บทที่ 2

แนวคิดและทฤษฎีที่เกี่ยวข้อง

การใช้รหัสผ่านเพื่อพิสูจน์ตัวจริงของผู้ใช้เป็นส่วนหนึ่งของการรักษาความปลอดภัยให้กับระบบคอมพิวเตอร์ที่ได้รับความนิยมในปัจจุบัน แต่วิธีดังกล่าวยังมีจุดอ่อนที่อาจถูกนำไปใช้ในการลักลอบเข้าสู่ระบบได้ ระบบรหัสผ่านแบบใช้ครั้งเดียวของคุณพิษณุเป็นอีกแนวทางที่ถูกพัฒนาขึ้นเพื่อเสริมประสิทธิภาพให้กับระบบการใช้รหัสผ่าน

เพื่อขยายประสิทธิภาพของระบบรหัสผ่านแบบใช้ครั้งเดียวของคุณพิษณุให้สมบูรณ์ยิ่งขึ้น จึงต้องทำการศึกษาแนวคิดและทฤษฎีที่เกี่ยวข้องที่สำคัญ ดังต่อไปนี้

1. ระบบรหัสผ่านแบบใช้ครั้งเดียวของคุณพิษณุ
2. วิทยาการเข้ารหัสลับ (cryptography)

ระบบรหัสผ่านแบบใช้ครั้งเดียวของคุณพิษณุ

ระบบรหัสผ่านแบบใช้ครั้งเดียวของคุณพิษณุ เป็นอีกวิธีหนึ่งที่สามารถป้องกันการลักลอบเข้าระบบจากการนำรหัสผ่านที่ได้มาจากกระทำต่าง ๆ ที่ไม่เหมาะสมกลับมาใช้ใหม่ เพราะรหัสผ่านที่ใช้เข้าระบบครั้งต่อไปจะถูกเปลี่ยนทุกครั้งหลังจากที่รหัสผ่านปัจจุบันถูกใช้เข้าระบบได้สำเร็จ ทั้งนี้การพัฒนาระบบจำเป็นต้องมีการเปลี่ยนแปลง แก้ไข ขั้นตอนและวิธีการทำงานของโปรแกรมล็อกอิน (login) ให้แตกต่างไปจากเดิมบ้าง เช่น การแยกส่วนของการตรวจสอบรหัสผ่านของลงบันทึกเข้าใช้ที่ใช้ระบบของรหัสผ่านแบบใช้ครั้งเดียวให้เป็นหน้าที่ของส่วนให้บริการรหัสผ่านแบบใช้ครั้งเดียว เป็นต้น สามารถสรุปการพัฒนาระบบ ได้ดังนี้

