Frank Klinker

Grundlagen: Das RSA-Verfahren

1 Die Grundidee des RSA-Verfahrens und eine Babyvariante

Die Idee des RSA-Verfahrens ist es, eine Nachricht durch Potenzieren zu verschlüsseln.

Dazu übersetzt man zunächst das zu codierende Alphabeth in Zahlen, zum Beispiel A = 1, B = 2, ..., Z = 26.

Als nächstes wählt man einen Schlüssel[1], zum Beipiel $e = 3$.

Unsere Nachricht lautet 'AHBZ=1,8,2,26' und diese gilt es zu verschlüsseln:

$$\begin{aligned} \mathrm{A} = 1 &\mapsto 1^3 = 1 \\ \mathrm{H} = 8 &\mapsto 8^3 = 512 \\ \mathrm{B} = 2 &\mapsto 2^3 = 8 \\ \mathrm{Z} = 26 &\mapsto 26^3 = 17576 \end{aligned}$$

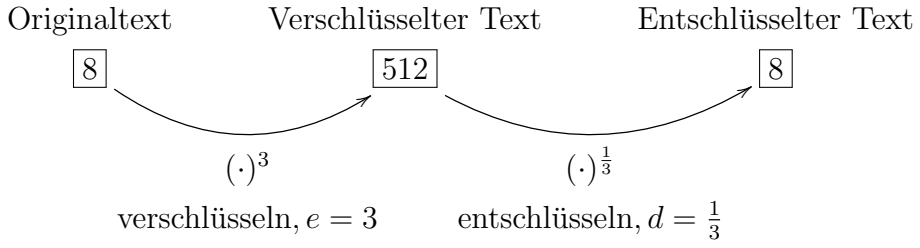
Damit lautet der verschlüsselte Text

$$\mathrm{AHBZ} = 1, 8, 2, 26 \mapsto 1, 512, 8, 17576$$

Wie entschlüsselt man nun den codierten Text?

Das ist hier recht einfach, da man lediglich Radizieren muss, und zwar mit der dritten Wurzel. Das lässt sich auch mit Hilfe von Potenzieren formulieren:

Das Entschlüsseln erfolgt über das Potenzieren mit dem Exponenten $d = \frac{1}{3}$.



Problem 1. • Kennen wir e, so auch d. Dabei spielt es keine Rolle ob e ganzzahlig ist, denn man erhält d als Lösung der leicht zu lösenden Gleichung

$$ex = 1 \tag{1}$$

Adresse: Eduard-Spranger-Berufskolleg, 59067 Hamm
E-Mail: mail@frank-klinker.de

[1] e: encrypt (verschlüsseln), d: decrypt (entschlüsseln)

- Man kann durch Raten und Probieren e herausfinden, wenn man etwa weiß, dass e und die Originalnachricht natürliche Zahlen sind und man den verschlüsselten Text kennt:

  Der verschlüsselte Txt sei $512 = 2^9$. Dann sind die möglichen Schlüssel $e = 9, e = 3$ oder $e = 1$ mit den Originalnachrichten

e	9	3	1
Nachricht	2	8	512

  Hat man nun mehrere verschlüsselte Texte, so kann man durch einfache Ausschlussverfahren auf das korrekte e schließen.

Der Grund für das simple Dekodieren ist:

Rechnen über den reellen Zahlen $\mathbb{R}$ ist zu einfach

2 Ein komplizierterer Zahlenraum

Statt über den reellen Zahlen zu rechnen, verwenden wir als Zahlenmenge die **Restklassenmenge** $\mathbb{Z}_N$ der Reste beim Teilen durch die festgelegte Zahl N. Wir schreiben für die möglichen Reste

$$\mathbb{Z}_N = \{0, 1, 2, \ldots, N-1\}$$

2.1 Rechnen in $\mathbb{Z}_N$

In $\mathbb{Z}_N$ können wir addieren und multiplizieren wie in den ganzen Zahlen $\mathbb{Z}$. Wir müssen nach einer Rechnung das Ergebnis lediglich so 'korrigieren', dass es tatsächlich in der Menge $\mathbb{Z}_N$ liegt. Das heißt wir berechnen den Rest beim Teilen durch N. Unsere Schreibweise dafür ist

$$9 \equiv 2 \bmod 7\,, \quad 123 \equiv 21 \bmod 51\,, \quad 12859 \equiv 3 \bmod 8\,, \quad -18 \equiv 2 \bmod 5$$

