การเพิ่มความมั่นคงให้กับจดหมายอิเล็กทรอนิกส์ด้วยโทรศัพท์มือถือ และ QR Code สำหรับลดข้อจำกัดการใช้งาน

Electronic Mail Security Enhancements Using Mobile Phones and QR Codes for Usability

จรัสพงษ์ โชคชัยสิริ และ ปราโมทย์ กั่วเจริญ
สาขาวิทยาการคอมพิวเตอร์ คณะสถิติประยุกต์ สถาบันบัณฑิตพัฒนบริหารศาสตร์
118 ถนนเสรีไทย แขวงคลองจั่น เขตบางกะปิ กรุงเทพฯ 10240
white_pawns@hotmail.com, pramote@as.nida.ac.th

บทคัดย่อ

การใช้งานจดหมายอิเล็กทรอนิกส์ได้รับการยอมรับอย่างกว้างขวางในการสื่อสารบนอินเตอร์เน็ต อย่างไรก็ตาม จดหมายอิเล็กทรอนิกส์ไม่ได้ออกแบบมาให้มีความมั่นคง และปลอดภัย เนื้อหาของจดหมายอิเล็กทรอนิกส์ที่ส่งนั้นสามารถถูกแก้ไขได้ระหว่างทาง หรือ ในขณะที่ถูกเก็บอยู่บนเซิร์ฟเวอร์ นอกจากนั้น การยืนยันตัวบุคคลของผู้ส่งที่แท้จริงไม่สามารถทำได้ เกิดเป็นช่องว่างซึ่งยากต่อการป้องกันการโจมตีจาก ภัยคุกคามอย่างเช่น Phishing attack

บทความนี้นำเสนอการเพิ่มความมั่นคงให้กับจดหมายอิเล็กทรอนิกส์โดยใช้โทรศัพท์มือถือ และ เทคโนโลยี QR Code แอปพลิเคชั่นนี้มีวัตถุประสงค์เพื่อสร้างทางเลือกสำหรับการเพิ่มความมั่นคงในการใช้งานจดหมายอิเล็กทรอนิกส์ โดยใช้เทคโนโลยี QR Code มาประยุกต์ใช้เพื่อลดข้อจำกัดในการพิมพ์บนโทรศัพท์มือถือ

คำสำคัญ: ความมั่นคงของจดหมายอิเล็กทรอนิกส์, บาร์โค้ดสองมิติ, เทคโนโลยีพีจีพี

Abstract

Electronic mail has been widely adopted as a means to communicate over the Internet. However, the electronic mail is inherently insecure. Its contents can be revealed or modified during transit and while stored on the server. Moreover, the identity of the sender cannot be verified, leaving the user vulnerable to a social engineering attack such as a phishing attack.

This paper presents security enhancements of electronic mail by using mobile phones and QR codes. The application provides the user with an alternative approach of communicating securely using electronic mail. The use of QR codes can mitigate the limitation of typing on mobile phones.

Keywords: Electronic Mail Security, QR Code, PGP

1. คำนำ

การใช้งานจดหมายอิเล็กทรอนิกส์ของผู้ใช้โดยทั่วไปไม่นิยมใช้การเข้ารหัสหรือการสร้างลายมือชื่อดิจิตอล ซึ่งอาจเป็นผลต่อเนื่องมาจากการขาดความรู้และความเข้าใจ การพัฒนาแอปพลิเคชั่นนี้ คาดหวังว่าจะช่วยเพิ่มความมั่นคงปลอดภัยให้กับการใช้งานจดหมายอิเล็กทรอนิกส์ เนื่องจากในปัจจุบันภัยคุกคามต่างๆ การหลอกลวง การโจมตีมีหลากหลายรูปแบบ เช่น Phishing Attack, Worm, Viruses, Spam Mail เป็นต้น โดยภัยร้ายที่มีการพบบ่อยครั้งมากที่สุดคือ Phishing Attack [1] โดยอาศัยการใช้งาน Spoofed Emails เพื่อหลอกลวงให้บุคคลที่ตกเป็นเหยื่อให้เปิดเผยข้อมูลส่วนตัวออกมา โดยมีเป้าหมายอยู่ที่ข้อมูลสำคัญ เช่น ข้อมูลด้านการเงิน ข้อมูลหมายเลขบัญชี รหัสผ่าน และรหัสบัตรประชาชน เป็นต้น การพัฒนาแอปพลิเคชั่นด้านความมั่นคง

