# โปรแกรม เข้ารหัสข้อมูลแบบข้ามแพลตฟอร์มเพื่อป้องกันข้อมูลในอุปกรณ์พกพา BuzzCrypt

นาย ยุทธพงษ์ พิมพระลับ และ สุรศักดิ์ ศรีสวรรค์

สาขาวิชาเทคโนโลยีสารสนเทศ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิยาลัยราชภัฏราชนครินทร์ ฉะเชิงเทรา
Email: Beerbuzzsniper5964@gmail.com, surasak.sri@csit.rru.ac.th

**บทคัดย่อ**

โครงงานนี้มีวัตถุประสงค์เพื่อ พัฒนาโปรแกรมที่สามารถช่วยปกป้องข้อมูลภายในคอมพิวเตอร์ให้ปลอดภัยจากถูกอ่านจากผู้ไม่ ประสงค์ดีหรือโจรกรรมข้อมูลภายในคอมพิวเตอร์ โดยใช้ทฤษฎีการ เข้ารหัสมาช่วยในป้องกันข้อมูลและปกป้องความความเป็นส่วนตัว การออกแบบและพัฒนาระบบด้วย โปรแกรม Netbeans และใช้ภาษาคอมพิวเตอร์อย่างจาวามาพัฒนาระบบทำให้โปรแกรมสามารถทำงานข้ามแพลตฟอร์มได้ นอกจากนี้ยังมีการทำอิมเมจดิสก์ในรูปแบบมาตรฐาน ISO 9660 เพื่อนำไฟล์ที่เข้ารหัสมาเก็บไว้เก็บไว้ในที่เดียวกัน จึงสามารถทำให้เคลื่อนย้ายได้สะดวกและจัดเก็บใส่อุปกรณ์พกพาได้อีกด้วย ถึงแม้ว่าไฟล์อิมเมจส์ดิสก์จะอยู่ในรูปแบบมาตรฐานแต่ถ้าเปิดด้วยโปรแกรมอื่นหรือไม่มีรหัสผ่านเปิดก็จะไม่สามารถอ่านไฟล์ดังกล่าวได้จึงสามารถทำให้ข้อมูลที่ถูกเข้ารหัสปลอดภัย

**Abstract**

This project aims to develop a computer program that can help protect data from being read by unauthorized parties. By using cryptography theory, the program can help protect data and user's privacy. The program was designed and developed using NetBeans and Java programming language in order to develop a cross-platform application. The image format used in this program is conformed to ISO 9660 standard. Although the image file is in a general format, the content of the file is shown as encrypted and unreadable if the file is opened using another program or without the correct password.

***คำสำคัญ*** –Image disk, Encryption, Privacy, Portability

## 1. บทนำ

ปัจจุบันเทคโนโลยีเข้ามามีบทบาทในชีวิตประจำวันมากขึ้น โดยเฉพาะเครือข่าย อินเทอร์เน็ต ที่ทำให้ทุกคนสามารถเชื่อมต่อหาซึ่งกันและกันได้ และยังเป็นแหล่งรวมสารสนเทศจากทุกมุมโลก ทุกสาขาวิชา ทุกด้าน ทั้งด้านบันเทิงและวิชาการตลอดจนการประกอบธุรกิจ อีกทั้งอุปกรณ์มากมายในปัจจุบันยังรองรับอินเทอร์เน็ต ทำสามารถเข้าถึงได้โดยทุกเพศทุกวัยอีกด้วย

เมื่ออินเทอร์เน็ตเป็นตัวกลางสามารถทำให้ทุกคนเชื่อมต่อหากันแล้ว ทำให้เสี่ยงต่อความปลอดภัยหรือความเป็นส่วนตัวมากยิ่งขึ้น โดยจะมีกลุ่มที่ประสงค์ร้ายและเป็นผู้ที่มีความรู้ด้านคอมพิวเตอร์ จะใช้ตัวกลางอย่างอินเทอร์เน็ตเป็นช่องทางไปในทางมุ่งร้าย เช่นการโจรกรรม เอกสาร รูปภาพ หรือข้อมูลสำคัญต่างๆ โดยเฉพาะอย่างยิ่งข้อมูลในสื่อพกพาซึ่งอาจตกไปอยู่ในมือผู้ประสงค์ร้ายได้ง่าย

ดังนั้นเพื่อให้เพิ่มความปลอดภัยให้ข้อมูล ผู้จัดทำโครงงานจึงได้พัฒนาโปรแกรมการเข้ารหัสข้อมูลที่สามารถจัดเก็บข้อมูลที่ได้รับการป้องกันในรูปแบบ อิมเมจดิสก์มาตรฐานอย่าง ISO 9660 เพื่อให้สะดวกในการจัดเก็บข้อมูลจำนวนมากไว้ในที่เดียวและสะดวกต่อการเคลื่อนย้ายอีกด้วย