Unser Fokus wird später auf der Multiplikation liegen, aber für die Zahlen $N = 7$ und $N = 10$ wollen wir auch die Addition hier beispielhaft durchführen:

$$\begin{aligned} 1 + 5 &\equiv 6 \bmod 7 \\ 3 + 4 \equiv 7 &\equiv 0 \bmod 7 \\ 6 + 8 \equiv 14 &\equiv 4 \bmod 10 \\ 7 + 3 \equiv 10 &\equiv 0 \bmod 10 \end{aligned}$$

Das liefert für $N = 7$ und $N = 10$ die folgenden zwei **Additionstabellen**

$|ZZ_7$

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$\mathbb{Z}_{10}$

+	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

Für die Multiplikation haben wir z. B.

$$1 \cdot 5 \equiv 5 \bmod 7$$
$$3 \cdot 4 \equiv 12 \equiv 5 \bmod 7$$
$$6 \cdot 8 \equiv 48 \equiv 8 \bmod 10$$
$$7 \cdot 3 \equiv 21 \equiv 1 \bmod 10$$

Das liefert für $N = 7$ und $N = 10$ die folgenden zwei **Multiplikationstabellen**[2]

$\mathbb{Z}_7$

·	1	2	3	4	5	6
∗1	1	2	3	4	5	6
∗2	2	4	6	1	3	5
∗3	3	6	2	5	1	4
∗4	4	1	5	2	6	3
∗5	5	3	1	6	4	2
∗6	6	5	4	3	2	1

$\mathbb{Z}_{10}$

·	1	2	3	4	5	6	7	8	9
∗1	1	2	3	4	5	6	7	8	9
2	2	4	6	8	0	2	4	6	8
∗3	3	6	9	2	5	8	1	4	7
4	4	8	2	6	0	4	8	2	6
5	5	0	5	0	5	0	5	0	5
6	6	2	8	4	0	6	2	8	4
∗7	7	4	1	8	5	2	9	6	3
8	8	6	4	2	0	8	6	4	2
∗9	9	8	7	6	5	4	3	2	1

2.2 Teilerfremdheit und die φ-Funktion

Bemerkung 2. • In den Multiplikationstabellen ist auffällig, dass in einigen Zeilen und analogen Spalten jede mögliche Zahl auch als Ergebnis vorkommt (das

[2]In den Multiplikationstabellen verzichten wir auf die Zeilen und Spalten für 0, da die Multiplikation mit 0 in jeder Restklassenmenge stets 0 ergibt.

sind die Zeilen mit $*$).

- In $\mathbb{Z}_7$ trifft dies auf jede Zeile zu, in $\mathbb{Z}_{10}$ nur in den Zeilen zu 1,3,7 und 9.
- In den anderen Zeilen tritt nicht nur nicht jede Zahl auf, sondern es tritt auch die Zahl 0 als Ergebnis einer Multiplikation auf. Das ist ein enormer Unterschied zu den reellen Zahlen $\mathbb{R}$, wo das nicht passieren kann.

Definition 3. Zwei Zahlen $a, b \in \mathbb{Z}$ mit $a, b \neq 0$ heißen **teilerfremd**, wenn sie als gemeinsamen Teiler lediglich die 1 haben. Wir schreiben dafür

$$\mathrm{ggT}(a, b) = 1$$

und sagen auch **der größte gemeinsame Teiler** ist 1.