ของจดหมายอิเล็กทรอนิกส์บนโทรศัพท์มือถือนั้น จึงมีส่วนที่ควรคำนึงถึงสองประการ คือ

- ความลับของข้อความ (Message Confidentiality) [2]: การเข้ารหัสข้อมูลไว้ทำให้สามารถปกปิดข้อมูลสำคัญไว้ได้ ไม่สามารถถูกเปิดอ่านโดยบุคคลที่ไม่พึงประสงค์
- ความถูกต้องของข้อความ (Message Authenticity) : การสร้างลายมือชื่อดิจิตอลช่วยในการระบุตัวตน ลดการปลอมแปลงจดหมายอิเล็กทรอนิกส์

การพัฒนาแอปพลิเคชั่นด้านความมั่นคงของจดหมายอิเล็กทรอนิกส์บนโทรศัพท์มือถือนั้น เป็นสิ่งสำคัญที่จะช่วยลดข้อจำกัดเรื่องการใช้งาน ทำให้เราสามารถรับ–ส่งจดหมายอิเล็กทรอนิกส์ได้ทุกที่ทุกเวลา ทำให้ผู้ใช้สามารถได้รับความมั่นใจ ความปลอดภัย ตลอดจนการปกปิดข้อมูลที่ไม่อยากให้ผู้อื่นรู้ อีกทั้งยังสามารถเก็บกุญแจที่ใช้ในการเข้ารหัส–ถอดรหัส หรือ การสร้างลายมือชื่อดิจิตอลไว้กับตัวได้ตลอดเวลา แม้ว่าจะมีอุปสรรคเรื่องการป้อนข้อมูลเข้าในการส่งจดหมายอิเล็กทรอนิกส์บนโทรศัพท์มือถือ แต่ว่าเราสามารถลดอุปสรรคนี้ไปได้ด้วยเทคโนโลยี QR Code

2. พื้นฐานและงานวิจัยที่เกี่ยวข้อง

เนื้อหาส่วนนี้นำเสนอความรู้พื้นฐานและงานวิจัยที่เกี่ยวข้องกับการเพิ่มความมั่นคงปลอดภัยให้กับจดหมายอิเล็กทรอนิกส์

2.1 พื้นฐานของการเพิ่ม Security ให้กับจดหมายอิเล็กทรอนิกส์

ในการใช้งานจดหมายอิเล็กทรอนิกส์เราต้องการที่จะพิสูจน์ตัวบุคคล และ เพิ่มความมั่นคงปลอดภัยในการส่งข้อมูลทำให้บุคคลที่สามไม่สามารถเข้าถึงข้อมูลที่ติดต่อกันได้ การพิสูจน์ตัวบุคคลจะเรียกว่า Authentication [3] การปกป้องเนื้อหาของข้อมูลจึงเป็นอีกอย่างหนึ่งที่ท้าทาย โดยมี 3 ส่วนที่สำคัญดังนี้

2.1.1 การเข้ารหัสข้อมูล - Data Encryption (Privacy)

การเข้ารหัสแบบ Symmetric Algorithm นั้นได้ถูกใช้เป็นมาตรฐานของการเข้ารหัสจดหมายอิเล็กทรอนิกส์ โดยมีข้อดีคือการคำนวณนั้นใช้เวลาน้อยกว่าแบบ Asymmetric Algorithm

2.1.2 ความบูรณภาพของข้อมูลและการพิสูจน์ตัวจริง (Message Integrity and Authentication)

