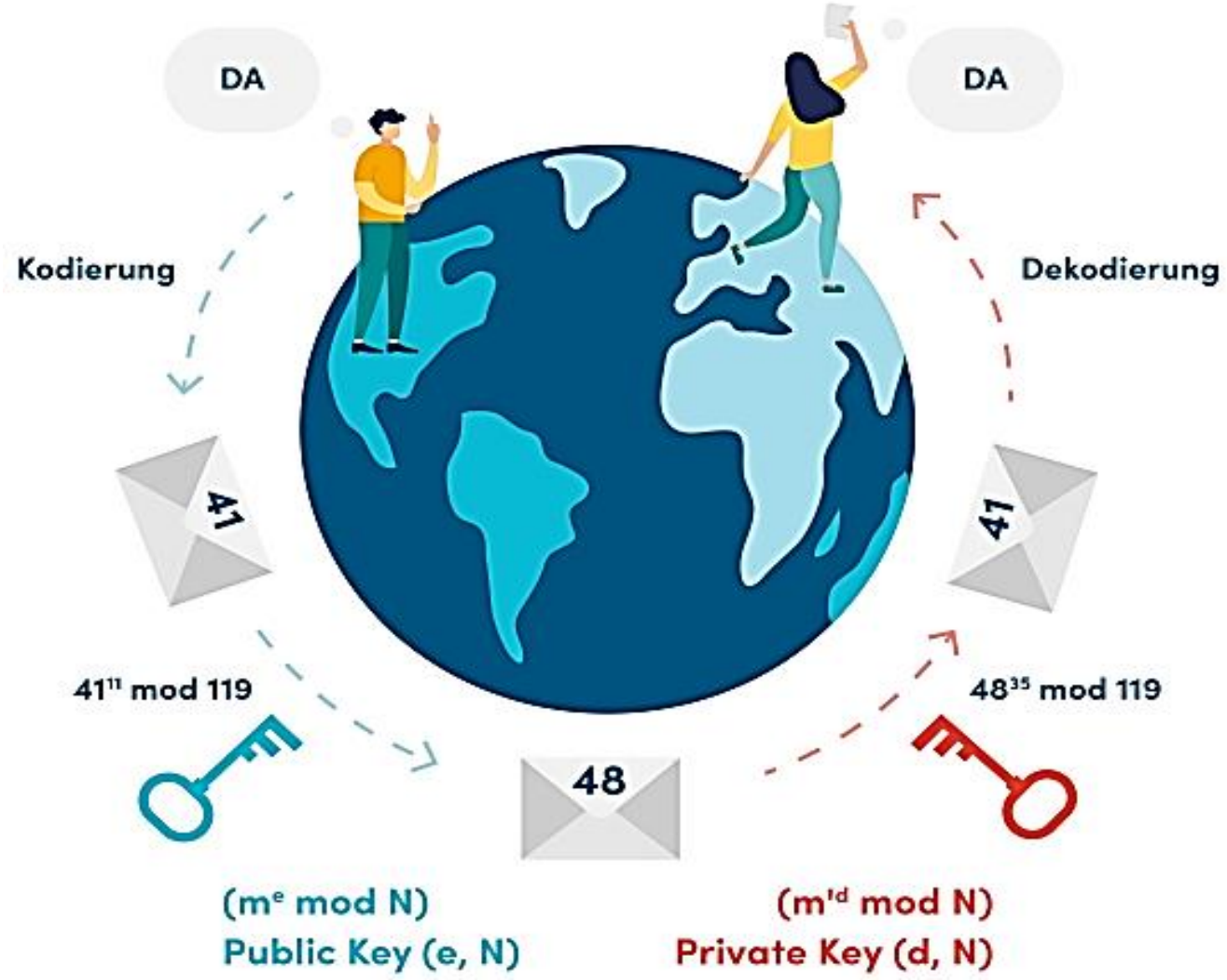
RSA- Verfahren



Asymmetrischer Schlüssel - RSA

Das RSA Verfahren *(mit kleinen Beispielwerten)*

1. **Wähle p und q zwei große Primzahlen.**

Berechne N = p · q.

Nächste Seite geht es weiter!

Asymmetrischer Schlüssel - RSA

Das RSA Verfahren *(mit kleinen Beispielwerten)*

1. **Wähle p und q zwei große Primzahlen.** *11 und 17*

Berechne N = p · q. $N = 11 \cdot 17 = 187$

Nächste Seite geht es weiter!

Asymmetrischer Schlüssel - RSA

Das RSA Verfahren *(mit kleinen Beispielwerten)*

1. **Wähle p und q zwei große Primzahlen.** *11 und 17*

   Berechne N = p · q. *N = 11 · 17 = 187*

2. **öffentlicher Schlüssel zum Chiffrieren: (e, N)**

   Wähle e. Eine ungerade Zahl mit 1 < **e < N** und teilerfremd zu **z = (p - 1) · (q - 1)**

Nächste Seite geht es weiter!