1. ส่วนประกอบที่สำคัญของระบบ

1.1 ส่วนให้บริการรหัสผ่านแบบใช้ครั้งเดียว

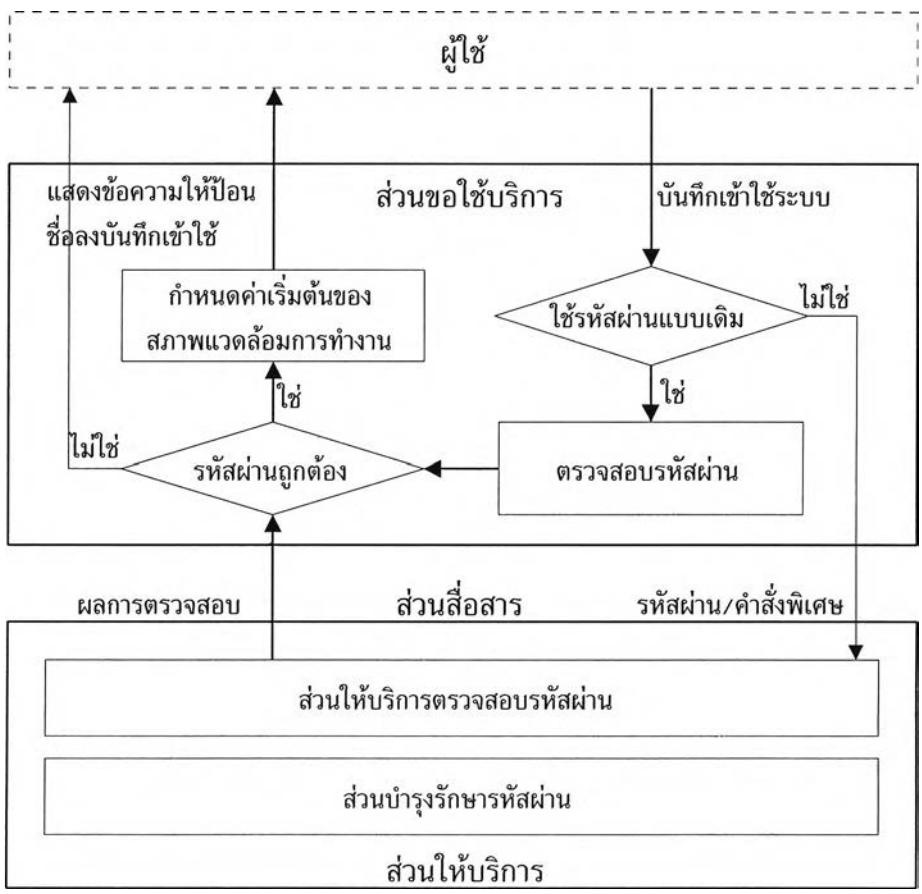
ทำหน้าที่บำรุงรักษารหัสผ่านแบบใช้ครั้งเดียว ให้บริการตรวจสอบรหัสผ่านที่ส่งมาจากส่วนขอใช้บริการ และส่งผลการตรวจสอบกลับไป โดยใช้เครื่อง PC ที่ทำงานภายใต้ระบบปฏิบัติการดอส

1.2 ส่วนขอใช้บริการรหัสผ่านแบบใช้ครั้งเดียว

ประกอบด้วยโปรแกรมอรรถประโยชน์ที่มากับระบบปฏิบัติการต่าง ๆ ที่ทำหน้าที่ในการพิสูจน์ตัวจริงของผู้ใช้ (authentication) เช่น โปรแกรมล็อกอินที่ได้รับการเปลี่ยนแปลงบางส่วนเพื่อให้สามารถกำหนดทางเลือกในการตรวจสอบรหัสผ่านให้เป็นแบบเดิม หรือใช้ระบบรหัสผ่านแบบใช้ครั้งเดียวได้

