RSA

$$n = p \cdot q$$
$$\phi = (p-1)(q-1)$$
$$e \rightarrow \text{tuje } \phi; 1 < e < \phi$$
$$d \rightarrow ed \bmod \phi = 1$$

$$c = m^e \bmod n$$
$$m = c^d \bmod n$$