เมื่อเนื้อหาของข้อมูลถูกยืนยันได้ว่าผู้ส่งเป็นใครและไม่มีการถูกแก้ไขโดยผู้อื่น จะต้องตกลงกันในเรื่อง Algorithm ที่ใช้ในการสร้างลายมือชื่อดิจิตอล และ Hash Function ที่ใช้ โดยส่วนแรกจะเป็นสิ่งที่ยืนยันถึงตันตนผู้ส่งข้อมูลและส่วนหลังจะเป็นตัวบอกว่าข้อมูลไม่ได้มีการแก้ไขโดยผู้อื่น

2.1.3 การจัดการจัดการกุญแจ (Key Management)

จากข้อมูลก่อนหน้าที่อธิบายการทำงานของการใช้กุญแจ เราจะเชื่อถือได้อย่างไรเนื่องมาจากการโจมตีแบบ Man-in-the-middle ซึ่งบุคคลที่สาม ซึ่งไม่ประสงค์ดีจะแอบดักเอากุญแจสาธารณะของผู้รับ–ส่ง ไว้แล้วส่งกุญแจสาธารณะของตนไปแทน โดยมีหัวใจหลักคือ

- การระบุตัวตนของเจ้าของกุญแจสาธารณะ
- การรับรองถึงกุญแจสาธารณะที่เปิดเผยออกมากับเจ้ากุญแจ

2.2 Pretty Good Privacy (PGP)

PGP [4] มีฟังชั่นการเพิ่มความมั่นคงและปลอดภัยให้กับจดหมายอิเล็กทรอนิกส์ เช่น การเข้ารหัส การสร้างลายมือชื่อดิจิตอล และการจัดการกุญแจที่ใช้ใน PGP โดยถูกกำหนดให้เป็นมาตรฐานโดย RFCs ในปี 1991, 2015 และ 2440 [5- 7] ตามลำดับ

กระบวนการทำงานของ PGP [8] มีดังนี้

- Digital Signature : Hash ของข้อความที่ได้ถูกสร้างจากการใช้Algorithm SHA1 โดยส่วนนี้จะถูกเข้ารหัสอีกทีด้วยการเข้ารหัสแบบ Asymmetric ด้วย RSA หรือ DSS
- Message Encryption : ข้อความที่ส่งจะถูกเข้ารหัสได้จากการเข้ารหัสแบบ Symmetric Algorithm เช่น AES IDEA และ Triple DES เป็นต้น ด้วยกุญแจชั่วคราวที่ถูกสร้างโดยผู้ส่ง ซึ่งกุญแจชั่วคราวนี้ถูกเข้ารหัสไว้อีกทีด้วยการเข้ารหัส

แบบ Asymmetric Algorithm เช่น Diffie-Hellman, RSA เป็นต้น จากนั้นนำกุญแจชั่วคราวที่ถูกเข้ารหัสแล้วปะเข้าไปกับข้อความที่ส่ง

- Compression : การบีบอัดข้อมูลมีวัตถุประสงค์เพื่อลดขนาดของข้อมูลโดยใช้ Algorithm เช่น Zip และ Zlib
- E-mail Compatibility : การส่งจดหมายอิเล็กทรอนิกส์ยินยอมให้มีการส่งรูปแบบของข้อมูลเฉพาะ ASCII text เพื่อให้สามารถทำงานได้อย่างสอดคล้องกับ PGP จึงได้อาศัย Algorithm Radix-64 ในการแปลงรหัสบิตข้อมูล ทำให้ขนาดของข้อมูลที่ส่งเพิ่มร้อยละ 33 เพื่อไม่ให้ขนาดของข้อมูลที่ส่งโตจนเกินไป จึงใช้การบีบอัดข้อมูลเช่นแบบ Zip จะสามารถเพิ่มอัตราส่วนการบีบอัดเป็น 2.0 ดังนั้นข้อมูลขนาด **A** words เมื่อส่งจริงจะมีขนาดเท่ากับ 1.33 x 0.5 x **A** = 0.665 x **A** ดังนั้นจะเห็นได้ว่าข้อมูลที่ส่งจริงยังคงมีการบีบอัด 1 ใน 3
- Transparency : ลดความยุ่งยากซับซ้อนในการใช้งานแอปพลิเคชั่นให้กับผู้ใช้งานจดหมายอิเล็กทรอนิกส์

