บทความวิจัย

การประชุมวิชาการ งานวิจัยและพัฒนาเชิงประยุกต์ ครั้งที่ 8

8th ECTI-CARD 2016, Hua Hin, Thailand

ระบบการเข้ารหัสข้อความสำหรับรหัสคิวอาร์

Character-based Encryption System for Quick Response Code

ณภัทร ยิ้มจันทร์[1] โสรยา สิงสาโร[2] ผุสดี มุหะหมัด[2] และ ลัดดา ปรีชาวีรกุล [1]

[1]ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยสงขลานครินทร์

ตู้ปณ. 3 คอหงส์ อ.หาดใหญ่ จ.สงขลา 90110 E-mail: nn.yimjan@gmail.com, ladda.p@psu.ac.th

[2]หน่วยเครื่องมือกลาง คณะวิทยาศาสตร์ มหาวิทยาลัยสงขลานครินทร์

อ.หาดใหญ่ จ.สงขลา 90110 E-mail: {soraya.s , phutsadee.m}@psu.ac.th

บทคัดย่อ

ข้อมูลเป็นหนึ่งในปัจจัยหลักในการดำเนินธุรกิจ การมีข้อมูลทำให้มีข้อได้เปรียบสำหรับการวางแผนงาน และการรักษาความปลอดภัยของข้อมูลนั้นก็จำเป็นเช่นกัน ข้อมูลถูกนำเสนอในหลากหลายรูปแบบ เพื่อสะดวกต่อการใช้งาน หนึ่งในรูปแบบนั้นคือ รหัสคิวอาร์ โดยรหัสคิวอาร์สามารถอ่านได้ผ่านทางกล้องของอุปกรณ์สื่อสารเคลื่อนที่ หรือ อุปกรณ์สำหรับอ่านรหัสคิวอาร์ อย่างไรก็ตาม ข้อมูลในรหัสคิวอาร์ไม่สามารถอ่านด้วยตาเปล่าได้ ซึ่งทำให้ผู้ไม่หวังดีสามารถแก้ไขดัดแปลงเพื่อนำไปใช้ประโยชน์ในทางไม่ดี เช่น การ phishing ที่มีการทำธุรกรรมทางการเงิน เพื่อหลอกเอาข้อมูลส่วนตัวของผู้ใช้ ดังนั้นบทความวิจัยนี้จึงเสนอ ขั้นตอนวิธีการเข้ารหัสข้อความก่อนจะทำการสร้างรหัสคิวอาร์ โดยมีกรณีศึกษาคือการเพิ่มความปลอดภัยให้กับระบบจัดการสารสนเทศห้องปฏิบัติการ (QR-LIMS) ของหน่วยเครื่องมือกลาง คณะวิทยาศาสตร์ มหาวิทยาลัยสงขลานครินทร์ โดยทำการเก็บผลการวิเคราะห์ตัวอย่างไว้ในรหัสคิวอาร์ และทำการแจกจ่ายให้ผู้ที่ขอใช้บริการทดสอบตัวอย่างจากการศึกษา พบว่ารหัสคิวอาร์ที่ถูกเข้ารหัสนั้นมีความปลอดภัยในการใช้งานมากกว่ารหัสคิวอาร์ที่ไม่ถูกเข้ารหัส

คำสำคัญ: ความปลอดภัย, บาร์โค้ด, รหัสคิวอาร์, อุปกรณ์สื่อสารเคลื่อนที่

Abstract

Information is one of the main factors in the business. The advantage of having data for planning and information security is needed as well. Information is presented in various formats, a QR code is one of the themes. QR code can be read via the camera of a mobile device or any other device supported them. However, the message in the QR code can be modified. Therefore, this paper proposes algorithm to encrypt the message before creating the QR code. The QR-LIMS of Central Equipment Division, Faculty of Science, Prince of Songkla University is applied to be our case study to increase the security. Stores the results of the sample analysis in the QR code and reports to the customers who request a test sample. The study result shows that the QR code is encrypted secured more than the QR code is not encrypted.

