Programming Project: Crypto Systems (15 pts)

Problem 1. Modern Symmetric Cipher & Decipher Implementation

Program to implement the DES **or** AES algorithm. You can choose either one based on your interest and use any programming language you like, such as C, C++, Java, and python. Directly using des or aes libraries receives 0 for this problem. Your program does not need to encode a plaintext exactly the same as the existing library function. But you need to specify in your report how you implement each component of the cipher/decipher in both text and code segments. And how many rounds? You can refer to the DES or AES algorithm designs in the lecture notes or some similar designs. Show that your encryption and decryption function work using example plaintexts.

Problem 2. RSA Crypto System. 1) Write a prime number check program to check any input number to be whether a prime number. 2) Find the 10th and the 19th prime numbers p and q between 1000 and 10000 to build an RSA crypto system. Write down the public key PU = {e, n} and the private key PR = {d, p, q}. 3) Program to implement the encipher and decipher. Test your RSA crypto system by encrypting and decrypting a message "rsa" (Map each letter to 0 - 25). 4) If an adversary obtains the public key PU = {e, n}, demonstrate how the adversary uses the exhaustive search to get the private key d and show the time cost of the search.

==========

You are required to write a project report by solving the above problems. Describe your design clearly and your observations. Submit a copy of your code. Your grade will be based on the clarity and thoroughness of your report.