Sะบบรหัสลับที่เพิ่มความปลอดภัยให้กับข้อมูล

Cryptosystem for Data Security

ดร.วรากร ศรีเชวงทรัพย์
อาจารย์ประจำสาขาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีไทย-ญี่ปุ่น

บทคัดย่อ

บทความฉบับนี้มีวัตถุประสงค์เพื่อนำเสนอวิวัฒนาการของการเข้ารหัสลับ โดยเริ่มต้นจากวิธีการเข้ารหัสแบบซีซาร์ ซึ่งการเข้ารหัสนี้ถูกตั้งชื่อตามจูเลียส ซีซาร์ ผู้ที่นำวิธีการเข้ารหัสลับมาใช้ในการติดต่อกับเหล่าแม่ทัพในยามศึกสงคราม ต่อมาได้มีการพัฒนาวิธีการเข้ารหัสลับแบบต่าง ๆ เพื่อให้การสื่อสารข้อมูลมีความปลอดภัยมากขึ้น จนกระทั่งในปัจจุบันวิธีการเข้ารหัสลับข้อมูลที่ได้รับนิยมเป็นอย่างมากมีอยู่ 2 วิธี ได้แก่ 1. การเข้ารหัสแบบกุญแจลับ 2. การเข้ารหัสลับแบบกุญแจสาธารณะ ในบทความฉบับนี้ได้เปรียบเทียบข้อดีและข้อเสียของวิธีการเข้ารหัสลับทั้ง 2 แบบ พร้อมทั้งแสดงวิธีการนำการเข้ารหัสลับแบบกุญแจสาธารณะด้วยวิธี RSA ไปใช้ประโยชน์ในเรื่องของความต้องการความเป็นส่วนตัวและการยืนยันตัวบุคคล สำหรับส่วนสุดท้ายของบทความฉบับนี้ได้กล่าวถึงปัจจัยที่มีผลต่อความปลอดภัยของวิธีการเข้ารหัสลับแบบกุญแจสาธารณะด้วยวิธี RSA

คำสำคัญ: การเข้ารหัสลับแบบกุญแจสาธารณะ การเข้ารหัสแบบกุญแจลับ RSA

Abstract

This article presents the evolution of cryptography since the initiation of Caesar cipher, the encryption technique named after Julius Caesar who had invented encryption to communicate with his generals during wartime. Later several methods have been developed to improve the communication security. Recently the secret key encryption and the public key encryption have become the most popular encryption techniques. The advantages and disadvantages of these two techniques have been discussed in this article. We also show how RSA, the most famous of

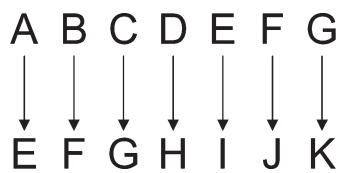
the public key cryptosystem, provides cryptographic privacy and authentication for data communication. Finally, the security issues related to RSA encryption have been discussed.

Keywords: Public key cryptography, Secret key cryptography, RSA

บทนำ

ในปัจจุบันเป็นยุคสังคมข่าวสารข้อมูล วิธีการที่ใช้ในการสื่อสารมีอยู่หลากหลายรูปแบบอย่างเช่น การส่งสัญญาณภาพและเสียงผ่านทางช่องสัญญาณดาวเทียม การส่งข้อมูลต่างๆ ผ่านทางเครือข่ายอินเทอร์เน็ต และการส่งสัญญาณเสียงผ่านทางระบบเครือข่ายโทรศัพท์ การสื่อสารด้วยวิธีต่างๆ ที่กล่าวมานั้นอาจถูกผู้ไม่หวังดีดักฟังหรือดักจับข้อมูลได้โดยไม่ยากนัก (Atkins, 1997) ซึ่งการดักฟังหรือดักจับข้อมูลนี้อาจก่อให้เกิดผลเสียหายต่อผู้ที่เกี่ยวข้อง อย่างเช่น ในวงการธุรกิจหากข้อมูลของบริษัทหนึ่งรั่วไหลไปยังบริษัทคู่แข่ง จะทำให้เกิดการเสียเปรียบอย่างมากในการแข่งขัน หรือในทางการทหาร หากฝ่ายหนึ่งสามารถล่วงรู้ความลับของอีกฝ่ายหนึ่ง อาจส่งผลให้การศึกนั้นจบลงด้วยความปราชัยของฝ่ายที่ปล่อยให้ความลับรั่วไหล ด้วยเหตุนี้จึงได้มีการพัฒนาวิธีการที่ช่วยให้การรับส่งข้อมูลเป็นความลับ ซึ่งวิธีการที่นำมาใช้นี้ได้แก่การเข้ารหัสลับ (Encryption) โดยการเข้ารหัสลับคือการเปลี่ยนข้อความปกติที่สามารถอ่านรู้เรื่อง (Plain text) ไปเป็นข้อความที่ถูกเข้ารหัส (Cipher text) ซึ่งเป็นข้อความที่ไม่สามารถอ่านรู้เรื่องได้ ในสมัยก่อนการเข้ารหัสลับถูกนำมาใช้เพื่อเพิ่มความปลอดภัยให้กับข้อมูลข่าวสารที่ส่งไป ถึงแม้ฝ่ายตรงข้ามจะสามารถจับผู้ที่นำข่าวสารและเห็นข้อความที่ถูกเข้ารหัสก็ไม่สามารถที่จะรู้ได้ว่าข้อความที่เห็นนั้นต้องการจะสื่อสารอะไร

