheinlichkeit, daß die Cycling-Attacke für irgendein $k \leq 2^{80}$ gelingt, ist somit $8/(\varphi(n)-1)$. Dies ist verschwindend klein.

- (b) Fixieren wir ein $n = pq$, das der Bedingung genügt, daß es Primzahlen r, s mit $s > 2^{80}$ derart gibt, daß $s \mid (r-1)$ und $r \mid (p-1)(q-1)$.

Wieder zieht für gegebenes $k \leq 2^{80}$ die Bedingung an e , daß

$$\text{für alle } m \text{ mit } \gcd(m, n) = 1 \text{ gilt, daß } m^{e^k} \equiv m \pmod{n}$$

nach sich, daß

$$e^k \equiv 1 \pmod{r}.$$

Ist $e \equiv g^a \pmod{s}$ für eine Primitivwurzel g zum Modul s , dann gilt wiederum die Abschätzung

$$(r-1)/\gcd(a, r-1) = \text{ord } e \leq k \leq 2^{80}.$$

Teilt s den $\gcd(a, r-1)$ nicht, dann hätten wir auch $s \cdot \gcd(a, r-1) \mid (r-1)$, was wegen $s > 2^{80}$ unmöglich ist. Also wissen wir $s \mid \gcd(a, r-1)$ und damit auch $s \mid a$. Somit ist der Anteil der Restklassen zum Modulus r , in die e fallen kann, von oben durch $1/s$ beschränkt.

Da diese Schranke von k nicht abhängt, erhalten wir für zufällig gezogenes e aus $[1, \varphi(n)-1]$ eine von oben durch $1/s < 2^{-80}$ beschränkte Wahrscheinlichkeit, daß für ein $k \leq 2^{80}$ die Cycling-Attacke zum Erfolg führt.