Keywords: bar code, mobile device, QR Code, Security

1. บทนำ

รหัสคิวอาร์เป็นหนึ่งในรูปแบบการนำเสนอข้อมูลระหว่างผู้รับและผู้ส่งสารในรูปแบบบาร์โค้ดสองมิติเพื่อให้เกิดความถูกต้องแม่นยำในการรับส่งข้อมูลและลดขนาดพื้นที่ในแสดง เช่นที่อยู่ของเว็บไซต์ (URL) แต่การใช้รหัสคิวอาร์นั้นมนุษย์ไม่สามารถอ่านด้วยตาเปล่าได้ อาจมีผู้ไม่หวังอาศัยช่องโหว่นี้ในการแก้ไขดัดแปลงรหัสคิวอาร์เพื่อนำผู้ใช้ไปเข้าสู่เว็บไซต์ที่ถูกสร้างมาเพื่อการหลอกลวง โดยในปีค.ศ. 2012, Narayanan ได้นำเสนอเกี่ยวกับปัญหาที่เกิดขึ้นจากการใช้งานรหัสคิวอาร์และนำเสนอวิธีการใช้งานในชีวิตประจำวันได้อย่างปลอดภัย [1] ต่อมา Krombholz และคณะ ได้สรุปงานวิจัยเกี่ยวกับความปลอดภัยในการใช้งานรหัสคิวอาร์ [2] ซึ่งกล่าวถึงภาพรวมของความปลอดภัยในการใช้งานรหัสคิวอาร์ รูปแบบการโจมตีที่เกิดขึ้นโดยการแก้ไขข้อมูลที่อยู่ในรหัสคิวอาร์ และการออกแบบรหัสคิวอาร์เพื่อการใช้งานอย่างปลอดภัย นอกจากนี้ Bani-Hani และคณะ ได้เสนอการสร้างระบบเพื่อความปลอดภัยของรหัสคิวอาร์ [3] โดยการเข้ารหัสข้อความก่อนที่จะทำการสร้างรหัสคิวอาร์ด้วยวิธีการเข้ารหัสแบบกุญแจอสมมาตรอีกทั้งยังทำการตรวจสอบความน่าเชื่อถือของข้อความเพื่อป้องกันภัยคุกคาม เช่น ฟิชชิง (Phishing) ฟาร์มมิ่ง (Pharming) และคำสั่งที่สามารถสั่งให้อุปกรณ์ทำงาน สำหรับงานวิจัยที่เกี่ยวกับความปลอดภัยของการส่งข้อมูล Sen และคณะ ได้เสนอกล่าวถึงการส่งข้อมูลระหว่างผู้ใช้งานอุปกรณ์สื่อสารเคลื่อนที่ [4] โดยจะทำการเข้ารหัสข้อความด้วยวิธีการแบบกุญแจสมมาตร ซึ่งผู้ใช้สามารถเลือกอัลกอริทึม AES หรือ RC4 และใส่กุญแจได้ด้วยตนเองด้วย แล้วทำการสร้างเป็นรหัสคิวอาร์เพื่อส่งให้ผู้ใช้อีกคน ส่วนผู้ใช้ที่ได้รับรหัสคิวอาร์เมื่อต้องการถอดรหัสข้อความต้องใส่กุญแจด้วยตัวเอง

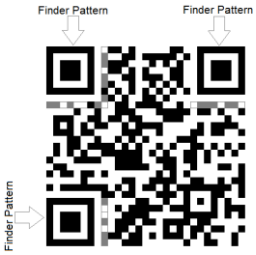
นอกจากนี้ รหัสคิวอาร์ยังได้ถูกนำมาประยุกต์ใช้อย่างแพร่หลายดังจะเห็นได้จากการประยุกต์ใช้รหัสคิวอาร์กับระบบการจัดการสารสนเทศห้องปฏิบัติการวิทยาศาสตร์[5] คณะวิทยาศาสตร์ มหาวิทยาลัยสงขลา-นครินทร์ วิทยาเขตหาดใหญ่ ซึ่งเป็นระบบที่เก็บ URL ของระบบไว้ในรหัสคิวอาร์และทำการแจกจ่ายให้ผู้เกี่ยวข้องกับการทดสอบตัวอย่างเพื่อลดความผิดพลาดจากการกรอก URL เพื่อเข้าใช้งานระบบ