วิธีการเข้ารหัสที่มีชื่อเสียงมากในสมัยก่อนได้แก่ การเข้ารหัสแบบซีซาร์ (Caesar Cipher) (Henk, 2000) โดยการเข้ารหัสนี้ถูกตั้งชื่อตาม จูเลียส ซีซาร์ ซึ่งเป็นผู้ที่ริเริ่มนำวิธีการเข้ารหัสมาใช้เพื่อติดต่อกับเหล่าแม่ทัพในช่วงทำสงคราม สำหรับหลักการเข้ารหัสแบบซีซาร์นั้นจะใช้การแทนที่ตัวอักขระที่ต้องการส่งด้วยตัวอักขระอื่นที่มีอยู่ถัดมา x ตำแหน่ง ยกตัวอย่างเช่น หากกำหนดให้ x = 4 และผู้ส่งต้องการที่จะส่งข้อความ “see you tomorrow” เมื่อใช้วิธีการเข้ารหัสแบบซีซาร์ จะได้ข้อความที่ถูกเข้ารหัสดังนี้ “wii csy xsqsvvsa” จากนั้นทางฝ่ายผู้รับจะแทนที่ตัวอักขระแต่ละตัวในข้อความด้วยตัวอักขระที่อยู่ก่อนหน้า x ตำแหน่ง ผลลัพธ์ที่ได้คือข้อความที่ผู้ส่งต้องการสื่อสาร เราสามารถแสดงตัวอย่างการแทนที่ตัวอักขระของข้อความต้นฉบับด้วยตัวอักขระที่ใช้ในการเข้ารหัสได้ดังรูปที่ 1



รูปที่ 1: ตัวอย่างการแทนที่ตัวอักขระของข้อความต้นฉบับด้วยตัวอักขระที่อยู่ถัดไป 4 ตำแหน่ง

ในระยะหลังการเข้ารหัสแบบซีซาร์ไม่ค่อยเป็นที่นิยมนัก เนื่องจากรูปแบบการเลื่อนหรือแทนที่ตัวอักขระสามารถทำได้เพียง 26 แบบ หากผู้ไม่หวังดีรู้วิธีการเข้ารหัสก็จะสามารถถอดรหัสข้อความได้ โดยการค่อยๆ เลื่อนตำแหน่งของตัวอักขระไปทีละ 1 ตำแหน่ง ตัวอย่างขั้นตอนการถอดรหัสข้อความของผู้ไม่หวังดีสามารถแสดงได้ดังนี้ หากข้อความที่ถูกเข้ารหัสเป็นดังนี้ “wii csy xsqsvvsa” เมื่อเลื่อนตัวอักขระของข้อความไป 1 ครั้ง จะได้ข้อความ “xjj dtz ytrtwwtb” ออกมา เมื่อเลื่อนตัวอักขระของข้อความไป 2 ครั้ง จะได้ข้อความ “ykk

eua zusuxxuc" และเมื่อเลื่อนตัวอักขระไป 22 ครั้ง จะได้ข้อความ "see you tomorrow" ซึ่งเป็นข้อความที่ผู้ไม่หวังดีสามารถอ่านรู้เรื่อง ผู้ไม่หวังดีจึงทราบว่าการถอดรหัสข้อความนั้นประสบความสำเร็จ

ในปัจจุบันได้มีการพัฒนาวิธีการเข้ารหัสแบบต่างๆ ขึ้นมา โดยจะใช้กุญแจ (Key) ซึ่งเป็นข้อมูลตัวเลขหรือตัวอักษรที่มีหน่วยความยาวเป็นบิต (Bit) ตัวอย่างของกุญแจสั้น ๆ ได้แก่ 5A4C4981 ซึ่งตัวเลขหรือตัวอักษรแต่ละตัวสามารถนำไปแทนได้ด้วยตัวเลขไบนารีหรือตัวเลขฐาน 2 ขนาด 4 บิต ยกตัวอย่างเช่นตัวเลข 5 ซึ่งเป็นข้อมูลตัวแรกของกุญแจจะมีค่าเท่ากับ 0101 และตัวอักษร A ซึ่งในระบบเลขฐาน 16 ตัวอักษรนี้ถูกนำมาใช้แทนตัวเลข 10 เมื่อนำตัวอักษรนี้มาเขียนแบบตัวเลขฐานสองขนาด 4 บิต จะได้มีค่าเท่ากับ 1010 เมื่อใช้หลักการแทนค่าข้างต้น ข้อมูลกุญแจ 5A4C4981 จะสามารถแทนได้ด้วยตัวเลขฐานสองขนาดความยาว 32 บิตดังนี้ 01011010010011000100100110000001 เมื่อต้องการเข้ารหัสก็จะนำข้อความที่ต้องการเข้ารหัสมาเปลี่ยนเป็นตัวเลขฐานสองเช่นเดียวกันกับข้อมูลกุญแจ โดยการเข้ารหัสข้อมูลคือการนำข้อมูลตัวเลขของกุญแจและข้อมูลตัวเลขของสิ่งที่ต้องการเข้ารหัสมาผ่านกระบวนการคำนวณทางคณิตศาสตร์ อย่างเช่น การบวก ลบ คูณ หาร ยกกำลัง และหารเอาเศษ ผลลัพธ์ที่ได้ถูกเรียกว่าข้อมูลที่ถูกเข้ารหัสลับ และเมื่อผู้รับต้องการที่ถอดรหัสก็จะนำข้อมูลที่ถูกเข้ารหัสลับและข้อมูลกุญแจมาผ่านกระบวนการคำนวณทางคณิตศาสตร์ โดยผลลัพธ์ที่ได้คือข้อมูลที่ผู้ส่งต้องการสื่อสาร