2.3 QR Code

QR code [9] ได้ผ่านการรับรองในมาตรฐานต่างๆ เช่น ISO/IEC 18004 เป็นต้น สามารถบรรจุข้อมูลได้มากทั้งข้อความและตัวเลข อีกทั้งยังตอบสนองได้รวดเร็ว ใช้งานง่าย เป็นที่แพร่หลายทั้งในโฆษณา และ แอปพลิเคชั่นต่างๆ

3. **กระบวนพัฒนาและการออกแบบ**

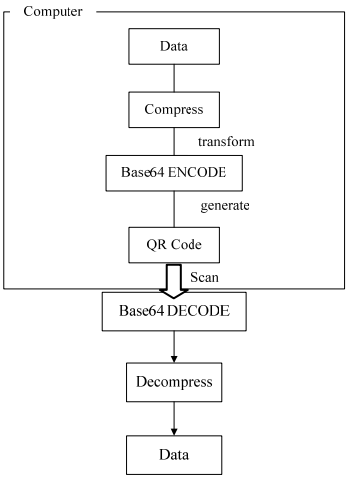
การเพิ่มความมั่นคงปลอดภัยให้กับการใช้งานจดหมายอิเล็กทรอนิกส์อาศัยเทคโนโลยีพีจีพีและบาร์โค้ดสองมิติเข้ามาช่วยในการลดปัญหา อุปสรรคที่เกิดขึ้นจากการป้อนข้อมูลบนอุปกรณ์โทรศัพท์มือถือโดยแบ่งกระบวนการพัฒนาออกเป็น 2 ส่วนดังนี้

3.1 กระบวนการทำงานของการส่งจดหมายอิเล็กทรอนิกส์

การทำงานของฝั่งส่งจดหมายอิเล็กทรอนิกส์แบ่งออกเป็นสองทางเลือกคือ

- การป้อนข้อมูลผ่านแบบฟอร์มของแอปพลิเคชั่นบนโทรศัพท์มือถือ
- การป้อนข้อมูลผ่านแอปพลิเคชั่นที่พัฒนาด้วยเทคโนโลยี Java Applet โดยผู้ใช้สามารถเลือกได้ว่าจะใช้งานเป็นแบบ Standalone รันเป็นโปรแกรมธรรมดาบนเครื่องทั่วไป หรือ เข้าไปที่ Website จากนั้นจึงสร้างเป็น QR Code

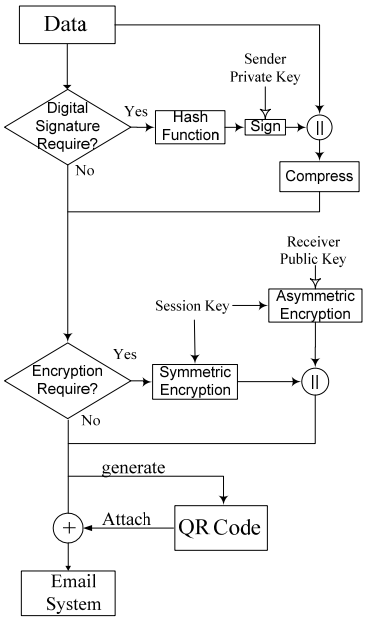
โดยทางเลือกที่สองนั้นมีวัตถุประสงค์เพื่อเพิ่มทางเลือก อำนวยความสะดวกแก่ผู้ใช้งาน และ ช่วยให้ลดข้อจำกัดด้านพิมพ์บนโทรศัพท์มือถือ เนื่องจากการพิมพ์บนโทรศัพท์มือถือทำได้ยาก โดยเริ่มการทำงานจาก ข้อมูลดิบจะถูกบีบอัดเพื่อลดขนาดลง จากนั้นจะทำการแปลงข้อมูลจากรูปแบบของบิตข้อมูลให้อยู่ในรูปของ Base64 Encoding เพื่อลดปัญหาที่เกิดขึ้นจากการแปลงรหัสบิตข้อมูล หลังจากนั้นจะมีการตรวจสอบขนาดของข้อมูลก่อนว่ามีขนาดเท่าไร ถ้าข้อมูลมีขนาดใหญ่จะถูกแบ่งออกเป็นหลายส่วน แล้วนำไปสร้างเป็น QR Code ทีละส่วนจนครบทุกส่วนของข้อมูล



