มหาวิทยาลัยธรรมศาสตร์

สาขาวิชาวิทยาการคอมพิวเตอร์ **คณะวิทยาศาสตร์และเทคโนโลยี**

CS324: Computer Security **ภาคการศึกษา 2/2567**

Security Labs: Cryptography - RSA and Signature **คะแนนเต็ม:** 100 คะแนน

นักศึกษาโปรดทราบ

1. **การบ้านนี้เป็นงานกลุ่ม กลุ่มละ 1 – 3 คน ต้องเขียนชื่อ-สกุล และ เลขทะเบียน ของสมาชิกในกลุ่มให้ครบถ้วน**
2. ทำงาน (task) ตามข้อกำหนดการบ้านในเอกสารฉบับนี้ ให้ครบถ้วน
3. การไม่ปฏิบัติตามคำสั่งต่าง ๆ ที่กำหนดไว้ด้านล่าง เช่น การตั้งชื่อแฟ้มข้อมูลตามรูปแบบที่กำหนด การเขียนข้อมูลของสมาชิกในกลุ่มที่ร่วมทำงานอย่างถูกต้องและครบถ้วน อาจมีผลให้การบ้านชิ้นนี้ของนักศึกษาไม่ได้รับการตรวจ
4. การลอกการบ้าน การทำซ้ำโปรแกรม ถือเป็นการกระทำผิดวินัยนักศึกษาอย่างร้ายแรง หากมีหลักฐานที่แน่ชัดผู้สอนมีสิทธิดำเนินการลงโทษนักศึกษาตามระเบียบข้อบังคับเกี่ยวกับการกระทำผิดวินัยนักศึกษาได้
5. การบ้านนี้แบ่งออกเป็น 3 ส่วน อ้างอิงตามชิ้นงาน Task 1 – 6 ในหัวข้อที่ 3 ของ Lab Sheet: RSA Encryption and Signature Lab ดังนี้
   - **ส่วนที่ 1 (25 คะแนน)** ได้แก่ ชิ้นงาน Task 1: Deriving the private key
   - **ส่วนที่ 2 (25 คะแนน)** ได้แก่ ชิ้นงาน Task 2 – 5 ดังรายละเอียดต่อไปนี้
     - Task 2: Encrypting a Message
     - Task 3: Decrypting a Message
     - Task 4: Signing a Message
     - Task 5: Verifying a Signature
   - **ส่วนที่ 3 (50 คะแนน)** ได้แก่ ชิ้นงาน Task 6: Manually Verifying an X.509 Certificate
6. ภายหลังจากทำสำเร็จครบทุกงาน (task) ตามข้อกำหนดในเอกสารฉบับนี้แล้วเสร็จ ให้จัดเตรียมไฟล์บีบอัดในรูปแบบ zip หรือ rar
   6.1. ตั้งชื่อไฟล์ตามข้อกำหนด คือ `CS324_Security_Lab01-Cryptography-RSA_Gxx.zip` หรือ `CS324_Security_Lab01-Cryptography-RSA_Gxx.rar` เมื่อ Gxx คือ หมายเลขประจำกลุ่มที่ได้รับจัดสรร
   6.2. ไฟล์บีบอัดที่นักศึกษาจัดส่งต้องรวมไฟล์รหัสต้นฉบับ (source code) และ รายงาน (report) ที่ต้องส่งทั้งหมด ดังรายละเอียดที่กำหนดไว้ในหัวข้อ สิ่งที่ต้องส่ง
7. ส่ง*ไฟล์บีบอัด* ในกล่องรับการบ้านที่จัดเตรียมไว้บนเว็บไซต์รายวิชาภายในเวลาที่กำหนด เท่านั้น
8. ทรัพยากรและรายการงาน (task) ในการบ้านชิ้นนี้อ้างอิงจาก SEED Labs 2.0 (RSA Public-Key Encryption and Signature Lab) โดย Dr. Wenliang Du

คำอธิบายการบ้าน

เอกสาร Lab Sheet: RSA Encryption and Signature Lab ประกอบด้วยหัวข้อต่าง ๆ ดังนี้

- หัวข้อที่ 1 เป็น ข้อมูลพื้นหลังเกี่ยวกับ RSA ซึ่งมีเนื้อหาสอดคล้องกับที่ได้อภิปรายกันในชั้นเรียน
- หัวข้อที่ 2 เป็น ข้อมูลพื้นหลังเกี่ยวกับ BIGNUM APIs สำหรับภาษาซี (C) และ คำสั่งสำหรับใช้งาน utility function ของภาษาไพธอน ที่นักศึกษาต้องใช้ในการทำชิ้นงานต่าง ๆ ของการบ้านนี้
- หัวข้อที่ 3 เป็น คำอธิบายชิ้นงาน (Task 1 - 6) นักศึกษาทำงานตามข้อกำหนดใน Task 1 - 6
- หัวข้อที่ 4 เป็น สรุปสิ่งที่นักศึกษาต้องนำส่ง