ในบทความฉบับนี้จะกล่าวถึงรายละเอียดของวิธีการที่ใช้ในการเข้ารหัสข้อมูล พร้อมทั้งแสดงตัวอย่างการใช้งาน โดยมีลำดับการนำเสนอดังนี้

1. ระบบการเข้ารหัสแบบกุญแจลับ (Secret key cryptography) (Mel, 2001)

2. ระบบการเข้ารหัสลับแบบกุญแจสาธารณะ (Public key cryptography) (Buchmann, 2004)

3. การเข้ารหัสลับแบบกุญแจสาธารณะด้วยวิธี RSA (Coutinho, 1999)

4. ความปลอดภัยของการเข้ารหัสลับแบบกุญแจสาธารณะด้วยวิธี RSA

ระบบการเข้ารหัสแบบกุญแจลับ (Secret key cryptography)

สำหรับระบบการเข้ารหัสแบบกุญแจลับนั้นจะใช้กุญแจลับดอกเดียวในการเข้ารหัสและถอดรหัสข้อมูล (Denning, 1982) ดังแสดงในรูปที่ 2 โดยการติดต่อระหว่างบุคคล 2 คน จะต้องใช้กุญแจลับ 1 ดอก ในกรณีที่มีบุคคลที่ต้องการติดต่อเป็นจำนวนมากก็จำเป็นที่จะต้องมีจำนวนของกุญแจลับที่ใช้งานเพิ่มขึ้นตามไปด้วย ยกตัวอย่างเช่น หากมีบุคคลที่ต้องการติดต่อสื่อสารด้วยจำนวน 10 คน จะต้องมีกุญแจลับทั้งหมดจำนวน $\binom{10}{2}$ หรือ 45 ดอก โดยที่ $\binom{n}{r} = \frac{n!}{(n-r)!\,r!}$

นอกจากนี้ผู้ส่งและผู้รับจะต้องหาทางตกลงกันเรื่องกุญแจลับที่ใช้ ซึ่งหากผู้ส่งและผู้รับไม่ได้อยู่ที่เดียวกัน ผู้ส่งจำเป็นที่จะต้องหาช่องทางหรือวิธีการสื่อสารที่ปลอดภัยในการแจ้งกุญแจลับให้กับผู้รับ ซึ่งหากช่องทางที่ว่ามีอยู่จริง ผู้ส่งและผู้รับควรจะใช้ช่องทางนั้นในการติดต่อสื่อสารกันโดยไม่ต้องเสียเวลาในการเข้ารหัส จากที่กล่าวมาข้างต้นจะเห็นว่าการจัดการกุญแจลับยังคงเป็นเรื่องที่ยุ่งยากในกรณีที่ผู้ส่งและผู้รับไม่ได้อยู่ที่เดียวกัน

ระบบการเข้ารหัสลับแบบกุญแจสาธารณะ (Public key cryptography)

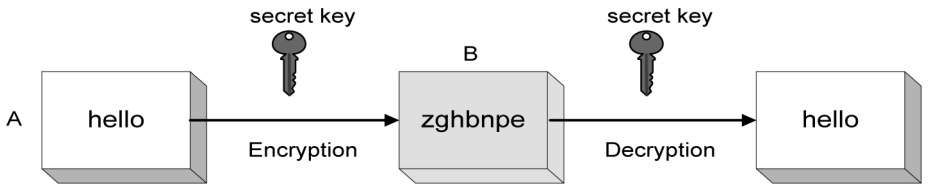
ระบบการเข้ารหัสลับแบบกุญแจสาธารณะถูกพัฒนาขึ้นมาเพื่อแก้ไขข้อจำกัดของระบบการเข้ารหัสแบบกุญแจลับ สำหรับระบบการเข้ารหัสลับแบบกุญแจสาธารณะนั้น จะกำหนดให้ผู้ใช้แต่ละรายถือกุญแจ 2 ดอก โดยกุญแจดอกแรกถูกเรียกว่ากุญแจส่วนตัว (Private key) และกุญแจดอกที่ 2 ถูกเรียกว่ากุญแจสาธารณะ (Public key) โดยมีเพียงเจ้าของกุญแจเท่านั้นที่ทราบกุญแจส่วนตัวของตนเอง ในขณะที่กุญแจสาธารณะจะถูกประกาศให้คนอื่นทราบได้ บุคคล 2 คน

สามารถส่งข้อมูลหากันได้เพียงแค่ทราบกุญแจสาธารณะของอีกฝ่ายหนึ่ง หากมีบุคคลที่ต้องการติดต่อสื่อสารจำนวน 10 คน จะต้องมีกุญแจส่วนตัวและกุญแจสาธารณะอย่างละ 10 ดอก จะพบว่าจำนวนกุญแจทั้งหมดที่ต้องใช้น้อยกว่าเมื่อเทียบกับการเข้ารหัสแบบกุญแจลับ