Beispiel 4.
- Die Zahlen 10 und 4 sind nicht teilerfremd, denn sie haben die gemeinsamen Teiler 1 und 2 und es ist $\mathrm{ggT}(4, 10) = 2$.
- Die Zahlen 10 und 9 sind teilerfremd, denn es ist $\mathrm{ggT}(9, 10) = 1$.
- Die Zahl 7 ist teilerfremd zu jeder Zahl außer zu ihren Vielfachen: Das gilt für jede Primzahl p:
$$\mathrm{ggT}(p, a) = 1, \text{ für } a \neq kp, k \in \mathbb{Z}$$

Fakt 5.
1. In der Multiplikationstabelle zu $\mathbb{Z}_N$ kommt in der Zeile zur Zahl a alle Zahlen von 1 bis $N-1$ vor, wenn N und a teilerfremd sind, also wenn $\mathrm{ggT}(N, a) = 1$.
2. In der Multiplikationstabelle zu $\mathbb{Z}_N$ kommen in den Zeilen zur Zahl a nicht alle Zahlen von 1 bis $N-1$ vor und es kommt die 0 vor, wenn N und a nicht teilerfremd sind, also wenn $\mathrm{ggT}(N, a) > 1$.

Da zu einem vorgegebenen Modus N die hierzu teilerfremden Zahlen eine besondere Rolle spielen, ist es auch wichtig, ihre Anzahl zu kennen:

Definition 6. Es sei N eine positive natürliche Zahl, dann bezeichnet

$$\varphi(N)$$

die Anzahl der zu N teilerfremden Zahlen in der Menge $\{1, 2, \ldots, N-1\}$. φ heißt die **Eulersche φ-Funktion**.

Beispiel 7.
- 1,2,3,4,5,6 sind teilerfremd zu 7, also $\varphi(7) = 6$
- 1,3,7,9 sind teilerfremd zu 10, also $\varphi(10) = 4$
- 1,3 sind teilerfremd zu 4, also $\varphi(4) = 2$
- 1,3,5,7 sind teilerfremd zu 8, also $\varphi(8) = 4$
- 1,7,11,13,17,19,23,29 sind teilerfremd zu 30, also $\varphi(30) = 8$
- 1,2,4,7,8,11,13,14 also $\varphi(15) = 8$

- 1,7,11,13,17,19,23,29,31,37,41,43,47,49,53,59,61,67,71,73,77,79,83,89,91,97,101, 103,107,109,113,119 sind teilerfremd zu 120, also $\varphi(120) = 32$

Fakt 8. 1. Die Berechnung von $\varphi(N)$ ist in der Regel kompliziert, insbesondere für große N.

2. Einfach ist es in dem Fall, wenn wir $\varphi(p)$ für eine Primzahl p ausrechnen wollen. Da alle Zahlen $1, 2, \ldots, p-1$ teilerfremd zu p sind, gilt:

$$\text{Ist } p \text{ eine Primzahl, so ist } \quad \varphi(p) = p - 1\,.$$

3. Es gilt eine eingeschränkte Multiplikationsregel:

   Lässt sich die Zahl N in das Produkt zweier teilerfremden Zahlen N_1 und N_2 zerlegen, also $N = N_1 \cdot N_2$, so gilt

$$\varphi(N) = \varphi(N_1)\varphi(N_2)$$

   Zum Beispiel:

   - Es ist $120 = 8 \cdot 15$ und $\mathrm{ggT}(8, 15) = 1$. Es ist $\varphi(8) \cdot \varphi(15) = 4 \cdot 8 = 32$ und das stimmt mit $\varphi(8 \cdot 15) = \varphi(120) = 32$ überein.
   - Anderseits ist auch $120 = 4 \cdot 30$ aber $\mathrm{ggT}(4, 30) = 2 > 1$. Es ist $\varphi(4) \cdot \varphi(30) = 2 \cdot 8 = 16$ und das stimmt nicht mit $\varphi(8 \cdot 15) = \varphi(120) = 32$ überein.