## 2. ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

**2.1 AES [1] (Advanced Encryption Standard)** เป็นมาตรฐานในเข้ารหัสแบบซิมเมตริกคีย์แบบบล็อกไซเฟอร์ โดยอัลกอริทึมที่ใช้คือ Rijndeal ซึ่งเป็นบล็อกไซเฟอร์ที่ออกแบบโดยนักออกแบบการเข้ารหัสที่มีชื่อว่า โจแอน เดเมน (Joan Daeman) และวินเซนต์ ริจเมน (Vincent Rijman) อัลกอริทึมนี้สามารถใช้ความยาวของบล็อกและคีย์ที่สามารถเปลี่ยนแปลงได้โดยมีขนาด128,192 หรือ 256 บิตได้เช่นกัน

**2.2 Image File [2]** คือ การเขียนข้อมูลจากสื่อ เช่น CD, VCD, DVD ให้รวมกันเป็นไฟล์หนึ่งเดียวเสมือนภาพของสื่อนั้นทั้งแผ่น โดย ปัจจุบันมาตรฐานของสื่อชนิดนี้คือ ISO9660

**2.3 Cross – Platform [3]** คือ การที่โปรแกรม คอมพิวเตอร์ ภาษาโปรแกรม ระบบปฏิบัติการ หรือ ซอฟต์แวร์ชนิดอื่นๆ สามารถทำงานได้ใน หลายแพลตฟอร์มคอมพิวเตอร์ตัวอยางเช่น โปรแกรมคอมพิวเตอร์สามารถทำงานได้บน ไมโครซอฟท์วินโดวส์สำหรับสถาปัตยกรรม x86 และ Mac OS X บน PowerPC แพลตฟอร์ม

**2.4 Java language [4]** ถูกพัฒนาขึ้นโดยบริษัท Sun Microsystem โดยพัฒนาให้เป็นภาษาที่ใช้ในการเขียนโปรแกรมเชิงวัตถุ (Object Oriented Programming) และให้สามารถทำงานบนเครื่องคอมพิวเตอร์ที่มีสภาพแวดล้อมต่างกันได้โดยไม่ต้องคอมไพล์ใหม่ ซึ่งเรียกคุณสมบัติเช่นนี้ว่า platform independent

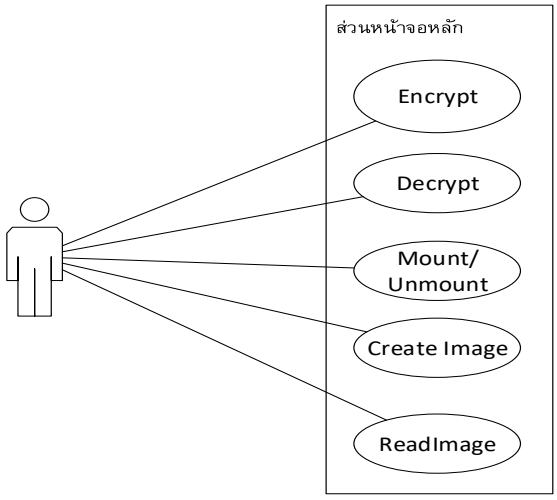
## 3. วิธีดำเนินการ

### 3.1 ศึกษาความเป็นไปได้ของระบบ

จากการศึกษาควาเป็นไปได้ของงโปรแกรมพบว่ามี ความเป็นไปได้ทางเทคนิคเพราะสามารถใช้เทคโนโลยีคอมพิวเตอร์เข้ามาช่วย โดยซอพต์แวร์ในการพัฒนาโปรแกรมและออกหน้าจอ คือ Netbeans

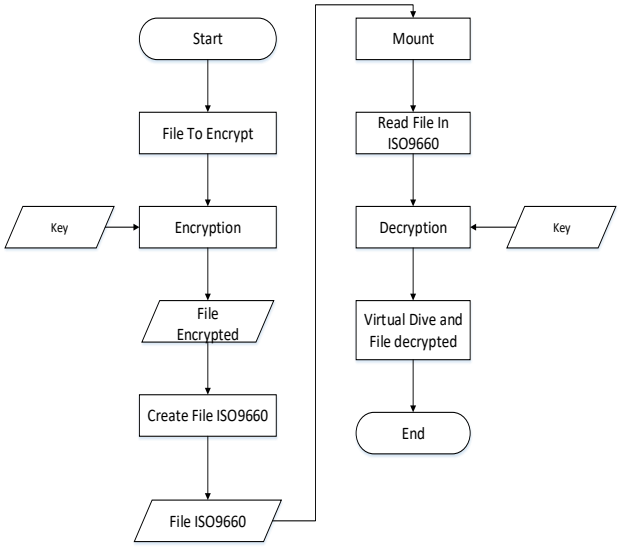
### 3.2 การออกแบบระบบ

ในการวิเคราะห์โครงสร้างและส่วนประกอบระบบงานนั้นได้ ผู้พัฒนาได้ใช้การวิเคราห์ระบบในรูปแบบ UML โดยใช้ ยูสเคสไดอะแกรม และ โฟลวชาร์ต ดังรูปที่ 1 และ รูปที่ 2