จากงานวิจัยที่กล่าวมาข้างต้นพบว่าได้มีการประยุกต์ใช้งานรหัสคิวอาร์และการวิจัยเพื่อความปลอดภัย อย่างไรก็ตามยังไม่มีการประยุกต์ใช้การเข้ารหัสแบบกุญแจสมมาตรและถอดรหัสข้อความโดยผู้ใช้ไม่มีส่วนเกี่ยวข้องกับการจดจำกุญแจเพื่อเข้าหรือถอดรหัสผ่านอุปกรณ์สื่อสารเคลื่อนที่ ดังนั้น งานวิจัยนี้จึงนำเสนอ ระบบเข้ารหัสข้อความชนิดตัวอักษรสำหรับรหัสคิวอาร์ (Character-based Encryption System for Quick Response Code หรือ CES4QR)

2. ทฤษฎีที่เกี่ยวข้อง

2.1 รหัสคิวอาร์

รหัสคิวอาร์ หรือ QR Code (Quick Responsible Code) คือบาร์โค้ดสองมิติ สามารถอ่านข้อมูลที่ถูกบรรจุอยู่ด้วยอุปกรณ์ที่รองรับเช่น อุปกรณ์สื่อสารเคลื่อนที่ ที่ติดตั้งโปรแกรมอ่านรหัสคิวอาร์ รหัสคิวอาร์สามารถบรรจุข้อมูล ตัวอักษร (Alphanumeric) ไบนารี (Binary) และ คันจิ (Kanji)ได้มีการนำรหัสคิวอาร์มาทำการเก็บข้อมูล URL ซึ่งเป็นข้อมูลชนิดตัวอักษรชนิดหนึ่งเพื่อลดความผิดพลาดในการกรอก URLโดยผู้ใช้และช่วยลดเวลาในการพิมพ์ รหัสคิวอาร์สามารถอ่านข้อมูลได้แม้มีบางส่วนเสียหาย โดยมีโครงสร้างดังภาพ Finder pattern ทำหน้าที่ระบุตำแหน่งและพิกัดเพื่อถอดรหัส ส่วนสีเทา Format information คือส่วนเก็บข้อมูลสำหรับตรวจสอบและแก้ไขข้อผิดพลาดของข้อมูล ส่วนที่เหลือคือ Encode data ส่วนสำหรับเก็บข้อมูล



รูปที่ 1 โครงสร้างรหัสคิวอาร์

2.2 วิทยาการเข้ารหัสลับ (Cryptography)

วิทยาการการเข้ารหัสลับ คือศาสตร์ที่ว่าด้วยการอำพรางข้อมูลโดยการเข้ารหัสเพื่อไม่ให้ผู้อื่นสามารถอ่านได้โดยง่ายโดยการดำเนินการเข้าและถอดรหัสนั้น จำเป็นต้องมีกุญแจ (Key) ซึ่งแบ่งออกเป็น 2 ประเภท คือการเข้ารหัสด้วยวิธีการแบบกุญแจสมมาตร โดยใช้กุญแจเพียงดอกเดียวในการเข้าและถอดรหัสข้อความตัวอย่างขั้นตอนวิธี เช่น AES DES RC4 และBlowfish และการเข้ารหัสด้วยวิธีแบบกุญแจอสมมาตร เป็นการใช้กุญแจสองดอกในการเข้าและถอดรหัสข้อความตัวอย่างขั้นตอนวิธี เช่น RSA DSA และECDH

สำหรับขั้นตอนการเข้ารหัสแบบ AES จะทำการเข้ารหัสข้อความเป็นบล็อค ขนาดบล็อคละ 128 บิต ใช้กุญแจขนาด 128 192 และ 256 บิตในการเข้ารหัสและถอดรหัสข้อความโดยมีการทำงานวนซ้ำขึ้นอยู่กับขนาดของกุญแจที่ใช้ในการเข้าและถอดรหัส [6]

ส่วนการเข้ารหัสด้วยกุญแจแบบอสมมาตรที่ใช้กันอย่างแพร่หลายคือ RSA ซึ่งพัฒนาโดย Ron Rivest Adi Shamir และ Leonard Adleman โดยเป็นการเข้ารหัสที่ใช้ความรู้ทางคณิตศาสตร์มอดุลาร์เข้ามาเกี่ยวข้อง โดยกุญแจจะถูกสุ่มขึ้นมาด้วยจำนวนเฉพาะขนาดที่ใหญ่มากซึ่งถูกแบ่งเป็นสองชุด: กุญแจส่วนตัว (Private Key) และกุญแจสาธารณะ (Public Key) แล้วทำการเข้ารหัสโดยใช้กุญแจส่วนตัวหรือกุญแจสาธารณะ [7]

