**QUIZ 3**

**CHAPTER 2 and Chapter 7**

**30 Minute Quiz**

1. **Write the answers on a blank sheet of paper.**
2. **Make sure you write your name on every page.**
3. **Mark each page with Quiz 3.**
4. **Write legibly.**
5. **Must show all steps for any credit.**
6. **Please turn in a single document with all the pages in it.**

**Colin Quinn**

1. Describe the steps needed to create pair of public key and private key of RSA. Use the symbols p,q,n,d and e in your steps. What is the public key and what is the private key.

Both p and q are prime numbers, to compute n, you must multiply p\*q and find an r value such that r = (p-1)\*(q-1). Using that r value, find 2 values that are relatively prime to n as values for e and d, and that their product such that e\*d = 1 mod r. The public and private keys are the values calculated for e and d respectively.

1. Given the following RSA encrypt the plaintext x =10. You may use square and multiply for exponentiation but you do not have to.

p = 5, q = 11, e = 7

n = 5\*11 = 55

r = 4\*10 = 40

e = 41

d = 81

therefore, 10101001 mod 55

h5 = 1 y = 10

h4 = 0 y = 102 mod 55 = 45

h3 = 1 y = 452 mod 55 = 45 \* 10 = 450 mod 55 = 10

h2 = 0 y = 102 mod 55 = 45

h1 = 0 y = 452 mod 55 = 45

h0 = 1 y = 452 mod 55 = 45 \* 10 = 450 mod 55 = 10

Therefore, after encrypting x = 10, y = 10.

1. Given the following RSA, find the private exponent and then using the private exponent, decrypt the ciphertext y =10. You MUST use square and multiply for exponentiation in this case.

p = 5, q = 11, e = 7

n = 55

r = 40

e = 41

d = 81

101010001 mod 55

H6 = 1 x = 10

H5= 0 x = 102 mod 55 = 45

H4 = 1 x = 452 mod 55 = 45 \* 10 = 450 mod 55 = 10

H3 = 0 x = 102 mod 55 = 45

H2 = 0 x = 452 mod 55 = 45

H1 = 0 x = 452 mod 55 = 45

H0 = 1 x = 452 mod 55 = 45 \* 10 = 450 mod 55 = 10

Therefore x = 10.