รูปที่ 1 แผนภาพการทำงานของยูสเคสระบบ

จากรูปที่ 1 แสดงสิ่งที่ผู้ใช้สามารถกระทำได้บนโปรแกรม ได้แก่ เข้ารหัสไฟล์ (Encrypt) ถอดรหัสไฟล์ (Decrypt) เม้าอิมเมจดิสก์และถอดอิมเมจดิสก์ (Mount / Unmount) สร้างอิมเมจดิสก์ (Create ISO) และ การอ่านอิมเมจดิสก์ (Read Image Disk)



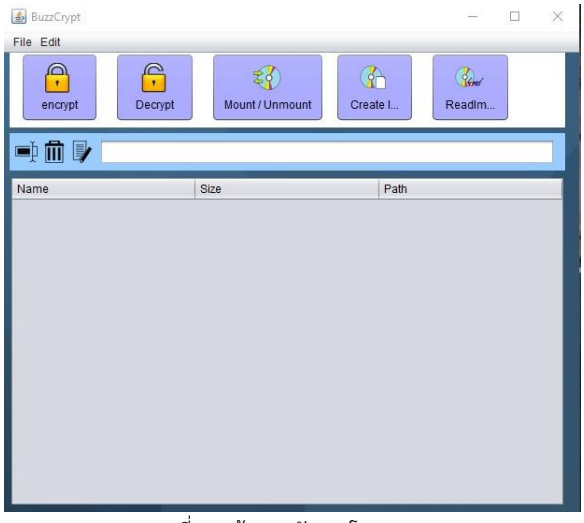

รูปที่ 2 แผนภาพการทำงานของระบบ ตั้งแต่เริ่มทำการเริ่มต้นการเข้ารหัส จนถึงกระบวนการถอดรหัสและทำการเม้าท์ไฟล์

อธิบายการกระบวนการทำงานเพิ่มเติมจาก รูปที่ 2 ในส่วนของขั้นตอนเข้ารหัส (Encryption) การเข้ารหัสจะใช้อัลกอริทึมของ AES โดยขั้นตอน มี ทั้งหมด 4 ขั้นตอน คือ 1. Subbytes 2.ShiftRows 3. MixColumn 4. AddRoundKey ในส่วนการใช้

คีย์ จะใช้คีย์ในรูปแบบกำหนดเอง ไม่ได้เป็นการใช้คีย์แบบสุ่ม โดยคีย์ที่นำมาเข้ารหัสจะอยู่ในรูปแบบ Plaintext และจะถูกเก็บแบบ Byte เพราะว่าใช้การเก็บข้อมูลแบบล็อกไซเฟอร์จึงต้องแปลง Plaintext เป็น Byte เสียก่อนจึงจะสามารถมาเข้ากระบวนการการเข้ารหัสได้ และทำการเก็บคีย์ที่กำหนดลงในหน่วยความจำ เมื่อมีการถอดรหัสจึงมีการเรียกใช้คีย์ที่เก็บไว้ภายในหน่วยความจำ