3. ระบบการเข้ารหัสและถอดรหัสข้อความสำหรับรหัสคิวอาร์

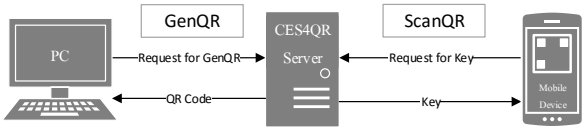
ในการออกแบบโมดูลการเข้ารหัสและถอดรหัสข้อความสำหรับรหัสคิวอาร์ จะคำนึงถึง ความปลอดภัยและความถูกต้องสมบูรณ์ของข้อมูลเป็นหลัก ซึ่งในที่นี้ ข้อมูลที่ถูกเข้ารหัสแล้วเมื่อถูกถอดรหัสก็จะได้ข้อมูลที่มีความสมบูรณ์ดังเดิม

3.1 ระบบ CES4QR

ระบบ CES4QR มีการทำงานหลัก 2 ส่วน คือ GenQR และ ScanQR ดังรูปที่ 2 และอธิบายการทำงานได้ดังนี้

1) GenQR คือขั้นตอนการสร้างรหัสคิวอาร์โดยการเข้ารหัสข้อความ (plaintext) ด้วยวิธีการแบบกุญแจสมมาตรด้วยอัลกอริทึม AES ด้วยกุญแจขนาด 128 บิต ก่อนจะทำการสร้างรหัสคิวอาร์

2) ScanQR คือขั้นตอนการอ่านรหัสคิวอาร์โดยการอ่านรหัสคิวอาร์แล้วทำการถอดรหัสเพื่อให้ได้ข้อความด้วยวิธีการแบบกุญแจสมมาตรด้วยอัลกอริทึม AES ด้วยกุญแจขนาด 128 บิต



รูปที่ 2 ระบบหลักของ CES4QR

สำหรับกระบวนการในการสร้างรหัสคิวอาร์ แสดงดังรูปที่ 3 และขั้นตอนการทำงานอธิบายได้ดังนี้

1) ผู้ใช้ส่งข้อความต้นฉบับไปยังเซิร์ฟเวอร์เพื่อสร้างรหัสคิวอาร์
2) เซิร์ฟเวอร์ทำการสร้างกุญแจ (AES Key) สำหรับการเข้ารหัส
3) เซิร์ฟเวอร์ทำการเก็บกุญแจไว้ในฐานข้อมูล

4) เซิร์ฟเวอร์ทำการเข้ารหัสข้อความด้วยอัลกอริทึม AES
5) เซิร์ฟเวอร์ทำการสร้างรหัสคิวอาร์ด้วยข้อความที่ถูกเข้ารหัส
6) เซิร์ฟเวอร์ส่งรหัสคิวอาร์ที่สร้างให้แก่ผู้ใช้

สำหรับกระบวนการในการอ่านรหัสคิวอาร์ แสดงดังรูปที่ 4 และขั้นตอนการทำงานอธิบายได้ดังนี้

1) ผู้ใช้ทำการติดตั้งโปรแกรม CES4QR Reader
2) ผู้ใช้ทำการสแกนรหัสคิวอาร์แล้วโดยใช้อุปกรณ์สื่อสารเคลื่อนที่และอุปกรณ์สื่อสารเคลื่อนที่จะทำการส่งข้อความของรหัสคิวอาร์(QR-Message)ไปยังเซิร์ฟเวอร์เพื่อร้องขอกุญแจ
3) เซิร์ฟเวอร์ทำการดึงกุญแจมาจากฐานข้อมูล
4) เซิร์ฟเวอร์เข้ารหัสกุญแจ(AES Key) ด้วยอัลกอริทึม RSA โดยใช้กุญแจส่วนตัว
5) เซิร์ฟเวอร์ส่งกุญแจที่ถูกเข้ารหัสไปยังอุปกรณ์สื่อสารเคลื่อนที่
6) อุปกรณ์สื่อสารเคลื่อนที่ทำการถอดรหัสกุญแจด้วยอัลกอริทึม RSA โดยใช้กุญแจสาธารณะของเซิร์ฟเวอร์
7) อุปกรณ์สื่อสารเคลื่อนที่นำกุญแจที่ได้มาทำการถอดรหัสข้อความของรหัสคิวอาร์ข้อความต้นฉบับด้วยอัลกอริทึม AES เพื่อให้ได้มาซึ่งข้อความต้นฉบับ

