**Math 132- Written HW Cryptography**

**This assignment is due on Tuesday, December 4th in class. Show all work! Answers magically appearing will receive no credit.**

1. From Barr Textbook

 p. 284 # 1c, 1d, 1e, 2b, 2e

1. Use successive squaring to calculate  MOD 101. (Answer is 63)

3. Suppose you and a friend set up an RSA encryption scheme with the two primes
*p =* 3and *q =* 11 and translate letters into numbers using a MOD 26 alphabet scheme.
a. Find *m* and *f.*
b. Using the enciphering exponent *e =* 7*,* encipher the message “FUN” as individual letters.
 (Answer for ciphertext is 14 26 7)
c. Find the deciphering exponent *d*.
d. Using the deciphering exponent *d,* decipher the message that was sent as 27 11 0 18.

4. Suppose you and a friend set up an RSA encryption scheme with the two primes
*p =* 5and *q =* 7 and translate letters into numbers using a MOD 26 alphabet scheme.
a. Find *m* and *f.*
b. Using the enciphering exponent *e =* 5*,* encipher the message “BILL” as individual letters.
 (Answer for ciphertext is 1 8 16 16)
c. Find the deciphering exponent *d*.
d. Using the deciphering exponent *d,,* decipher the message that was sent as 13 9 8 16.