

RSA-Verfahren

– Lösungshinweis –

Das RSA-Verfahren, benannt nach deren Entwicklern R. Rivest, A. Shamir und L. Adleman, zählt zu den asymmetrischen Verschlüsselungsverfahren. Asymmetrisch bedeutet dabei, dass zwei verschiedene „Schlüssel“ zum Ver- und Entschlüsseln einer Nachricht benutzt werden. In diesem Zusammenhang sind Schlüssel Methoden bzw. Algorithmen, um eine Nachricht entweder in eine verschlüsselte Form zu überführen oder aus dieser wieder lesbar zu machen. Da es sich beim RSA-Verfahren um ein mathematisches Verfahren handelt, wird jede Art von Nachricht als Zahl kodiert.

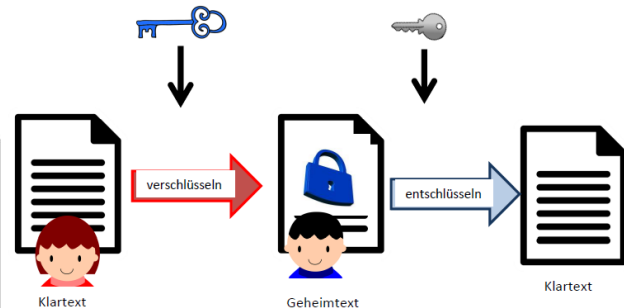


Abbildung 1: Schema des RSA-Verfahrens mit public key (blau) und secret key (grau).



Wie funktioniert das RSA-Verfahren und wie sicher ist es?

Aufgabe 1: Um die Funktionsweise des RSA-Verfahrens zu verstehen, wollen wir den Algorithmus an einem Zahlenbeispiel durchgehen.

- Generieren Sie einen öffentlichen Schlüssel (e, n) und einen privaten Schlüssel d zu den beiden Primzahlen $p = 13$ und $q = 17$. Begründen Sie Ihre Wahl der Komponenten e des öffentlichen Schlüssels.
- Bestimmen Sie nachvollziehbar, wie viele Möglichkeiten es für die Komponente e des öffentlichen Schlüssels gibt.

Aufgabe 1a)

Mit den beiden Primzahlen ist $n = pq = 13 \cdot 17 = 221$ und $\varphi(n) = (p - 1) \cdot (q - 1) = 12 \cdot 16 = 192$. Wähle z.B. für $e = 35$.

Begründung: Die PFZ von 35 ist $35 = 5 \cdot 7$. Da sowohl $5 \nmid 192$ als auch $7 \nmid 192$ gilt, haben 35 und 221 keinen gemeinsamen Teiler größer als 1 und somit gilt $\text{ggT}(35, 192) = 1$.

Mit Hilfe des erweiterten euklidischen Algorithmus bestimmt man d :

- I. $192 = 5 \cdot 35 + 17$
- II. $35 = 2 \cdot 17 + 1$
- III. $17 = 17 \cdot 1 + 0$
- IV. $2 = 2 \cdot 1 + 0$

Damit ist dann $1 \stackrel{\text{III.}}{\equiv} 35 - 2 \cdot 17 \stackrel{\text{II.}}{\equiv} 35 - 2 \cdot (192 - 5 \cdot 35) \stackrel{\text{I.}}{\equiv}$
 $(221 - 3 \cdot 85) - 20 \cdot (85 - (336 - 3 \cdot 85)) = -2 \cdot 192 + 11 \cdot 35$

Zusatzinformation: Vorzeichen beachten! Hat der Koeffizient vor e ein **negatives Vorzeichen**, so muss ein der positive Repräsentant der Restklasse gewählt werden, der kleiner als der Modul ist.
 Bsp.: $d = -181 \equiv -181 + 192 \equiv 11 \pmod{192}$.

Betrachtet man die Gleichung modulo $\varphi(n) = 192$, dann ist $d = 11 \bmod 336$.

Insgesamt ist der öffentliche Schlüssel $(e, n) = (35, 221)$ und der private Schlüssel $d = 11$.

Aufgabe 1b)

Für die Komponente e des öffentlichen Schlüssels gilt, dass es sich um eine natürliche Zahl kleiner als $\varphi(n) = 192$ handeln muss mit $\text{ggT}(e, \varphi(n)) = \text{ggT}(e, 192) = 1$ („teilerfremd“).

Dies sind genau $\varphi(192)$ viele natürliche Zahlen. Um diesen Ausdruck zu berechnen, benötigt man zunächst die PFZ von 192.

Zusatzinformation: Diese lässt sich entweder iterativ durch Dividieren mit geeigneten Primteilern oder mittels eines digitalen Werkzeugs bestimmen.

Es ist $192 = 2^6 \cdot 3$. Mit Hilfe der Rechenregeln für die Eulersche Phi-Funktion erhält man

$$\varphi(192) = \varphi(2^6 \cdot 3) = \varphi(2^6) \cdot \varphi(3) = (2^6 - 2^5) \cdot 2 = 64.$$

Somit existieren 64 Möglichkeiten, um e zu wählen.

Aufgabe 2: Im Folgenden sollen nun mittels des öffentlichen und privaten Schlüssels (aus Aufgabe 1) Nachrichten – kodiert als natürliche Zahlen – verschlüsselt und entschlüsselt werden.