4. การพัฒนาระบบ

4.1 สภาพแวดล้อมการพัฒนาและทดสอบระบบ

ระบบ CES4QR พัฒนาขึ้นด้วยภาษาจาวา โดยรับส่งข้อมูลผ่าน socket การสร้างและอ่านรหัสคิวอาร์ใช้ไลบรารีของ com.google.zxing ส่วนการเข้ารหัสข้อมูลใช้ไลบรารีของ javax.cryptoโดยมีขั้นตอนวิธีในการสร้างและอ่านรหัสคิวอาร์ดังรูปที่ 5 และ 6 ตามลำดับ

4.2 ตัวอย่างการทำงานของระบบ CES4QR

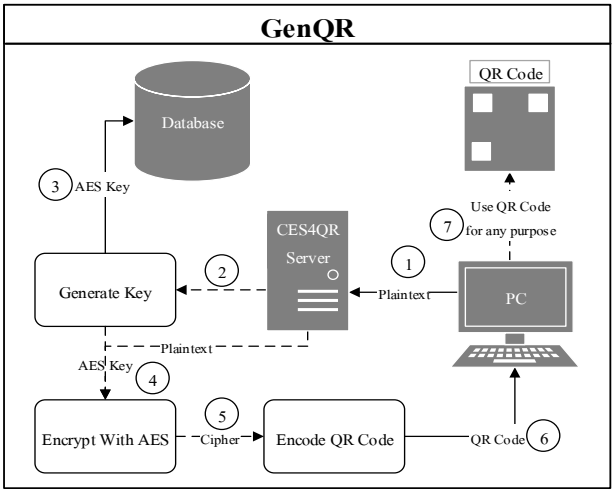
การใช้ระบบ CES4QR ได้ทำการทดสอบกับ ระบบจัดการสารสนเทศห้องปฏิบัติการหน่วยเครื่องมือกลาง คณะวิทยาศาสตร์ มหาวิทยาลัย-สงขลานครินทร์ โดยนำข้อมูลผลการวิเคราะห์ตัวอย่างทำการเข้ารหัสแล้วสร้างเป็นรหัสคิวอาร์เพื่อส่งให้ลูกค้าผู้ร้องขอการวิเคราะห์ผลโดยมีขั้นตอนการทำงานดังนี้

4.2.1 ขั้นตอนการสร้างรหัสคิวอาร์

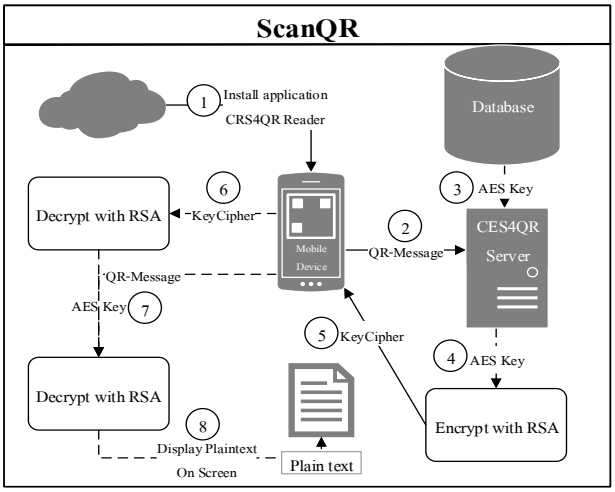
เมื่อเจ้าหน้าที่ทำการบันทึกผลการทดลองลงในฐานข้อมูลแล้ว ระบบจะนำข้อมูลผลการทดสอบมาทำการเข้ารหัสแล้วบันทึกไว้ในฐานข้อมูล โดยมีตัวอย่างข้อมูลดังตารางที่ 1 และใช้กุญแจ “ftz05:i.Nr;tpgds” ในการเข้ารหัสข้อความ ดังตารางที่ 1.ก