1.3 การสื่อสารระหว่างส่วนให้บริการกับส่วนขอใช้บริการ

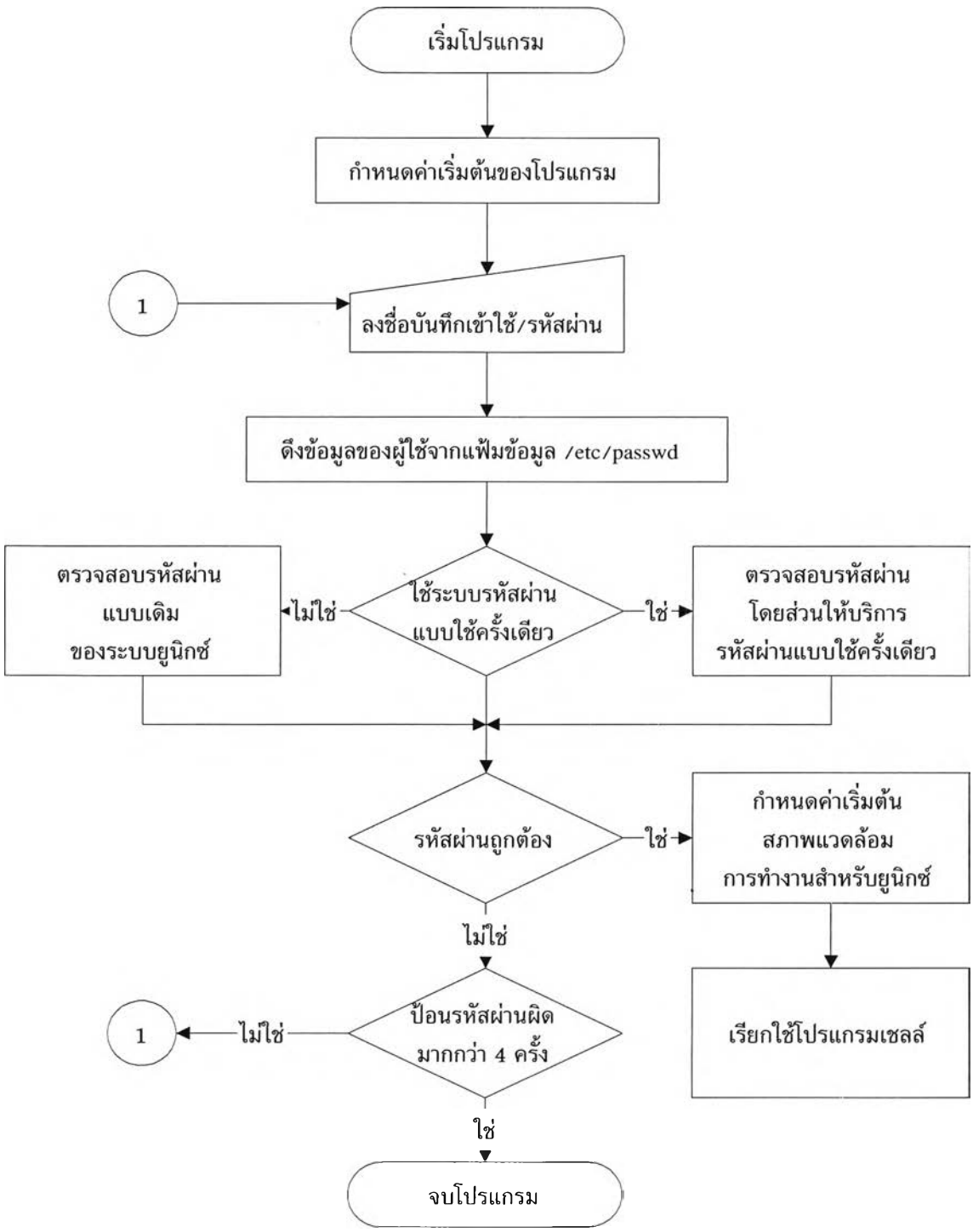
เนื่องจากการสื่อสารระหว่างส่วนให้บริการกับส่วนขอใช้บริการมีลักษณะเป็นแบบสอบถามตอบสนอง คือ เมื่อฝ่ายใดฝ่ายหนึ่งทำการส่งข้อมูลออกไป ต้องรอจนกว่ามีข้อมูลโต้ตอบกลับมา ถ้าระยะเวลาที่รอนานเกินกว่าช่วงเวลาที่กำหนดไว้ ฝ่ายรอจะส่งกลุ่มข้อมูลเดิมซ้ำไปอีกครั้งหนึ่ง อีกทั้งกลุ่มข้อมูลที่ใช้ในการรับส่งมีขนาดเล็ก โปรโตคอลยูพีดี (UPD, User Datagram Protocol) ซึ่งเป็นส่วนหนึ่งของชุดโปรโตคอลทีซีพี/ไอพี (TCP/IP Protocol Suite, Transmission Control Protocol/Internet Protocol) จึงถูกนำมาใช้ในการวิจัยนี้



รูปที่ 2.1 แผนภูมิการทำงานของระบบให้บริการรหัสผ่านแบบใช้ครั้งเดียว

2. ขั้นตอนการทำงานของโปรแกรมล็อกอิน

ในรูปที่ 2.2 แสดงขั้นตอนการทำงานของโปรแกรมล็อกอินหลังจากได้รับการพัฒนา รายละเอียดสามารถหาดูได้จากการพัฒนาระบบของคุณพิษณุ ในบทที่ 4



