การแก้ไขปัญหาการแลกเปลี่ยนกุญแจสาธารณะสำหรับลายมือชื่อดิจิทัล

Solving the Problem of Public Key Distribution for Digital Signature

สมนึก พ่วงพรพิทักษ์[1], ณัฐวุฒิ ศรีวิบูลย์[2]

Somnuk Puangpronpitag[1], Nattavut Sriwiboon[2]

Received: 14 October 2015; Accepted: 17 February 2016

บทคัดย่อ

ลายมือชื่อดิจิทัลมีพื้นฐานมาจากการเข้ารหัสแบบอสมมาตร โดยมีบทบาทสำคัญ ในการตรวจสอบบูรณภาพของข้อความและการพิสูจน์ตัวจริงของผู้ส่งข้อความ ทั้งนี้ในการใช้งานลายมือชื่อดิจิทัลต้องมีการแลกเปลี่ยนกุญแจสาธารณะของคู่สนทนาทั้งสองฝ่าย อย่างไรก็ตาม จากการศึกษางานวิจัยก่อนหน้านี้พบว่าการแลกเปลี่ยนกุญแจสาธารณะยังมีปัญหาอยู่มาก กุญแจสาธารณะเหล่านี้อาจถูกปลอมแปลงและส่งผลให้การใช้ลายมือชื่อดิจิทัลประสบความล้มเหลว ดังนั้นงานวิจัยนี้จึงมุ่งหมายที่จะแก้ไขปัญหาดังกล่าวโดยได้ประเมินเทคโนโลยีลายมือชื่อดิจิทัลในปัจจุบันและปัญหาของมัน จากนั้นได้ออกแบบและพัฒนาซอฟต์แวร์ต้นแบบในการแก้ปัญหาและได้ทดลองเพื่อประเมินซอฟต์แวร์ต้นแบบที่พัฒนาขึ้น ผลการทดลองได้แสดงให้เห็นถึงความสำเร็จของแนวทางการแก้ปัญหาที่นำเสนอ

คำสำคัญ: ลายมือชื่อดิจิทัล การเข้ารหัสแบบอสมมาตร ปัญหาการแลกเปลี่ยนกุญแจสาธารณะ

Abstract

Digital signature is based on asymmetric encryptions. It has a very important role to ensure message integrity and sender authenticity. To deploy digital signature, public key exchange must be done between two sides of the communicators. However, from literature review, public key exchange is still problematic. Public keys can be spoofed, and ultimately cause the failure of the digital signature. So, this research aims to fix this problem. The evaluation of current digital signature technologies and their problems has been completed. After that, a solution was designed and prototyped. The experiments were done on prototyped software. The experimental results demonstrated the success of our solution.

Keywords: Digital Signature, Asymmetric Key Cryptography, Public Key Exchange Problem

บทนำ

ลายมือชื่อดิจิทัล (Digital Signature) เป็นเทคนิควิธีที่ได้รับการยอมรับ ในการพิสูจน์ผู้ส่งว่าเป็นตัวจริง (Sender Authentication) และข้อความที่มาถึงปลายทางไม่ถูกเปลี่ยนแปลงแก้ไขอย่างไม่ถูกต้อง (Message Integrity Check) โดยเฉพาะอย่างยิ่งได้มีกฎหมายออกมาเพื่อรองรับเทคนิควิธีดังกล่าว เช่น พรบ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์และลายมือชื่ออิเล็กทรอนิกส์ พ.ศ. 2544 ของประเทศไทย โดยลายมือชื่อดิจิทัลถือเป็นเทคนิควิธีที่สุดในขณะนี้ที่ถูกนำไปใช้เป็นลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signature) เพื่อช่วยในระบบพาณิชย์อิเล็กทรอนิกส์ต่างๆ

[1] *อาจารย์, สาขาวิทยาการคอมพิวเตอร์ คณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม อำเภอกันทรวิชัย จังหวัดมหาสารคาม 44150 ประเทศไทย*

[2] *นิสิตปริญญาโท*

[1] *Lecturer, Department of Computer Science, Faculty of Informatics, Mahasarakham University, Kantarawichai District, Maha Sarakham 44150, Thailand.* [2] *Master's degree student*

* *Corresponding author: Somnuk Puangpronpitag, Lecturer, Department of Computer Science, Faculty of Informatics, Mahasarakham University, Kantarawichai District, Maha Sarakham 44150, Thailand. somnuk.p@msu.ac.th*

แต่การใช้ลายมือชื่อดิจิทัล ผู้สื่อสารจะต้องแลกเปลี่ยนกุญแจสาธารณะ (Public Key) เพื่อนำไปใช้ในการพิสูจน์ลายมือชื่อ ซึ่งจากการศึกษางานวิจัยที่เกี่ยวข้องพบว่า เป็นจุดอ่อนให้ผู้โจมตี (Hacker) ปลอมแปลงกุญแจสาธารณะ (Public Key Spoof) และนำไปสู่การโจมตีระบบลายมือชื่อดิจิทัลได้ จึงได้มีการออกแบบการรับรองกุญแจสาธารณะโดยใช้หน่วยงาน Certificate Authority (CA) เข้ามาช่วยในการยืนยันกุญแจสาธารณะ ในรูปแบบใบรับรองอิเล็กทรอนิกส์ (Certificate) แต่ก็ได้มีงานวิจัยหลายชิ้น[1-2] ที่เสนอวิธีการโจมตีระบบ CA และสามารถปลอมการลงและพิสูจน์ลายมือชื่อดิจิทัลของข้อมูลได้ ทำให้ได้มีงานวิจัยหลายชิ้น[3-7] ได้ถูกเสนอเพื่อแก้ไขปัญหาการกระจายกุญแจสาธารณะดังกล่าว อย่างไรก็ตามจากการวิเคราะห์พบว่างานวิจัยเหล่านี้ ยังมีปัญหาและต้องมีการปรับปรุงแก้ไข

ดังนั้นในข้อเสนองานวิจัยนี้จึงเสนอที่จะออกแบบและพัฒนาระบบสร้างกุญแจคู่ (Key Pair) และการแลกเปลี่ยนกุญแจสาธารณะ เพื่อแก้ไขปัญหาการกระจายกุญแจสาธารณะของลายมือชื่อดิจิทัล โดยจะออกแบบอัลกอริธึมการเข้ารหัสในกระบวนการสร้างกุญแจโดยอาศัย RSA Algorithm[8] ร่วมกับ Identity-Based Cryptography[9] และปรับวิธีการในการสร้างกุญแจและยืนยันความเป็นเจ้าของกุญแจสาธารณะ โดยจะพัฒนาโปรแกรมต้นแบบเพื่อนำไปใช้ในการทดสอบแสดงให้เห็นถึงความมั่นคงของอัลกอริธึมและประสิทธิภาพของระบบต้นแบบ

ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

1. วิทยาการรหัสลับ (Cryptology)

วิทยาการรหัสลับ (Cryptology) เป็นการเข้ารหัสลับหรือการเปลี่ยนแปลงข้อความปกติ (Plain Text) ให้เป็นข้อความที่ถูกเข้ารหัส (Cipher Text) รวมถึงกระบวนการรับรองความถูกต้องของข้อมูลเพื่อการพิสูจน์ตัวจริง (Authentication) ระหว่างผู้ส่งกับผู้รับ โดยเรียกกระบวนการเปลี่ยนข้อความปกติให้เป็นข้อความที่ถูกเข้ารหัสว่าการเข้ารหัสข้อมูล (Encryption) และเรียกกระบวนการเปลี่ยนข้อความที่ถูกเข้ารหัสให้เป็นข้อความปกติว่าการถอดรหัสข้อมูล (Decryption)

2. การเข้ารหัสด้วยกุญแจลับ (Secret Key Encryption: SKE)

การเข้ารหัสด้วยกุญแจลับ (Secret Key Encryption: SKE) เป็นวิทยาการรหัสลับที่ใช้การเข้ารหัสแบบกุญแจลับ (Secret Key) ทั้งกระบวนการเข้ารหัสและถอดรหัสข้อมูล การเข้ารหัสประเภทนี้ผู้รับและผู้ส่งข้อมูลต้องมีการตกลงกุญแจลับก่อนการส่งข้อมูลดังแสดงใน (Figure 1)