Hinweis: Nutzen Sie für die Modulo-Rechnungen die bereitgestellten digitalen Medien.

- Wählen Sie (geheim!) eine natürliche Zahl N , die als geheime Botschaft fungiert. Verschlüsseln Sie diese Nachricht mittels des öffentlichen Schlüssels (e, n) .
- Entschlüsseln Sie die verschlüsselte Nachricht mit dem geheimen Schlüssel d .
- An welchen Stellen gehen beim Verfahren die Informationen des öffentlichen Schlüssels ein?

Zusatzinformation: In dieser Aufgabe wird sowohl die Aktivität des Verschlüsselns als auch Entschlüsselns durchgeführt, was in Realität natürlich nicht dieselbe Person ist. Dies dient zunächst dem Verständnis des Verfahrens.

Für die Ver- und Entschlüsselung stehen bspw. ein GeoGebra-Applet oder die Webseite „WolframAlpha“ zur Verfügung.

Aufgabe 2a)

Wählt man z.B. $N = 3$, so ist die verschlüsselte Nachricht $V = N^e = 3^{35} \equiv 61 \bmod 221$. Diese kann nun öffentlich geteilt werden.

Aufgabe 2b)

Um die Nachricht zu entschlüsseln, berechnet man $V^d = 61^{11} \equiv 3 \bmod 221$. Die geheime Nachricht und die entschlüsselte Nachricht stimmen überein.

Aufgabe 2c)

Die Komponente e benötigt man (als Exponent), um die geheime Nachricht zu verschlüsseln. Die Komponente n benötigt man erstens zur Wahl der geheimen Nachricht (es muss $N < n$ gelten) und zweitens als Modul in der Ver- und Entschlüsselung.

Aufgabe 3: Im Folgenden soll die Sicherheit des RSA-Verfahrens näher untersucht werden.

- a. Arbeiten Sie dazu in einer Dreiergruppe und nehmen Sie die Rollen von Alice, Bob und Charlie ein¹.

Bob: Wählen Sie (geheim) zwei Primzahlen kleiner als 30, generieren Sie einen öffentlichen Schlüssel (e, n) sowie einen geheimen Schlüssel d .

Alice: Verschlüsseln Sie damit eine geheime Nachricht.

Charlie: Können Sie anhand des öffentlichen Schlüssels und der verschlüsselten Nachricht die geheime Nachricht entschlüsseln? Beschreiben und begründen Sie Ihr Vorgehen.

- b. Für welche Primzahlen p und q sowie Komponenten e war es für Charlie schwieriger die Nachricht zu „knacken“?

Zusatzinformation: In dieser Aufgabe dürfen/sollen digitale Werkzeuge genutzt werden!

Aufgabe 3a)

Bob: Wähle exemplarisch $p = 17$ und $q = 29$. Dann ist $n = pq = 493$ und $\varphi(n) = (p - 1)(q - 1) = 16 \cdot 28 = 448$. Als Komponente e kann man bspw. $e = 5$ wählen, da $\text{ggT}(5, 448) = 1$ gilt. Der geheime Schlüssel ist $d = 269$

Alice: Die geheime Nachricht N sei 123. Dann ist $V = N^e = 123^5 \equiv 480 \pmod{493}$.

Charlie: Zur Verfügung stehen $(e, d) = (5, 493)$ sowie $V = 480$.

Eine Herangehensweise kann es sein, eine natürliche Zahl (kleiner 493) durch **Ausprobieren** zu suchen, die die Bedingung $N^5 \equiv 480 \pmod{493}$ erfüllt. Aber schon bei diesem Beispiel zeigt sich, dass dies nicht praktikabel ist. Um die entschlüsselte Nachricht zu bestimmen, wird daher der Schlüssel d benötigt.

Man weiß, dass $ed \equiv 1 \pmod{\varphi(n)}$ gilt und könnte mit dem erweiterten euklidischen Algorithmus d bestimmen, sofern $\varphi(n)$ bekannt ist. Daher muss nun $\varphi(n)$ aus n bestimmt werden. Hierfür benötigt man die PFZ von n , die nach Voraussetzung des RSA-Verfahrens aus zwei Primzahlen besteht. Mögliche Vorgehensweisen:

- Testen von n auf Teilbarkeit durch verschiedene Primzahlen.
- Multiplikation verschiedener Primzahlen bis n „getroffen“ wird (vgl. GeoGebra Applet).

In diesem Fall kann man $n = 17 \cdot 29$ und damit $\varphi(n) = 448$ bestimmen und somit $d = 269$. Damit bestimmt man die geheime Nachricht: $480^{269} \equiv 123 \pmod{493}$.

Aufgabe 3b)

Die Schwierigkeit hängt im Wesentlichen davon ab, wie schnell man die PFZ der Zahl n bestimmen kann. Dies ist umso schwerer, je größer die gewählten Primzahlen sind. Zudem sollten die gewählten Primzahlen unterschiedlich sein, da n ansonsten eine Quadratzahl ist und sich deren Wurzel (verhältnismäßig) leicht bestimmen lässt.

Des Weiteren sollte die Komponente e nicht zu klein gewählt werden, da ansonsten Rückschlüsse auf die geheime Nachricht durch Ausprobieren möglich sind.

¹ Dies sind die Bezeichnungen der Kryptographie für Sender, Empfänger und Dritte, unbefugte Person, die versucht die Nachricht zu entschlüsseln.