รูปที่ 2.2 แสดงขั้นตอนการทำงานของโปรแกรมล็อกอินในระบบของคุณพิษณุ

3. กลุ่มข้อมูลที่ใช้ในการติดต่อสื่อสาร

จากรูปที่ 2.2 การสื่อสารระหว่างส่วนขอใช้และส่วนให้บริการรหัสผ่านระบบของคุณพิษณุจะเกิดขึ้นเมื่อโปรแกรมล็อกอินต้องการตรวจสอบรหัสผ่าน สร้างรหัสผ่านชุดใหม่ หรือกระทำการใด ๆ ที่เกี่ยวข้องกับรหัสผ่านเท่านั้น กลุ่มข้อมูลที่สอดคล้องกับตารางที่ 2.1 จะถูกส่งจากโปรแกรมล็อกอินให้กับส่วนให้บริการตรวจสอบรหัสผ่านทำการตรวจสอบและส่งผลการทำงานกลับให้โปรแกรมล็อกอิน สำหรับรายละเอียดของข้อมูลที่เกี่ยวข้องและชนิดของกลุ่มข้อมูล อธิบายได้จากตารางที่ 2.2 และตารางที่ 2.3 ตามลำดับ

ฟิลด์	รูปแบบ	รายละเอียด
Time_val	Char[10]	เวลาที่สร้างกลุ่มข้อมูลนี้
Cli_addr	Char[16]	ไอพีแอดเดรสของผู้ขอบริการ
Type	Int	ชนิดของกลุ่มข้อมูล
Acc_name	Char[8]	ชื่อลงบันทึกเข้าใช้ของผู้ใช้
Data	Char[70]	ข้อมูลที่เกี่ยวข้อง

ตารางที่ 2.1 แสดงถึงรูปแบบของกลุ่มข้อมูลที่ใช้ในการติดต่อสื่อสาร

ข้อมูล	รายละเอียด
******	รหัสผ่านปัจจุบัน
******>	เลื่อนไปใช้รหัสผ่านตัวแรกในคอลัมน์ถัดไป
******>>	เลื่อนไปใช้รหัสผ่านตัวแรกในแฟ้มรหัสผ่านชุดถัดไป
******G หรือ ******g	สร้างรหัสผ่านชุดใหม่
Ok	รหัสผ่านถูกต้อง
Not-ok	รหัสผ่านไม่ถูกต้อง
Message	ข้อความต่าง ๆ
Error Message	ข้อผิดพลาดต่าง ๆ

ตารางที่ 2.2 แสดงข้อมูลที่เกี่ยวข้อง

ชนิด	ส่ง/รับ	เหตุการณ์ที่เกี่ยวข้อง
1	L/P	เมื่อต้องการตรวจสอบรหัสผ่าน
2	P/L	ผลของการตรวจสอบรหัสผ่านกลับสู่โปรแกรมล็อกอิน
4	L/P	เมื่อต้องการสร้างรหัสผ่านชุดใหม่
5	L/P	เมื่อต้องการเลื่อนไปใช้รหัสผ่านตัวแรกในคอลัมน์ถัดไป
6	L/P	เมื่อต้องการเลื่อนไปใช้รหัสผ่านตัวแรกในแฟ้มรหัสผ่านชุดถัดไป
9	P/L	1. ผลของการสร้างรหัสผ่านชุดใหม่ 2. ผลของการเลื่อนไปใช้รหัสผ่านตัวแรกในคอลัมน์ถัดไป 3. ผลของการเลื่อนไปใช้รหัสผ่านตัวแรกในแฟ้มรหัสผ่านชุดถัดไป
99	P/L	เมื่อมีความผิดพลาดในการทำงาน