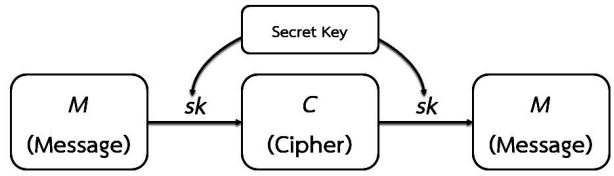

Figure 1 Secret Key Encryption

จาก (Figure 1) จะเห็นได้ว่าการเข้ารหัสแบบ SKE ใช้กุญแจลับ (Secret Key: sk) เป็นกุญแจ (Key) ที่เหมือนกันทั้งในกระบวนการเข้ารหัสและถอดรหัส ข้อดีของ SKE คือความเร็วในการเข้ารหัสและถอดรหัสส่วนข้อเสียคือ 1) การจัดการกุญแจเนื่องจาก SKE มีการเข้ารหัสและถอดรหัสข้อมูลที่ใช้กุญแจลับ ดังนั้นการเข้ารหัสและถอดรหัสข้อมูลผู้ส่งต้องมีจำนวน sk เท่ากับจำนวนของการจับคู่สนทนา 2) การแลกเปลี่ยนกุญแจลับระหว่างผู้ส่งกับผู้รับเนื่องจากการออกแบบ SKE ด้วยแนวคิดการใช้กุญแจลับในกระบวนการเข้ารหัสและถอดรหัสข้อมูล ในทางปฏิบัติผู้ส่งข้อมูลจะต้องส่ง sk ให้กับผู้รับเพื่อใช้ในกระบวนการถอดรหัสข้อมูล ดังนั้นจะเห็นได้ว่า sk ถือว่าไม่ใช่กุญแจที่เป็นความลับเพราะนอกจากผู้ส่งข้อมูลที่เป็นเจ้าของ sk แล้วยังมีผู้รับที่ทราบ sk 3) ความมั่นคงของการแลกเปลี่ยนกุญแจระหว่างผู้ส่งกับผู้รับอาจถูกดักจับกุญแจโดยผู้โจมตีเนื่องจากมีการเปิดเผยกับบุคคลที่สามแล้วการสื่อสารข้อมูลก็ไม่มีความมั่นคง หากมีการรั่วไหลของกุญแจโดยผู้รับหรือผู้ส่ง ก็จะเป็นปัญหาว่า ยากจะหาว่าใครเป็นผู้รับผิดชอบเพียงผู้เดียว เพราะเป็นกุญแจร่วม (shared key)

3. การเข้ารหัสด้วยกุญแจสาธารณะ (Public Key Encryption: PKE)

การเข้ารหัสด้วยกุญแจสาธารณะ (Public Key Encryption: PKE) ออกแบบให้มีลักษณะการทำงานใช้กุญแจที่แตกต่างกันในกระบวนการเข้ารหัสและถอดรหัสข้อมูล ตัวอย่างการทำงานของ PKE แสดงตัวอย่างใน (Figure 2)

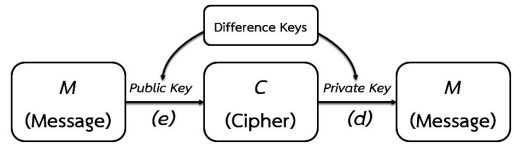

Figure 2 Public Key Encryption

จาก (Figure 2) จะเห็นได้ว่าการเข้ารหัสแบบ PKE มีการใช้กุญแจที่แตกต่างกันในกระบวนการเข้ารหัสและถอดรหัส ซึ่งผู้รับจะต้องสร้างกุญแจคู่ ที่ประกอบด้วยกุญแจส่วนตัว (Private Key) และกุญแจสาธารณะ (Public Key) เมื่อมีการสื่อสารข้อมูลผู้รับข้อมูลจะส่งกุญแจสาธารณะให้กับผู้ส่งข้อมูล เมื่อผู้ส่งข้อมูลต้องการส่งข้อมูลไปยังผู้รับจะใช้กุญแจ

สาธารณะของผู้รับเข้ารหัสข้อมูลในขั้นตอนนี้เป็นการยืนยันว่าข้อมูลที่ถูกส่งไปให้ผู้รับเป็นความลับ เนื่องจากมีเพียงผู้รับเท่านั้นที่สามารถถอดรหัสข้อมูลได้เพราะครอบครองกุญแจส่วนตัวเพียงผู้เดียว

4. แนวคิดกุญแจเซสชัน (Session Key Concept)

แนวคิดกุญแจเซสชัน (Session Key Concept) เป็นวิทยาการรหัสลับที่ใช้ข้อดีระหว่างการเข้ารหัสแบบ SKE และ PKE โดยจากที่กล่าวมาแล้วข้อดีของ SKE คือมีความเร็วในการประมวลผลการเข้ารหัสและถอดรหัสข้อมูล ส่วน PKE มีข้อดีคือสะดวกในการจัดการกุญแจ โดยการทำงานของ Session Key Concept แสดงดัง (Figure 3)

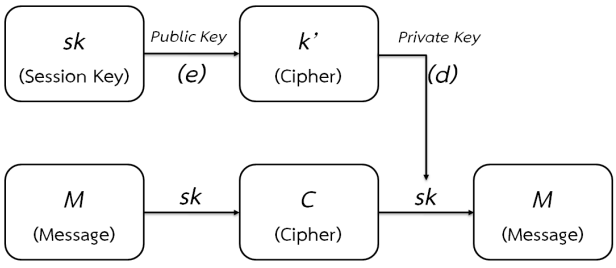

Figure 3 Session Key Concept

จาก (Figure 3) แสดงกระบวนการ Session Key Concept โดยผู้รับจะส่งกุญแจสาธารณะให้กับผู้ส่งข้อมูลจากนั้นผู้ส่งข้อมูลดำเนินการสุ่มค่า sk ซึ่งเป็น Session Key แล้วเข้ารหัสด้วยกุญแจสาธารณะของผู้รับในขั้นตอนนี้เป็นการยืนยันว่าการส่ง Session Key เป็นความลับระหว่างผู้ส่งกับผู้รับเนื่องจากมีเพียงผู้รับเท่านั้นที่สามารถถอดรหัส Session Key ได้ เมื่อผู้รับได้รับ k' ซึ่งเป็น Session Key ที่ถูกเข้ารหัสแล้วจะถอดรหัสด้วยกุญแจส่วนตัวได้เป็น sk กล่าวโดยสรุป Session Key Concept มีการตกลงใช้กุญแจระหว่างผู้ส่งและผู้รับก่อนการสื่อสารข้อมูลโดยกระบวนการแลกเปลี่ยนกุญแจ sk ใช้วิทยาการรหัสลับแบบ PKE และตลอดการสื่อสารข้อมูลระหว่างผู้ส่งและผู้รับจะใช้กุญแจ sk เข้ารหัสและถอดรหัสข้อมูลโดยใช้วิทยาการรหัสลับแบบ SKE ข้อเสียของ Session Key Concept มีดังนี้

1) **การปลอมตัว (Spoof)** โดยการโจมตีแบบ**ปลอมตัว**คือผู้โจมตีสามารถปลอมเป็นผู้ส่งข้อมูลเพื่อแทรกระหว่างการสื่อสารข้อมูล โดยที่ทั้งผู้รับไม่สามารถตรวจสอบได้ว่าถูกผู้โจมตีปลอมเป็นคู่สนทนา เนื่องจากกุญแจ sk ถูกสุ่มขึ้นโดยผู้ส่งข้อมูลและเข้ารหัสด้วยกุญแจสาธารณะของผู้รับที่ถูกเปิดเผย ดังนั้นการโจมตีด้วยวิธีนี้ผู้โจมตีสามารถสุ่มกุญแจ sk แล้วเข้ารหัสด้วยกุญแจสาธารณะของผู้รับ

2) การปลอมกุญแจสาธารณะ การที่ผู้ส่งข้อมูลใช้กุญแจสาธารณะของผู้รับเข้ารหัสกุญแจ sk ด้วยกลไกของ Session Key Concept ที่ไม่มีกระบวนการพิสูจน์ความเป็นเจ้าของกุญแจสาธารณะ เมื่อผู้โจมตีแทรกกลางการสื่อสารระหว่างผู้ส่งและผู้รับแล้วส่งกุญแจสาธารณะของผู้โจมตีไปให้ผู้ส่งข้อมูล เมื่อผู้ส่งข้อมูลต้องการส่ง sk ไปยังผู้รับจะใช้กุญแจสาธารณะของผู้โจมตีเข้ารหัสกุญแจ sk ผู้โจมตีสามารถถอดรหัสและทราบกุญแจ sk ได้ จากนั้นผู้โจมตีก็ใช้กุญแจสาธารณะของผู้รับเข้ารหัสกุญแจ sk แล้วส่งให้ผู้รับข้อมูล ดังนั้นการสื่อสารข้อมูลที่เกิดขึ้นทั้งผู้ส่ง ผู้รับข้อมูลและผู้โจมตีจะใช้กุญแจ sk เดียวกันในการเข้ารหัสและถอดรหัสทำให้ผู้โจมตีสามารถถอดรหัสข้อมูลที่ส่งระหว่างผู้ส่งกับผู้รับได้

