

บทที่ 5

สรุปปัญหาและข้อเสนอแนะ

5.1 สรุปขั้นตอนการวิจัย

การสร้างกุญแจอิเล็กทรอนิกส์เริ่มจากการศึกษาการทำงานของพอร์ต USB การเขียนโปรแกรมติดต่อกับพอร์ต USB การเข้ารหัสลับแบบ RSA และการลดทอนสมการการเข้ารหัสด้วยทฤษฎีการลดทอนของ Montgomery ซึ่งแนวคิดของการจำกัดสิทธิ์การใช้งานโปรแกรมประยุกต์ ที่ต้องการความปลอดภัยจึงสร้างกุญแจอิเล็กทรอนิกส์ขึ้นมาทำให้เพิ่มระดับความปลอดภัยกับให้กับโปรแกรมประยุกต์เหล่านั้นมากขึ้น

5.2 ปัญหาและข้อเสนอแนะ

ปัญหา

1. หลังจากการสร้างกุญแจอิเล็กทรอนิกส์แล้วลักษณะรูปร่างภายนอกและขนาดของ กุญแจอิเล็กทรอนิกส์ โดยรวมยังใหญ่กว่าที่คาดไว้ เนื่องจากอุปกรณ์ภายในและต้องใช้ชิพที่ทำหน้าที่เป็น latch หลายตัวทำให้เมื่อประกอบวงจรแล้วกุญแจอิเล็กทรอนิกส์ จึงมีขนาดใหญ่กว่าที่คาดไว้เล็กน้อย
2. ไมโครคอนโทรลเลอร์ที่สามารถต่อประสานกับพอร์ต USB ได้ค่อนข้างมีจำหน่ายน้อย และหาได้ยากเนื่องจากเป็นเทคโนโลยีใหม่ที่เพิ่งจะมีไมโครคอนโทรลเลอร์ ประเภทนี้จำหน่ายในเมืองไทย
3. เมื่อเลือกไมโครคอนโทรลเลอร์ เพื่อใช้กับงานนี้ได้แล้วพบว่ายังมีข้อจำกัดเรื่องการเขียนโปรแกรมติดต่อกับไมโครคอนโทรลเลอร์ เนื่องจากผู้วิจัยต้องใช้เครื่องมือที่บริษัทผู้ผลิตชิพให้มาพร้อมกับผลิตภัณฑ์ ทำให้ในการพัฒนาต้องใช้เครื่องมือนี้เท่านั้นไม่สามารถใช้เครื่องมืออื่นได้ เป็นผลให้ผู้วิจัยไม่สามารถประยุกต์ใช้กับงานได้ตามคล่องตัวตามต้องการ

ข้อเสนอแนะ

1. ควรใช้ไมโครคอนโทรลเลอร์ที่สามารถเขียนโปรแกรมติดต่อกับพอร์ต USB ได้และสามารถสร้างสแตนด์ลิงค์ไลบรารี (Static Link Library :SLL) ใช้ภายในโปรแกรมได้เช่นโปรแกรมภาษา C เนื่องจากเมื่อนำไปใช้งานจริงโปรแกรมอื่นจะไม่สามารถเรียกใช้งานสแตนด์ลิงค์ไลบรารีซึ่งอยู่ภายในโปรแกรมได้ จึงส่งผลให้ระบบจะเข้มแข็งสร้างความยุ่งยากให้กับผู้บุกรุกมากยิ่งขึ้น

2. ระบบสามารถเข้ารหัสลับข้อมูลได้เพียง 8 บิต เนื่องจากเป็นข้อจำกัดของไมโครคอนโทรลเลอร์ที่สามารถคำนวณตัวเลขสูงสุดได้เพียง 4,724,434,591 แม้ว่าจะใช้ทฤษฎีการลดทอนแบบ Montgomery ช่วยในการลดทอนค่าตัวเลขแล้วก็ตาม เนื่องจากทฤษฎีการลดทอนนี้ประสิทธิภาพจะสูงเมื่อข้อมูลดิบหรือ M มีค่ามาก ๆ นั้นหมายความว่าข้อมูลต้องมีขนาดมาก ๆ เช่น 16 บิต หรือ 32 บิต

5.3 แนวโน้มในการพัฒนาต่อไปในอนาคต

1. กุญแจอิเล็กทรอนิกส์ ที่ผู้วิจัยสร้างขึ้นนี้นำไปประยุกต์ใช้กับโปรแกรมที่พัฒนาขึ้นด้วย Visual Basic 6.0 เท่านั้น ไม่สามารถนำไปใช้กับโปรแกรมอื่นหรือระบบปฏิบัติการอื่นได้ซึ่งในอนาคตอาจพัฒนาให้สามารถใช้งานได้ทั้งระบบปฏิบัติการวินโดวส์และระบบปฏิบัติการยูนิกซ์ ทั้งนี้ขึ้นอยู่กับผู้ผลิตชิพที่จะเปิดเผยข้อมูลในการเขียนโปรแกรมติดต่อกับพอร์ต USB เป็นสำคัญ
2. อาจพัฒนาให้สามารถตรวจสอบผู้ใช้งานผ่านทางเครือข่ายคอมพิวเตอร์ หรือจัดทำระบบกุญแจอิเล็กทรอนิกส์ ให้สามารถยืนยันการใช้โปรแกรมประยุกต์ที่ต้องการจำกัดสิทธิ์ผ่านทางเว็บเบราว์เซอร์