รูปที่ 1 การทำงานเพื่อส่งข้อมูลเข้าสู่แอปพลิเคชั่นบนโทรศัพท์มือถือ

เมื่อเสร็จสิ้นกระบวนการทำงานของแอปพลิเคชั่นนี้แล้ว นำโทรศัพท์มือถือที่มี แอปพลิเคชั่นจากการศึกษานี้มาสแกน

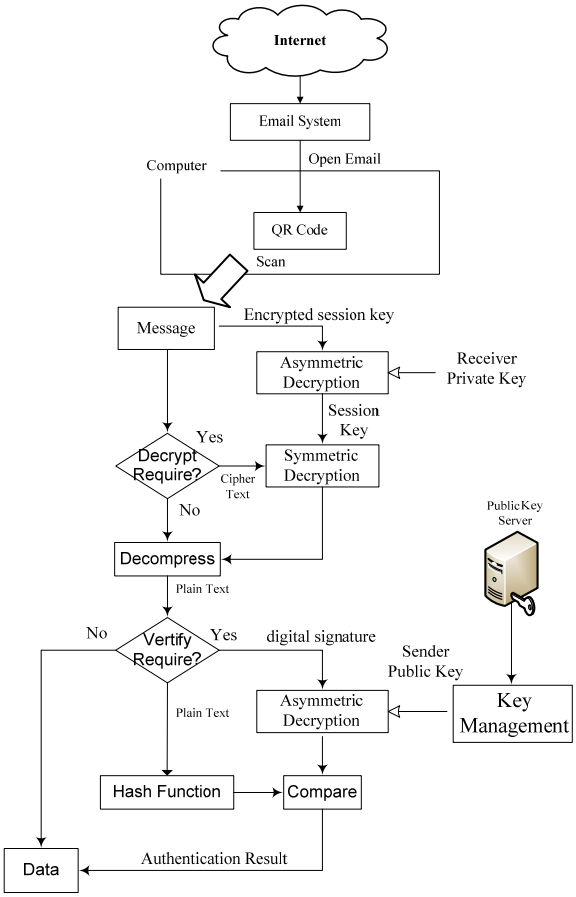
QR Code แล้วแปลงรหัสบิตข้อมูล พร้อมทั้งคลายการบีบอัดข้อมูล จะได้ข้อมูลแบบเดียวกับที่ป้อนผ่านแอปพลิเคชั่นที่พัฒนาด้วย Java Applet โดยมีขั้นตอนดังแสดงในรูปที่ 1 ขั้นตอนถัดไปคือกระบวนการการสร้างกุญแจมีขั้นตอนเริ่มจากการสร้างกุญแจ ซึ่งกุญแจแบ่งได้ออกเป็นสองประเภทคือ กุญแจสาธารณะและกุญแจส่วนตัว ซึ่งจะถูกเข้ารหัสไว้ด้วย Symmetric Algorithm เพื่อป้องกันไม่ให้คนอื่นสามารถใช้ได้ถ้าไม่รู้ Passphrase โดยกุญแจสาธารณะที่ได้นี้ จะมีการบริหารจัดการผ่าน CA (Certificate Authority) หรือ แบบที่ง่ายสุดสามารถทำได้โดยไม่ต้องเสียค่าใช้จ่ายคือ ใช้การแลกเปลี่ยนกันโดยตรงกับบุคคลที่เราต้องการติดต่อด้วย