## 4. ผลการพัฒนาระบบ

ผู้จัดทำได้ศึกษาและได้ทำการวิเคราะห์และออกแบบระบบแล้ว จึงได้จัดทำโปรแกรมดังนี้



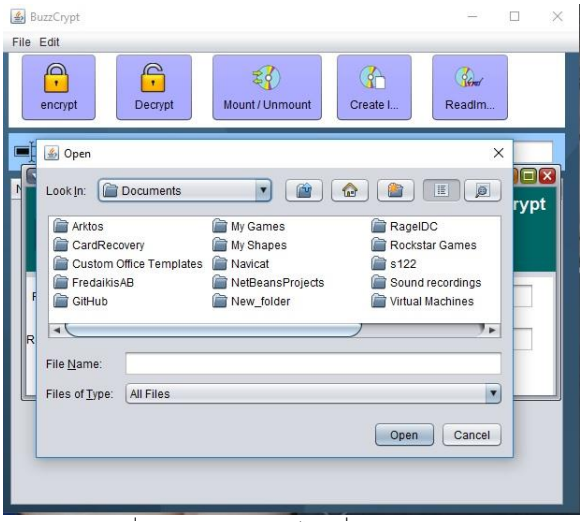

รูปที่ 3 หน้าจอหลักของโปรแกรม

จากรูปที่ 3 เป็นหน้าจอหลักของโปรแกรม โดยแต่ละปุ่มจะนำไปสู่หน้าจอถัดไปดังนี้

### 4.1 การเข้ารหัสไฟล์ ( encrypt )

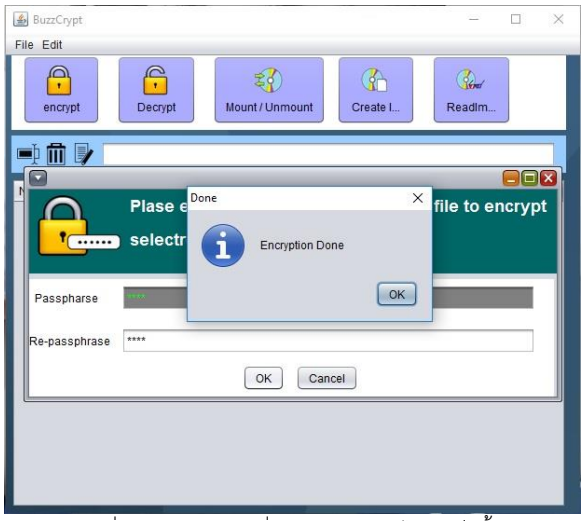

รูปที่ 4 หน้าจอของการเข้ารหัสไฟล์

จากรูปที่ 4 เมื่อได้เลือกหัวข้อการเข้ารหัสไฟล์ (Encrypt) จะนำไปสู่ช่องให้ใส่รหัสป้องกัน โดยมีจำนวนสองช่องด้วยกัน ให้ทำการใส่รหัสป้องกัน ถ้าในกรณีที่รหัสป้องกันไม่ตรงกันโปรแกรมจะไม่สามารถดำเนินการได้ต่อและต้องกรอกรหัสผ่านใหม่อีกครั้ง ถ้าใส่ข้อมูลตรงกันแล้วให้กดปุ่ม ok




รูปที่ 5 หน้าจอการเลือกไฟล์ที่จะนำมาเข้ารหัส

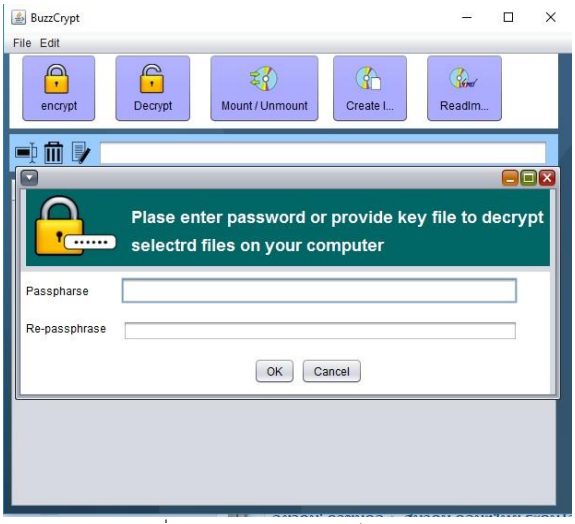
จากรูปที่ 5 ระบบจะนำไปสู่การเลือกไฟล์ที่จะนำมาเข้ารหัส โดยผู้ใช้จะต้องทำการเลือกไฟล์ที่จะนำมาเข้าสู่กระบวนการเข้ารหัส จากนั้นให้กดปุ่มที่มีคำว่า Open ระบบจะทำการเข้ารหัสไฟล์ที่เลือกไว้ข้างต้น




รูปที่ 6 หน้าจอแสดงเมื่อทำการเข้ารหัสไฟล์เสร็จสิ้น

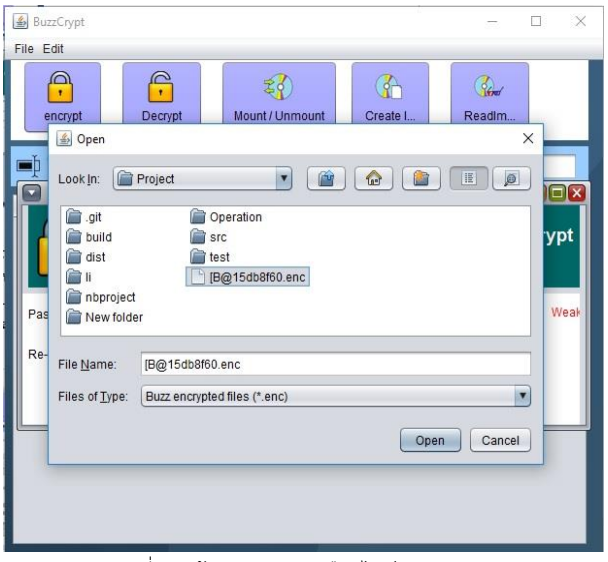
### 4.2 การถอดรหัสไฟล์ ( decrypt )

