RSA Example with CRT

$p = 11 \quad q = 17 \quad n = p \cdot q = 187 \quad \varphi(n) = (11-1)\cdot(17-1) = 160$

$e = 7 \quad d = 23 \quad e \cdot d \equiv 1 \mod \varphi(n)$ Message $m = 3$

RSA Solution (without CRT):

$$\text{sig} = m^d \mod n$$

$$= 3^{23} \mod 187 = 94\,143\,178\,827 \mod 187 = \underline{\underline{181}}$$

<u>CRT</u>

$$\left.\begin{aligned} m^d &\equiv m_1 \mod p \\ m^d &\equiv m_2 \mod q \end{aligned}\right\} \rightarrow \text{Find solution } m^d$$

$$\Rightarrow m^d \equiv \text{sig} \mod pq$$

<u>Solution with CRT</u>:

$d_p = d \mod (p-1) = 23 \mod 10 = 3$

$d_q = d \mod (q-1) = 23 \mod 16 = 7$

$m_1 = m^{d_p} \mod p = 3^3 \mod 11 = 27 \mod 11 = 5$

$m_2 = m^{d_q} \mod q = 3^7 \mod 17 = 2187 \mod 17 = 11$

one solution with CRT: $m^d = \sum a_i e_i = a_1 e_1 + a_2 e_2$

with $e_1 = q \cdot [q^{-1}]_p \rightarrow q \cdot [q^{-1}]_p \equiv 1 \mod p$ $17 \cdot [q^{-1}]_p \equiv 1 \mod 11$

$\hookrightarrow [q^{-1}]_p = 2$

$e_2 = p \cdot [p^{-1}]_q \rightarrow p \cdot [p^{-1}]_q \equiv 1 \mod q$ $11 \cdot [p^{-1}]_q \equiv 1 \mod 17$

$\hookrightarrow [p^{-1}]_q = 14$

$\rightarrow e_1 = 17 \cdot 2 = 34$

$e_2 = 11 \cdot 14 = 154$

$$m^d = \underset{\overset{\uparrow}{a_1}}{m_1} \cdot e_1 + \underset{\overset{\uparrow}{a_2}}{m_2} e_2 = 5 \cdot 34 + 11 \cdot 154 = 1864$$ one solution

unique solution mod n:

$$1864 \mod 187 = \underline{\underline{181}}$$