รูปที่ 2 การเพิ่มความมั่นคงให้กับข้อมูล

จากรูปที่ 2 เมื่อได้กุญแจแล้วจึง นำข้อมูลเข้าสู่กระบวนการเพิ่มความมั่นคง เช่น การเข้ารหัสและการสร้างลายมือชื่อดิจิตอล จากนั้นนำข้อมูลที่ได้สร้างเป็น QR Code ออกมาแนบเข้าไปกับจดหมายอิเล็กทรอนิกส์ เพื่ออำนวยความสะดวกให้ผู้รับ ในกรณีที่เปิดอ่านจากคอมพิวเตอร์สาธารณะ แล้วต้องการพิสูจน์ตัวบุคคลหรือถอดรหัสข้อมูล

3.2 การทำงานของฝั่งรับ



รูปที่ 3 การเปิดอ่านข้อมูลจดหมายอิเล็กทรอนิกส์

การทำงานของฝั่งรับจดหมายอิเล็กทรอนิกส์ ดังแสดงในรูปที่ 3 เริ่มต้นเมื่อข้อมูลถูกส่งมาผ่านมายัง E-mail System ผู้รับเปิดอ่านจดหมายอิเล็กทรอนิกส์ ด้วยการสแกน QR Code ที่แนบมาจากจดหมายอิเล็กทรอนิกส์ไปยังมือถือที่ติดตั้งแอปพลิเคชั่นนี้

เมื่อได้รับข้อมูลครบถ้วนแล้ว ในกรณีที่ข้อมูลถูกเข้ารหัส ขั้นตอนถัดไปคือ การถอดรหัสโดยใช้กุญแจส่วนตัวของผู้รับ และถ้ามีการลงลายมือชื่อดิจิตอล จะมีการยืนยันตัวบุคคลโดยจะใช้กุญแจสาธารณะของผู้ส่งจาก Public Key Server เมื่อเสร็จสิ้นกระบวนการแล้ว จึงได้ข้อมูลที่แท้จริงที่ส่งมา พร้อมกับการรับรองการยืนยันตัวบุคคลและความถูกต้องของข้อมูล

4. การทดสอบและผลการดำเนินงาน

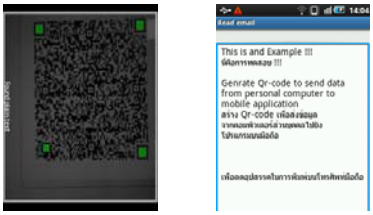
ขั้นตอนในส่วนของการทดสอบทำงานสามารถแบ่งได้เป็นหลายส่วน ตั้งแต่ส่วนของแอปพลิเคชั่นที่พัฒนาด้วยเทคโนโลยี Java Applet กระบวนการในการเข้ารหัส การทำลายมือชื่อดิจิตอล การจัดการกุญแจ การถอดรหัสข้อมูล และ การยืนยันตัวบุคคล หลังจากที่ได้พัฒนาระบบเป็นที่เรียบร้อยจึงได้ผลทดสอบการทำงานออกมาดังนี้

4.1 การทำงานของแอปพลิเคชั่นที่พัฒนาด้วยเทคโนโลยี Java Applet

รูปที่ 4 ผลการสร้างข้อมูลให้อยู่ในรูปของ QR Code

การใช้งานแอปพลิเคชั่นนี้ทำให้เราสามารถป้อนข้อมูลได้สะดวกและรวดเร็วในกรณีที่ผู้ใช้มีเครื่องคอมพิวเตอร์เมื่อได้ QR Code ดังแสดงในรูปที่ 4 แล้วการสแกนข้อมูลเข้าสู่โทรศัพท์มือถือจะใช้เวลาไม่นาน เมื่อเปรียบเทียบกับการป้อนข้อมูลผ่านโทรศัพท์โดยตรงแล้วพบว่า สามารถป้อนข้อมูลเพื่อใช้ในส่งจดหมายอิเล็กทรอนิกส์ได้สะดวก รวดเร็วกว่า

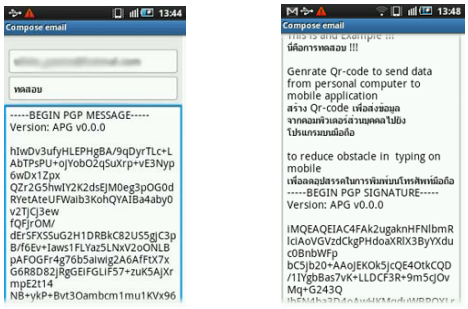
4.2 การทำงานของแอปพลิเคชั่นบนโทรศัพท์มือถือ



