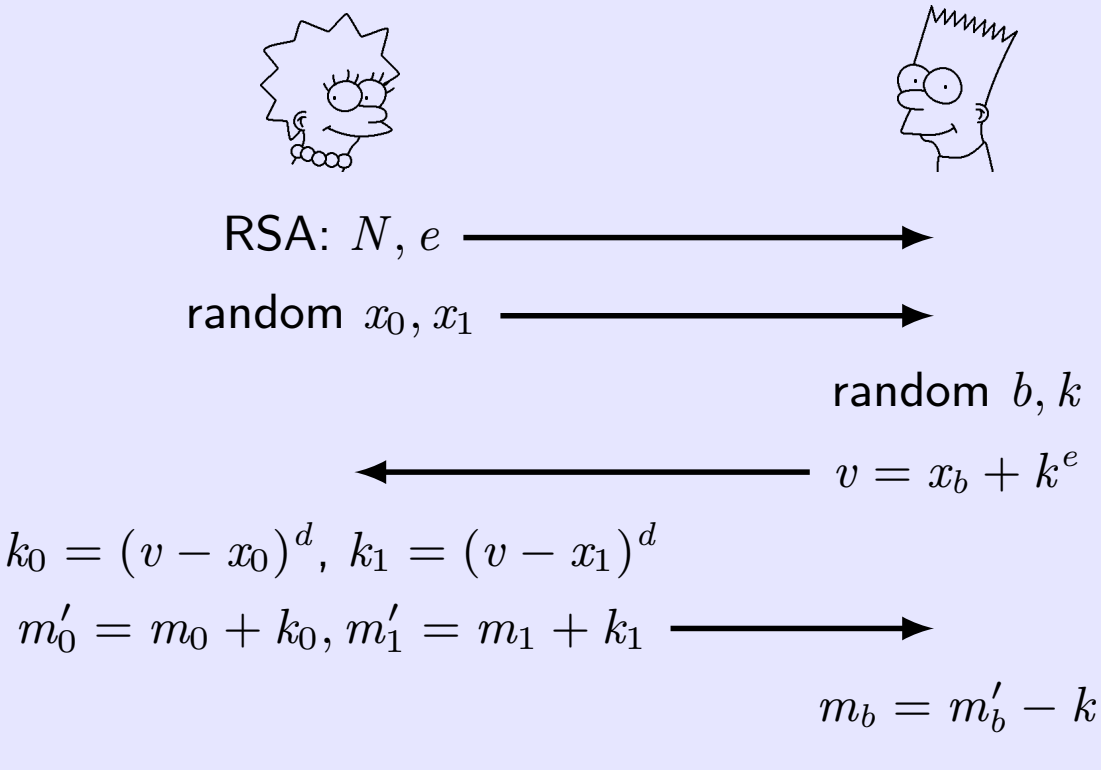
Tikz Test


RSA: N, e
random x_0, x_1
random b, k
$v = x_b + k^e$
$k_0 = (v - x_0)^d,\ k_1 = (v - x_1)^d$
$m'_0 = m_0 + k_0, m'_1 = m_1 + k_1$
$m_b = m'_b - k$