5. ลายมือชื่อดิจิทัล (Digital Signature)

ลายมือชื่อดิจิทัล (Digital Signature) ใช้หลักการเข้ารหัสแบบ PKE ทำให้การสื่อสารข้อมูลมีความมั่นคง ลายมือชื่อดิจิทัลจะมีการลงนาม (Sign) ในเอกสารหรือข้อความซึ่งผลลัพธ์จากการลงนามจะได้เป็นลายมือชื่อดิจิทัลแล้วส่งข้อความต้นฉบับพร้อมกับลายมือชื่อดิจิทัลไปยังผู้รับซึ่งข้อดีของลายมือชื่อดิจิทัลผู้รับปลายทางสามารถพิสูจน์ (Verify) และยืนยันลายมือชื่อดิจิทัลได้ว่าเป็นของผู้ส่งจริงและสามารถนำลายมือชื่อดิจิทัลไปเป็นหลักฐานในชั้นศาลได้ โดยในประเทศไทยมีพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ฯ[10] กำหนดหลักเกณฑ์เรื่องลายมือชื่อดิจิทัลในมาตราที่ 9 และมาตราที่ 26 ตัวอย่างการทำงานของลายมือชื่อดิจิทัลแสดงตัวอย่างใน (Figure 4)

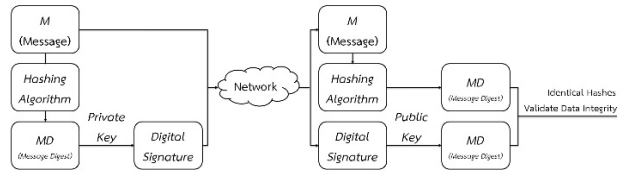

Figure 4 Digital Signature

จาก (Figure 4) แสดงให้เห็นว่าลายมือชื่อดิจิทัลมีกระบวนการคล้ายกับการเข้ารหัสแบบ PKE คือใช้กุญแจคู่สำหรับลงนามและพิสูจน์ข้อมูล อย่างไรก็ตามลายมือชื่อดิจิทัลมีข้อเสียคือผู้โจมตีสามารถดักจับกุญแจสาธารณะที่ใช้สำหรับพิสูจน์ลายมือชื่อดิจิทัลโดยผู้โจมตีสามารถเปลี่ยนกุญแจสาธารณะที่แลกเปลี่ยนระหว่างผู้ส่งกับผู้รับ เมื่อผู้รับข้อมูลใช้กุญแจสาธารณะของผู้โจมตีพิสูจน์ลายมือชื่อดิจิทัลแล้วได้ผล Valid ผู้รับข้อมูลจะเชื่อว่าผู้โจมตีเป็นผู้ส่งและเชื่อว่ากุญแจสาธารณะที่ถูกใช้งานเป็นของผู้ส่งข้อมูล

6. Certificate Authority (CA)

จากปัญหาของ PKE, Session Key Concept และ ลายมือชื่อดิจิทัลที่ประสบปัญหาการแลกเปลี่ยนกุญแจสาธารณะส่งผลให้การสื่อสารข้อมูลไม่มั่นคงเนื่องจากผู้ส่งข้อมูลไม่สามารถพิสูจน์ได้ว่ากุญแจสาธารณะที่ใช้เข้ารหัสเป็นของผู้รับจริงหรือไม่ทำให้การเข้ารหัสแบบ **PKE** และ Session Key Concept ล้มเหลว อีกทั้งในกระบวนการลายมือชื่อดิจิทัลการที่ผู้ส่งข้อมูลไม่สามารถพิสูจน์ได้ว่ากุญแจสาธารณะที่ใช้เข้ารหัสข้อมูลเป็นของผู้รับ ส่งผลให้เมื่อผู้ส่งใช้กุญแจสาธารณะของผู้โจมตีพิสูจน์ลายมือชื่อดิจิทัลของผู้โจมตีแล้วจะได้ผล Valid และผู้ส่งข้อมูลจะเชื่อว่าผู้โจมตีเป็นผู้รับข้อมูล

ดังนั้นจึงเกิดหน่วยงานที่เรียกว่า Certificate Authority (CA) ทำหน้าที่รับรองกุญแจสาธารณะ ตัวอย่างการทำงานของ CA เช่นผู้รับข้อมูลสร้างกุญแจคู่แล้วนำกุญแจสาธารณะและข้อมูลที่ยืนยันความเป็นตัวตนของผู้รับติดต่อไปยัง CA เมื่อ CA ตรวจสอบข้อมูลและพิสูจน์ได้ว่าเป็นผู้รับจริง CA ก็จะนำกุญแจส่วนตัวของ CA ลงลายมือชื่อดิจิทัลรับรองกุญแจสาธารณะเพื่อออกใบรับรองอิเล็กทรอนิกส์ (Certificate) ให้กับผู้รับข้อมูล เมื่อผู้รับต้องการติดต่อกับผู้ส่งข้อมูลจะส่งใบรับรองอิเล็กทรอนิกส์ไปยังผู้ส่งข้อมูล ซึ่งที่เครื่องผู้ส่งข้อมูลจะต้องติดตั้งกุญแจสาธารณะของ CA เพื่อใช้ในกระบวนการพิสูจน์ใบรับรองอิเล็กทรอนิกส์ของผู้รับข้อมูล ซึ่งการติดตั้งกุญแจสาธารณะของ CA ผู้ส่งข้อมูลจะต้องเชื่อว่ากุญแจสาธารณะเป็นของ CA จริง เมื่อการพิสูจน์ใบรับรองอิเล็กทรอนิกส์ของผู้รับถูกต้องผู้ส่งข้อมูลจึงจะใช้กุญแจสาธารณะของผู้รับเข้ารหัสข้อมูลที่ต้องการส่งไปยังผู้รับ

7. งานวิจัยที่เกี่ยวข้อง

RSA Algorithm[8] เสนอโดย Rivest และคณะเมื่อปี ค.ศ. 1978 เป็นอัลกอริธึมที่ใช้ได้ทั้งการเข้ารหัสข้อมูล ถอดรหัสข้อมูล และการลงลายมือชื่อดิจิทัล RSA Algorithm ออกแบบให้มีคุณสมบัติเป็นการเข้ารหัสแบบ PKE โดยมีกุญแจคู่ประกอบด้วยกุญแจสาธารณะ ใช้สำหรับกระบวนการเข้ารหัสข้อมูลและกุญแจส่วนตัวใช้สำหรับกระบวนการถอดรหัสในส่วนของลายมือชื่อดิจิทัลเพื่อการยืนยันตัวจริงความเป็นเจ้าของข้อมูลจะใช้กุญแจส่วนตัวสำหรับลงลายมือชื่อดิจิทัลและใช้กุญแจสาธารณะสำหรับพิสูจน์ลายมือชื่อดิจิทัล

ID-Based Encryption (IBE) ถูกเสนอโดย Shamir[9] เมื่อปี ค.ศ. 1985 จากปัญหาการแลกเปลี่ยนกุญแจสาธารณะของ RSA Algorithm โดย IBE มีแนวคิดเสนอการเข้ารหัสแบบ PKE ที่ผู้ใช้สามารถลงลายมือชื่อดิจิทัลและพิสูจน์ลายมือชื่อดิจิทัลได้โดยไม่ต้องมีกระบวนการแลกเปลี่ยนกุญแจลับหรือกุญแจสาธารณะระหว่างกันและผู้ใช้ไม่ต้องจัดเก็บกุญแจลับระหว่างกัน อีกทั้งมีแนวคิดที่ไม่ใช้ Third Party สำหรับรับรองกุญแจสาธารณะให้กับผู้ใช้โดยระบบใช้ Private Key Generator (PKG) สำหรับรับรองกุญแจส่วนตัวให้กับผู้ใช้ซึ่ง PKG ถูกออกแบบระบบให้ปิดการใช้งานหลังจากรับรองกุญแจส่วนตัวให้กับผู้ใช้ในระบบ โดย IBE เหมาะสำหรับใช้กับระบบปิดเช่น ระบบธนาคารหรือระบบสำหรับผู้บริหารระดับสูงเป็นต้น

