

RSA-Verfahren – Lösungen

1. Verschlüsseln

Man benötigt zwei (große) Primzahlen p und q , die man multipliziert, um die Zahl N zu erhalten. Außerdem benötigt man eine Verschlüsselungszahl e (*encipher = verschlüsseln*). Dafür kann man fast jede Zahl nehmen. Sie muss nur kleiner als n und teilerfremd zu $(p - 1)(q - 1)$ sein.

Beide Zahlen sind öffentlich.

Wenn man die Zahl M (*Message*) verschlüsseln will, berechnet man die Zahl C (*Cipher*) durch

$$C = M^e \pmod{N}$$

Beispiel:

Nimm $p = 11$ und $q = 17$, dann ist $N = p \cdot q = 187$.

Für e nimm die Zahl 7.

Verschlüssele nun die Zahl $M = 59$.

Dann ist $C = 59^7 \equiv 59^4 \cdot 59^3 \equiv 135 \cdot 53 = 7155 \equiv 49 \pmod{187}$.

Verschlüssele weitere Zahlen mit diesem Schlüssel. Diese müssen kleiner als 187 sein.

2. Entschlüsseln

Hier benötigt man die (geheime) Entschlüsselungszahl d (*decipher = entschlüsseln*). (Was für Eigenschaften diese haben muss, steht unter 3.)

Wenn man die Zahl C entschlüsseln will, berechnet man

$$M = C^d \pmod{N}$$

Beispiel:

Hier ist $d = 23$.

Entschlüssele damit die Zahlen, die dein Nachbar verschlüsselt hat.

$49^{23} = (49^3)^7 \cdot 49^2 \equiv 104 \cdot 157 = 16328 \equiv 59 \pmod{187}$

Was ist, wenn man Zahlen verschlüsselt, die größer als 187 sind?

3. Eigenschaft der Zahl d

Die Entschlüsselungszahl d muss folgende Eigenschaft haben:

$$e \cdot d \equiv 1 \pmod{(p - 1) \cdot (q - 1)},$$

d.h. modulo der Zahl $(p - 1) \cdot (q - 1)$ muss $e \cdot d \equiv 1$ sein.

Beispiel:

Überprüfe, ob dies für die Zahlen aus unserem Beispiel erfüllt ist.

Ein anderes Beispiel: $p = 3$, $q = 11$, also $N = 33$.

Es soll $e = 7$ gewählt werden.

Suche eine Zahl d , die die geforderte Eigenschaft erfüllt. 3

Wenn p und q groß sind, kann man d nicht mehr so einfach durch Probieren finden. Es gibt aber ein Verfahren, mit dem man d schnell bestimmen kann, wenn p und q sowie e bekannt sind.

4. Warum funktioniert das entschlüsseln?

Die verschlüsselte Nachricht ist $C = M^e \pmod{N}$

Das Entschlüsseln funktioniert also, wenn $C^d \equiv M \pmod{N}$ ist.

Nach den Potenzgesetzen ist $C^d = (M^e)^d = M^{e \cdot d}$.

Behauptung: $M^{e \cdot d} \equiv M \pmod{N}$

Beweis: Die Zahlen e und d sind so gewählt, dass

$$e \cdot d \equiv 1 \pmod{(p-1) \cdot (q-1)}$$

Also gibt es eine Zahl k , so dass $e \cdot d = k \cdot ((p-1) \cdot (q-1)) + 1$.

Folglich ist $M^{e \cdot d} = M^{k \cdot ((p-1) \cdot (q-1)) + 1} = M^{k \cdot ((p-1) \cdot (q-1)) + 1} \cdot M = (M^{(p-1)})^{k \cdot (q-1)} \cdot M$.

Nach dem kleinen Satz von Fermat ist $M^{p-1} \equiv 1 \pmod{p}$.

Damit: $M^{e \cdot d} - M = (M^{(p-1)})^{k \cdot (q-1)} \cdot M - M \equiv 1^{k \cdot (q-1)} \cdot M - M \equiv M - M \equiv 0 \pmod{p}$.

Genauso ist nach dem kleinen Satz von Fermat: $M^{q-1} \equiv 1 \pmod{q}$.

Damit $M^{e \cdot d} - M = (M^{(q-1)})^{k \cdot (p-1)} \cdot M - M \equiv 1^{k \cdot (p-1)} \cdot M - M \equiv M - M \equiv 0 \pmod{q}$.

Die Primzahlen p und q teilen also beide die Zahl $M^{e \cdot d} - M$. Da p und q Primzahlen sind, folgt daraus, dass auch $p \cdot q$ die Zahl $M^{e \cdot d} - M$ teilt.

Also ist $M^{e \cdot d} - M \equiv 0 \pmod{N}$ oder anders ausgedrückt $M^{e \cdot d} \equiv M \pmod{N}$.

q.e.d.

5. Warum ist das RSA-Verfahren sicher?

Öffentlich sind nur die Zahlen N und e , die Zahl d ist geheim. N ist das Produkt zweier Primzahlen $N = p \cdot q$. Wenn man p und q kennt, kann man d schnell berechnen.

Aber für große Zahlen ist es praktisch unmöglich, N in seine beiden Primfaktoren zu zerlegen. Und ohne p und q zu kennen, kann man d nicht bestimmen.