(สำหรับวิชา CS324 ให้นักศึกษาปฏิบัติตามที่กำหนดในหัวข้อ ***สิ่งที่ต้องส่ง*** ของเอกสารฉบับนี้)

ในปฏิบัติการนี้ เครื่องคอมพิวเตอร์ของนักศึกษาต้องถูกตั้งค่าให้มีสภาพแวดล้อมซึ่งรองรับการทำงานที่สนับสนุนการใช้งาน BIGNUM APIs สำหรับภาษาซี, ไลบรารี OpenSSL, อัลกอริทึมสำหรับสร้างแฮช (Hash) ของข้อความตามมาตรฐาน SHA, และ การใช้งานชุดคำสั่งภาษาไพธอน ตามที่ระบุใน Lab Sheet

คำแนะนำ

(1) ระบบปฏิบัติการ Ubuntu 16.04 และ Ubuntu 20.04 มีสภาพแวดล้อมที่สนับสนุนการทำงานทั้งหมดในการบ้านนี้ โดยนักศึกษาสามารถติดตั้งระบบปฏิบัติการ Ubuntu 16.04 หรือ Ubuntu 20.04 ลงบนเครื่อง physical machine ของนักศึกษา หรือ ดาวน์โหลดเครื่องเสมือน (virtual machine) เพื่อใช้งาน

- ดาวน์โหลด**เครื่องเสมือน SEED Ubuntu 20.04 VM** (SEED-Ubuntu20.04.zip) จากเว็บไซต์ SEED LAB
- ดาวน์โหลด**เครื่องเสมือน SEED Ubuntu 16.04 VM** (SEEDUbuntu-16.04-32bit.zip) จากเว็บไซต์ SEED LAB

(2) **ระบบปฏิบัติการ Mac OS-X** มีสภาพแวดล้อมที่สนับสนุนการทำงานทั้งหมดในการบ้านนี้

(3) สำหรับ**ระบบปฏิบัติการ MS-Windows** นักศึกษาสามารถติดตั้ง Windows Subsystem for Linux (WSL) ซึ่งมีสภาพแวดล้อมที่สนับสนุนการทำงานทั้งหมดในการบ้านนี้

หากนักศึกษาไม่ส่งการบ้านหรือส่งงานไม่ครบถ้วนภายในวันและเวลาที่กำหนด นักศึกษาจะไม่ได้รับคะแนนในส่วนของการบ้านชิ้นนี้ ไม่รับการบ้านที่ส่งล่าช้า

สิ่งที่ต้องส่ง

นักศึกษาต้องส่งไฟล์บีบอัด ชื่อ `CS324_Security_Lab01 -Cryptography-RSA_Gxx.zip` หรือ `CS324_Security_Lab01 -Cryptography-RSA_Gxx.rar` หรือ `CS324_Security_Lab01 -Cryptography-RSA_Gxx.tgz` เมื่อ Gxx คือ หมายเลขประจำกลุ่มที่ได้รับจัดสรร

ไฟล์บีบอัดที่ส่งต้องเป็นไฟล์ที่รวมไฟล์รหัสต้นฉบับ (source code) และ รายงาน (report) ที่ต้องจัดส่งทั้งหมดสำหรับการบ้านส่วนที่ 1 – 3 ดังรายละเอียดต่อไปนี้

1. การบ้านส่วนที่ 1 นักศึกษาต้องส่ง

1.1. ไฟล์รหัสต้นฉบับ (source code) ตั้งชื่อแฟ้มข้อมูลเป็น

`CS324_Security_Lab01-Cryptography-RSA_Gxx_task-1.c`

ซึ่งมีชุดคำสั่งภาษาซี ทำงานตามที่กำหนดใน Task 1 ของ Lab Sheet

1.2. ไฟล์รายงาน

`CS324_Security_Lab01-Cryptography-RSA_Gxx_task-1_report.pdf`

ซึ่งอธิบายขั้นตอนการทำงานของโปรแกรมในข้อ 1.1 และ วิธีการคิดขั้นตอนของการแก้ปัญหา

เนื้อความและการเขียนรายงานต้องแสดงให้เห็นว่านักศึกษาเข้าใจการทำงานของขั้นตอนการคำนวณค่า Private Key ของอัลกอริทึม RSA และสามารถนำไปอิมพลีเมนต์ได้อย่างถูกต้อง

