




# 1. AB: RSA – Vertraulichkeit und Authentizität

☑ Zur <b>Verschlüsselung</b> berechnet der Sender	$c = m^e \bmod n$
☑ Zur <b>Entschlüsselung</b> berechnet der Empfänger	$m = c^d \bmod n$
☑ Zum <b>Signieren</b> berechnet der Sender	$s = m^d \bmod n$
☑ Zur <b>Verifikation</b> berechnet der Empfänger	$m = s^e \bmod n$

## 1.1. Aufgabe: Alice:verschlüsselt→ Bob: signiert → Ted:verifiziert

1. Alice schickt einen verschlüsselten Text an Bob.
2. Bob entschlüsselt diesen Text und sendet ihn signiert an Ted.
3. Ted verifiziert den Text.
4. Ted sagt Alice was sie Bob 'sagen' wollte.

Alice	Bob	Ted
 <p>verschlüsseln →</p>	 <p>signieren →</p>	 <p>verifizieren</p>
<ol style="list-style-type: none"> <li>1. empfängt v. Bob pub_bob</li> <li>2. verschlüsselt einen Originaltext</li> <li>3. sendet verschlüsselten Text an Bob</li> </ol>	<ol style="list-style-type: none"> <li>1. erzeugt Schlüssel</li> <li>2. sendet pub_bob an Ted</li> <li>3. sendet pub_bob an Alice</li> <li>4. empfängt v. Alice den verschlüsselten Text</li> <li>5. entschlüsselt den Text</li> <li>6. signiert diesen entschlüsselten Text von Alice</li> <li>7. sendet den signierten Text an Ted</li> </ol>	<ol style="list-style-type: none"> <li>1. empfängt v. Bob pub_bob</li> <li>2. empfängt v. Bob den signierten Text</li> <li>3. verifiziert den Text</li> <li>4. vergleicht den verifizierten Text mit dem Originaltext v. Alice</li> </ol>

Hilfsmittel:

<http://web2.0rechner.de/>

## 1.2. Bob: Schlüssel erzeugen

1. Wähle zwei große Primzahlen mit  $p \neq q$  →  $p = \underline{\hspace{2cm}}$  ,  $q = \underline{\hspace{2cm}}$
2. Berechne den RSA Modul  $n$ : →  $n = \underline{\hspace{2cm}}$
3. Berechne  $\phi(n)$ : →  $\phi(n) = \underline{\hspace{2cm}}$
4. Wähle den Verschlüsselungs-Exponenten  $e$ : →  $e = \underline{\hspace{2cm}}$
5. Welche Bedingungen gelten für die Wahl von  $e$ ? →  $\underline{\hspace{2cm}}$
6. Berechne den Entschlüsselungs-Exponenten  $d$ : →  $d = \underline{\hspace{2cm}}$

## 1.3. Bob: sendet public-key an Alice und Ted

$(e,n) = (\underline{\hspace{1cm}}, \underline{\hspace{1cm}})$  .... **Public-Key**      $(d,n) = (\underline{\hspace{1cm}}, \underline{\hspace{1cm}})$  .... **Private-Key**

## 1.4. Alice: verschlüsselt und schickt c an Bob

<b>m (Buchst.)</b>						
<b>m (kodiert)</b>						
<b><math>c = m^e \bmod n</math></b>						

## 1.5. Bob: entschlüsselt

<b>Ciphertext: c</b>						
<b><math>m = c^d \bmod n</math></b>						
<b>m (Buchst.)</b>						

## 1.6. Bob: signiert und schickt s an Ted

<b>m (Buchst.)</b>						
<b>m (kodiert)</b>						
<b><math>s = m^d \bmod n</math></b>						

## 1.7. Ted: verifiziert und sagt Alice was sie an Bob geschickt hat

<b>signierter Text: s</b>						
<b>m (kodiert) <math>m = s^e \bmod n</math></b>						
<b>m (Buchst.)</b>						