ในกรณีนี้เมื่อผู้ใช้งานจะประสงค์ทำการถอดรหัสไฟล์ใดไฟล์หนึ่งจากไฟล์ที่เข้ารหัส สามารถเลือกทำหัวข้อนี้ได้



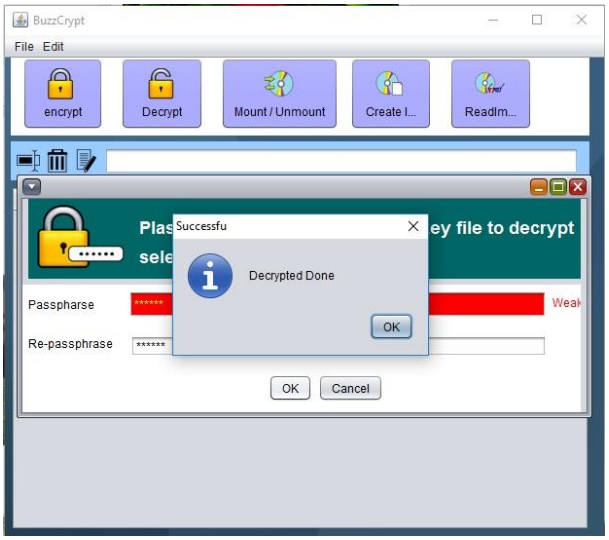

รูปที่ 7 หน้าจอการถอดรหัสไฟล์

จากรูปที่ 7 เมื่อผู้ใช้เลือกหัวข้อการถอดรหัสไฟล์ ( decrypt ) จะนำไปสู่กล่องให้ใส่รหัสผ่านสำหรับถอดรหัสข้อมูล โดยถ้าในกรณีที่ใส่ข้อมูลไม่ตรงกัน จะไม่สามารถถอดรหัสได้



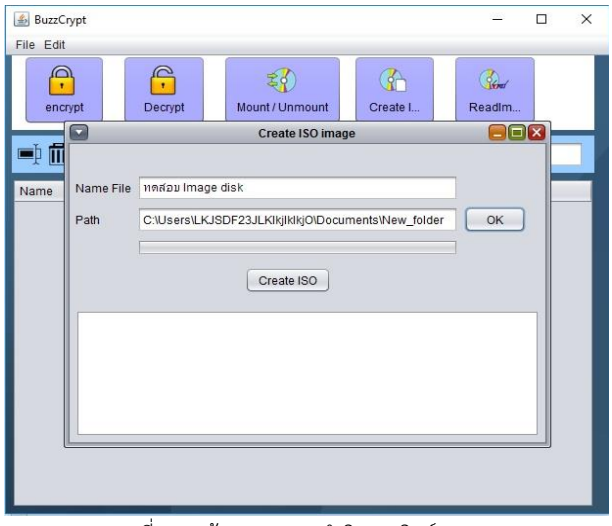

รูปที่ 8 หน้าจอแสดงการเลือกไฟล์มาถอดรหัส

จากรูปที่ 8 เมื่อกรอกข้อมูลถูกต้องระบบจะนำไปสู่การเลือกไฟล์ที่จะนำมาถอดรหัส โดยไฟล์ที่ถูกเข้ารหัสจะมีนามสกุลไฟล์ลงท้ายด้วย .enc และชื่อไฟล์จะมีเป็นชื่อที่ไม่สามารถอ่านเข้าใจได้ เมื่อเลือกเสร็จแล้วให้กดคำว่า Open ระบบจะทำการถอดรหัสไฟล์ดังกล่าว



