Frank Klinker

Zahlentheorie

Teil 3: 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 Alphabet in Zahlen, zum Beispiel A = 1, B = 2, ..., Z = 26.

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

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

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

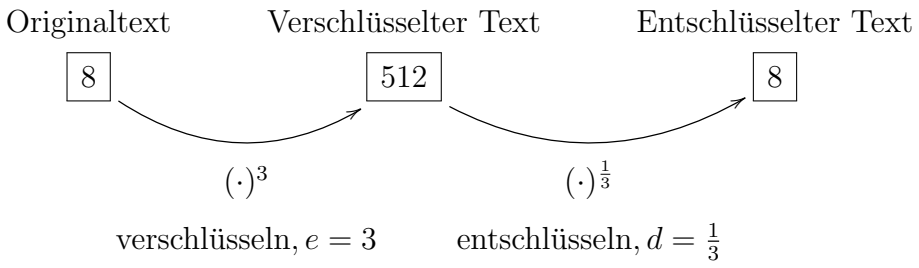
Damit lautet der verschlüsselte Text

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

Wie entschlüsselt man nun den codierten Text?

Das ist hier recht einfach, da man lediglich eine Wurzel ziehen muss, und zwar die dritte Wurzel. Das lässt sich auch mit Hilfe von Potenzieren formulieren:

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



Adresse: Eduard-Spranger-Berufskolleg, 59067 Hamm
E-Mail: mail@frank-klinker.de
Version: 28. Mai 2024
[1] e: encrypt (verschlüsseln), d: decrypt (entschlüsseln)

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

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

- 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 Text 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:

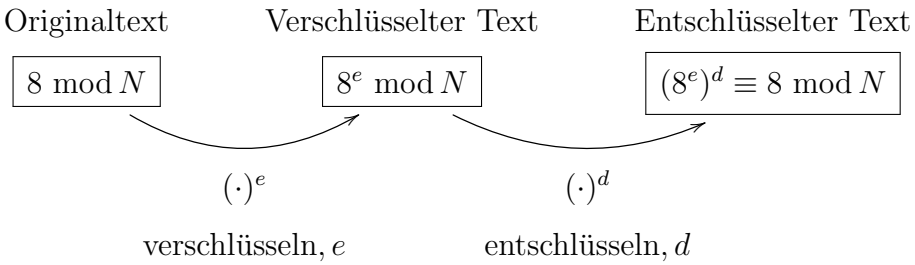
Rechnen über den reellen Zahlen $\mathbb{R}$ ist zu einfach

2 RSA-Verfahren über $\mathbb{Z}_N$

Statt über den reellen Zahlen zu rechnen, verwenden wir als Zahlenmenge die **Restklassenmenge** $\mathbb{Z}_N$ der Reste beim Teilen durch die positive ganze Zahl N:

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

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 nötig.
- Dass heißt der Schlüssel zum Verschlüsseln ist (e, N) und der zum Entschlüsseln ist (d, N)

2.1 Erzeugen 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 2. 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 $\mathrm{ggT}(e, \varphi(N)) = 1$.

Bemerkung 3.

- 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 wissen bereits, 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.

- Aus dem gleichen Grund ist es auch nicht sinnvoll Primzahlen als Modus zu wählen, da dann $\varphi(N)$ leicht zu bestimmen ist.

Bemerkung 4. Um die Bestimmung von $\varphi(N)$ sehr schwer zu gestalten, die Berechenbarkeit selbst aber verhältnismäßig 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.

2.2 Zur Lösung der Gleichung $e \cdot x \equiv 1 \bmod \varphi(N)$

Die Bestimmung der Lösung von (2), also von

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

geschieht mit Hilfe des erweiterten Euklidischen Algorithmus:

> 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 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.[2]

3 Beispiel: 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 $e = 23$.[3]
Zur Bestimmung von d suchen wir zunächst Zahlen k und ℓ, sodass

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

Das machen wir mit dem euklidischen Algorithmus:

$$\begin{array}{|rcl|rcl|}
\hline
\underline{192} = 8 \cdot \underline{23} + \underline{8} & \to & & \underline{8} = \underline{192} - 8 \cdot \underline{23} \\
\underline{23} = 2 \cdot \underline{8} + \underline{7} & \to & & \underline{7} = \underline{23} - 2 \cdot \underline{8} \\
 & & & = \underline{23} - 2 \cdot (\underline{192} - 8 \cdot \underline{23}) \\
 & & & = 17 \cdot \underline{23} - 2 \cdot \underline{192} \\
\underline{8} = 1 \cdot \underline{7} + \boxed{1} & \to & \boxed{1} & = \underline{8} - \underline{7} \\
 & & & = (\underline{192} - 8 \cdot \underline{23}) - (17 \cdot \underline{23} - 2 \cdot \underline{192}) \\
 & & & = 3 \cdot \underline{192} - 25 \cdot \underline{23} \\
\underline{7} = 7 \cdot \underline{1} & & & \\
\hline
\end{array}$$

[2] 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 $e \cdot d \equiv 1 \bmod \varphi(N)$.

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

Das gibt uns

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

Wir wählen damit

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

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:

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

Damit ist der verschlüsselte Text:

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

Zum Decodieren müssen wir nun Folgendes berechnen:[4]

$$\begin{aligned}
1^{167} &\equiv 1 \bmod 221\\
83^{167} &\equiv (83^8)^{20} \cdot (83^2)^3 \cdot 83 \equiv 38^3 \cdot 83 \equiv 64 \cdot 83 \equiv 8 \bmod 221\\
111^{167} &\equiv 111^2 \cdot (111^3)^{55} \equiv 111^2 \cdot (83)^{55} \equiv 111^2 \cdot 83 \cdot (83^{16} \cdot 83^2)^3 \equiv 111^2 \cdot 83 \cdot 38^3\\
&\equiv 111^2 \cdot 83 \cdot 64 \equiv 111^2 \cdot 8 \equiv 166 \cdot 8 \equiv 2 \bmod 221\\
104^{167} &\equiv (8 \cdot 13)^{167} \equiv (2^{24})^{20} \cdot 2^{20} \cdot 2 \cdot (13^{23})^7 \cdot (13^3)^2 \equiv 152 \cdot 2 \cdot (-13)^7 \cdot (-13)^2\\
&\equiv -83 \cdot (13^3)^3 \equiv 83 \cdot 13^3 \equiv -83 \cdot 13 \equiv 26 \bmod 221
\end{aligned}$$

Der decodierte Text ist damit

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

[4] Wir wollen Euler nicht benutzen, da wir $\varphi(221)$ "nicht kennen". Aber wir nutzen die vorigen Rechnungen und z. B. $2^{24} \equiv 2^{23} \cdot 2 \equiv 111 \cdot 2 \equiv 222 \equiv 1 \bmod 221$, $38^4 \equiv 38^2 \cdot 38^2 \equiv 118^2 \equiv 1 \bmod 221$ oder $83^2 \equiv 38 \bmod 221$