Assignment 1 5 คะแนน

วันออก assignment 1 พฤศจิกายน 2559 วันส่ง : 15 พฤศจิกายน 2559

Elgamal Encryption and Signature

ให้นักศึกษาเขียนโปรแกรม ซึ่งโปรแกรมนี้เมื่อนักศึกษาเขียนเสร็จแล้วสามารถนำมาใช้ในการเข้ารหัส ถอดรหัส สร้างลายเซ็นอิเล็กโทรนิกส์ ตรวจสอบลายเซ็น โดยใช้อัลกอริทึมของ Elgamal Public Key CryptoSystem และใช้ RWHash เป็นอัลกอริทึมสำหรับการทำ Cryptographic Hash Function โดยโปรแกรมมี Requirement ดังต่อไปนี้

1. โปรแกรมนี้เมื่อนำไปใช้งานผู้ใช้สามารถเลือกเมนูได้อย่างน้อย 6 เมนูดังต่อไปนี้
    - GenKey ใช้ในการสร้าง Public Key และ Private Key ของ Elgamal
    - Encryption ใช้ในการเข้ารหัสด้วย Elgamal
    - Decryption ใช้ในการถอดรหัสด้วย Elgamal
    - Sign ใช้ในการสร้างลายเซ็นอิเล็กโทรนิกส์ด้วย Elgamal
    - Verify ใช้ในการตรวจสอบลายเซ็นอิเล็กโทรนิกส์ด้วย Elgamal
    - CryptoHash ใช้ในการหา Message Digest ด้วย RWHash
2. โปรแกรมนี้สามารถรับข้อมูลและแสดงผลได้ทั้งจากหน้าจอ Text และ ไฟล์
3. ในการสร้างสิ่งเหล่านี้ ต้องใช้อัลกอริทึมที่เรียนในห้องเรียน
    - อัลกอริทึมในการสร้าง generator
    - Lehman Test
4. ต้องมีอัลกอริทึมต่อไปนี้จะเขียนเองหรือดาวน์โหลด method จาก อินเทอร์เน็ต ได้หมดแต่ต้องมี
    - Euclid Extened GCD
    - Lehman test
5. ในการสร้างคีย์ (GenKey) ให้มีพารามิเตอร์ 2 ตัวคือ n และ *file*
    - n คือ จำนวนบิตของข้อมูลที่นักศึกษาใช้ในการเข้ารหัส (ขนาดของ message แต่ละบลอก)
    - file คือ ชื่อไฟล์ที่นักศึกษาใช้ในการอ่านค่ามาสร้างค่า p โดย ค่า $2^{n-1} < p < 2^n$
    - การสร้างคีย์ทำได้โดย
        - หา p ก่อน โดยอ่านข้อมูลจากไฟล์ออกมา n-1 บิต
        - แปลงค่า n-1 บิตที่อ่านออกมาเป็นจำนวนเต็ม => x
        - นำจำนวนเต็ม (x) นั้นไปตรวจสอบว่าเป็น จำนวนเฉพาะหรือไม่
        - ถ้าไม่ให้ทำการเพิ่มค่าทีละหนึ่งจนกว่า x จะเป็นจำนวนเฉพาะ
        - เมื่อได้ค่า p ให้ทำการสร้าง public และ private keys ตามอัลกอริทึม

6. สำหรับ RWHash นั้นให้ทำงานดังนี้
    1. ให้นำ Message ที่ต้องการหาค่า Hash ไปเข้า SHA-1 M_{SHA-1}
    2. นำ output ที่ได้จากข้อ 1 มาทำการเข้าสมการ PolyHash
    3. โดย PolyHash มีพารามิเตอร์ทั้งหมด 4 ตัวคือ
        - M_{SHA-1} - Message Digest ที่ได้จาก SHA-1
        - p คือ ค่า p เดียวกับที่ได้จากการ GenKey
        - n คือจำนวนบิต
        - k คือ จำนวนบลอกข้อมูลใน h_i

RwHash(k,p,M):

Message = $b_1b_2b_3b_4b_5b_6$.....

RwHash ได้มาจากการ break message ออกเป็น block (Bi) ที่มีขนาด เท่ากับ n บิต ในกรณีที่ยาวไม่พอ ให้ทำการ นำตัวอักษรตัวสุดท้ายมาต่อจนครบขนาด

$$h_1 = \alpha, B_1, B_2, \dots, B_{k-1} \quad mod\ p$$
$$h_2 = h_1, B_k, B_{k+1}, \dots, B_{2k-2} \quad mod\ p$$
$$h_3 = h_2, B_{2k-1}, B_{2k}, \dots, B_{3k-3} \quad mod\ p$$
$$h_l = h_l, B_{lk-l-1}, \dots, B_{lk-l} \quad mod\ p$$

$h_0 = \propto =$ *length of the message*

h_i =($\sum_{i=1}^{k-1} h_i$) + ${h_{i-1}}^2$ *(mod p)*