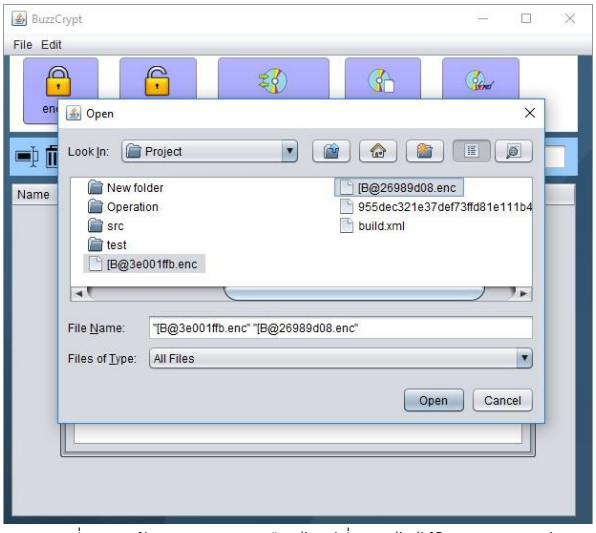

รูปที่ 9 หน้าจอแสดงเมื่อโปรแกรมทำการถอดรหัสไฟล์เสร็จสิ้น

### 4.3 การทำอิมเมจดิสก์ (Create Image)



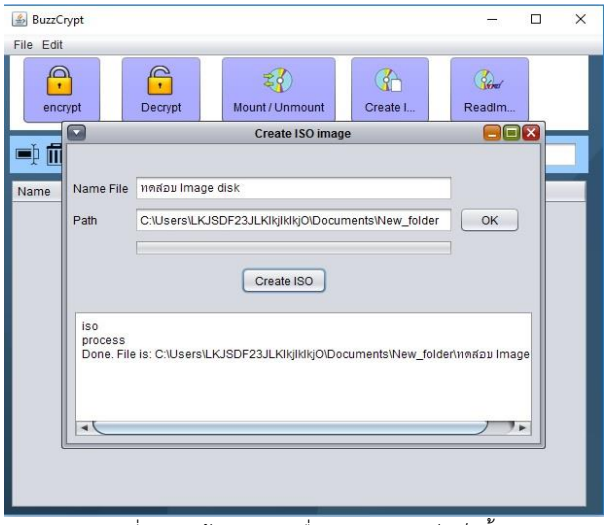

รูปที่ 10 หน้าจอของการทำอิมเมจดิสก์

จากรูปที่ 10 เมื่อผู้ใช้เลือกหัวข้อ สร้างอิมเมจดิสก์ (Create Image) จะนำไปสู่กล่องที่ต้องกรอกข้อมูล ให้ใส่ชื่อที่ต้องการตั้ง และ เส้นทางที่จะนำไฟล์เก็บไว้ ( Path ) เมื่อกำหนดเสร็จแล้วให้กดปุ่มด้านล่างที่เขียนว่า Create ISO



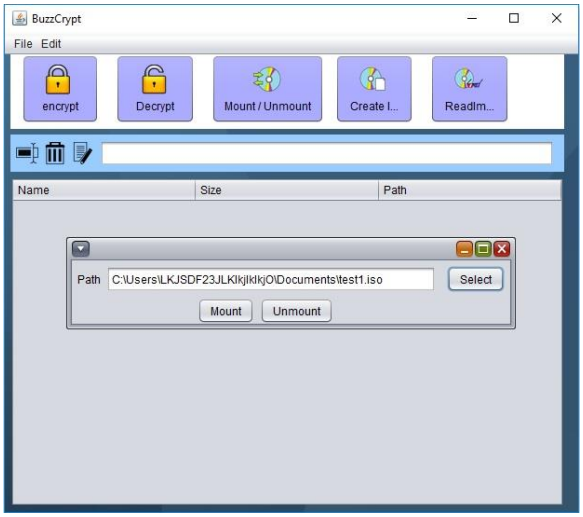

รูปที่ 11 หน้าจอแสดงการเลือกไฟล์ที่จะนำไปไว้ในอิมเมจดิสก์

จากรูปที่ 11 ให้เลือกไฟล์เข้ารหัสไปเก็บในอิมเมจดิก์



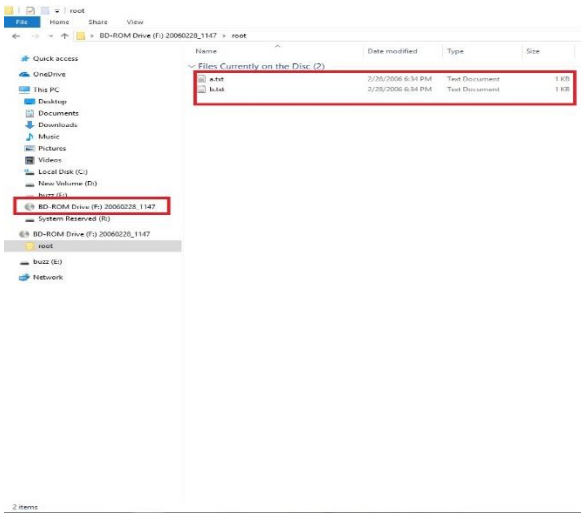

รูปที่ 12 หน้าจอแสดงเมื่อทำอิมเมจดิสก์เสร็จสิ้น

### 4.4 การใส่และถอดอิมเมจดิสก์ (Mount / Unmount)



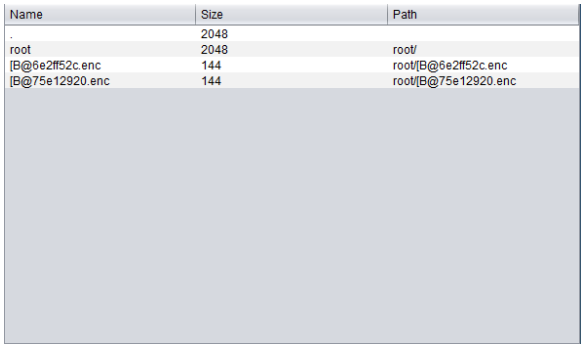

รูปที่ 13 แสดงหน้าจอการเม้าส์และอันเม้าไฟล์

จากรูปที่ 13 เมื่อผู้ใช้งานที่จะทำการใส่ไฟล์อิมเมจดิสก์ที่สร้างมาก่อนหน้านี้ ให้ทำการเลือกที่อยู่ของอิมเมจไฟล์ เมื่อเลือกเสร็จแล้ว ให้กดปุ่ม Mount เพื่อใส่อิมเมจดิสก์