อย่างไรก็ตาม IBE ที่ระบุว่าไม่ใช้ Third Party ซึ่งจากการศึกษาพบว่า IBE ใช้ PKG เป็น Third Party สำหรับรับรองกุญแจส่วนตัวให้กับผู้ใช้มีลักษณะเหมือนกับ CA ที่รับรองกุญแจสาธารณะให้กับผู้ใช้แล้วการใช้งานระบบผู้ใช้ต้องติดตั้งกุญแจสาธารณะของ PKG ไว้บนเครื่องผู้ใช้และข้อเสียของ IBE ที่ผิดหลักความมั่นคง (Information Security) ในกระบวนการรับรอง Identity ของ PKG ที่สามารถรับรองกุญแจส่วนตัวให้กับผู้ใช้ใดๆ และค่ากุญแจส่วนตัวที่ได้ไม่ถูกเก็บเป็นความลับเพราะนอกจากผู้ใช้ผู้เป็นเจ้าของ Identity แล้วยังมี PKG ที่ทราบกุญแจส่วนตัวของผู้ใช้ รวมถึง IBE ไม่สามารถแก้ไขปัญหาการแลกเปลี่ยนกุญแจสาธารณะเนื่องจากระบบไม่มีกลไกสำหรับตรวจสอบกุญแจสาธารณะของ PKG

Boneh และ Franklin[11] ในปี ค.ศ. 2001 เสนองานวิจัยที่นำแนวคิดในงานวิจัยของ Shamir มาปรับปรุงและพัฒนาอัลกอริธึมใหม่เพื่อให้ IBE มีความมั่นคงมากขึ้นจากการศึกษารายละเอียดของงานวิจัยพบว่างานวิจัยยังอาศัยแนวคิดของ Shamir ที่ใช้ PKG เป็น Third Party เพื่อรับรองกุญแจส่วนตัวให้กับผู้ใช้ อย่างไรก็ตามสิ่งที่งานวิจัยของ Boneh และ Franklin แตกต่างจาก Shamir คือการใช้อัลกอริธึม ElGamal Signature[12] สำหรับเข้ารหัสและถอดรหัสข้อมูลแทน RSA Algorithm ที่ Shamir เลือกใช้เนื่องจากอัลกอริธึม ElGamal Signature มีความเร็วในกระบวนการเข้ารหัสและถอดรหัสมากกว่า RSA Algorithm

Harn และ Ren[13] ในปี ค.ศ. 2008 เสนองานวิจัยที่ออกแบบอัลกอริธึมเพื่อแก้ไขปัญหาการถูกโจมตีด้วยวิธี Chosen-Plaintext Attack ซึ่งเป็นวิธีการโจมตีที่ใช้โจมตีการเข้ารหัสข้อมูลที่ผู้โจมตีสามารถเข้าถึงข้อความต้นฉบับและได้กุญแจลับที่ใช้สำหรับถอดรหัส โดยในงานวิจัยเสนอวิธีการสร้างลายมือชื่อดิจิทัลแบบ Multi-Signature โดยกระบวนการรับรอง Identity ออกแบบให้ PKG สร้างกุญแจลับให้กับผู้ใช้ที่สามารถป้องกันการโจมตี Chosen-Plaintext Attack ที่เกิดขึ้นกับกุญแจลับของ PKG และออกแบบกระบวนการลงและพิสูจน์ลายมือชื่อดิจิทัลแบบ Multi-Signature โดยการสุ่มค่าเพื่อเพิ่มความซับซ้อนให้กับลายมือชื่อดิจิทัล

Tripathi และคณะ[14] ในปี ค.ศ. 2011 เสนองานวิจัยเพื่อแก้ไขปัญหาการแลกเปลี่ยนกุญแจสาธารณะของ RSA Algorithm โดยใช้ Identity เป็นกุญแจสำหรับการเข้ารหัส จากการศึกษางานวิจัยแสดงให้เห็นว่าการรับรองความถูกต้องของกุญแจสาธารณะเป็นปัญหาที่สำคัญสำหรับของการเข้ารหัสแบบ PKE โดยระบบขนาดใหญ่อย่างเช่นระบบเว็บไซต์ใช้ CA สำหรับรับรองกุญแจสาธารณะ อย่างไรก็ตามปัญหาของ CA มีค่าใช้จ่ายในการดำเนินการและระบบไม่มีความมั่นคง ดังนั้นในงานวิจัยจึงเสนอวิธีการหลีกเลี่ยงการใช้ใบรับรองอิเล็กทรอนิกส์โดยนำ Identity อย่างเช่น Email Address เป็นส่วนของกุญแจสาธารณะเนื่องจาก Identity สามารถยืนยันตัวบุคคลได้โดยไม่ต้องได้รับการรับรองจาก Third Party ซึ่งอัลกอริธึมที่เสนอเป็นการปรับปรุงกระบวนการคำนวณส่วนของ $Public\ Key\ (e)$ ของ RSA Algorithm

Muhammadi และคณะ[15] ในปี ค.ศ. 2013 เสนองานวิจัยเพื่อเพิ่มประสิทธิภาพให้กับอัลกอริธึมของ Tripathi และคณะ ที่ผลการนำ Identity เป็นส่วนของกุญแจสาธารณะเมื่อนำ Identity ผ่าน Hashing Function แล้วผลลัพธ์ที่ได้เปรียบเทียบกับเงื่อนไขของ RSA Algorithm ที่กำหนดให้ส่วนของ $Public\ Key\ (e)$ มีค่าตามเงื่อนไข $1<e<\phi(n)$ และ $gcd(e,\phi(n))=1$ ได้ผลคือ Identity จำนวน 53.33% ที่ไม่สามารถใช้เป็นส่วนของ $Public\ Key\ (e)$ ได้ ดังนั้นในงานวิจัยจึงเสนออัลกอริธึมเพื่อปรับปรุงงานวิจัยของ Tripathi และคณะให้มีประสิทธิภาพในการสร้างส่วนของ $Public\ Key\ (e)$ มากขึ้น ซึ่งผลจากการพัฒนาอัลกอริธึมแสดงให้เห็นว่ามีจำนวนของ Identity ที่ไม่สามารถเป็นส่วนของ $Public\ Key\ (e)$ ลดลงเป็น 33.33%

วิธีดำเนินการวิจัย

1. การวิเคราะห์ปัญหาความมั่นคงของงานวิจัยก่อนหน้านี้

1) ปัญหาความมั่นคงของ Public Key Encryption (PKE)

ปัญหาการแลกเปลี่ยนกุญแจสาธารณะและปัญหาการพิสูจน์ความเป็นเจ้าของกุญแจสาธารณะโดยผู้โจมตีอาศัยวิธีการโจมตีแบบต่าง ๆ เช่นการโจมตีแบบ Man-In-The-Middle (MITM) attack เพื่อเปลี่ยนแปลงกุญแจสาธารณะก่อนไปถึงผู้ส่งโดยที่ผู้ส่งไม่สามารถพิสูจน์ได้ว่ากุญแจสาธารณะที่ใช้เข้ารหัสข้อมูลเป็นของจริงหรือไม่ เมื่อข้อมูลถูกเข้ารหัสด้วยกุญแจสาธารณะของผู้โจมตี ดังนั้นผู้โจมตีสามารถใช้กุญแจส่วนตัวเพื่อถอดรหัสข้อมูลได้ โดยแสดงตัวอย่างการโจมตีเพื่อเปลี่ยนแปลงกุญแจสาธารณะดัง (Figure 5)

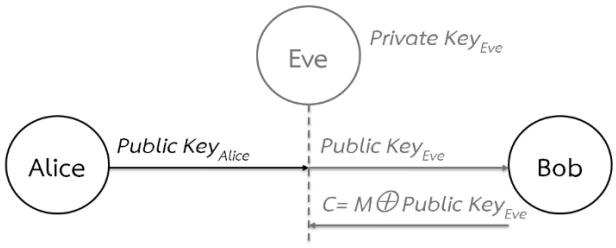

Figure 5 The Problem of Exchanging Public Keys

จาก (Figure 5) เป็นตัวอย่างการโจมตีเพื่อเปลี่ยนแปลงกุญแจสาธารณะโดยให้ Alice และ Bob เป็นคู่สนทนาที่ต้องการใช้วิธีการเข้ารหัสและถอดรหัสด้วย PKE โดยในขั้นตอนแรก Alice จะส่ง $PublicKey_{Alice}$ ให้กับ Bob เมื่อข้อมูลถูกส่งไปในช่องทางการสื่อสารอย่างเช่นระบบเครือข่ายอินเทอร์เน็ตแล้ว Eve เป็นผู้โจมตีโดยที่ Eve ใช้วิธีโจมตีแบบแทรกกลางการสื่อสารระหว่าง Alice กับ Bob เมื่อข้อมูลถึงเครื่อง Eve แล้ว $PublicKey_{Alice}$ จะถูกเปลี่ยนแปลงเป็น $PublicKey_{Eve}$ แล้วส่งไปให้กับ Bob เมื่อ Bob ต้องการเข้ารหัสข้อมูลเพื่อส่งให้กับ Alice จะเชื่อว่า $PublicKey_{Eve}$ เป็นของ Alice ซึ่งในขั้นตอนการส่งข้อมูล Cipher Text (C) ข้อมูลก็จะถูกส่งผ่านเครื่องของ Eve ดังนั้นข้อมูลที่เข้ารหัสด้วย $PublicKey_{Eve}$ ก็สามารถใช้ $PrivateKey_{Eve}$ สำหรับถอดรหัสข้อมูลได้