4. Der vorige Punkt ist jedoch nur bedingt nützlich, da es in der Regel schwierig ist, eine Zahl in ein Produkt teilerfremder Zahlen zu zerlegen

5. Damit ist auch die Berechnung von $\varphi(N)$ in der Regel kompliziert, insbesondere für große N.

2.3 Potenzieren in $\mathbb{Z}_N$

Das Potenzieren mit natürlichen Zahlen im Restklassenraum $\mathbb{Z}^N$ ist eigentlich kein Problem, denn es ist lediglich eine Multiplikation durchzuführen. Dabei lohnt es sich Potenzgesetze zu verwenden und sich im Wesentlichen auf kleine Potenzen zurückzuziehen:

Beispiel 9.

$$\begin{aligned}
2^7 &\equiv 128 \equiv 9 \bmod 17\\
2^7 &\equiv 2^4 \cdot 2^3 \equiv 16 \cdot 8 \equiv (-1) \cdot 8 \equiv -8 \equiv 9 \bmod 17\\
2^{66} &\equiv (2^4)^{16} \cdot 2^2 \equiv (-1)^{16} \cdot 4 \equiv 4 \bmod 17\\
8^{21} &\equiv 8 \cdot ((8^2)^2)^5 \equiv 8 \cdot (9^2)^5 \equiv 8 \cdot (4)^5 \equiv 8 \cdot 4 \cdot (4^2)^2 \equiv 8 \cdot 4 \cdot 5^2 \equiv 8 \cdot 4 \cdot 3 \bmod 11\\
&\equiv 8 \cdot 12 \equiv 8 \cdot 1 \equiv 8 \bmod 11\\
8^{10} &\equiv (8^2)^5 \equiv (9)^5 \equiv (-2)^5 \equiv -32 \equiv 1 \bmod 11
\end{aligned}$$

Bemerkung 10. Wenn wir bereits wissen, dass es eine Potenz gibt, sodass $a^K \equiv 1 \bmod N$ gilt, so können wir das nutzen, um einen beliebigen Exponenten zu verkleinern. Es ist etwa in dem obigen Beispiel $8^{10} \equiv 1 \bmod 11$, sodass

$$8^{21} = 8^{10\cdot 2+1} \equiv (8^{10})^2 \cdot 8 \equiv 1^2 \cdot 8 \equiv 8 \bmod 11\,.$$

Etwas formaler lautet das:

$$a^K \equiv 1 \bmod N \quad \text{und} \quad \ell = m \bmod K \quad \text{dann gilt} \quad a^\ell \equiv a^m \bmod N\,.$$

Wir brauchen dann nur noch die Potenzen $a^1, a^2, \ldots, a^{K-1}$ berechnen und kennen danach bereits alle!

Das Problem besteht nun darin: Wie finden wir zu vorgegebener Basis a einen solchen Exponenten K?

Da hilft uns der folgende Satz von Euler (daher hat die Funktion φ ihren Namen):

Satz 11. Ist N eine positive, natürliche Zahl und a teilerfremd zu N, d. h. $\mathrm{ggT}(a, N) = 1$ so gilt

$$a^{\varphi(N)} = 1 \bmod N\,.$$

Schreiben wir das etwas anders, so ist

$$a^{\varphi(N)+1} \equiv a \bmod N\,.$$

Bemerkung 12. 1. Das Ergebnis des Satzes ist erstaunlich, da es besagt, dass es einen Exponenten mit der in Bemerkung 10 gewünschten Eigenschaft gibt, der für alle Basen der gleiche ist!