Asymmetrischer Schlüssel - RSA

Das RSA Verfahren *(mit kleinen Beispielwerten)*

1. **Wähle p und q zwei große Primzahlen.** *11 und 17*

   Berechne N = p · q. *N = 11 · 17 = 187*

2. **öffentlicher Schlüssel zum Chiffrieren: (e, N)**

   Wähle e. Eine ungerade Zahl mit 1 < **e < N** und teilerfremd zu **z = (p - 1) · (q - 1)**

   (11 – 1) · (17 – 1) = 160 → z. B. e = 7,
   weil 7 < 187 und 7 ∤ 160

Nächste Seite geht es weiter!

Asymmetrischer Schlüssel - RSA

Was bisher geschah...

p = 11, q = 17, z = 160
N = 187, e = 7 (öffentlich)

3 **geheimer Schlüssel zum Dechiffrieren: (d; N)**

Bestimme ein **d**, so das gilt:

$$e \cdot d \bmod z \equiv 1$$

Asymmetrischer Schlüssel - RSA

Was bisher geschah...

p = 11, q = 17, z = 160

N = 187, e = 7 (öffentlich)

3 **geheimer Schlüssel zum Dechiffrieren: (d; N)**

Bestimme ein **d**, so das gilt:

$$e \cdot d \bmod z \equiv 1$$

161 mod 160 ≡ 1

Asymmetrischer Schlüssel - RSA

Was bisher geschah...

p = 11, q = 17, z = 160
N = 187, e = 7 (öffentlich)

3 **geheimer Schlüssel zum Dechiffrieren: (d; N)**

Bestimme ein **d**, so das gilt:

$$e \cdot d \bmod z \equiv 1$$

161 mod 160 ≡ 1 → *161 : 7 = 23*
→ *(7 · 23) mod 160 ≡ 1*
→ *d = 23*

Asymmetrischer Schlüssel - RSA

Was bisher geschah...

p = 11, q = 17, z = 160
N = 187, e = 7 (öffentlich)

3 **geheimer Schlüssel zum Dechiffrieren: (d; N)**

Bestimme ein **d**, so das gilt:

$$e \cdot d \bmod z \equiv 1$$

$161 \bmod 160 \equiv 1$ → $161 : 7 = 23$
→ $(7 \cdot 23) \bmod 160 \equiv 1$
→ $d = 23$

N = 187, d = 23 (privat)

Es ist kein direkter Zusammenhang zwischen e, d und N erkennbar.

Asymmetrischer Schlüssel - RSA

Ein Zeichen (z.B. Buchstaben) der Nachricht kann nun verschlüsselt und entschlüsselt werden.

e, N ist der **öffentlichen RSA-Schlüssel.**
d, N ist der **private RSA-Schlüssel.**

Verschlüsseln
$V \equiv K^{e} \bmod N$

Entschlüsseln
$K \equiv V^{d} \bmod N$

Asymmetrischer Schlüssel - RSA

Ein Zeichen (z.B. Buchstaben) der Nachricht kann nun verschlüsselt und entschlüsselt werden.

e, N ist der **öffentlichen RSA-Schlüssel.**
d, N ist der **private RSA-Schlüssel.**

Verschlüsseln
$V \equiv K^{e} \bmod N$

Entschlüsseln
$K \equiv V^{d} \bmod N$

$N = 187,\ e = 7,\ d = 23$

H (-> 72): $72^{7} \bmod 187 \equiv 30$

A (-> 65): $65^{7} \bmod 187 \equiv 142$

Asymmetrischer Schlüssel - RSA

Ein Zeichen (z.B. Buchstaben) der Nachricht kann nun verschlüsselt und entschlüsselt werden.

e, N ist der **öffentlichen RSA-Schlüssel.**
d, N ist der **private RSA-Schlüssel.**

Verschlüsseln
$V \equiv K^{e} \bmod N$

Entschlüsseln
$K \equiv V^{d} \bmod N$

$N = 187,\ e = 7,\ d = 23$

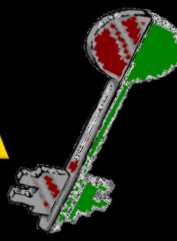
$H\ (\rightarrow 72)$: $72^{7} \bmod 187 \equiv 30$

$30^{23} \bmod 187 \equiv 72\ (\rightarrow H)$

$A\ (\rightarrow 65)$: $65^{7} \bmod 187 \equiv 142$

$142^{23} \bmod 187 \equiv 65\ (\rightarrow A)$

Asymmetrischer Schlüssel -RSA



Das RSA-Verfahren – Anwendung

• wird nicht für komplette Datenverschlüsselung genutzt, weil es sonst zu lange dauert, sondern der Algorithmus wird meist nur zum Verschlüsseln von Schlüsseln verwendet.
Man kombiniert RSA mit einem symmetrischen Verfahren, mit RSA wird dann nur der Schlüssel verschlüsselt.

• RSA-Verschlüsselung bei PINs

• Internetverbindungen via SSL