จากปัญหาการแลกเปลี่ยนกุญแจสาธารณะแสดงให้เห็นว่าการเข้ารหัสแบบ PKE มีปัญหาด้านความมั่นคงเมื่อถูกโจมตีเปลี่ยนแปลงกุญแจสาธารณะผลคือทำให้การสื่อสารข้อมูลถูกดักจับ (Sniff) และการปลอมตัว ซึ่งผู้โจมตีสามารถหลอกลวงเหยื่อได้ว่าเป็นคู่สนทนาในระบบสื่อสารข้อมูล

2) ปัญหาความมั่นคงของ Certificate Authority (CA)

ถึงแม้ CA ถูกออกแบบมาเพื่อแก้ไขปัญหาการแลกเปลี่ยนกุญแจสาธารณะของการเข้ารหัสแบบ PKE อย่างไรก็ตามจากการศึกษากระบวนการทำงานของ CA ปัญหาความมั่นคงและงานวิจัยที่ถูกเสนอโดย Durumeric และคณะ[16] สามารถสรุปปัญหาของ CA ได้ดังนี้

1. จำนวนของ CA ที่ถูกใช้งานและมีอำนาจในการออกใบรับรองอิเล็กทรอนิกส์มีเป็นจำนวนมากจึงเป็นปัญหาสำหรับการควบคุมและตรวจสอบใบรับรองอิเล็กทรอนิกส์ว่าเป็นของจริงที่ออกโดย CA ที่น่าเชื่อถือหรือไม่

2. การใช้ CA เพื่อรับรองกุญแจสาธารณะเป็นวิธีที่ถูกเสนอให้เป็นมาตรฐานสำหรับแก้ไขปัญหาการแลกเปลี่ยนกุญแจสาธารณะอย่างไรก็ตาม CA ไม่มีความมั่นคงโดยมีงานวิจัยและวิธีการโจมตีมากมายที่ถูกเสนอเพื่อโจมตี

3. มี CA ที่มีอำนาจในการออกใบรับรองอิเล็กทรอนิกส์โดยไม่เสียค่าใช้จ่ายจึงเป็นปัญหาสำหรับการควบคุมและตรวจสอบใบรับรองอิเล็กทรอนิกส์ว่าเป็นของจริงที่ออกโดย CA ที่น่าเชื่อถือหรือไม่

4. จากจำนวนของ CA ที่ถูกใช้งานและมีอำนาจในการออกใบรับรองอิเล็กทรอนิกส์มีเป็นจำนวนมาก ดังนั้นจึงไม่เหมาะสำหรับนำไปประยุกต์ใช้ในระดับองค์กรที่ต้องการควบคุมความมั่นคงและต้องการ CA ที่มีความน่าเชื่อถือ ดังตัวอย่างการโจมตีเพื่อลักลอบขโมยกุญแจส่วนตัวที่เกิดกับ CA ชื่อ DigiNatar เมื่อ 2 กันยายน ค.ศ. 2011[1] และเมื่อ 12 ตุลาคม ค.ศ. 2015[2] ได้เกิดปัญหากับ CA ชื่อ Symantec ได้รายงานการตรวจสอบภายในพบว่าไม่มีความโปร่งใสในกระบวนการออกใบรับรองอิเล็กทรอนิกส์ โดยพบใบรับรองอิเล็กทรอนิกส์ที่ออกโดยไม่ได้รับอนุญาตจำนวน 164 ใบ และมีอีก 2,458 ใบที่รับรองโดเมนที่ไม่เคยมีการจดทะเบียน

5. จากการศึกษาของ Durumeric และคณะ[16] แสดงให้เห็นว่าขนาดของกุญแจที่ CA เลือกใช้ในกระบวนการรับรองกุญแจสาธารณะเพื่อออกใบรับรองอิเล็กทรอนิกส์มีความอ่อนแอและถูกใช้งานเป็นจำนวนมากในขนาด 1024 bits ซึ่งมีขนาดต่ำกว่ามาตรฐานที่ประกาศล่าสุดเมื่อเดือนพฤษภาคม ปี ค.ศ. 2015[17] ระบุว่าขนาดของกุญแจที่ใช้กับ RSA Algorithm ต้องอยู่ระหว่าง 2048 bits ถึง 3072 bits

3) ปัญหาของงานวิจัยที่เสนอ ID-Based Encryption IBE)

ปัญหาของงานวิจัยที่เสนอให้ใช้ IBE เพื่อแก้ไขปัญหาการแลกเปลี่ยนกุญแจสาธารณะของ PKE และ CA จากการศึกษาแสดงให้เห็นว่า

1) การที่ IBE เสนอให้ใช้ PKG เป็น Third Party เพื่อรับรองกุญแจส่วนตัวให้กับผู้ใช้ ซึ่งผิดหลักความมั่นคงเนื่องจากกุญแจส่วนตัวไม่ได้เป็นความลับที่ผู้ใช้เท่านั้น

2) กลไกของ IBE ไม่สามารถแก้ไขปัญหาการแลกเปลี่ยนกุญแจสาธารณะได้เนื่องจากผู้ใช้ต้องติดตั้งกุญแจสาธารณะของ PKG เพื่อพิสูจน์ลายมือชื่อดิจิทัลซึ่ง IBE ไม่ได้ออกแบบกลไกสำหรับตรวจสอบว่ากุญแจสาธารณะของ PKG เป็นของจริงหรือไม่หากเกิดการปลอมแปลงกุญแจสาธารณะของ PKG การพิสูจน์ลายมือชื่อดิจิทัลระหว่างผู้ใช้จะล้มเหลว

2. สรุปปัญหาความมั่นคงของงานวิจัยก่อนหน้านี้

จากการวิเคราะห์ปัญหาความมั่นคงที่เกิดขึ้นกับงานวิจัยก่อนหน้านี้แสดงให้เห็นว่าปัญหาความมั่นคงที่เกิดขึ้นมีสาเหตุมาจากปัญหาการแลกเปลี่ยนกุญแจสาธารณะกล่าวโดยสรุปดังนี้

1) ผลจากการที่ PKE ไม่มีกลไกสำหรับตรวจสอบและพิสูจน์ตัวจริงว่าใครเป็นเจ้าของกุญแจสาธารณะ ทำให้ผู้โจมตีสามารถปลอมตัวเป็นคู่สนทนาและดักจับข้อมูลได้

2) ผลจากการที่ Session Key Concept ที่ไม่มีกลไกสำหรับพิสูจน์ตัวจริงว่าใครเป็นเจ้าของกุญแจสาธารณะ ทำให้ผู้โจมตีสามารถปลอมตัวเป็นคู่สนทนาและดักจับ Session Key ได้

3) การออกแบบและพัฒนาให้ CA เป็นหน่วยงานที่ทำหน้าที่รับรองกุญแจสาธารณะให้กับผู้ใช้ ผลจากการศึกษาแสดงให้เห็นว่า CA ไม่มีความน่าเชื่อถือ

4) IBE เสนอวิธีแก้ไขปัญหาการแลกเปลี่ยนกุญแจสาธารณะ โดยการนำ PKG รับรอง Identity เพื่อออกกุญแจส่วนตัวให้กับผู้ใช้ถือว่าผิดหลักความมั่นคงของข้อมูล เนื่องจากกุญแจส่วนตัวถูกเปิดเผยกับ PKG อีกทั้ง IBE ยังไม่ได้ออกแบบกลไกให้กับผู้ใช้ในการตรวจสอบกุญแจสาธารณะของ PKG

3. แนวคิดการออกแบบและพัฒนาอัลกอริธึมใหม่

การออกแบบและพัฒนาอัลกอริธึมใหม่ จึงกำหนดให้มีแนวคิดเพื่อแก้ไขปัญหาการแลกเปลี่ยนกุญแจสาธารณะระหว่างผู้ส่งกับผู้รับ เนื่องจากการสื่อสารหากสามารถพิสูจน์และยืนยันได้ว่ากุญแจสาธารณะที่ใช้เป็นของจริงการรับส่งข้อมูลก็จะมีความมั่นคง อีกทั้งหากระบบมีกลไกการแลกเปลี่ยนกุญแจสาธารณะที่มั่นคงจะส่งผลให้ผู้ใช้ไม่ต้องใช้และเชื่อถือหน่วยงาน CA รวมถึงผู้ใช้ไม่ต้องใช้และเปิดเผยกุญแจส่วนตัวให้กับ PKG