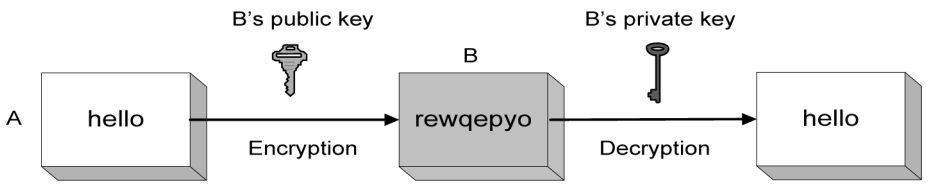
การเข้ารหัสลับแบบกุญแจสาธารณะนั้น สามารถนำไปใช้งานตามวัตถุประสงค์ต่างๆ ดังนี้

1. ความต้องการความเป็นส่วนตัว

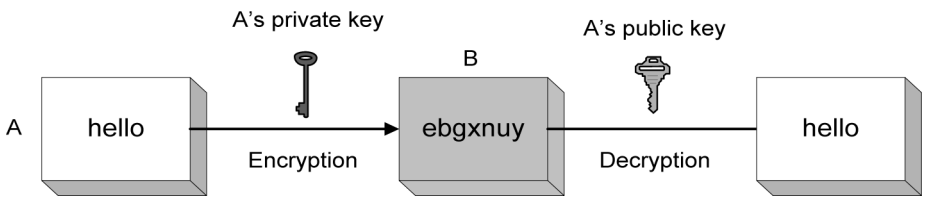
หากผู้ใช้ A ต้องการส่งข้อมูลไปยังผู้ใช้ B อย่างเป็นความลับ ผู้ใช้ A สามารถทำได้โดยนำกุญแจสาธารณะของผู้ใช้ B มาเข้ารหัสข้อมูล จากนั้นจึงส่งข้อมูลที่ถูกเข้ารหัสไปให้ B ดังแสดงในรูปที่ 3 จะสังเกตได้ว่าผู้ใช้คนอื่นๆ ไม่สามารถถอดรหัสข้อมูลได้ จะมีเพียงแต่ผู้ใช้ B เพียงรายเดียวเท่านั้นที่สามารถถอดรหัสข้อมูลนั้นได้ เนื่องจากผู้ใช้ B เป็นผู้ที่ถือกุญแจส่วนตัวเพียงคนเดียว เราจึงสามารถนำวิธีการเข้ารหัสแบบนี้ไปใช้ในการส่งข้อมูลแบบส่วนตัวได้ แต่วิธีการนี้ไม่สามารถยืนยันตัวผู้ที่ส่งข้อมูลได้ เนื่องจากผู้ใช้รายใดก็ตามที่ทราบกุญแจสาธารณะของ B สามารถปลอมข้อมูลขึ้นมาและส่งข้อมูลไปหา B ได้



