1. Find the square roots of 57 mod 107.

2. (a).Consider $Z_5[x]$ mod $x^8 + x^4 + x^3 + x + 1$. Show that $h(x) = 3x^5 + 2x^3 + x^2 + 4x + 4$ is reducible.

   Hint: consider $q(x) = 4x^3 + 3x^2 + 4$ and do a division.

   (b). Find the multiplicative inverse of $1 + 2x$ in $Z_3[x] \bmod x^2 + 1$

3.(a) Let the input message be 100010110101 and the key be 111000111. Perform two complete rounds of encryption using the simplified DES type algorithm.

   (b). Starting with the results from 3(a), decrypt the ciphertext by using the algorithm in "reverse".

4. The ciphertext is 182 and was obtained from the RSA algorithm using $n = 437$ and $e = 283$. Find the plaintext. {Hint: you can use trial and error (small integers) to determine d or use the Extended Euclidean Algorithm}

5. Determine $L_3(6)$ mod 31, using the "Baby Step-Giant Step" method.