Homework 2 on RSA.
Due: Monday, September 11, 2017 before 1pm EST.

Problem 1 DPV 1.12

What is $2^{2^{2006}} \mod 3$?

Answer:

Problem 2 DPV 1.25

Calculate $2^{125} \mod 127$.

Answer:

Problem 3 DPV 1.28

In an RSA cryptosystem, $p = 7$ and $q = 11$. Find appropriate exponents d and e.

Answer:

Problem 4 DPV 1.42

Suppose that instead of using a composite $N = pq$ in the RSA cryptosystem, we simply use a prime modulus p. As in RSA, we would have an encryption exponent e, and the encryption of a message m mod p would be $m^e \mod p$. Prove that this new cryptosystem is not secure, by giving an efficient algorithm to decrypt: that is, an algorithm that given p, e, and $m^e \mod p$ as input, computes m mod p. **Justify the correctness and analyze the running time of your decryption algorithm**.

Answer: