Homework 3

CSL7480: Cryptography

Note - Submitting the code files in a Zip file with a single report explaining the working is mandatory. Follow the naming conventions as "[Roll_No]_[Name]_Assignment3.zip"

Questions:

1. (a) Generate two prime numbers p and q of 512 bits each.
   (b) Using these prime numbers, generate a public key and private key pair. Store the results in "PublicKey.txt" and "PrivateKey.txt", respectively.
   (c) Draft a "Plaintext.txt" file with the content - "Hello, I am [Your Name]_[Roll_No], a student of IIT Jodhpur."
   (d) Encrypt the text file generated above using textbook RSA algorithm and store the results in another text file - "Ciphertext.txt"
   (e) Decrypt the "Ciphertext.txt" file and compare it with the "Plaintext.txt".
   (f) Perform the above task (d) & (e)
      1) With OpenSSL library and
      2) Without using the inbuilt library.
      3) In the second scenario, decrypt the ciphertext using the Chinese Remainder Theorem as well. How much speed improvement do you get by using the CRT?

   Libraries for mathematical functions can be used.
   Submit all the files along with the code as **three folders** where each folder contains
   - "PublicKey.txt"
   - "PrivateKey.txt"
   - "Plaintext.txt"
   - "Ciphertext.txt"
   - "Decrypted.txt"

   One folder is generated using the OpenSSL library and the other folders contain the file generated by manual implementation with & without CRT, respectively. [6]

2. What are the insecurities of the textbook RSA algorithm and how padding resolves it?[2]
   Hint: Study about Optimal Asymmetric Encryption Padding (OAEP)

3. Implement the Diffie Hellman Secret Key Exchange using OpenSSL, where two parties share a secret key over an insecure communication channel. [2]