Zertifizierung der öffentlichen Schlüssel

Bertold will Anton eine Nachricht senden und wissen, daß (e_A, n_A) wirklich zu A gehört "authentisch" ist

Eine Vertrauensinstanz V habe einen öffentlichen Schlüssel (e_V, n_V)

sie signiert die Liste $m_{AV} = \{\text{Anton}, e_A, n_A\}$ mit ihrem geheimen Schlüssel d_V $\boxed{c_{AV} \equiv_{n_V} m_{AV}^{d_V}}$ und stellt jedem die Liste zur Verfügung $\{\text{Anton}, e_A, n_A, c_{AV}\}$

Bertold berechnet nun $c_{AV}^{e_V} \bmod n_V$ und erhält daraus $\{\text{Anton}, e_A, n_A\} = m_{AV}$

Wenn sich dann das gleiche ergibt

$\Rightarrow$ Vertrauen: (e_A, n_A) das ist der richtige Schlüssel von A

Beweis der Durchführbarkeit

V. hat d_V geheim mit $M^{d_V \cdot e_V} \equiv_{n_V} M^1$

also $d_V e_V \equiv_{\varphi(n_V)} 1$

$$c_{AV}^{e_V} \equiv_{n_V} \left(m_{AV}^{d_V}\right)^{e_V} \equiv_{n_V} m_{AV}^{d_V \cdot e_V} \equiv_{n_V} m_{AV}$$