หมายเหตุ การส่งการบ้านไม่ครบตามข้อกำหนดการจัดส่ง จะทำให้การบ้านส่วนที่ 1 ไม่ได้รับการตรวจให้คะแนน

2. การบ้านส่วนที่ 2 นักศึกษาต้องส่ง

2.1. ไฟล์รหัสต้นฉบับ (source code) ตั้งชื่อแฟ้มข้อมูลเป็น

`CS324_Security_Lab01-Cryptography-RSA_Gxx_task-2-5.c`

ซึ่งมีชุดคำสั่งภาษาซี ทำงานตามที่กำหนดใน Task 2-5 ของ Lab Sheet

2.2. ไฟล์รายงาน

`CS324_Security_Lab01-Cryptography-RSA_Gxx_task-2-5_report.pdf`

ซึ่งมีรายละเอียด ดังต่อไปนี้

2.2.1. ชุดคำสั่งทั้งภาษาซีและภาษาไพธอนที่นักศึกษาใช้ในการทำงานตามข้อกำหนด Task 2 – 5 ของ Lab Sheet พร้อมคำอธิบายการทำงานของแต่ละคำสั่ง (สามารถเขียนในรูปแบบคอมเมนต์ประกอบแต่ละคำสั่งได้)

2.2.2. ภาพหน้าจอแสดงผลลัพธ์ของการทำงาน

2.2.3. อภิปราย ผลลัพธ์ / สิ่งที่สังเกตได้ / ตอบคำถาม ที่ระบุไว้ในแต่ละ task อย่างถูกต้อง พร้อมระบุเหตุผลประกอบอย่างเหมาะสม การเขียนอภิปรายและการตอบคำถามจะต้องแสดงให้เห็นถึงความเข้าใจในเนื้อหาของการนำอัลกอริทึม RSA ไปใช้ในการสร้างความปลอดภัยให้กับข้อมูล

หมายเหตุ การส่งการบ้านไม่ครบตามข้อกำหนดการจัดส่ง จะทำให้การบ้านส่วนที่ 2 ไม่ได้รับการตรวจให้คะแนน

3. การบ้านส่วนที่ 3 นักศึกษาต้องส่ง

3.1. ไฟล์รหัสต้นฉบับ (source code) ตั้งชื่อแฟ้มข้อมูลเป็น

`CS324_Security_Lab01-Cryptography-RSA_Gxx_task-6.c`

ซึ่งมีชุดคำสั่งภาษาซี ซึ่งทำงานตามที่กำหนดใน Task 6 ของ Lab Sheet

3.2. ไฟล์รายงาน

`CS324_Security_Lab01-Cryptography-RSA_Gxx_task-6_report.pdf`

ซึ่งมีรายละเอียด ดังต่อไปนี้

3.2.1. ชุดคำสั่งทั้งภาษาซีและภาษาไพธอนที่นักศึกษาใช้ในการทำงานตามข้อกำหนด Task 6 ของ Lab Sheet พร้อมคำอธิบายการทำงานของแต่ละคำสั่ง (สามารถเขียนในรูปแบบคอมเมนต์ประกอบแต่ละคำสั่งได้)

3.2.2. ภาพหน้าจอแสดงผลลัพธ์ของการทำงาน

3.2.3. อภิปราย ผลลัพธ์ / สิ่งที่สังเกตได้ / ตอบคำถาม ที่ระบุไว้อย่างถูกต้อง พร้อมระบุเหตุผลประกอบอย่างเหมาะสม การเขียนอภิปรายและการตอบคำถามจะต้องแสดงให้เห็นถึงความเข้าใจในเรื่องการนำอัลกอริทึม RSA ไปใช้ในการรับประกัน Public Key ของเซิฟเวอร์ ในรูปแบบของใบรับรองดิจิทัล (Digital Certificate)

หมายเหตุ การส่งการบ้านไม่ครบตามข้อกำหนดการจัดส่ง จะทำให้การบ้านส่วนที่ 3 ไม่ได้รับการตรวจให้คะแนน