บทที่ 7

สรุปการวิจัยและข้อเสนอแนะ

<u>สรุปผลการวิจัย</u>

ในการทำวิทยานิพนธ์นี้ เพื่อต้องการที่จะให้มีการศึกษา ออกแบบ และสร้างระบบรักษาความปลอดภัยของข้อมูลด้วยวิธีการเข้ารหัสโดยใช้อุปกรณ์ฮาร์ดแวร์ที่สร้างขึ้นมาในรูปของคาร์ด เพื่อติดตั้งเข้ากับคอมพิวเตอร์ส่วนบุคคล โดยคาร์ดดังกล่าวสามารถเข้ารหัสข้อมูลตามมาตรฐานของ DES ได้ 4 โหมด คือ

1. Electronic Code Book ซึ่งเป็นบล็อคไซเฟอร์
2. Cipher Block Chaining เป็นบล็อคไซเฟอร์
3. Cipher FeedBack เป็นสตรีมไซเฟอร์
4. Output FeedBack เป็นสตรีมไซเฟอร์

และยังสามารถทำการรับรองข้อความ (Authentication) หรือข้อมูลได้

ในการออกแบบนั้นเดิมต้องการจะให้มีการเข้ารหัสข้อมูลพร้อมส่งข้อมูลจากเครื่องคอมพิวเตอร์ต้นทาง ผ่านข่ายสายโทรศัพท์สาธารณะสู่เครื่องปลายทางในขั้นตอนเดียวกัน แต่เนื่องจากความเร็วในการเข้ารหัสของ IC 8294 ต่ำ (ประมาณ 640 บิต/วินาที หรือ 80 ไบท์/วินาที) ถ้าหากข้อมูลมีขนาดใหญ่จะทำให้ต้องใช้คู่สายโทรศัพท์เป็นเวลานาน ดังนั้นจึงได้เปลี่ยนวิธีการมาเป็นการเข้ารหัสข้อมูลหรือรับรองข้อความให้เสร็จเรียบร้อยก่อน จึงทำการส่งข้อมูลไปยังปลายทาง

วิธีการเข้ารหัส ทำได้โดยการเรียกโปรแกรมที่พัฒนาขึ้นมา เพื่ออำนวยความสะดวกในการตั้งค่าเริ่มต้น (Initialization) ของคาร์ดใส่คีย์ ชื่อไฟล์ก่อนการเข้ารหัส และหลังจากเข้ารหัสแล้ว ในระหว่างที่คาร์ดกำลังทำการเข้ารหัสข้อมูลก็จะมีข้อความแสดงว่ากำลังทำงาน และมีเวลาที่ใช้โดยประมาณ หลังจากเข้ารหัสเสร็จแล้ว เราสามารถที่จะเรียกดูกราฟที่แสดงเวลาที่ใช้ในการเข้ารหัสของแต่ละโหมด และขนาดของไฟล์ได้ นอกจากนี้ยังได้อำนวยความสะดวกแก่ผู้ใช้งานโดยการสร้าง

โปรแกรมที่ใช้ สำหรับดูข้อความหรือไฟล์ใด ๆ ก็ได้ ทั้งที่เป็นเพลนไฟล์และไซเฟอร์ไฟล์ และยังได้สร้างโปรแกรมที่สามารถพิมพ์ข้อความที่เป็นตัวอักษรปกติ และอักษรพิเศษในไซเฟอร์ไฟล์ออกมาได้

ในกรณีที่ผู้ใช้งานไม่ทราบว่าจะใช้งานโปรแกรมอย่างไรหรือไม่เข้าใจศัพท์เฉพาะทางเทคนิคบางคำในโปรแกรม ก็สามารถที่จะดูข้อความช่วยเหลือทุก ๆ ขั้นตอนในการทำงาน นอกจากนี้ถ้าหากเกิดข้อผิดพลาดขึ้นในขั้นตอนของการป้อนค่าให้โปรแกรมหรือเกิดจากอุปกรณ์เชื่อมต่อเช่นเครื่องพิมพ์ โปรแกรมก็สามารถที่จะแจ้งให้ทราบให้ดำเนินการแก้ไขได้

ในส่วนของการรับรองข้อความได้สร้างอัลกอริธึ่มใหม่ขึ้นมาซึ่งมีความปลอดภัยกว่าแบบที่เคยมีการนำเสนอไว้ โดยแบบเดิมจะทำการเข้ารหัสข้อมูลพร้อมกับสร้าง AC เพื่อเป็นตัวรับรองข้อความ ซึ่งถ้าหากมีแการแก้ไขข้อความในไฟล์ก็จะทำให้ AC ผิดไป