รูปที่ 2: ขั้นตอนการเข้ารหัสและถอดรหัสข้อมูลของระบบการเข้ารหัสแบบกุญแจลับ



รูปที่ 3: ความเป็นส่วนตัวในระบบกุญแจสาธารณะ



รูปที่ 4: การยืนยันตัวบุคคลในระบบกุญแจสาธารณะ

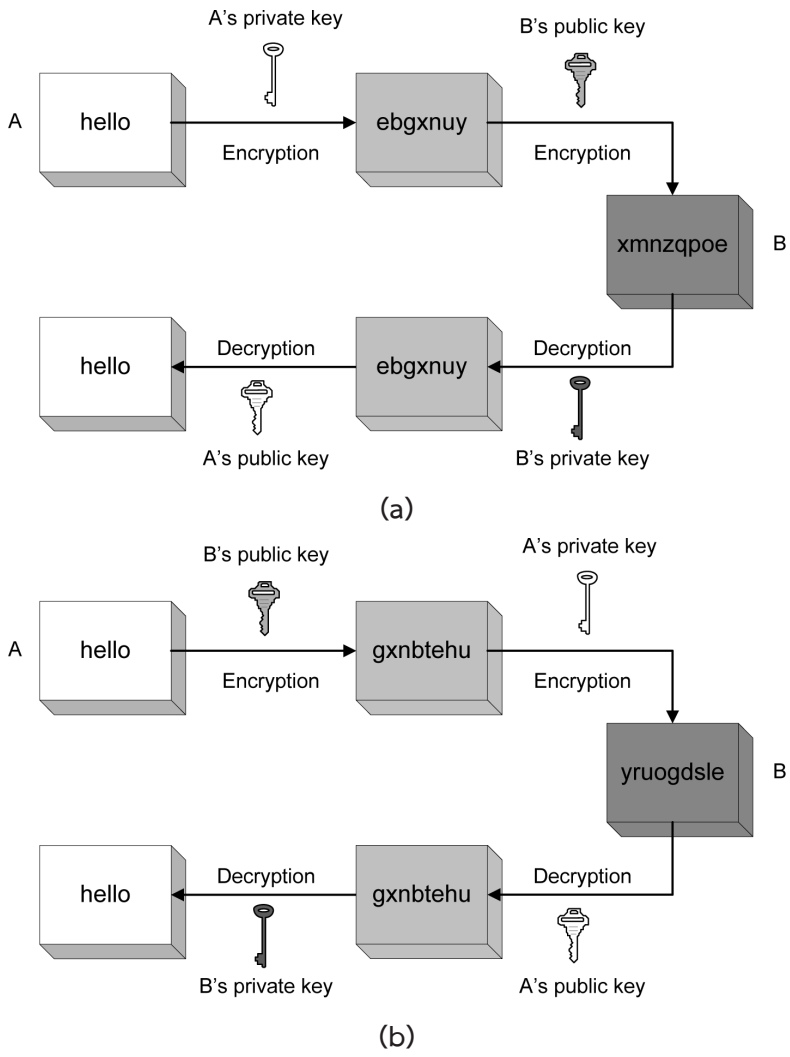
2. การยืนยันตัวบุคคล

หากผู้ใช้ A ต้องการยืนยันให้ผู้ใช้ B ทราบว่า ข้อมูลที่ส่งไปนั้นมาจากผู้ใช้ A สามารถทำได้โดยการใช้กุญแจส่วนตัวของ A ในการเข้ารหัสข้อมูล เมื่อผู้ใช้ B ได้รับข้อมูลที่ถูกเข้ารหัส ก็จะนำกุญแจสาธารณะของ A มาถอดรหัส ดังแสดงในรูปที่ 4 หากสามารถถอดรหัสได้ ผู้ใช้ B ก็สามารถมั่นใจได้ว่าข้อมูลนั้นถูกส่งมาจากผู้ใช้ A จริงๆ เนื่องจากมีผู้ใช้ A เพียงรายเดียวที่เข้ารหัสข้อมูลได้

เราเรียกวิธียืนยันตัวบุคคลนี้ว่าการใช้ “ลายมือชื่อดิจิทัล (Digital Signature)” (Mao, 2004) เพื่อการยืนยันตัวบุคคล แต่วิธีการนี้ไม่สามารถรับรองได้ว่าข้อมูลที่ส่งไปจะเป็นความลับ เนื่องจากมีหลายบุคคลที่ทราบกุญแจสาธารณะของ A และบุคคลเหล่านั้นสามารถถอดรหัสลับข้อมูลได้

3. การรับประกันทั้งเรื่องความเป็นส่วนตัวและการยืนยันตัวบุคคล

หากต้องการที่จะรับประกันทั้งเรื่องความเป็นส่วนตัวและการยืนยันตัวบุคคล สามารถทำได้โดยให้ผู้ใช้ A เข้ารหัสข้อมูลด้วยกุญแจส่วนตัวของตนเอง จากนั้นจะนำข้อมูลที่ถูกเข้ารหัสมาเข้ารหัสอีกชั้นหนึ่งโดยใช้กุญแจสาธารณะของผู้ใช้ B จะพบว่าผู้ที่สามารถถอดรหัสข้อมูลชั้นแรกได้มีเพียงผู้ใช้ B รายเดียวเท่านั้น และเมื่อผู้ใช้ B นำกุญแจสาธารณะของผู้ใช้ A มาถอดรหัสข้อมูลอีกชั้นก็จะสามารถอ่านข้อมูลที่ถูกส่งมาจากผู้ใช้ A ได้ ดังแสดงในรูปที่ 5(a) วิธีการนี้จึงสามารถยืนยันได้ว่าข้อมูลนั้นถูกส่งมาจากผู้ใช้ A และมีเพียงผู้ใช้ B เพียงรายเดียวที่สามารถอ่านข้อมูลนั้นได้ นอกจากนี้หากสลับลำดับกุญแจที่ใช้ในการเข้ารหัสและถอดรหัสจะพบว่าวิธีการนี้ก็ยังสามารถรับประกันทั้งเรื่องความเป็นส่วนตัวและการยืนยันตัวบุคคลได้ ดังแสดงในรูปที่ 5(b)



รูปที่ 5: ความเป็นส่วนตัวและการยืนยันข้อมูลในระบบกุญแจสาธารณะ

การเข้ารหัสลับแบบกุญแจสาธารณะด้วยวิธี RSA

RSA เป็นอัลกอริทึมการเข้ารหัสลับแบบกุญแจสาธารณะ ซึ่งสามารถรองรับความต้องการในเรื่องความเป็นส่วนตัวและการยืนยันตัวบุคคลได้ ผู้ที่คิดค้น RSA ขึ้นมาได้แก่ Ronald Rivest, Adi Shamir และ Leonard Adleman โดยคำว่า RSA ได้มาจากตัวอักขระตัวแรกของนามสกุลผู้คิดค้นทั้ง 3 คน

สำหรับรายละเอียดการสร้างกุญแจส่วนตัวและกุญแจสาธารณะของอัลกอริทึม RSA (DI Management Services Pty Limited, 2011) สามารถแสดงเป็นขั้นตอนได้ดังนี้

ขั้นที่ 1 ให้เลือกจำนวนเฉพาะซึ่งมีค่ามาก 2 ค่า ในที่นี้กำหนดให้เป็นตัวแปร p และ q

ขั้นที่ 2 คำนวณค่าผลคูณระหว่าง p และ q โดยกำหนดให้ $n = p*q$

ขั้นที่ 3 หาค่าผลคูณระหว่าง $p-1$ และ $q-1$ โดยกำหนดให้ $\phi(n) = (p-1)*(q-1)$

ขั้นที่ 4 เลือกค่า e ขึ้นมา โดยค่า e จะต้องมากกว่า 1 และน้อยว่า $\phi(n)$ นอกจากนี้ค่า e และ $\phi(n)$ จะต้องเป็นจำนวนเฉพาะสัมพัทธ์กัน นั่นคือค่า e และ $\phi(n)$ ต้องมีตัวหารร่วมมากเท่ากับ 1

ขั้นที่ 5 คำนวณหาค่า d ซึ่งทำให้ $ed \bmod \phi(n) = 1$ นั่นคือผลคูณระหว่าง และ d เมื่อถูกหารด้วย $\phi(n)$ จะต้องได้เศษของการหารเท่ากับ 1 โดย mod หมายถึงตัวดำเนินการมอดูลัส (Modulus) ซึ่งมีหน้าที่หาค่าเศษของการหารออกมา