4.2.2 ขั้นตอนการส่งอีเมล์

หลังจากได้ทำการเข้ารหัสข้อความต้นฉบับแล้วระบบจะทำการนำข้อความไซเฟอร์มาทำการสร้างรหัสคิวอาร์ ผลลัพธ์ดังตารางที่ 1.ข แล้วส่งอีเมลล์ไปยังผู้ขอรับบริการวิเคราะห์ตัวอย่างรับทราบ



รูปที่ 3 ขั้นตอน GenQR



รูปที่ 4 ขั้นตอน ScanQR

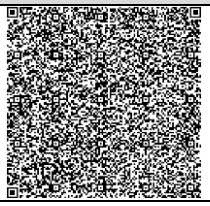
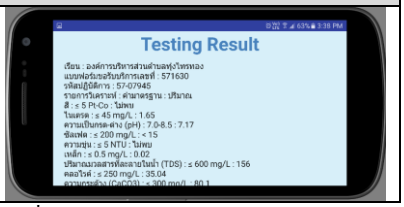
```
Algorithm createQR(plain_text, key_lenght)
1:  key = GenerateKey(key_lenght)
2:  cipher_text = EncryptAES(plain_text, key)
3:  StoreCipherAndKey(cipher_text, key)  //store to database
4:  qr_message = CreateQRMessage(cipher_text)
5:  qr_code = Encode(qr_message)
```

รูปที่ 5 ขั้นตอนวิธีการสร้างรหัสคิวอาร์

```
Algorithm scanQR (qr_code, user_id)
1:  CheckUserAndQR(user_id, qr_code)
2:  qr_message = Decode(qr_code)
3:  cipher_text = getCipher(qr_message)
4:  key = DecryptRSA(getKey(CES4QR_Server), public_key)
5:  plain_text = DecryptAES(cipher_text, key)
```

รูปที่ 6 ขั้นตอนวิธีการอ่านรหัสคิวอาร์

ก.ข้อความต้นฉบับ
เรียน : บริษัท กรีนรีเวอร์พาเนล (ประเทศไทย) จำกัด
แบบฟอร์มขอรับบริการเลขที่ : 530001
รหัสปฏิบัติการ : 53-0001
รายการวิเคราะห์ : ค่ามาตรฐาน : ปริมาณ
สี : ≤ 5 Pt-Co : 1
ซัลเฟต : ≤ 200 mg/L : 1
ความเป็นกรด-ด่าง (pH) : 7.0-8.5 : 1
เหล็ก : ≤ 0.5 mg/L : 1
ความขุ่น : ≤ 5 NTU : 1
คลอไรด์ : ≤ 250 mg/L : 1
ปริมาณมวลสารที่ละลายในน้ำ (TDS) : ≤ 600 mg/L : 1
สารพิษอื่นๆ เช่น สารหนู สารตะกั่ว : ต้องไม่มี : 1
ความกระด้าง (CaCO3) : ≤ 300 mg/L : 1
ไนเตรต : ≤ 45 mg/L : 1

ข.รหัสคิวอาร์ QR Code	ค.ผลลัพธ์การอ่านรหัสคิวอาร์ฝั่งผู้ใช้บริการ
	

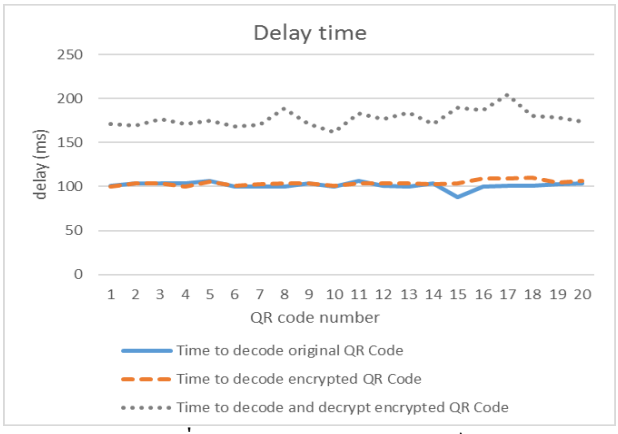
ตารางที่ 1 ตัวอย่างข้อมูล

4.2.3 ขั้นตอนการถอดรหัส

เมื่อผู้ใช้ทำการใช้อุปกรณ์สื่อสารเคลื่อนที่สแกนรหัสคิวอาร์ผ่านโปรแกรม CES4QR Reader (QR-LIMS version) โปรแกรมจะร้องขอกุญแจจากเซิร์ฟเวอร์เพื่อทำการถอดรหัสข้อความ ผลลัพธ์ดังตารางที่ 1.ค

