1 Tutorial 4

1. Use the Miller-Rabin primality test to determine whether the following numbers are likely to be prime. Try with bases $b = 2, 3, 4$. Show all the steps in the computation i.e., the value of b^y where $n - 1 = 2^e \cdot y$ and then the values in each iteration of the computation of $b^{y^{2^e}}$.
   - 125.
   - 561.
   - 3017049239485840259629.
   - 5472011961261553846573217.
2. For a DES key of $0x0123456789ABCDEF$ and a plaintext of $0x0123456789ABCDEF$, show all the intermediate values of the computation in getting from L_0, R_0 to L_1, R_1. You can verify the final values using the CGI script des.cgi. Note that I have removed the part of the script that expands the F function.
3. Show that the following property holds for DES encryption

   $$\overline{DES_k(X)} = DES_{\overline{k}}(\overline{X})$$

   That is, encrypting the complement of a block with the complement of the key results in the complement of the cipher text.

For each of these questions you may write a program to solve it. You must show (and demonstrate understanding) of all the steps needed to arrive at the answer.