ดังนั้นออกแบบอัลกอริธึมใหม่เพื่อแก้ไขจุดบกพร่องของลายมือชื่อดิจิทัลให้มีความมั่นคงมากขึ้น เพื่อนำอัลกอริทึมที่ได้ใช้ยืนยันและพิสูจน์ได้ว่ากุญแจสาธารณะเป็นของจริง โดยปรับปรุง RSA Algorithm ร่วมกับข้อดีของ IBE ที่สามารถพิสูจน์ลายมือชื่อดิจิทัลได้โดยใช้ Identity เช่น Email Address เพื่อกำหนดเงื่อนไขในการออกแบบอัลกอริธึมให้สามารถแก้ไขปัญหาของ PKE กับ IBE และปัญหาการใช้งาน Third Party เพื่อรับรองกุญแจสาธารณะที่เกิดขึ้นกับ CA และ IBE

1) อัลกอริธึมที่ใช้ในกระบวนการลงและพิสูจน์ลายมือชื่อดิจิทัลแก้ไขปัญหา Third Party ของ CA และ IBE

2) แก้ไขปัญหาการแลกเปลี่ยนกุญแจสาธารณะที่เกิดขึ้นกับ PKE และ IBE

3) พัฒนาระบบลงและพิสูจน์ลายมือชื่อดิจิทัลให้มีความมั่นคงให้สามารถใช้งานได้จริง

สำหรับการพัฒนาระบบต้นแบบจากอัลกอริธึมที่ออกแบบให้สามารถใช้งานได้จริงมีแนวคิดในการพัฒนาระบบต้นแบบจากอัลกอริธึมที่ออกแบบให้สามารถใช้งานได้จริงดังนี้

1) ระบบต้นแบบพัฒนาด้วยภาษา JavaScript สามารถลงและพิสูจน์ลายมือชื่อดิจิทัลได้อย่างมั่นคง เนื่องจาก

ภาษา JavaScript สามารถประมวลผลได้หลาย Platform

2) สามารถนำไปใช้งานได้โดยไม่ต้องติดตั้ง

3) รองรับการทำงานแบบ Multi-Platform คือ สามารถใช้งานได้กับอุปกรณ์ที่แตกต่างกันเช่นบนคอมพิวเตอร์ส่วนบุคคล (Personal Computer: PC) หรืออุปกรณ์ Smart-phone เป็นต้น

4. การกำหนดเกณฑ์สำหรับประเมินประเมินประสิทธิภาพ

งานวิจัยนี้ได้กำหนดเกณฑ์สำหรับประเมินระบบต้นแบบที่เสนอในงานวิจัยนี้กับงานวิจัยก่อนหน้านี้แบ่งออกเป็น 2 ส่วนคือ

1) แสดงผลการวิเคราะห์เพื่อแสดงให้เห็นว่าระบบสามารถลงและพิสูจน์ลายมือชื่อดิจิทัลได้ สามารถแลกเปลี่ยนกุญแจสาธารณะได้อย่างมั่นคง

2) ระบบสามารถรองรับการทำงานแบบ Multi-Platform และแสดงเวลาหน่วยเป็น Millisecond (ms) ของการประมวลผลของขั้นตอนประกอบด้วยการสร้างกุญแจ (Generate Key) การลงลายมือชื่อดิจิทัล (Sign) และการพิสูจน์ลายมือชื่อดิจิทัล (Verify)

5. เครื่องมือและสภาพแวดล้อมสำหรับประเมินประสิทธิภาพ

เครื่องมือและสภาพแวดล้อมที่ถูกกำหนดให้เป็น Test-bed ประกอบด้วย

1) PC Desktop คอมพิวเตอร์ที่ใช้ทดสอบระบบต้นแบบ คือ Intel ® Core ™ 2 Duo 2.66 GHz RAM 4 GB ติดตั้งระบบปฏิบัติการ Kali Linux 64 bit และ Windows โดยทดสอบในระบบปฏิบัติการ Windows 8

2) Macbook Air คือ Intel Core i5 1.6 GHz RAM 4 GB ติดตั้งระบบปฏิบัติการ OS X

3) iPhone 5s ติดตั้งระบบปฏิบัติการ iOS 9.2.1

4) Samsung Galaxy Tab 10.1 ติดตั้งระบบปฏิบัติการ ANDROID 4.4

5) Web Browser ใช้ Google Chrome ที่สามารถรองรับทั้งระบบปฏิบัติการ Windows, Linux, OS X, iOS และ ANDROID

ผลการวิจัย

ในส่วนนี้จะกล่าวถึงผลการประเมิน ผลการออกแบบและผลการพัฒนาระบบต้นแบบโดยอัลกอริธึมและระบบต้นแบบที่เสนอในงานวิจัยนี้เรียกว่า ISAN Identity-based RSA (IIR) เป็นอัลกอริธึมและระบบที่สามารถลงและพิสูจน์ลายมือชื่อดิจิทัลได้อย่างมั่นคงและแก้ไขปัญหาการแลกเปลี่ยนกุญแจสาธารณะ รวมถึงแสดงผลการประเมินประสิทธิภาพโดยมีรายละเอียดดังนี้

1. ผลการออกแบบและพัฒนาอัลกอริธึมใหม่

จากแนวคิดการออกแบบอัลกอริธึมใหม่ของงานวิจัยนี้ที่กำหนดให้สามารถแก้ไขปัญหาการแลกเปลี่ยนกุญแจสาธารณะ แสดงผลการออกแบบอัลกอริธึมดัง (Figure 6)

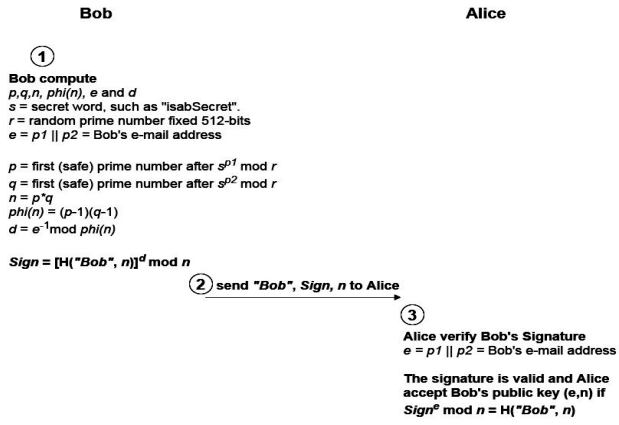

Figure 6 Our Proposed Algorithm

จาก (Figure 6) แสดงผลการออกแบบอัลกอริธึม IIR ที่สามารถลงและพิสูจน์ลายมือชื่อดิจิทัลได้อย่างมั่นคงประกอบด้วย 3 ขั้นตอนโดยมีรายละเอียดของแต่ละขั้นตอนดังนี้

1) Bob คำนวณกุญแจคู่ที่ประกอบด้วย $Public\ \ Key\ (e,n)$ และ $Private\ \ Key\ (d,n)$ โดยใช้ขั้นตอนการคำนวณตาม RSA Algorithm อย่างไรก็ตามเพื่อการลงและพิสูจน์ลายมือชื่อดิจิทัลอย่างมั่นคงในงานวิจัยนี้กำหนดให้ใช้ค่า $e = p1 \| p2 = Bob's\ \ Email\ \ Address$ เมื่อ Bob ส่งลายมือชื่อดิจิทัลไปยัง Alice แล้วการพิสูจน์ลายมือชื่อดิจิทัล Alice สามารถใช้ Email Address ของ Bob เพื่อพิสูจน์ลายมือชื่อดิจิทัลได้ ดังนั้นในกระบวนการนี้สามารถแก้ไขปัญหาการแลกเปลี่ยนกุญแจสาธารณะที่เกิดขึ้นกับ PKE และ IBE ได้ จากนั้น Bob ลงลายมือชื่อดิจิทัลรับรองข้อความตามสมการ $Sign = [H("Bob", n)]^d \bmod n$ โดยที่ $Sign$ คือลายมือชื่อดิจิทัลและ H คือ Hashing function