5. ผลการศึกษาและบทสรุป

จากการศึกษาระบบการเข้ารหัสข้อความสำหรับรหัสคิวอาร์ โดยสุ่มตัวอย่างข้อมูล 20 ชุดทำการทดลองชุดละ 5 ครั้ง พบว่าการแปลรหัสคิวอาร์ จากรหัสคิวอาร์ซึ่งข้อมูลไม่ถูกเข้ารหัสและรหัสคิวอาร์ซึ่งข้อมูลได้ถูกเข้ารหัสนั้นไม่มีความแตกต่าง แต่การอ่านรหัสคิวอาร์ซึ่งข้อมูลถูกเข้ารหัสนั้นใช้เวลามากขึ้นประมาณ 75% เมื่อเทียบกับการอ่านรหัสคิวอาร์ซึ่งข้อมูลไม่ถูกเข้ารหัสโดยเวลาที่เพิ่มขึ้นคือเวลาที่ใช้ในการถอดรหัสข้อความ ดังแสดงในรูปที่ 7 อย่างไรก็ตาม เนื่องจากข้อมูลที่ใช้ในการทดสอบเป็นข้อมูลเฉพาะสำหรับผู้ขอรับบริการวิเคราะห์ตัวอย่างเท่านั้น ไม่สามารถเผยแพร่ให้ผู้ไม่มีส่วนเกี่ยวข้อง เมื่อต้องแลกกับการที่ข้อมูลไม่ถูกดัดแปลงเห็นได้ว่าความปลอดภัยของข้อมูลสำคัญกว่าดังนั้นการที่ใช้เวลาอ่านรหัสคิวอาร์เพิ่มขึ้น 75% หรือประมาณ 75 มิลลิวินาทีเพื่อแลกกับความปลอดภัยของข้อมูลถือได้ว่าเหมาะสม โดยการประยุกต์ใช้กับระบบ QR-LIMS สามารถป้องกันการถูกปลอมแปลงรหัสคิวอาร์ได้ดี



รูปที่ 7 ระยะเวลาการแปลรหัสคิวอาร์

เอกสารอ้างอิง

[1] A. Sankara Narayanan: “QR Code and Security Solution”; International Journal of Computer Science and Telecommunications Volume 3, Issue 7, pp.69-72, July 2012.

[2] K. Krombholz, P. Frühwirt, P. Kieseberg, I. Kapsalis, M. Huber: "QR Code Security: A Survey of Attacks and Challen ges for Usable Security"; Lecture Notes in Computer Science, pp. 79-90, 2014.

[3] Raed M. Bani-Hani, Yarub A. Wahsheh, Mohammad B. Al-Sarhan: “Secure QR Code System”; 10th International Conference on Innovations in Information Technology (IIT'14), At Al-Ain, UAE, November 2014.

[4] Abhijit Sen, Yourdon Jou: "Secure Data Transmission Technique for iPhone using Quick Response Code”; MI-BEST-2015. Vol. 1, pp. 53-62, 2015.

[5] ชีวิน ชนะวรรโณ, เนาวัล ศิริพัธนะ, ผุสดี มุหะหมัด และลัดดา ปรีชาวีรกุล: “การประยุกต์ใช้ QR code กับระบบการจัดการสารสนเทศห้องปฏิบัติการวิทยาศาสตร์”; ECTI-CARD Proceedings เชียงใหม่ ประเทศไทย ,2014.

[6] ADVANCED ENCRYPTION STANDARD (AES); Federal Information Processing Standards Publication 197, November 2001.

[7] R.L. Rivest, A. Shamir, and L. Adleman: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems; MIT Laboratory for Computer Science Communications of the ACM, February 1978.

นาย ณภัทร ยิ้มจันทร์

นักศึกษา ปริญญาตรี ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยสงขลานครินทร์

งานวิจัยที่สนใจเกี่ยวกับ Information Security