# Kryptografie: Zertifizierung mit RSA

Anton hat sein RSA-Schlüsselpaar veröffentlicht: $(e_A, n_A)$. Nun kann jeder mit ihm sicher kommunizieren. Allerdings muss sichergestellt sein, dass niemand dieses Schlüsselpaar unbemerkt durch ein eigenes Paar $(e_X, n_X)$ ersetzt und dann Nachrichten an Anton abfängt und liest.
Dazu wendet sich Anton an ein Vertrauensbüro (Trustcenter) und lässt seine Schlüssel **zertifizieren**.

1) Das Vertrauensbüro hat selbst ein RSA-Schlüsselpaar $(e_V, n_V)$.
2) Es signiert mit seinem geheimen $d_V$ den Datensatz
   $m_A = (Anton, e_A, n_A)$ durch die Rechnung $c_A \underset{n_v}{\equiv} m_A^{d_V}$.
   Hier steht das Wort "Anton" für Antons vollständigen (eindeutigen) Namen.
3) Anton veröffentlicht jetzt seinen **zertifizierten RSA-Schlüssel** $(Anton,\ e_A,\ n_A,\ c_A)$ und er nennt sein Vertrauensbüro.

Anwendungsphase:

i. Berta will eine Nachricht $m_B$ an Anton senden.
ii. Sie findet seinen zertifizierten Schlüssel $(Anton,\ e_A,\ n_A,\ c_A)$ und auf der Internetsite des genannten Vertrauensbüros $(e_V, n_V)$.
iii. Berta berechnet $m_{test} \underset{n_V}{\equiv} c_A^{e_V}$. Wenn $m_{test} = m_A$ ist, sie also mit $m_{test}$ Antons Identität und seine Schlüssel selbst berechnen konnte, dann hält sie Antons Schlüssel für authentisch.
iv. Sie berechnet $c_B \underset{n_A}{\equiv} m_B^{e_A}$ und schickt dieses an Anton.
v. Anton berechnet $m_B \underset{n_A}{\equiv} c_B^{d_A}$ und liest Bertas Nachricht.

---

Beweis der Durchführbarkeit der Zertifizierung und ihrer Prüfung:
Das Vertauensbüro hat $d_V$ mit $d_v \cdot e_v \underset{\varphi_v}{\equiv} 1$ und in den Exponenten von Rechnungen modulo $n_V$ muss modulo $\varphi_V$ gerechnet werden.

$$m_{test} \underset{n_V}{\equiv} c_A^{e_V} = \left(\left(m_A\right)^{d_V}\right)^{e_V} = \left(m_A\right)^{d_V e_V} \underset{n_v}{\equiv} m_A^1 = m_A$$

RSA-Durchführbarkeit (wie schon bekannt):

Anton rechnet $c_B^{d_A} = \left(\left(m_B\right)^{e_A}\right)^{d_A} = \left(m_B\right)^{e_A d_A} \underset{n_A}{\equiv} m_B^1 = m_B$