2) Bob ส่ง $"Bob", Sign, n$ ให้ Alice

3) Alice พิสูจน์ค่า $Sign$ ของ Bob โดยใช้ $Public\ \ Key\ (e,n)$ สำหรับพิสูจน์ลายมือชื่อดิจิทัล ดังนั้นในขั้นตอนนี้ Alice จะใช้ n ที่ได้รับจาก Bob และกำหนดค่า $e = p1 \| p2 = Bob's\ \ Email\ \ Address$ โดยการพิสูจน์ลายมือชื่อดิจิทัลจะได้ผลลัพธ์ Valid ก็ต่อเมื่อ $Sign^e \bmod n = H("Bob", n)$ หากการพิสูจน์ลายมือชื่อดิจิทัลได้ผล Valid แล้ว Alice จะยอมรับและกุญแจสาธารณะของ Bob เพื่อใช้สำหรับการสื่อสารข้อมูล

ผลการพัฒนาระบบต้นแบบจากอัลกอริธึมใหม่ให้สามารถใช้งานได้จริง

ระบบต้นแบบที่พัฒนาโดยภาษา JavaScript เป็นระบบต้นแบบที่สามารถแลกเปลี่ยนกุญแจสาธารณะได้อย่างมั่นคงและมีประสิทธิภาพสำหรับการลงและพิสูจน์ลายมือชื่อดิจิทัลโดยแสดงรายละเอียดขั้นตอนการใช้งานระบบต้นแบบ IIR ดัง (Figure 7)

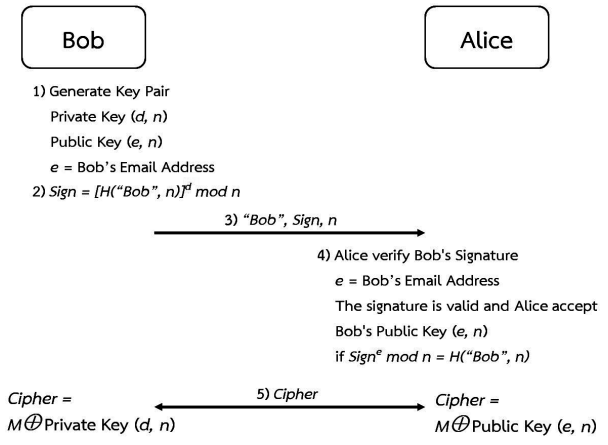

Figure 7 Work Flow of IIR Digital Signature

จาก (Figure 7) แสดงรายละเอียดขั้นตอนการใช้งานระบบต้นแบบ IIR ประกอบด้วย 5 ขั้นตอนมีรายละเอียดดังนี้

1) Bob คำนวณกุญแจคู่ประกอบด้วย $Private\ Key\ (d,n)$และ$Public\ Key\ (e,n)$ตามกระบวนการของ RSA Algorithm โดยที่ระบบต้นแบบที่เสนอโดยงานวิจัยนี้ส่วนของ $Public\ Key\ (e)$ กำหนดให้เป็น Identity คือ Email Address ของ Bob

2) Bob ลงลายมือชื่อดิจิทัลเพื่อรับรองกุญแจสาธารณะของBobตามสมการ$Sign=[H("Bob",n)]^d \bmod n$

3) Bob ส่ง $"Bob"$, $Sign$, n ให้ Alice

4) Alice พิสูจน์ลายมือชื่อดิจิทัลของ Bob โดย Alice ใช้ส่วนของ $Public\ Key\ (e)$ ที่เป็น Email Address ของ Bob ซึ่ง Alice ทราบอยู่แล้ว โดยที่ Alice จะยอมรับและใช้งาน $Public\ Key\ (e,n)$ ของ Bob เมื่อได้ผลลัพธ์ของการพิสูจน์ลายมือชื่อดิจิทัล Valid

5) การสื่อสารข้อความระหว่าง Alice กับ Bob ข้อความที่ถูกส่งจะอยู่ในรูปของข้อมูลที่ถูกเข้ารหัส โดยกุญแจที่ Alice ใช้สำหรับเข้ารหัสและถอดรหัสข้อมูลคือ $Public\ Key\ (e,n)$ ของ Bob และกุญแจที่ Bob ใช้สำหรับเข้ารหัสและถอดรหัสข้อมูลคือ $Public\ Key\ (e,n)$ และแสดงตัวอย่างส่วนการทำงานของระบบต้นแบบในขั้นตอนการยืนยันและการพิสูจน์ตัวจริงระหว่าง Alice กับ Bob ดัง (Figure 8) คือขั้นตอนที่ Bob คำนวณกุญแจคู่แล้วลงลายมือชื่อดิจิทัลรับรองกุญแจสาธารณะและ(Figure 9) คือขั้นตอนที่ Alice พิสูจน์ลายมือชื่อดิจิทัลของ Bob

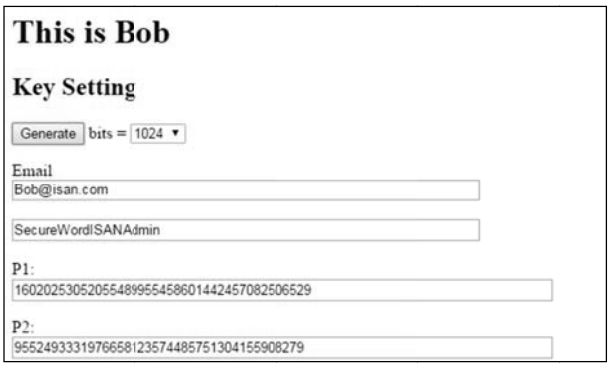

Figure 8 Generating a key pair

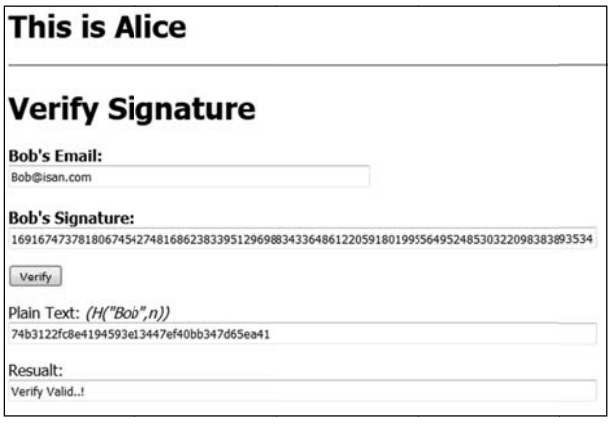

Figure 9 Verifying the digital signature

ผลการประเมินประสิทธิภาพ

1. ผลการวิเคราะห์ความมั่นคงของอัลกอริธึมใหม่

ในงานวิจัยนี้ได้ปรับปรุง RSA Algorithm ที่มีคุณสมบัติลงและพิสูจน์ลายมือชื่อดิจิทัล เพื่อให้การแลกเปลี่ยนกุญแจสาธารณะมีความมั่นคง จาก RSA Algorithm ที่กุญแจคู่ประกอบด้วย $Public\ Key\ (e,n)$และ $Private\ Key\ (d,n)$ เมื่อนำ Identity ที่เป็นสาธารณะเช่น Email Address เป็นส่วนของ $Public\ Key\ (e)$ ทำให้การนำกุญแจสาธารณะใช้เพื่อพิสูจน์ลายมือชื่อดิจิทัลมีความมั่นคงมากขึ้น สามารถยืนยันได้ว่าผู้เป็นเจ้าของลายมือชื่อดิจิทัล เป็นตัวจริง ดังตัวอย่างที่แสดงให้เห็นว่า เมื่อ Bob ต้องการส่งลายมือชื่อดิจิทัลเพื่อให้ Alice ตรวจสอบ Alice ก็ทราบอยู่แล้วว่าส่วนหนึ่งของกุญแจสาธารณะที่ใช้เพื่อพิสูจน์ลายมือชื่อดิจิทัลของ Bob คือ Email Address ของ Bob โดยที่ไม่ต้องมีกระบวนการแลกเปลี่ยนกุญแจสาธารณะ

อีกทั้งจากผลการปรับปรุงอัลกอริธึม สามารถแก้ไขปัญหาความมั่นคงในกรณีที่ผู้ใช้ต้องการใช้งานระบบกับ

หลายๆ Platform อย่างเช่น Alice ต้องการใช้งานระบบกับทั้งคอมพิวเตอร์ส่วนบุคคล (Personal Computer: PC) และ Smartphone การใช้งานระบบของ Alice ไม่จำเป็นต้องนำกุญแจส่วนตัวที่ถูกสร้างขึ้นในคอมพิวเตอร์ส่วนบุคคลมาติดตั้งบน Smartphone เพียงแค่ Alice กำหนด Secret Word ก็สามารถสร้างกุญแจคู่แล้วเริ่มขั้นตอนการสนทนากับ Bob ได้ และยังสามารถแก้ไขปัญหาความมั่นคงในกรณีที่ Alice ทำอุปกรณ์สูญหายซึ่งอาจทำให้กุญแจส่วนตัวของ Alice รั่วไหลอีกด้วย