เมื่อทำครบทั้ง 5 ขั้นตอนจะได้กุญแจสาธารณะเท่ากับ (n,e) และกุญแจส่วนตัวเท่ากับ (n,d)

ตัวอย่างการคำนวณหากุญแจส่วนตัวและกุญแจสาธารณะ สามารถแสดงได้ดังนี้

ขั้นที่ 1 กำหนดให้ $p = 11$ และ $q = 13$

ขั้นที่ 2 คำนวณหาค่า n ได้ดังนี้

$$\begin{aligned} n &= p*q \\ &= 11*13 \\ &= 143 \end{aligned}$$

ขั้นที่ 3 คำนวณหาค่า $\phi(n)$ ได้ดังนี้

$$\begin{aligned} \phi(n) &= (p-1)*(q-1) \\ &= 10*12 \\ &= 120 \end{aligned}$$

ขั้นที่ 4 เลือกค่า e ขึ้นมา โดยค่า e จะต้องน้อยกว่า 120 และต้องเป็นจำนวนเฉพาะสัมพัทธ์กับ 120 ในที่นี้เลือกค่า e เท่ากับ 7

ขั้นที่ 5 คำนวณหาค่า d ที่ทำให้ $7d \bmod 120 = 1$ จะได้ค่า $d = 103$

ผลลัพธ์ที่ได้จากการคำนวณเป็นดังนี้ ได้กุญแจสาธารณะเท่ากับ (143,7) และได้กุญแจส่วนตัวเท่ากับ (143,103)

สำหรับการนำอัลกอริทึม RSA มาใช้ในเรื่องความต้องการความเป็นส่วนตัว สามารถแสดงได้ดังนี้

หากผู้ใช้ A ต้องการส่งข้อมูลตัวเลข m ไปให้ผู้ใช้ B สามารถทำได้โดยการใช้กุญแจสาธารณะของผู้ใช้ B เข้ารหัสข้อมูลได้ค่า c ออกมา สำหรับสมการการเข้ารหัสข้อมูลสามารถแสดงได้ดังนี้

$$c = m^e \bmod n$$

หากกำหนดให้กุญแจสาธารณะของผู้ใช้ B เท่ากับ (143,7) และค่า m เท่ากับ 4 จะสามารถคำนวณหาค่า c ได้ดังนี้

$$\begin{aligned} c &= 4^7 \bmod 143 \\ &= 82 \end{aligned}$$

เมื่อผู้ใช้ B ได้รับข้อมูลที่ถูกเข้ารหัสไว้ก็จะใช้กุญแจส่วนตัวของตนเองในการถอดรหัสข้อมูล โดยสามารถแสดงสมการการถอดรหัสข้อมูลได้ดังนี้

$$m = c^d \bmod n$$

หากกำหนดให้กุญแจส่วนตัวของผู้ใช้ B เท่ากับ (143,103) จะสามารถแสดงการถอดรหัสข้อมูลเพื่อหาค่า m ได้ดังนี้

$$\begin{aligned} m &= 82^{103} \bmod 143 \\ &= 4 \end{aligned}$$

จากตัวอย่างที่แสดงข้างต้น จะเห็นว่าข้อมูลต้นฉบับและข้อมูลที่ถอดรหัสได้เป็นข้อมูลเดียวกันและมีเพียง

ผู้ใช้ B เพียงคนเดียวที่สามารถถอดรหัสได้ ทำให้ผู้ใช้ A มั่นใจได้ว่าข้อมูลนั้นมีความเป็นส่วนตัวมาก

สำหรับการนำอัลกอริทึม RSA มาใช้เพื่อยืนยันตัวบุคคลสามารถแสดงได้ดังนี้

หากผู้ใช้ A ต้องการส่งข้อมูลตัวเลข m ไปให้ผู้ใช้ B สามารถทำได้โดยการใช้กุญแจส่วนตัวของผู้ใช้ A ในการเข้ารหัสข้อมูล และจะได้ค่า c ซึ่งเป็นข้อมูลที่ถูกเข้ารหัสไว้ สำหรับการเข้ารหัสข้อมูลสามารถแสดงเป็นสมการได้ดังนี้

$$c = m^d \bmod n$$

หากกำหนดให้กุญแจส่วนตัวของผู้ใช้ A เท่ากับ (143,103) และค่า เท่ากับ 4 จะสามารถคำนวณหาค่าได้ดังนี้

$$c = 4^{103} \bmod 143$$
$$= 108$$

เมื่อผู้ใช้ B ได้รับข้อมูลที่ถูกเข้ารหัสไว้ก็จะใช้กุญแจสาธารณะของผู้ใช้ A ในการถอดรหัสข้อมูล โดยสามารถแสดงสมการการถอดรหัสข้อมูลได้ดังนี้

$$m = c^e \bmod n$$

หากกำหนดให้กุญแจสาธารณะของผู้ใช้ A เท่ากับ (143,7) จะสามารถแสดงการถอดรหัสข้อมูลเพื่อหาค่า m ได้ดังนี้

$$m = 108^7 \bmod 143$$
$$= 4$$

จากตัวอย่างที่แสดงข้างต้นพบว่า มีเพียงผู้ใช้ A ที่รู้กุญแจส่วนตัว ดังนั้น A จึงเป็นผู้ใช้รายเดียวที่สามารถเข้ารหัสข้อมูลได้ ทำให้สามารถยืนยันได้ว่าข้อมูลที่ถูกส่งมานั้นมาจากผู้ใช้ A