(a) การสแกน QR Code (b) ผลจากการสแกน QR Code

รูปที่ 5 การอ่านข้อมูลจาก QR Code เข้าสู่โทรศัพท์มือถือ

เมื่อเรียกใช้งานเมนูสแกนจะเข้าสู่โหมดการอ่านข้อมูล รอการสแกน QR Code เมื่อโปรแกรมอ่าน QR Code สามารถตรวจอ่านกับ Tag ของ QR Code ดังแสดงในรูปที่ 5 (a) ได้อย่างถูกต้องครบจนทุกรูปแล้ว จะได้ข้อมูลออกมาดังแสดงในรูปที่ 5 (b) หลังจากนั้นเข้าสู่การบริหารจัดการกุญแจเลือกสร้างตาม Algorithms ที่ต้องการเช่น RSA หรือ Diffie-Hellman เป็นต้น โดยกุญแจส่วนตัวจะถูกเข้ารหัสไว้ด้วย Passphrase เพื่อให้แน่ใจได้ว่ามีเพียงผู้สร้างเท่านั้นที่สามารถใช้งานได้ และ สามารถกำหนดการใช้งานกุญแจนี้ได้ว่าสามารถใช้ได้ทั้งสำหรับการเข้ารหัส, การสร้างลายมือชื่อดิจิตอล หรือเพียงอย่างใดอย่างหนึ่ง



(a) ผลจากการเข้ารหัส (b) ผลการสร้างลายมือชื่อดิจิตอล

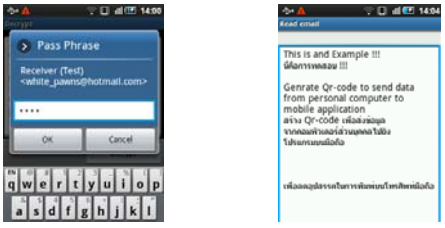
รูปที่ 6 ผลที่ได้จากกระบวนการเพิ่มความมั่นคงให้กับข้อมูล

กระบวนการเพิ่มความมั่นคงปลอดภัยให้กับจดหมายอิเล็กทรอนิกส์สามารถทำได้โดยการเข้ารหัส หรือ การสร้างลายมือชื่อดิจิตอลซึ่งจะได้ผลลัพธ์ดังแสดงในรูปที่ 6 (a) และ 6 (b) ตามลำดับ โดยใช้เวลาเพียงไม่นานในกระบวนการทำงาน เนื่องจากใช้หลักการของ Thread โดยมี Progress Bar เพื่อบอกความคืบหน้าของการทำงาน

รูปที่ 7 ข้อมูลจดหมายอิเล็กทรอนิกส์ที่มีการเข้ารหัสไว้

การเปิดอ่านข้อมูลแบ่งเป็น 2 กรณีดังนี้

- กรณีแรก เมื่อผู้ใช้สามารถเข้าถึงได้โดยตรงผ่านระบบสัญญาณอินเตอร์เน็ตบนโทรศัพท์มือถือ ผู้ใช้งานไม่จำเป็นต้องใช้ QR Code ที่แนบมา
- กรณีที่สอง เมื่อไม่มีระบบสัญญาณอินเตอร์เน็ตบนโทรศัพท์มือถือ แต่ผู้ใช้สามารถเข้าถึงผ่านระบบคอมพิวเตอร์จากร้านอินเตอร์เน็ต หรือ แหล่งอื่น เมื่อเปิดอ่านจดหมายอิเล็กทรอนิกส์ผู้รับจะเห็นข้อมูลดังแสดงในรูปที่ 7 เราสามารถถอดรหัสข้อมูลได้ด้วยการสแกนข้อมูลจาก QR Code ที่แนบมากับจดหมายอิเล็กทรอนิกส์แล้วใช้กุญแจส่วนตัวของผู้รับถอดรหัสข้อมูล ซึ่งต้องมีการใส่ Passphrase ก่อนถึงสามารถเรียกใช้งานกุญแจได้ ดังแสดงในรูปที่ 8 (a) เมื่อถอดรหัสแล้วจะได้ข้อมูลออกมาดังแสดงในรูปที่ 8 (b) ในทำนองเดียวกันการยืนยันตัวบุคคลสามารถทำได้โดย ใช้กุญแจสาธารณะของผู้ส่งในการระบุตัวตน