2. ผลการประเมินประสิทธิภาพ

จากการออกแบบอัลกอริธึม ISAN Identity-based RSA (IIR) และการพัฒนาต้นแบบเพื่อรองรับการใช้งานแบบ Multi-Platform การประเมินประสิทธิภาพแสดงให้เห็นว่าระบบที่พัฒนาในงานวิจัยนี้จากอัลกอริธึม IIR รองรับการทำงานแบบ Multi-Platform โดยแสดงผลการทดสอบในส่วนของการสร้างกุญแจคู่ (Generate Key **Pair)** ดัง (Figure 10) และขั้นตอนการลงลายมือชื่อดิจิทัล (Sign) และพิสูจน์ลายมือชื่อดิจิทัล (Verify) ดัง (Figure 11)

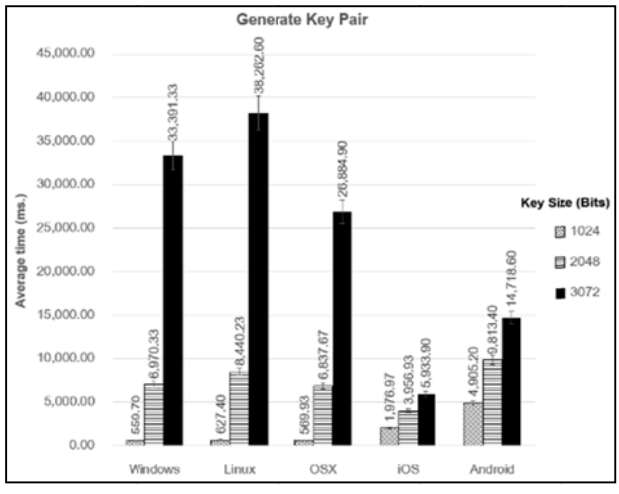

Figure 10 Generating a key pair

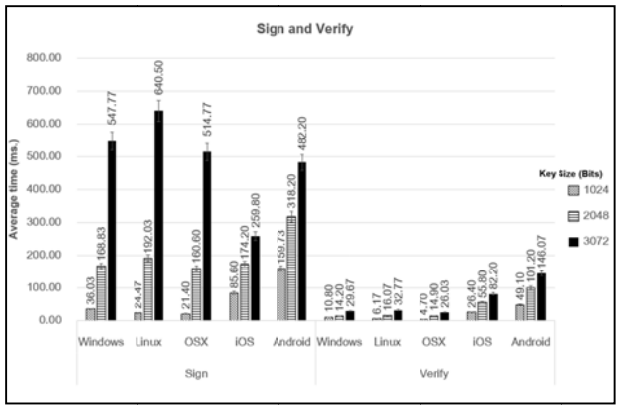

Figure 11 Signing and Verifying the digital signature

จาก **(**Figure 10) และ (Figure 11) แสดงการทดสอบระบบที่พัฒนาจากอัลกอริธึม IIR รองรับการทำงานกับทุก Platform เนื่องจากภาษา JavaScript ที่งานวิจัยนี้เลือกใช้สำหรับพัฒนาระบบรองรับกับการทำงานบน Web Browser กับทุก Platform และการทดสอบได้กำหนดขนาดกุญแจเป็นไปตามมาตรฐานที่ประกาศใน[17] ที่ระบุว่าขนาดของกุญแจที่ใช้กับ RSA Algorithm สำหรับลงลายมือชื่อดิจิทัลต้องอยู่ระหว่าง 2048 bits ถึง 3072 bits และขนาดกุญแจขั้นต่ำสำหรับเข้ารหัสข้อมูลคือ 1024 bits

สรุปผลและข้อเสนอแนะ

การสื่อสารข้อมูลในระบบเครือข่ายถือเป็นวิธีการสื่อสารข้อมูลที่ใช้งานอย่างแพร่หลาย สำหรับความมั่นคงของข้อมูลมีความสำคัญสำหรับการสื่อสารข้อมูล ข้อมูลในระบบจะต้องมีความมั่นคงโดยที่ข้อมูลมีความสมบูรณ์ไม่ถูกเปลี่ยนแปลงแก้ไขระหว่างส่งข้อมูล รักษาข้อมูลให้เป็นความลับเพื่อยืนยันว่าผู้รับเท่านั้นสามารถดูข้อมูลได้เพียงคนเดียวและสามารถพิสูจน์ได้ว่าข้อมูลที่ส่งมายังผู้รับ เป็นการส่งข้อมูลจากผู้ส่งจริง

ในงานวิจัยนี้ได้ออกแบบและพัฒนาอัลกอริธึม ISAN Identity-based RSA (IIR) สำหรับลงและพิสูจน์ลายมือชื่อดิจิทัล เพื่อให้การแลกเปลี่ยนกุญแจสาธารณะมีความมั่นคง ซึ่งทำให้การสื่อสารข้อมูลสามารถพิสูจน์ตัวตนได้ว่าคู่สนทนาเป็นตัวจริงหรือไม่ และการส่งข้อมูลเป็นความลับ ซึ่งผลของงานวิจัยนี้สามารถแก้ไขปัญหาการแลกเปลี่ยนกุญแจสาธารณะของงานวิจัยก่อนหน้านี้ และจากผลการวิเคราะห์ความมั่นคงแสดงให้เห็นว่าอัลกอริธึม IIR สามารถแก้ไขปัญหาการแลกเปลี่ยนกุญแจสาธารณะ รวมถึงผลจากการทดสอบประสิทธิภาพระบบที่พัฒนาจากอัลกอริธึม IIR แสดงให้เห็นว่าระบบรองรับการทำงานแบบ Multi-Platform

กิตติกรรมประกาศ

โครงการนี้ได้รับการสนับสนุนการวิจัย งบประมาณรายได้คณะวิทยาการสารสนเทศ ประจำปีงบประมาณ 2558 มหาวิทยาลัยมหาสารคาม

เอกสารอ้างอิง

1. Arnbak A, Asghari H, Eeten M, et al. Security Collapse in the HTTPS Market. Journal of ACM Queue; 12: 1–15.
2. Symantec Corporation. Online fraud: pharming, 2008, http://us.norton.com/cybercrime-pharming.

3. Diffie W, Hellman M. New directions in cryptography. IEEE Transactions on Information Theory; 22: 644-654.
4. Dierks T, Allen C. The TLS Protocol Version 1.0: IETF RFC 2246, January 1999.
5. Ibrahem M. Modification of Diffie–Hellman Key Exchange Algorithm for Zero Knowledge Proof. Proceedings of International Conference on Future Communication Networks; Baghdad, 2012: 147 - 152.
6. Khader A, Lai D. Preventing Man-In-The-Middle Attack in Diffie-Hellman Key Exchange Protocol. Proceedings of International Conference on Telecommunications (ICT 2015); Sydney, NSW, 2015:204 - 208.
7. Hodges J, Jackson C, Barth A. HTTP Strict Transport Security (HSTS): IETF RFC 6797, November 2012.
8. Rivest R, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, ; 21: 120-126.
9. Shamir A. Identity-based cryptosystems and signature schemes. Proceedings of the CRYPTO 84 on Advances in cryptology; New York, USA :47-53.
10. พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และฉบับแก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2551, http://ictlawcenter.etda.or.th/files/law/file/3/292de62a21d94b42a21218ba21abe0c5.pdf.
11. Boneh D, Franklin M. Identity-Based Encryption from the Weil Pairing. Proceedings of the CRYPTO ‹01 Proceedings of the Annual International Cryptology Conference on Advances in Cryptology; California, USA, 2011: 213-229.
12. Elgamal T. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. IEEE Transactions on Information Theory, 31: 469 - 472.
13. Harn L, Ren J. Efficient identity-based RSA multisignatures. The International Journal of Computers & Security; 27: 12-15.
14. Tripathi S, Biswas G, Kisan S. Cryptographic keys generation using identity. Proceedings of International Conference on Advances in Recent Technologies in Communication and Computing (ARTCom 2011); Bangalore, 2011:148 - 151.
15. Muhammadi N, Zaini J, Saman M. Loop-based RSA key generation algorithm using string identity. Proceedings of International Conference on Control, Automation and Systems (ICCAS 2013); Bangalore, 2013 :255 - 258.
16. Durumeric Z, Kasten J, Bailey M, et al. Analysis of the HTTPS certificate ecosystem. Proceedings of IMC ‹13 Proceedings of conference on Internet measurement conference 2013; New York, USA, 2013: 291-304.
17. Polk W, Dodson D, Burr W, et al. Cryptographic Algorithms and Key Sizes for Personal Identity Verification, U.S. Department of Commerce, NIST Special Publication 800-78-4.