

## M 343 L Midterm

name:

1. Bill and Bob both set up RSA cryptosystems with the same modulus  $n = 1003$ . Bill's encryption exponent is  $e_1 = 3$  and Bob's encryption exponent is  $e_2 = 5$ . Alice wishes to send the same message  $m$  to both Bill and Bob, so she encrypts and sends out the encryption to both of them. You are trying to eavesdrop their communication and sees that Alice has sent  $c_1 = 211$  to Bill and  $c_2 = 267$  to Bob. Find  $m$ .

2. How many multiplications modulo  $n$  are required to compute  $m^{21} \bmod n$ ? Compute  $10^{21} \bmod 1003$ .

3. Compute  $591^4 \bmod 1003$  and use this calculation to factor 1003.