Quiz 7

written by Alvin Wan . alvinwan.com/cs70

Wednesday, September 28, 2016

This quiz does not count towards your grade. It exists to simply gauge your understanding. Treat this as though it were a portion of your midterm or final exam.

1 RSA

1. **Prove or Disprove**: Given two different public keys, N_1 and N_2, $d = \gcd(N_1, N_2)$ cannot be composite.

2. **Prove or Disprove** There are finitely many polynomials in mod p for some prime p. (If true, find an expression for the number of polynomials. If false, prove the opposite.)