2. Ist p eine Primzahl, so ist $\varphi(p) = p-1$, und es gilt für alle Zahlen $a = 1, 2, \ldots, p-1$

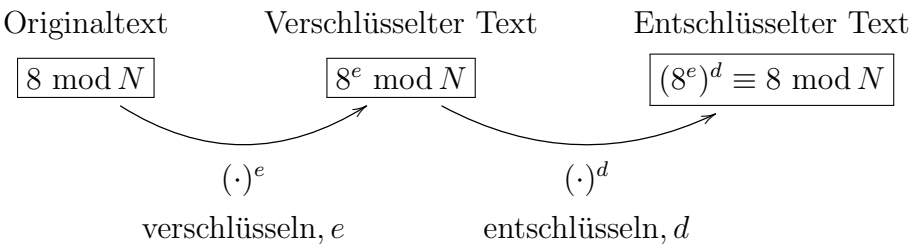
$$a^{p-1} = 1 \bmod p\,.$$

Schreiben wir das etwas anders, so ist

$$a^p \equiv p \bmod p$$

3 RSA-Verfahren über $\mathbb{Z}_N$

Die Idee ist wieder die gleiche wie im ersten Abschnitt:



- Wir starten mit einem Schlüssel e, den wir zum Potenzieren unserer Originalnachricht verwenden. Die Rechnung führen wir nun in $\mathbb{Z}_N$ durch.
- Um eine Chance zum Entschlüsseln zu haben, auch wenn man den passenden Schlüssel d hat, ist der Modus N.
- Dass heißt der Schlüssel zum Verschlüsseln ist (e, N) und der zum Entschlüsseln ist (d, N)

3.1 Generierung der Schlüssel (e, N) und (d, N)

Das Problem der Schlüsselgenerierung ist im Prinzip das gleiche wie in der Babyvariante: Wenn ich den Schlüssel e kenne, dann muss ich, um den Schlüssel d herauszufinden bzw. zu bestimmen, 'nur' ein d finden mit

$$(a^e)^d \equiv a^{ed} \equiv a \bmod N$$

oder etwas umgeschrieben

$$a^{ed-1} \equiv 1 \bmod N\,.$$

Mit Hilfe des Satzes von Euler wissen wir nun, dass $a^{ed-1} = 1$ immer dann gilt, wenn d so gewählt ist, dass $ed-1$ ein Vielfaches von $\varphi(N)$ ist. Also benötigen wir ein d sodass $ed - 1 \equiv 0 \bmod \varphi(N)$.

Das heißt, zur Bestimmung von d lösen wir die Gleichung

$$ex \equiv 1 \bmod \varphi(N)\,, \tag{2}$$

siehe auch die analoge Gleichung (1) im Babybeispiel.

Bemerkung 13. Wir können nicht mit jedem Schlüssel e starten, da wir gewährleisten müssen, das die Gleichung (2) auch lösbar ist. Dazu müssen e und $\varphi(N)$ teilerfremd sein, also $\mathrm{ggT}(e, \varphi(N)) = 1$, siehe Fakt 5.1.

Bemerkung 14.
- Kenne ich nun als Hersteller des Verschlüsselungsverfahrens N und $\varphi(N)$, so kann ich den öffentlichen Schlüssel (e, N) und den geheimen Schlüssel (d, N) mit Hilfe von (2) erzeugen.
- Wir haben oben bereits geschrieben, dass es in der Regel schwierig ist $\varphi(N)$ zu berechnen. Da man aber, nachdem man einmal d erzeugt hat, $\varphi(N)$ nicht mehr benötigt, kann man diese Information löschen. Damit ist ein wichtiger Teil nicht mehr verfügbar, den man zur Rekonstruktion des (geheimen) Schlüssels (d, N) benötigt! Ein Angriff auf dieses Verfahren ist somit sehr schwierig, siehe Fakten 8.4 und 8.5.
- Aus dem gleichen Grund ist es auch nicht sinnvoll Primzahlen als Modus zu wählen, da dann $\varphi(p)$ leicht zu bestimmen ist.

Bemerkung 15. Um die Bestimmung von $\varphi(N)$ sehr schwer zu gestalten, die Berechenbarkeit selbst aber einfach, trifft man folgende Wahlen.

- Wähle zwei große Primzahlen p und q.

- Wähle $N = p \cdot q$.
- Damit ist $\varphi(N) = \varphi(p) \cdot \varphi(p) = (p-1)(q-1) = pq-(p+q)+1 = N+1-(p+q)$.

