BÀI TẬP

Bài 2

1. Cho hai số a, b, hãy dùng thuật toán Extended Euclidean để tìm USCLN (a, b) và hai tham số s và t. Biết a = 35, b = 168.
2. Cho hai số a, b, hãy dùng thuật toán Extended Euclidean để tìm USCLN (a, b) và hai tham số s và t. Biết a = 27, b = 108.
3. Giải phương trình Diophantine tuyến tính với hai biến x và y: 20x+5y = 100.
4. Giải phương trình Diophantine tuyến tính với hai biến x và y: 14x+21y = 35.
5. Cho bản P = 10010110 và khóa K = [2, 3, 1], hãy dùng thuật toán RC4 bản rút gọn 3 bít để mã hóa P?
6. Cho p = 11, q = 17 hãy dùng RSA để tính bản mã từ bản rõ M = 5.
7. Cho p = 11, q = 7, hãy dùng chữ ký số RSA để tạo chữ ký và xác thực chữ ký trên thông điệp M=9
8. Cho P = 10011101 hãy tính mã Check sum sử dụng đa thức sinh CRC4: $X^4 + X + 1$

Digital Signature

Viết chương trình mô phỏng quá trình ký và xác thực chữ ký trên một thông điệp (ảnh), cụ thể như sau:

- 1. Dùng chữ ký số dựa trên thuật toán RSA
- 2. Thực hiện ký trên hàm băm SHA1
- 3. Thông điệp gửi đi được mã hóa bằng thuật toán RSA
- 4. Mô phỏng quá trình: trên file jupyter notebook hoặc ngôn ngữ lập trình có giao diện.

Notes: Lớp đã trình bài thuật toán, nhưng chưa có bản mô phỏng

Assigments

1. *Write a python-based program for AES key expansion of the size 128 bits.*
2. *Wire a software (just POC level) to demonstrate the use of AES in the five models discussed today:*
   + Dashboard
   + Select one of the model above
   + Input a file with its size >>128 bits
   + Represent iteration (stream) manner

Notes: (2) chưa hoàn thành