ความปลอดภัยของการเข้ารหัสลับแบบกุญแจสาธารณะด้วยวิธี RSA

สำหรับความปลอดภัยของวิธี RSA นั้น ขึ้นอยู่กับความยากง่ายในการแยกตัวประกอบค่า n ออกเป็นค่า p และ q ตัวอย่างของการทดสอบเรื่องความปลอดภัยของข้อมูลที่ถูกเข้ารหัสด้วยอัลกอริทึม RSA เกิดขึ้นในปี พ.ศ. 2520 โดยผู้คิดค้นทั้ง 3 คนได้เสนอโจทย์ปัญหาในหนังสือ Scientific American (Janeba, 1994) ในโจทย์ได้บอกค่ากุญแจสาธารณะดังนี้

กำหนดให้

e = 9007, n = 114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541

และข้อมูลที่ถูกเข้ารหัสเป็นดังนี้

c = 9686961375462206147714092225435588290575999112457431987469512093081629822514570835693147662288398962801339199055182994515781515 4

โจทย์ได้กำหนดให้หาข้อมูลต้นฉบับ โดยใช้ข้อมูลที่กำหนดมาให้ข้างต้น สำหรับขั้นตอนที่ยากที่สุดในการถอดรหัสข้อมูล คือการแยกตัวประกอบ n ออกเป็นจำนวนเฉพาะ p และ q เมื่อได้ค่า p และ q จะสามารถนำไปใช้ในการคำนวณหาค่ากุญแจส่วนตัว d ได้โดยง่าย โจทย์ที่ผู้คิดค้นทั้ง 3 คนได้ตั้งในช่วงนั้น ไม่มีใครสามารถหาคำตอบได้ จนกระทั่งในปี พ.ศ. 2537 Paul Leyland, Derek Atkins, Michael Graff และ Arjen Lenstra ได้พยายามที่จะแก้ปัญหานี้อีกครั้งและได้รับความช่วยเหลือจากอาสาสมัครมากกว่า 600 คน จากประเทศต่างๆ มากกว่า 20 ประเทศ และใช้เวลาเพียงแค่ 8 เดือนก็สามารถแยกตัวประกอบ n ออกเป็นจำนวนเฉพาะ 2 ตัวคูณกัน

โดยจำนวนเฉพาะตัวแรกได้แก่ 3490529510847650949147849619903898133417764638493387843990820577

และจำนวนเฉพาะตัวที่ 2 ได้แก่ 3276913299326670954996198819083446141317764296799294253979828853 3

จากนั้นนำจำนวนเฉพาะทั้ง 2 ตัวมาใช้ในการคำนวณกุญแจส่วนตัวได้ผลลัพธ์ดังนี้

d = 106698614368578024442868771328920154780709906633937862801226224496631063125911774470873340168597462306553968544513277109053606095

เมื่อนำค่ากุญแจส่วนตัวมาใช้ในการถอดรหัสได้ข้อมูลต้นฉบับดังนี้

m = 200805001301070903002315180419000118050019172105011309190800151919090618010705

จากนั้นให้แทนเลขต่างๆ ด้วยตัวอักขระดังนี้ 01 = A, 02 = B, ..., 26 = Z จะได้ข้อความ “THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE” ออกมา

จากที่ได้กล่าวมาในข้างต้นสรุปได้ว่าความปลอดภัยของการเข้ารหัสด้วยวิธี RSA ขึ้นกับปัจจัยต่างๆ ดังนี้

1. ความยาวของกุญแจที่ใช้ ตัวอย่างข้างต้นแสดงให้เห็นว่าการใช้กุญแจที่มีความยาวเท่ากับ 428 บิต มีความปลอดภัยไม่เพียงพอในการใช้งานจริง ยิ่งเครื่องคอมพิวเตอร์ที่ใช้งานกันอยู่ทุกวันนี้สามารถทำงานได้รวดเร็วกว่าเครื่องคอมพิวเตอร์ในสมัยก่อนมาก การใช้งานในปัจจุบันจึงได้กำหนดให้ใช้กุญแจที่มีความยาวอย่างน้อยเท่ากับ 1024 บิต จึงจะยอมรับว่าการเข้ารหัสมีความปลอดภัยสูงเพียงพอ

2. ความยากในการแยกตัวประกอบ หากมีผู้ที่สามารถคิดค้นวิธีการแยกตัวประกอบที่ง่ายและรวดเร็วกว่าวิธีที่มีทั้งหมดในปัจจุบัน วิธีการ RSA ก็จะไม่สามารถนำมาใช้งานได้เลย เนื่องจากมีความปลอดภัยไม่เพียงพอ

สรุปและข้อเสนอแนะ

บทความฉบับนี้ได้นำเสนอวิวัฒนาการของการเข้ารหัสลับ และได้กล่าวถึงวิธีการต่าง ๆ ที่ใช้ในการเข้ารหัสลับในปัจจุบัน ซึ่งได้แก่ 1. การเข้ารหัสแบบกุญแจลับ 2. การเข้ารหัสลับแบบกุญแจสาธารณะ และได้เปรียบเทียบวิธีการเข้ารหัสลับทั้ง 2 แบบ ทั้งในเรื่องของความยากง่ายในการจัดการกุญแจ และจำนวนกุญแจที่ต้องใช้เมื่อมีบุคคลที่ต้องการติดต่อกันมากขึ้น