Die Rekonstruktion von p und q aus N und damit die Bestimmung von $\varphi(N)$ ist ein sehr schwieriges Problem, sodass ein Angriff auf das Verfahren, d. h. die Bestimmung von (d, N) aus (e, N), sehr schwierig ist.

3.2 Zur Lösung der Gleichung (2)

Die Bestimmung der Lösung von (2), also von

$$e \cdot x \equiv 1 \bmod \varphi(N)\,,$$

geschieht mit Hilfe des (erweiterten) Euklidischen Algorithmus aus Abschnitt 5, den man wie folgt zusammenfassen kann:

Satz 16. Sind a und b ganze Zahlen, dann gibt es ganze Zahlen k und ℓ, sodass $a \cdot k + b \cdot \ell = \mathrm{ggT}(a, b)$.

Wir wissen, dass e so gewählt werden muss, dass $\mathrm{ggT}(e, \varphi(N)) = 1$. Damit gibt es also ganze Zahlen k und ℓ, sodass

$$e \cdot k + \varphi(N) \cdot \ell = 1\,. \tag{3}$$

Damit ist dann

$$e \cdot k + \varphi(N) \cdot \ell \equiv e \cdot k \equiv 1 \bmod \varphi(N)$$

und $d = k$ ist eine Wahl für den Schlüssel zum Entschlüsseln.[3]

4 Beispiel für das RSA-Verfahren in $\mathbb{Z}_{221}$

Wir wählen $p = 13$ und $q = 17$ und somit $N = 13{\cdot}17 = 221$ und $\varphi(N) = 12{\cdot}16 = 192$.

Weiter wählen wir $e = 23$.[4]

Zur Bestimmung von d suchen wir zunächst k, ℓ, sodass

$$23 \cdot k + 192 \cdot \ell = 1$$

mit Hilfe des Euklidischen Algorithmus:

$$\begin{aligned} \underline{192} &= 8 \cdot \underline{23} + \underline{8} \\ \underline{23} &= 2 \cdot \underline{8} + \underline{7} \\ \underline{8} &= 1 \cdot \underline{7} + \boxed{1} \end{aligned}$$

[3] Liefert der Euklidische Algorithmus für k keinen Wert zwischen 1 und $\varphi(N) - 1$, so kann man ein beliebiges Vielfaches von $\varphi(N)$ zu k addieren oder subtrahieren, und d als diesen Wert wählen. Das ändert nichts an der Eigenschaft $e \cdot d \equiv 1 \bmod \varphi(N)$.

[4] Wegen $\varphi(N) = 192 = 2^6 \cdot 3$ und, da $e = 23$ eine Primzahl ist, sind e und $\varphi(N)$ teilerfremd

$$(\underline{7} = 7 \cdot \underline{1})$$

Zurückrechnen liefert

$$\begin{aligned}
\boxed{1} &= \underline{8} - 1 \cdot \underline{7} \\
&= \underline{8} - 1 \cdot (\underline{23} - 2 \cdot \underline{8}) \\
&= 3 \cdot \underline{8} - 1 \cdot \underline{23} \\
&= 3 \cdot (\underline{192} - 8 \cdot \underline{23}) - 1 \cdot \underline{23} \\
&= 3 \cdot \underline{192} - 25 \cdot \underline{23}
\end{aligned}$$

und damit

$$k = -25 \quad \text{und} \quad \ell = 3\,.$$

Wir haben also

$$d = -25 + 192 = 167$$

und machen die Probe:

$$e \cdot d \equiv 23 \cdot 167 \equiv 3841 \equiv 20 \cdot 192 + 1 \equiv 1 \bmod 192\,.$$

Unser öffentlicher Schlüssel ist nun $(23, 221)$ und der geheime Schlüssel zum Decodieren ist $(167, 221)$.

