Quiz

1. First say True/False, and then explain briefly your answers.

(1) The one-time pad encryption scheme is CPA-secure.

(2) For a perfectly secure encryption scheme with message space $\mathcal{M}$ and key space $\mathcal{K}$, $|\mathcal{K}| \geq |\mathcal{M}|$ has to hold.

2. Let $p = 5, q = 11$, and $N = 55$. For a positive integer k, define $\pi_k(x) := x^k \bmod N$.

(1) Show that π_3 is a permutation of $\mathbb{Z}_{55}^*$.

(2) Determine an integer d such that $\pi_d = \pi_3^{-1}$.

(2) Determine $\pi_3^{-1}(6)$ using the Chinese remainder theorem.