รูปที่ 14 ผลลัพธ์จากการเม้าท์อิมเมจดิส์

จากรูปที่ 14 เมื่อใส่อิมเมจดิสก์ตามขั้นตอนก่อนหน้านี้จะได้ไดร์ฟที่เกิดจากการใส่อิมเมจและไฟล์ที่ถูกถอดรหัส

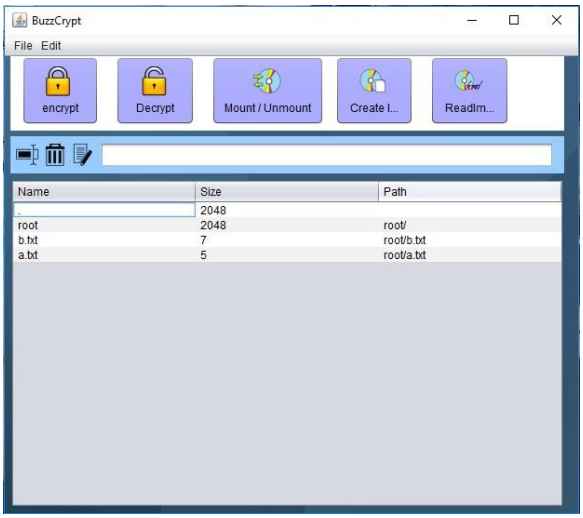


| Name | Size | Path |
|---|---|---|
| . | 2048 | |
| root | 2048 | root/ |
| [B@6e2ff52c.enc | 144 | root/[B@6e2ff52c.enc |
| [B@75e12920.enc | 144 | root/[B@75e12920.enc |

รูปที่ 15 ผลลัพธ์จากการถอดอิมเมจดิสก์

จากรูปที่ 15 เมื่อผู้ใช้งานได้ทำถอดอิมเมจดิสก์ (Unmount) แล้ว ไฟล์ที่อยู่ในอิมเมจดิสก์จะถูกเข้ารหัสและเก็บไว้ในอิมเมจดิสก์คงเดิม

### 4.5 การอ่านไฟล์อิมเมจ (Read Image)




รูปที่ 16 หน้าจอแสดงเมื่อทำการอ่านไฟล์อิมเมจดิสก์

จากรูปที่ 16 เมื่อนำอิมเมจดิสก์ที่มีไฟล์เข้ารหัสอยู่มาเปิดกับโปรแกรมก็จะเห็นชื่อไฟล์ที่ไม่เข้ารหัสทำให้รู้ว่าในอิมเมจไฟล์มีไฟล์อะไรอยู่ด้านในบ้าง

### 4.6 การติดตั้งและทดสอบระบบ

ผู้พัฒนาระบบใช้วิธีการทำการทดสอบระบบเข้ารหัสข้อมูล โดยใช้ผู้ที่เชี่ยวชาญทางด้านคอมพิวเตอร์ จำนวน 5 คน และผู้ใช้งานจริงจำนวน 5 คน ทำการทดสอบการทำงานของโปรแกรมส่ามีกระบวนการถูกต้องตามวัตถุประสงค์ที่ต้องการหรือไม่ ซึ่งผู้พัฒนาได้ออกแบบสอบถามเพื่อประเมินความพึงพอใจใน 4 ด้าน ประกอบด้วย 1.ด้านการทำงานตามฟังก์ชันของระบบ 2. ด้านประสิทธิภาพ 3. ความง่ายต่อการใช้งานระบบ 4.ด้านความปลอดภัยของข้อมูลในระบบ และกำหนดเกณฑ์ในการประเมินได้ดัง ตารางที่ 2

ตารางที่ 2 เกณฑ์การให้คะแนน

| ระดับคะแนน | ระดับความพึงพอใจ |
|---|---|
| 0.0 – 1.49 | ปรับปรุง |
| 1.50 – 2.49 | พอใช้ |
| 2.50 – 3.49 | ปานกลาง |
| 3.50 – 4.49 | ดี |
| 4.50 – 5.0 | ดีมาก |

## 5. ผลการประเมินระบบ

ได้ทำการทดสอบ การใช้งาน และความปลอดภัยของข้อมูลที่ได้รับการเข้ารหัส โดยผู้เชี่ยวชาญจำนวน 5 คนและผู้ใช้งานจริง จำนวน 5 คน แสดงดัง ตารางที่ 2