Wir verschlüsseln damit wieder die Nachricht 'AHBZ' aus dem Babybeispiel:

$$\begin{aligned}
\mathrm{A} = 1 &\longmapsto 1^{23} \equiv 1 \bmod 221 \\
\mathrm{B} = 2 &\longmapsto 2^{23} \equiv 8 \cdot (2^{10})^2 \equiv 8 \cdot 140^2 \equiv 8 \cdot 4 \cdot 70^2 \equiv 8 \cdot 4 \cdot 38 \equiv 111 \bmod 221 \\
\mathrm{H} = 8 &\longmapsto 8^{23} \equiv (2^{23})^3 \equiv 111^3 \equiv 111 \cdot 111^2 \equiv 111 \cdot 166 \equiv 83 \bmod 221 \\
\mathrm{Z} = 26 &\longmapsto 26^{23} \equiv 2^{23} \cdot 13^{23} \equiv 111 \cdot 13^2 \cdot (13^3)^7 \equiv 111 \cdot 13^2 \cdot (-13)^7 \\
&\qquad \equiv -111 \cdot (13^3)^3 \equiv -111 \cdot (-13)^3 \equiv -111 \cdot 13 \equiv 104 \bmod 221
\end{aligned}$$

Damit ist der verschlüsselte Text:

$$\mathrm{AHBZ} = 1, 8, 2, 26 \longmapsto 1, 83, 111, 104$$

Zum Decodieren müssen wir nun Folgendes berechnen:[5]

$$\begin{aligned}
1^{167} &\equiv 1 \bmod 221 \\
83^{167} &\equiv 83^5 \cdot (83^1 8)^9 \equiv 83^5 \cdot 38^9 \equiv 83^5 \cdot 38 \equiv 38 \cdot ((83)^2)^2 \cdot 83 \equiv 38 \cdot 38^2 \cdot 83 \\
&\equiv 38^3 \cdot 83 \equiv 64 \cdot 83 \equiv 8 \bmod 221 \\
111^{167} &\equiv 111^2 \cdot (111^3)^{55} \equiv 111^2 \cdot (83)^{55} \equiv 111^2 \cdot 83 \cdot (83^{18})^3 \equiv 111^2 \cdot 83 \cdot 38^3 \\
&\equiv 111^2 \cdot 8 \equiv 166 \cdot 8 \equiv 2 \bmod 221 \\
104^{167} &\equiv (8 \cdot 13)^{167} \equiv 2^{501} \cdot 13^{167} \equiv (2^{24})^{20} \cdot 2^{20} \cdot 2 \cdot (13^{23})^7 \cdot (13^3)^2 \\
&\equiv 152 \cdot 2 \cdot (-13)^7 \cdot (-13)^2 \equiv -83 \cdot (13^3)^3 \equiv 83 \cdot 13^3 \equiv -83 \cdot 13 \equiv 26 \bmod 221
\end{aligned}$$

Der decodierte Text ist damit

$$1, 8, 2, 26 = \mathrm{AHBZ}\,.$$

[5] Wir wollen Euler nicht benutzen, da wir $\varphi(221)$ 'nicht kennen'. Aber wir nutzen die vorigen Rechnungen und z. B. $2^{24} \equiv 2^{23} \cdot 2 \equiv 111 \cdot 2 \equiv 222 \equiv 1 \bmod 221$

5 Euklidischer Algorithmus

Der Euklidische Algorithmus liefert einem für zwei positive, ganze Zahlen a, b den $\mathrm{ggT}(a, b)$ dieser zwei Zahlen. Das Schema des Algorithmus verläuft wie folgt

$$
\begin{array}{lllllllll}
(1) & \underline{b} & = & k_1 & \cdot & \underline{a} & + & \underline{r_1} \\
(2) & \underline{a} & = & k_2 & \cdot & \underline{r_1} & + & \underline{r_2} \\
(3) & \underline{r_1} & = & k_3 & \cdot & \underline{r_2} & + & \underline{r_3} \\
 & \vdots & & & & & & \\
(m-1) & \underline{r_{m-3}} & = & k_{m-1} & \cdot & \underline{r_{m-2}} & + & \underline{r_{m-1}} \\
(m) & \underline{r_{m-2}} & = & k_m & \cdot & \underline{r_{m-1}} & + & \boxed{r_m} \\
(m+1) & \underline{r_{m-1}} & = & k_{m+1} & \cdot & \underline{r_m} & &
\end{array}
$$

