National Institute of Technology Calicut
CS4021D Number Theory and Cryptography
Monsoon 2022

Programming Assignment

Instructions: You have to implement solutions to the three questions mentioned in this assignment and upload on eduserver before the deadline. For each question, the following supporting documents has to be included in the solution.

1. *Solution code (in c, cpp or python)*
2. *Sample input and output as .txt files*
3. *Sufficient screenshots of executions with clear input and output*

*For each question, upload three separate **.zip** files which contains all the supporting documents. For questions 2,3, **do not** use standard libraries to implement DES, RSA or SHA-512.*

1. NIC has received three document files which contains some encrypted message using the classical cryptographic techniques. It is known that the techniques used are Affine cipher, Vigenere cipher and Hill cipher. However the keys used are not known. It is also known that the Vigenere cipher key does not exceed 10 characters and the hill cipher matrix is 4×4. Perform cryptanalysis on the encrypted messages and decrypt each **meaningful** message separately using a brute force technique. Note that the code should receive the file contents mentioned below and produce the plain text using the key internally generated. Key **should not** be a user input. You are allowed to use three different programs as solutions.

   File 1 contents:
   CCCYTWACWKYWSARTIBMHZAEKFGZPDGBFWKAFKEL
   XCCGSDBTUBNLUGANEDJBRFDEOCCCYTMAKFBRYAO
   BUPHOFTWNP

   File 2 contents:
   NUTALDQIQTAYRQNJDHHNLDMTLDHYVNAEDPHDMYR
   DAHPQDYCDTAYDLQTYFRUNMRVPJDAYRQNJDHHNLD
   YRDAHPQDYCDTAYDLQTYFRUNJDHHNLDERYCYCDJD
   HHNLDNAMYCDJDHHNLDMTLDHYNQDADDMDM

   File 3 contents:
   IYEGXPXMMOETTNZKAYAUYYTTBBMVFFYYKKKCIGX
   ELZFXBAVSIJZOXQBBNXUWIOYZVTFRVABXMZXWYR
   OXAZRTXOEOLSKUTJAEKMGWABWHVAMYKPHQVCQLF
   MQNWOEOBRMETXOFVTQMGHJIIGIRWTKEVYQVFIFA
   JAEKMGWALYYVAVMUCKIYJQHLNHGGZZWGQBUTXGI
   MFYLRYVUDAVPIGVL

2. Implement standard DES algorithm using the default s-boxes and p-boxes and show the middle texts in all the 16 rounds. Modify the algorithm in such a way that all the 16 rounds are identical. Compare the middle texts during encryption and decryption. During implementation, ensure to implement encryption and decryption as separate programs. Use an intermediate file to store cipher text. Read from the cipher text file and perform decryption.

3. **Implement a confidential communication using digital signature scheme**. Given an input message M to be transferred from Alice to Bob, do the following:

    1. Compute the 512-bit message digest using SHA-512 algorithm. Implement 80 round SHA-512 algorithm using standard constant values and initial digest values (as mentioned in Forouzan).
    2. Create two private - public key pairs for Alice and Bob (The key pairs should not be constant. For each run of the program, you should create different key pairs).
    3. Encrypt the digest using RSA Digital Signature Scheme to obtain the signature S.
    4. Append the signature S to the mesasge M and encrypt using DES.
    5. Send it to Bob and upon receiving perform decryption of the message and verification of the signature.

    Note: Reuse the DES implementation of question 2. Need not demonstrate the communication, instead perform all the operations that is done in sender and receiver side in **separate** programs. Use text files to store plain text and cipher text. Read the cipher text from the file and perform decryption and signature validation. Key pairs (RSA) and secret key (DES) should be written on files for communicating with the decrypting/validating code.