นอกจากนี้ยังได้แสดงตัวอย่างวิธีการนำอัลกอริทึม RSA ไปใช้งานทางด้านความต้องการความเป็นส่วนตัวและการยืนยันตัวบุคคล และแสดงให้เห็นถึงปัจจัยต่างๆ ที่มีผลต่อความปลอดภัยของการเข้ารหัสลับแบบกุญแจสาธารณะด้วยวิธี RSA โดยปัจจัยเหล่านี้ได้แก่ ความยาวของกุญแจที่ใช้ และความยากในการแยกตัวประกอบ

สำหรับข้อเสนอแนะเกี่ยวกับวิธีการเข้ารหัสลับมีดังนี้

1. วิธีการเข้ารหัสแบบกุญแจลับและวิธีการเข้ารหัสลับแบบกุญแจสาธารณะมีข้อดีข้อเสียแตกต่างกัน โดยวิธีการเข้ารหัสแบบกุญแจลับมีข้อดีตรงที่การเข้ารหัสและการถอดรหัสสามารถทำได้อย่างรวดเร็ว แต่มีความยากลำบากในการจัดการกุญแจ ในขณะที่วิธีการเข้ารหัสลับแบบกุญแจสาธารณะมีข้อดีตรงที่การจัดการกุญแจทำได้ง่าย และเมื่อมีบุคคลที่ต้องการติดต่อกันมากขึ้นจำนวนกุญแจที่ใช้ก็ไม่มากนักเมื่อเทียบกับวิธีการเข้ารหัสแบบกุญแจลับ แต่วิธีการนี้มีข้อจำกัดตรงที่การเข้ารหัสและถอดรหัสทำได้ช้า หากสามารถนำเอาวิธีการทั้ง 2 มาใช้งานร่วมกันได้ จะสามารถปรับปรุงข้อจำกัดของแต่ละวิธีได้ สำหรับตัวอย่างการนำวิธีการเข้ารหัสทั้ง 2 แบบมาใช้งานในปัจจุบันได้แก่ ระบบ PGP (Pretty Good Privacy) (Feisthammel, 2004) ซึ่งใช้ในการเข้ารหัสจดหมายอิเล็กทรอนิกส์และยืนยันตัวบุคคลที่ส่งจดหมายอิเล็กทรอนิกส์

2. ความปลอดภัยของการเข้ารหัสลับแบบกุญแจสาธารณะขึ้นอยู่กับความยาวของกุญแจที่ใช้ แต่ถ้ากุญแจที่ใช้มีความยาวมากก็จะทำให้การเข้ารหัสและการถอดรหัสเสียเวลามากเช่นกัน ดังนั้นในกรณีที่ข้อมูลที่ต้องการส่งมีความสำคัญในช่วงระยะเวลาหนึ่งๆ อย่างเช่นข้อมูลที่ใช้ในช่วงการเลือกตั้ง ซึ่งเมื่อสิ้นสุดการเลือกตั้งข้อมูลที่เคยใช้ในการติดต่อสื่อสารอาจจะไม่มีความสำคัญเลย ในกรณีนี้อาจจะใช้กุญแจสาธารณะที่มีความยาวไม่มากนัก แต่มีความยาวเพียงพอที่จะรับประกัน

ความเป็นส่วนตัวในช่วงเวลาก่อนการเลือกตั้ง วิธีการนี้จะช่วยให้การเข้ารหัสและถอดรหัสมีความรวดเร็วมากขึ้น

บรรณานุกรม

Atkins, D., Snyder, J., Hare, C. (1997). *Internet Security Professional Reference 2nd edition.* Indianapolis: New Riders Publishing.

Buchmann, J.A. (2004). *Introduction to cryptography.* New York: Springer.

Coutinho, S.C. (1999). *The Mathematics of Ciphers: Number Theory and RSA Cryptography.* Massachusetts: A K Peters Press.

Denning, D.E. (1982). *Cryptography and data security.* Massachusetts: Addison-Wesley Publishing.

DI Management Services Pty Limited. (2011). *RSA Algorithm.* Retrieved January 15, 2011, from RSA Algorithm Website: http://www.di-gt.com.au/rsa_alg.html

Feisthammel, P. (2004). *PGP - Pretty Good Privacy.* Retrieved January 15, 2011, from PGP/GnuPGP/OpenPGP - Pretty Good Privacy Website: http://www.rubin.ch/pgp/pgp.en.html

Henk, C. A. (2000). *Fundamentals of Cryptology.* Boston: Kluwer Academic Publishers.

Janeba, M. (1994). *Factoring Challenge Conquered - With a Little Help From Willamette.* Retrieved January 15, 2011, from RSA-129 article Website: http://www.willamette.edu/~mjaneba/rsa129.html

Mao, W. (2004). *Modern Cryptography, Theory & Practice.* New Jersey: Prentice Hall.

Mel, H. X., Baker, D. (2001). *Cryptography decrypted.* Boston: Addison-Wesley.

Warakorn Srichavengsup obtained the B.Eng., M.Eng. and Ph.D. degree in electrical engineering from Chulalongkorn University, Bangkok, Thailand, in 1998, 2003 and 2009, respectively. He is currently a lecturer with the Department of Computer Engineering at Thai-Nichi Institute of Technology (TNI), Bangkok, Thailand. Prior to joining TNI, he was a visiting research student during 2008 with the Laboratory for Information and Decision Systems (LIDS) at the Massachusetts Institute of Technology (MIT). His main research interests are MAC protocol for high speed wireless local area networks.