Name: Magahet Mediola ID: mmediola3 1

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:

$2^{2^{2006}} \equiv 1^{2^{2006}} \mod 3 \equiv 1 \mod 3 = \boxed{1}$

Problem 2 DPV 1.25

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

Answer:

$2^7 = 128, \quad 2^6 = 64$

$2^{125} = 128^{17} \cdot 2^6$

$2^{125} \equiv 1^{17} \cdot 2^6 \mod 127 = \boxed{64}$

Problem 3 DPV 1.28

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

Answer:

$N = 77$

$\phi = 6 \cdot 10 = 60 = 5 \cdot 3 \cdot 2 \cdot 2$

$e = 7$ $(\gcd(7, 60) = 1)$

$60 = 7(8) + 4$ $= 7(43) + 60(-5)$

$7 = 4(1) + 3$ $= 7(3) + 4(-5)$

$4 = 3(1) + 1$ $= 3(3) + 4(-2)$

$3 = 1(2) + 1$ $1 = 3 + 1(-2)$

$1 = 1(1) + 0$

$7^{-1} \bmod 60 = 43$

$e = 7, d = 43$

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:

$m^{ed} \equiv m \mod p$ for $ed \equiv 1 \mod p-1$ (Fermat's Little Theorem)

Compute $d = e^{-1} \mod p-1$ with Ext-Euclid$(e, p-1)$ $O(n^3)$

$m = (m^e \mod p)^d \mod p$ using Fast-mod exp $O(n^3)$

runtime: $O(n^3)$