- Schritt 1: Wir stellen b als Vielfaches von a mit Rest dar: Rest ist r_1
- Schritt 2: Wir stellen a als Vielfaches von r_1 mit Rest dar: Rest ist r_2
- Schritt 2: Wir stellen r_1 als Vielfaches von r_2 mit Rest dar: Rest ist r_3
- Wir wiederholen dies so lange, bis es keinen Rest mehr gibt (das klappt, da in jedem Schritt der positive Rest kleiner wird)
- Im vorletzten $m$ten Schritt hat man dann als Rest den $\mathrm{ggT}(a, b)$ stehen

Um jetzt die Darstellung

$$a \cdot k + b \cdot \ell = \mathrm{ggT}(a, b)$$

aus Satz 16 zu erhalten gehen wir wie folgt vor:

- Wir lösen die ersten m Gleichungen des Algorithmus nach dem Rest auf
- Wir ersetzen in der $m$ten Gleichung r_{m-1} durch die nach r_{m-1} aufgelöste $(m-1)$te Gleichung
- Wir ersetzen in der erhaltenen Gleichung r_{m-2} durch die nach r_{m-2} aufgelöste $(m-2)$te Gleichung
- damit fahren wir fort, bis wir die nach r_1 aufgelöste erste Gleichung eingesetzt haben. Dann sind wir fertig!

Ein Beispiel hatten wir bereit in Abschnitt 4 gesehen. Ein weiteres folgt nun:

Beispiel 17. Wir starten mit $a = 158$ und $b = 288$ und berechnen $\mathrm{ggT}(158, 288)$ mit dem euklidischen Algorithmus

$$\begin{aligned}
\underline{288} &= 1 \cdot \underline{158} + \underline{130} \\
\underline{158} &= 1 \cdot \underline{130} + \underline{28} \\
\underline{130} &= 4 \cdot \underline{28} + \underline{18} \\
\underline{28} &= 1 \cdot \underline{18} + \underline{10} \\
\underline{18} &= 1 \cdot \underline{10} + \underline{8} \\
\underline{10} &= 1 \cdot \underline{8} + \boxed{2} \\
\underline{8} &= 4 \cdot \underline{2}
\end{aligned}$$

Um $\mathrm{ggT}(158, 288)$ nun als Kombination von 158 und 288 darzustellen, setzen wir von unten beginnend die Reste rückwärts ein:

$$\begin{aligned}
\underline{2} &= \underline{10} - 1 \cdot \underline{8} \\
&= \underline{10} - 1 \cdot (\underline{18} - 1 \cdot \underline{10}) \\
&= -\underline{18} + 2 \cdot \underline{10} \\
&= -\underline{18} + 2 \cdot (\underline{28} - 1 \cdot \underline{18}) \\
&= 2 \cdot \underline{28} - 3 \cdot \underline{18} \\
&= 2 \cdot \underline{28} - 3 \cdot (\underline{130} - 4 \cdot \underline{28}) \\
&= -3 \cdot \underline{130} + 14 \cdot \underline{28} \\
&= -3 \cdot \underline{130} + 14 \cdot (\underline{158} - 1 \cdot \underline{130}) \\
&= 14 \cdot \underline{158} - 17 \cdot \underline{130} \\
&= 14 \cdot \underline{158} - 17 \cdot (\underline{288} - 1 \cdot \underline{158}) \\
&= -17 \cdot \underline{288} + 31 \cdot \underline{158}
\end{aligned}$$

Wir haben somit schließlich

$$\mathrm{ggT}(2, 88, 158) = 2 = 31 \cdot 158 - 17 \cdot 288\,.$$