(a) การเรียกใช้งานกุญแจส่วนตัว (b) ข้อมูลจริงที่ได้รับ

รูปที่ 8 การใช้งานแอปพลิเคชั่นเพื่อถอดรหัสข้อมูล

5. สรุปผลและข้อเสนอแนะ

จากการศึกษาและพัฒนาแอปพลิเคชั่นนี้ นอกจากทำให้สามารถนำเทคโนโลยีที่มีอยู่ในปัจจุบันมาใช้ให้เกิดประโยชน์สูงสุดในด้านความมั่นคงปลอดภัย บนระบบเครือข่ายคอมพิวเตอร์แล้ว ยังช่วยให้ค้นพบปัญหาของการพัฒนารวมทั้ง อุปสรรค ข้อจำกัด แนวทางแก้ไข เช่น ปัญหาด้านอุปกรณ์ที่มีขีดจำกัดด้านสมรรถนะ ปัญหาด้านความแตกต่างกันของซอฟต์แวร์ระบบ เป็นต้น ผู้พัฒนาควรคำนึงถึงปัญหาเหล่านี้พร้อมหาแนวทางแก้ไขให้ดี

การพัฒนาแอปพลิเคชั่นด้านความมั่นคงปลอดภัยควรนำเสนออยู่ในรูปแบบที่ไม่ซับซ้อน เข้าใจง่ายในการใช้งาน ผู้ใช้ไม่จำเป็นต้องมีความรู้ในเรื่องความมั่นคงปลอดภัยมากนัก ถ้าเราพัฒนาให้มีความยุ่งยาก ซับซ้อนสูง ถึงแม้ว่าจะได้ประโยชน์ทางด้านความมั่นคงปลอดภัย แต่การที่ผู้ใช้เข้าใจยาก แอปพลิเคชั่นที่เราพัฒนาขึ้นนั้นอาจจะไม่นิยม และควรยึดเอามาตรฐานสากลทั้งในเรื่องของ รูปแบบ Algorithm ที่เป็นที่นิยมมีความมั่นคงปลอดภัยสูง ผ่านการพิสูจน์มาแล้วจนได้รับความเชื่อถือ

6. เอกสารอ้างอิง

[1] J. Crain, L. Opyrchal and A. Prakash, "Fighting Phishing with Trusted Email," Int. Conf. on Availability Reliability and Security, 2010

[2] L. Harn and J. Ren, "Design of Fully Deniable Authentication Service for E-mail Applications," Commun. Lett. IEEE, vol. 12, no. 3, Mar. 2008

[3] Mars. T. Rose and D. Strom, “Secure E-Mail: Problems Standards and Prospects,” vol. 2, no. 1, pp. 30-42, Mar. 1999

[4] S. Garfinkel., “PGP: Pretty Good Privacy”. O’Reilly & Associates, 1994.

[5] D. Atkins, W. Stallings, and P. Zimmermann. RFC 1991, “PGP message exchange formats”, August 1996.

[6] J. Callas et al., “OpenPGP message format,” RFC 2440, November 1998.

[7] M. Elkins, “MIME security with pretty good privacy (PGP),” RFC 2015, October 1996.

[8] W. Stallings, Cryptography and Network Security, 5th ed., Upper Saddle River, NJ: Prentice Hall, 2010, pp. 594-598.

[9] J. Gao, et al., “A 2D Barcode-Based Mobile Payment System”, Int. Conf. on Multimedia and Ubiquitous Eng., pp. 320-322, October 2009