1. Consider an electronic cash system where a coin is a randomly generated unique serial number, blindly signed by the bank (i.e. as in Chaum's cash). Assume a homomorphic cryptosystem is used in implementation of it (i.e. unpadded RSA). Given a coin C, produce another coin C' such that C' contains a valid signature of the bank.

2. Show that the second pre-image resistance implies one-wayness (pre-image resistance).

3. Show that $\bmod n$ and modular exponent $g^x \bmod n$ are not cryptographic hash functions.