Multiple Choice Questions  (3 pts each question, 36 pts total)

1. Question about arithmetic over GF(2^3)
2. Question about the Blum Blum Shub Generator
3. Encryption using the Hill Cipher
4. Question about irreducible polynomials in GF(2^3)
5. Question about one of the transformations in full AES
6. Question about encryption placement
7. Question about Triple DES
8. Question about the five cipher modes in chapter 6
9. Question about full DES
10. Question about full AES
11. Question about XTS-AES
12. Question about inverses in Z_p

Short Answer Questions (8 pts each question)
(Select 8 out of 9, 64 pts total, put an X through the problems omitted)
You must show all of your work for each of these questions.

1. Random number generation using linear congruence
2. Key generation in simple DES
3. Encryption using a playfair matrix
4. Encryption using the Vigenere cipher
5. Question about improving security in full DES
6. Question about using S-Boxes in full DES
7. Question about the mix columns in full AES
8. Question about key expansion in full AES
9. Question about key distribution

You can use a HANDHELD calculator capable of hexadecimal calculations on the exam. You CANNOT use any computer even to access the built-in calculator. You cannot access any other resources other than the handout that will be provided.