วิธีการที่นำเสนอนี้จะทำการสร้าง AC 2 ครั้ง เพื่อป้องกันการแก้ไขไฟล์ทั้งในเพลนไฟล์และไซเฟอร์ไฟล์ คือเมื่อต้องการจะส่งไฟล์ที่มีการรับรองผ่านช่องสื่อสาร เราจะทำการรีจิสเตอร์ไฟล์นั้นก่อน โดยการใช้เมนู File Register เพื่อเป็นการสร้าง AC ขึ้นมารับรองไฟล์นั้น และไฟล์ก็ยังคงถูกเก็บไว้ในรูปเพลนไฟล์ ในที่ที่ไม่จำเป็นต้องเป็นความลับ เสร็จแล้วค่อยนำไฟล์นั้น (ที่ประกอบด้วยข้อความ+AC) มาทำการเข้ารหัส และรับรองข้อความอีกที แล้วจึงส่งผ่านช่องสื่อสาร

ในกรณีที่ไฟล์ที่ผ่านการรีจิสเตอร์ถูกแก้ไขไปเราจะสามารถรู้ได้ทันทีเนื่องจากในการทำการรับรองข้อความครั้งที่ 2 นั้น ก่อนที่จะทำการเข้ารหัสและรับรองข้อความ จะมีการตรวจสอบ AC ของไฟล์ที่ผ่านการลงทะเบียน แล้วกับที่คำนวณขึ้นมาใหม่ถ้าหากเท่ากัน ก็ถือได้ว่าไฟล์นั้นเป็นต้นฉบับจริง แต่หากไม่เท่ากันก็แสดงว่าไฟล์นั้นถูกแก้ไข

เนื่องจากการคำนวณหาค่าAC ในการทำการลงทะเบียนไฟล์เป็นการทำการบวกแบบโมดูโล-2 ของแต่ละบล็อคที่ประกอบขึ้นเป็นไฟล์นั้น อาจจะทำให้เกิดคำถามที่ว่า ถ้าเราเพิ่มบล็อคที่เหมือนกันทุกประการเข้าไป 2 บล็อค ก็จะทำให้ AC ที่ได้ไม่เปลี่ยนแปลงไปจากเดิม ซึ่งถือเป็นข้อผิดพลาดหรือจุดอ่อนของอัลกอริธึ่ม แต่โดยความจริงแล้วบล็อคของข้อมูลที่เราจะนำมาบวกแบบโมดูโล-2 นั้นเป็นข้อมูลที่ผ่านการเข้ารหัสแล้ว หรือเป็นไซเฟอร์เท็กซ์ จึงเป็นการยากมากที่จะทำเพลนเท็กซ์ใด ๆ มาเพื่อที่จะก่อให้เกิดไซเฟอร์เท็กซ์ที่เหมือนกันทุกประการ 2 ชุด เพราะว่าการเลือกโหมดที่ใช้ในการ

เข้ารหัสนี้ก็ได้คำนึงถึงจุดนี้ไว้แล้ว จึงได้เลือกใช้โหมด CBC ซึ่งมีการเชนนิ่ง ทำให้ไซเฟอร์เท็กซ์ที่ได้ออกมาค่อนข้างเกิดขึ้นแบบสุ่ม

ในด้านการรับข้อความนั้นจะทำการตรวจสอบAC ที่รับมาได้กับ AC ที่คำนวณขึ้นมาใหม่ในทำนองเดียวกับด้านการส่งหากมีค่าไม่ตรงกันก็จะแสดงข้อความว่าไฟล์ดังกล่าวถูกแก้ไขมาแล้วหรือไม่ตรงกับต้นฉบับ

ข้อเสนอแนะ

ถึงแม้ว่าทั้งฮาร์ดแวร์และโปรแกรมควบคุมรวมทั้งอัลกอริธึ่มต่าง ๆ ที่ได้พัฒนาขึ้นมา จะทำงานได้ตามความต้องการแต่สิ่งหนึ่งที่เป็นข้อจำกัดของงานชิ้นนี้ คือ ความเร็วในการทำงานซึ่งถือว่าต่ำมาก ดังนั้นถ้าหากจะพัฒนาให้เกิดความกว้างขวางในการประยุกต์ใช้งานผู้วิจัยเห็นว่าควรมีการเลือกใช้ IC เบอร์อื่นที่มีความเร็วมากกว่านี้หรืออาจจะใช้การออกแบบและสร้าง IC ขึ้นมาใช้เองโดยใช้เทคโนโลยีทางด้าน FPGA (Filed Programable Gate Array) และทางด้านซอฟท์แวร์ก็สามารถที่จะพัฒนาให้ทำงานภายใต้โปรแกรมวินโดว์ได้นอกจากนั้นควรจะมีการสร้างวิธีการรับส่งให้ทางด้านรับสามารถตรวจรู้โหมดในการเข้ารหัสได้ด้วยตัวเองแทนการตกลงกันล่วงหน้าแบบที่ใช้อยู่