หมายเหตุ

L/P : โปรแกรมล็อกอินส่งความต้องการให้กับส่วนให้บริการรหัสผ่าน

P/L : โปรแกรมล็อกอินรับผลการทำงานจากส่วนให้บริการรหัสผ่าน

ตารางที่ 2.3 แสดงชนิดของกลุ่มข้อมูลที่ใช้ในการติดต่อสื่อสาร

วิทยาการเข้ารหัสลับ

วิทยาการเข้ารหัสลับเป็นศาสตร์ที่ถูกคิดขึ้นมาเพื่อสร้างความปลอดภัยให้กับข้อมูลที่ต้องการส่งไปยังผู้รับ หลักการทำงานคือ ผู้ส่งจะทำการเข้ารหัส (encryption) ข้อมูล (plaintext หรือ cleartext) ก่อนส่งไปยังผู้รับ ด้วยอัลกอริทึมทางคณิตศาสตร์เพื่อให้ได้ผลลัพธ์ (ciphertext) ที่ผู้อื่นซึ่งได้อาจรับข้อมูลนี้จากการรั่วไหลหรือลักลอบดักฟังข้อมูล ไม่สามารถเข้าใจได้ จะมีเพียงแต่ผู้รับที่ทราบวิธีการถอดรหัส (decryption) นี้เท่านั้นที่สามารถถอดรหัสข้อมูลที่ส่งมาให้ได้ ดังรูปที่ 2.3

รูปที่ 2.3 การเข้ารหัสข้อมูล

เทคนิคที่ใช้ในการเข้ารหัสสามารถแบ่งออกได้เป็น 3 ประเภท ดังนี้

1) ฟังก์ชันแบบแฮช (hashing function)

2) การเข้ารหัสโดยใช้คีย์ลับเฉพาะ (Private key encryption)

3) การเข้ารหัสโดยใช้คีย์สาธารณะ (Public key encryption)

1. ฟังก์ชันแบบแฮช

ฟังก์ชันแบบแฮชเป็นการใช้เพียงกระบวนการทางคณิตศาสตร์เพื่อมาทำการเข้ารหัส โดยมีรูปแบบทั่วไปดังนี้

$$H = f(M)$$

M คือ ข้อมูลที่ป้อนเข้าฟังก์ชัน มีขนาดไม่แน่นอน
H คือ ผลลัพธ์ที่ได้จากฟังก์ชัน มีขนาดคงที่

ฟังก์ชันแบบแฮชถูกออกแบบมาให้มีคุณสมบัติดังนี้

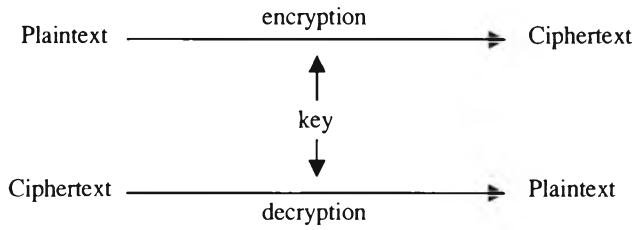
1. สามารถรองรับข้อมูลที่ป้อนเข้าได้หลายขนาด
2. ผลลัพธ์ที่ได้จากฟังก์ชัน มีขนาดคงที่
3. เมื่อฟังก์ชันถูกให้ค่า M สามารถคำนวณหาผลลัพธ์ได้โดยง่าย
4. จากฟังก์ชัน เมื่อมีเพียงค่า H ไม่สามารถหาค่า M ได้
5. ถ้าให้ $f(x) = f(y)$ ค่า x ต้องเท่ากับค่า y เสมอ

ตัวอย่างของฟังก์ชันแบบแฮช ได้แก่ MD2 MD4 และ MD5 [5]

ปัญหาที่เกิดขึ้นจากการพัฒนาอัลกอริทึมใหม่ คือ ต้องใช้ระยะเวลานานพอควรในการพัฒนาและอธิบายอัลกอริทึมใหม่ให้กับผู้ที่ต้องการติดต่อ แต่ไม่สามารถเก็บอัลกอริทึมใหม่ให้เป็นความลับได้นาน แนวโน้มในปัจจุบัน การใช้คีย์เป็นรหัสลับในการเข้ารหัสร่วมกับอัลกอริทึมที่อาจรู้จักกันอย่างแพร่หลายจึงได้รับความนิยมเพิ่มขึ้น ทำให้ความปลอดภัยของข้อมูลที่ถูกเข้ารหัสขึ้นอยู่กับคีย์ที่ใช้ ซึ่งหมายความว่าข้อมูลที่ถูกดักฟังไม่สามารถถูกนำไปถอดรหัสโดยใช้อัลกอริทึมเพียงอย่างเดียวได้

