Colin Quinn, Quiz 2

**QUIZ 2**

**CHAPTER 2 and Chapter 4**

**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 2.**
4. **Write legibly.**
5. **Must show steps for any credit.**
6. Provide the equation for encrypting and decrypting using stream cipher. What is the size of the key if the input stream has K bits.

Both encryption and decryption process the plain text byte to byte. A key is generated that is the same length as the plain text and is then applied to the plaintext. Such as p1, p2, … gets applied with k1, k2, … until the cipher text is completed. To decrypt this message, the XOR operation is applied between the ciphertext and the key, also byte by byte. The size of the key must be the same length as the number of bytes in the input stream, so the ciphertext must also include K bits.

1. The mix column operation is performed on the input matrix B whose first column is shown below to produce matrix C. **Find the first column of C.**

Find the entries of the matrix C. The irreducible polynomial used in AES is x8 + x4 + x3 + x +1

1. Find the result of g function used in key generation of AES on the following 32 bits.

62 62 62 62

NOTE THAT YOU NEED NOT GENERATE ALL OF THE ROUND 1 KEY- ONLY FIND THE RESULT OF g function.

