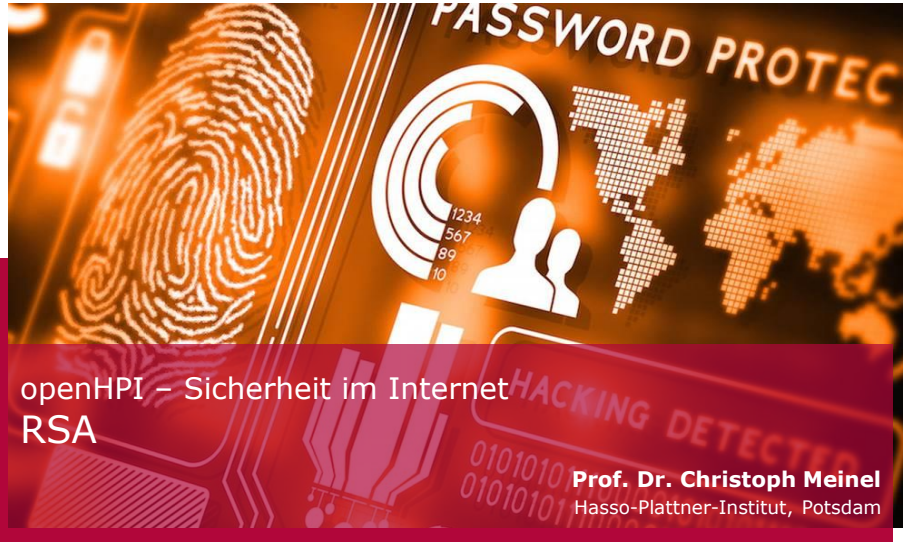




openHPI – Sicherheit im Internet  
RSA

Prof. Dr. Christoph Meinel  
Hasso-Plattner-Institut, Potsdam

## RSA – Populärste 2-Schlüssel Verschlüsselung (1/6)

**RSA-Verschlüsselung** ist das berühmteste und am weitesten verbreitete 2-Schlüssel Verschlüsselungsverfahren

- Entwickelt 1977 von Ron **R**ivest, Adi **S**hamir und Leonard **A**dleman
- RSA basiert auf praktisch (also in realistischer Zeit) unlösbarem mathematischen Problem der **Faktorisierung**:
  - Produkt zweier sehr großer, zufällig ausgewählter Primzahlen lässt sich ohne Kenntnis der beiden Zahlen praktisch (also in realistischer Zeit) nicht faktorisieren ...

## RSA – Populärste 2-Schlüssel Verschlüsselung (2/6)

**RSA-Verfahren:** (Zahlenbeispiel mit kleinen Zahlen)

**Ausgangspunkt:**

1. Wahl zweier Primzahlen, z.B.  $p = 17$  und  $q = 31$
2. Berechnung des Produktes:
  - $N = p * q$
  - Zahlenbeispiel:  $N = 17 * 31 = 527$
3. Berechnung der sogenannten Eulerschen Phi-Funktion:
  - $\varphi(N) = \varphi(p) * \varphi(q) = (p-1)*(q-1)$   
Für Primzahlen gilt:  $\varphi(\text{Primzahl}) = (\text{Primzahl}-1)$
  - Zahlenbeispiel:  $\varphi(N) = 16 * 30 = 480$

**Erzeugung eines Schlüsselpaares für Teilnehmer ...**

## RSA – Populärste 2-Schlüssel Verschlüsselung (3/6)

**Erzeugung eines Schlüsselpaares für Teilnehmer A:**

4. Wahl einer zu  $\varphi(N)$  teilerfremden Zahl  $e$  mit  $e < \varphi(N)$ 
  - Zahlenbeispiel  $e = 13$
  - $(e, N) = (13, 527)$  ist **öffentlicher Schlüssel von A**
5. Berechnung des multiplikativen Inversen  $d$  zu  $e$  bezüglich  $\varphi(N)$ , d.h.  $e * d \bmod \varphi(N) = 1$ 
  - Zahlenbeispiel:  
 $d = 37$  da  $e * d \bmod \varphi(N) = 13 * 37 \bmod 480 = 1$
  - $(d, N) = (37, 527)$  ist **privater Schlüssel von A**

## RSA – Populärste 2-Schlüssel Verschlüsselung (4/6)

### Bemerkung:

- Letztendlich werden nur  $e, d, N$  benötigt, um
  - öffentlichen Schlüssel  $(e, N)$  und
  - privaten Schlüssel  $(d, N)$  zu erzeugen

### Anwendung des Verfahrens:

- Verschlüsseln/ Entschlüsseln mit öffentlichem/ privatem Schlüssel
  - Chiffre = Nachricht  $^e \bmod N$
  - Nachricht = Chiffre  $^d \bmod N$
- Verschlüsseln/ Entschlüsseln mit privatem/ öffentlichem Schlüssel
  - Chiffre = Nachricht  $^d \bmod N$
  - Nachricht = Chiffre  $^e \bmod N$

## RSA – Populärste 2-Schlüssel Verschlüsselung (5/6)

### Anwendung des Verfahrens – unser Zahlenbeispiel:

Kommunikationspartner B will A Nachricht „456“ senden:

- B besorgt sich öffentlichen Schlüssel von A  
 $(e, N) = (13, 527)$  und verschlüsselt damit Nachricht „456“:

$$456^e \bmod N \rightarrow 456^{13} \bmod 527 = 447$$

- B sendet „447“ über offenes Internet an A
- A kann „447“ mit seinem privaten Schlüssel  
 $(d, N) = (37, 527)$  entschlüsseln:

$$447^d \bmod N \rightarrow 447^{37} \bmod 527 = 456$$

**Korrektheit des RSA Verfahrens** beruht auf bekanntem Satz der Zahlentheorie:

**Kleinem Fermat'schen Satz:**

- Für beliebiges  $a$  und Primzahl  $p$  gilt:  
 $a^{p-1} \equiv 1 \pmod{p}$ , falls  $a$  kein Vielfaches von  $p$
- Beweisargument:  
Gilt  $e * d \equiv 1 \pmod{(p-1)*(q-1)}$   
Existiert ein  $x$  mit  $e*d - 1 = x*(p-1)*(q-1) \dots$