2. การเข้ารหัสโดยใช้คีย์ลับเฉพาะ

เป็นเทคนิคที่ใช้สำหรับเข้ารหัสและถอดรหัสข้อมูลโดยใช้คีย์เดียวกัน ดังนั้นทั้งสองฝ่ายจึงต้องทราบคีย์ที่ใช้ร่วมกัน ปัญหาที่เกิดขึ้นคือ เรื่องความปลอดภัยในการกระจายคีย์ แต่มีข้อดีของการเข้ารหัสประเภทนี้ คือ สามารถทำงานได้รวดเร็ว



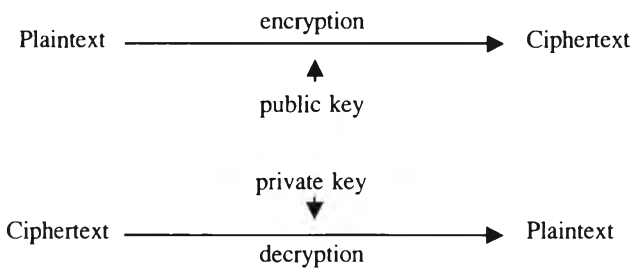
รูปที่ 2.4 การเข้ารหัสโดยใช้คีย์ส่วนตัว

ตัวอย่างของการเข้ารหัสโดยใช้คีย์ลับเฉพาะ ได้แก่ DES IDEA [5]

3. การเข้ารหัสโดยใช้คีย์สาธารณะ

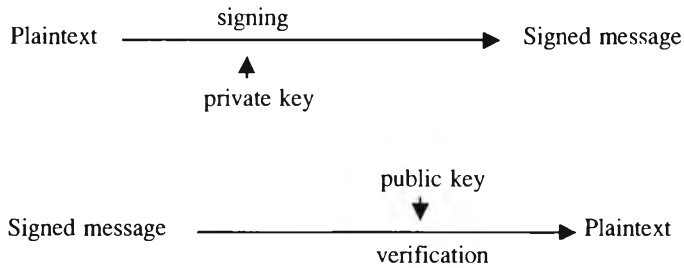
เป็นเทคนิคที่ใช้สำหรับเข้ารหัสและถอดรหัสข้อมูลโดยใช้คีย์จำนวน 2 ตัว รูปแบบการใช้งานจะแตกต่างกัน ดังนี้

3.1 เข้ารหัสด้วยคีย์สาธารณะและถอดรหัสโดยใช้คีย์ส่วนตัว ใช้ในกรณีที่ต้องการให้เจ้าของคีย์ส่วนตัวเท่านั้นที่สามารถถอดรหัสได้



รูปที่ 2.5 การเข้ารหัสโดยใช้คีย์สาธารณะ

3.2 เข้ารหัสด้วยคีย์ส่วนตัวและถอดรหัสโดยใช้คีย์สาธารณะ ใช้ในกรณีที่ต้องการแสดงความเป็นเจ้าของข้อมูล ซึ่งเปรียบเสมือนการลงชื่อกำกับในเอกสารแต่ทำบนข้อมูลอิเล็กทรอนิคส์แทน (digital signature)



รูปที่ 2.6 การถอดรหัสโดยใช้คีย์สาธารณะ

ข้อดีของการเข้ารหัสโดยใช้คีย์สาธารณะคือ ไม่ต้องเปิดเผยคีย์ส่วนตัวจะเปิดเผยเฉพาะคีย์สาธารณะเท่านั้นทำให้มีความปลอดภัยในการนำมาใช้เพื่อการพิสูจน์แสดงตัว แต่ประสิทธิภาพในการทำงานจะต่ำกว่าการเข้ารหัสโดยใช้คีย์ลับเฉพาะจึงไม่เหมาะสำหรับข้อมูลขนาดใหญ่

ตัวอย่างของการเข้ารหัสโดยใช้คีย์สาธารณะ ได้แก่ RSA [5]