ตารางที่ 3 สรุปผลการประเมิน

| รายการประเมิน | ค่าเฉลี่ย | S.D. |
|---|---|---|
| การทำงานได้ตามฟังก์ชัน (Functionality) | 4.20 | 0.6 |
| ประสิทธิภาพ (Performance) | 4.10 | 0.53 |
| ง่ายต่อการใช้งาน (Usability) | 4.00 | 0.63 |
| การรักษาความปลอดภัย (Security) | 4.8 | 0.40 |
| ความพึงพอใจโดยรวมเฉลี่ย | 4.27 | 0.54 |

สรุปการประเมินความพึงพอใจทั้ง 4 ด้าน คือ 1. การทำงานได้ตามฟังก์ชั่นอยู่ในระดับดี 2. มีประสิทธิภาพอยู่ในระดับดี 3. ง่ายต่อการใช้งานอยู่ในระดับดี 4. การรักษาคามปลอดภัยอยู่ในระดับดี โดยรวมเฉลี่ย 4 ด้านได้คะแนนเฉลี่ยเท่ากับ 4.27 และค่าเบี่ยงเบนมาตรฐานเท่ากับ 0.54 พบว่าระบบมีความพึงพอใจอยู่ในระดับดี

## 6.สรุปผล

### 6.1 สรุปผล

โครงานนี้มีวัตถุประสงค์เพื่อพัฒนาโปรแกรมสำหรับเข้ารหัสข้อมูลสำหรับผู้ที่ประสงค์จะปกป้องข้อมูลให้ปลอดภัยจากภัยคุกคามที่นำมาสู่การโจรกรรมข้อมูลภายในเครื่องคอมพิวเตอร์ และเป็นการนำเทคโนโลยีการข้ามแพลต์ฟอร์มมาใช้ ซึ่งมาจากใช้ภาษาคอมพิวเตอร์อย่าง Java มาพัฒนาโปรแกรม ทำให้มีความสะดวกมากยิ่งขึ้นในการใช้งานโปรแกรมบนคอมพิวเตอร์ที่ระบบปฏิบัติการต่างกัน และง่ายต่อการเคลื่อนย้ายข้อมูล ซึ่งการใช้งานใช้งานพบว่าความพึงพอใจอยู่ในระดับดีจากการสำรวจจากผู้ใช้ จำนวน 10 คน

### 6.2 ข้อเสนอแนะ

หน้าจอการแสดงการทำงานยังไม่ได้มีการออกแบบให้สวยงาม และโปรแกรมยังไม่เสร็จสมบูรณ์ครบถ้วนเนื่องจากบางฟังก์ชั่นยังมีปัญหา จึงทำให้ผู้เชี่ยวชาญทางด้านคอมพิวเตอร์และผู้ใช้ทั่วไปค่อนข้างใช้งานไม่สะดวก และอีกหนึ่งปัญหาคือในส่วนของฮาร์ดแวร์คอมพิวเตอร์บางเครื่องที่มีอายุมากกว่า 10 ปี หรือเทคโนโลยีในหน่วยประมวลผลต่ำ จะไม่สามารถทำงานได้เต็มประสิทธิภาพนัก เพราะ ตัวประมวลผลต้องคำนวณหลักคณิตศาสตร์ในปริมาณมาก ทำให้เทคโนโลยีหน่วยประมวลผลรุ่นเก่า ทำงานได้ช้า หรือ ทำงานไม่ได้เลย ซึ่งในอนาคตจะพัฒนาโปรแกรมให้ง่ายต่อการใช้งานและเพิ่มเติมฟังก์ชั่นการใช้งานให้ครบถ้วนรวมไปถึงให้มีการรองรับสำหรับคอมพิวเตอร์ที่มีอายุการใช้งานนานหรือ หน่วยประมวลผลรุ่นเก่า อีกด้วย

## 7.อ้างอิง

[1] จตุชัย แพงจันทร์. Master of security 3rd Edition. พิมพ์ครั้งที่ 1. นนทบุรี : สำนักพิมพ์ไอดีซี, 2558

[2] ISO Image file. [Online]. สืบค้นเมื่อ 15 กุมภาพันธ์ 2560. จาก : http://group.wunjun.com/tcc/topic/311771-9006.

[3] Cross Platform. [Online]. สืบค้นเมื่อ 17 กุมภาพันธ์ 2560 จาก : https://sites.google.com/site/tinnamin5712612007/kham-phaeltfxrm-cross-platform.

[4] ธีรวัฒน์ ประกอบผล. เขียนโปรแกรมเชิงวัตถุภาษา Java. พิมพ์ครั้งที่ 2. กรุงเทพฯ :สำนักพิมร์รีไวว่า, 2558.