Quiz

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

   (1) The pseudo 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.

   (3) The RSA assumption is stronger than the assumption that factoring is hard.

   (4) No deterministic encryption scheme can be CCA-secure.

2. Let n be a positive integer. The *affine cipher* modulo n is defined as follows. A key (a, b) consists of an element $a \in \mathbb{Z}_n^*$ and an element $b \in \mathbb{Z}_n$. For a message $m \in \mathbb{Z}_n$, the ciphertext is $C = Enc_{(a,b)}(m) = (am + b) \mod n$. If we *randomly* choose a key (a, b) for each message m to be encrypted, is this affine cipher *perfectly* secure? Explain your answer.