บทที่ 4

การทดสอบ และผลการทดลองระบบ

หลังจากที่ผู้วิจัยทำการออกแบบและสร้างกุญแจอิเล็กทรอนิกส์แล้ว เพื่อให้แน่ใจถึงความปลอดภัยและประสิทธิภาพการทำงานของกุญแจอิเล็กทรอนิกส์ จึงทำการทดสอบการใช้งานแต่ละขั้นตอนและจำลองเหตุการณ์ต่าง ๆ ที่อาจเกิดขึ้นในระหว่างผู้ใช้นำกุญแจอิเล็กทรอนิกส์ ไปใช้งาน โดยมีหัวข้อต่าง ๆที่ต้องพิจารณาดังนี้

1. วิธีการทดสอบ
2. ผลการทดสอบ
3. การป้องกันการเจาะระบบ
4. ประสิทธิภาพการลดทอนของ Montgomery
5. ความเร็วในการประมวลผลและขนาดของโค้ดโปรแกรม

4.1 วิธีการทดสอบ

ในระหว่างการสร้างกุญแจอิเล็กทรอนิกส์ ผู้วิจัยได้ทำการทดสอบการทำงานเป็นระยะโดยแบ่งการทดสอบออกเป็น 4 ขั้นดังนี้

4.1.1 เขียนโปรแกรมทดสอบการเข้ารหัสลับบนเครื่องคอมพิวเตอร์ โดยไม่ใช้ทฤษฎีการลดทอนแบบ Montgomery จุดประสงค์ในการทดสอบวิธีนี้เพื่อให้แน่ใจถึงค่าจำนวนเฉพาะต่าง ๆ ที่ได้จากการสุ่มสามารถนำไปใช้ในการเข้ารหัสได้

4.1.2 เขียนโปรแกรมทดสอบการเข้ารหัสลับบนเครื่องคอมพิวเตอร์ โดยใช้ทฤษฎีการลดทอน เพื่อพิสูจน์การลดทอนค่าตัวเลขที่เกิดขึ้นจากสมการ $C= M^e \bmod n$ ซึ่งพบว่าสามารถลดทอนจำนวนตัวเลขได้มากหลายเท่า แต่ในการลดทอนนี้ยังมีข้อจำกัด ซึ่งแสดงให้เห็นในขั้นตอนที่ 2 ของฟังก์ชัน Monpro ในบทที่ 2

4.1.3 เขียนโปรแกรมทดสอบการเข้ารหัสบนไมโครคอนโทรลเลอร์ โดยใช้ทฤษฎีการลดทอน เพื่อทดสอบกับอุปกรณ์ที่ใช้ในระบบจริง ซึ่งพบว่าสามารถเข้ารหัสบนไมโครคอนโทรลเลอร์ได้ ทำให้สามารถนำผลการทดสอบไปสร้างเป็นกุญแจอิเล็กทรอนิกส์ได้

4.1.4 เขียนโปรแกรมทดสอบการใช้งานกุญแจอิเล็กทรอนิกส์ เพื่อให้เครื่องแม่ข่ายสามารถรับส่งข้อมูลที่เข้ารหัสแล้วเพื่อติดต่อกับกุญแจอิเล็กทรอนิกส์ และทำการตรวจสอบค่ารหัสประจำตัวที่อยู่ภายใน กุญแจอิเล็กทรอนิกส์ซึ่งในโปรแกรมดังกล่าว ผู้วิจัยได้แยกโค้ดโปรแกรม

โปรแกรมออกเป็น 2 ส่วนคือ ส่วนที่อยู่ภายในไดนามิกส์ลิงค์ไลบรารี่และส่วนที่อยู่ภายนอกไดนามิกส์ลิงค์ไลบรารี่ เพื่อให้ระบบปลอดภัยมากที่สุด

เมื่อผู้วิจัยทดสอบระบบต่างๆ ตามขั้นตอนแล้วจึงสร้างกุญแจอิเล็กทรอนิกส์ ขึ้นมาใหม่ ซึ่งจากเดิมประกอบขึ้นจากบอร์ดสำเร็จรูป โดยดำเนินการออกแบบวงจรใหม่และตัดส่วนที่ไม่จำเป็นในบอร์ดเดิมออกไปเช่น วงจรที่ใช้ในการดาวน์โหลดโปรแกรมลงบอร์ดทำให้วงจรใหม่ที่ได้มีขนาดที่เล็กลง เพื่ออำนวยความสะดวกแก่ผู้ใช้งาน

4.2 ผลการทดสอบ

ผู้วิจัยได้สร้างบัญชีผู้ใช้งานขึ้นมา 3 บัญชีเพื่อจำลองการใช้งานโปรแกรมสำเร็จรูปที่ต้องการจำกัดสิทธิ์การใช้งาน โดยที่ผู้มีสิทธิ์ใช้งานโปรแกรมนี้ต้องมีบัญชีผู้ใช้และมีกุญแจอิเล็กทรอนิกส์ ที่ใช้กับกุญแจอิเล็กทรอนิกส์นี้เท่านั้น จากนั้นเมื่อเสียบกุญแจอิเล็กทรอนิกส์ เข้ากับเครื่องคอมพิวเตอร์ก่อนการล็อกอินใช้งานโปรแกรม ดังภาพประกอบ 4-1

ภาพประกอบ 4-1 ผู้ใช้ล็อกอิน

กรณีผู้ใช้ไม่เสียบกุญแจอิเล็กทรอนิกส์ เข้ากับเครื่องคอมพิวเตอร์ระบบจะแจ้งให้ผู้ใช้ทราบดังภาพประกอบ 4-2

ภาพประกอบ 4-2 กรณีผู้ใช้ไม่เสียบกุญแจก่อนใช้งาน

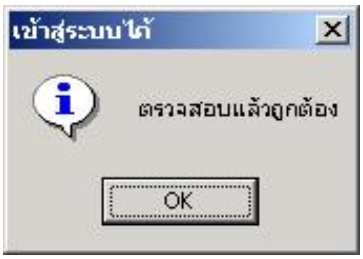
กรณีผู้ใช้กรอกบัญชีผู้ใช้หรือรหัสผ่านผิด ระบบจะแจ้งให้ผู้ใช้ทราบดังแสดงภาพประกอบ 4-3

ภาพประกอบ 4-3 กรณีผู้ใช้กรอกบัญชีผู้ใช้ หรือรหัสผ่านผิด

กรณีผู้ใช้กรอกบัญชีผู้ใช้และรหัสผ่านถูกต้องแต่เสียบกุญแจผิดดอก ระบบจะแจ้งเตือนให้ผู้ใช้งานทราบดังแสดงตามภาพประกอบ 4-4

ภาพประกอบ 4-4 กรณีผู้ใช้เสียบกุญแจผิดดอก

กรณีผู้ใช้กรอกบัญชีผู้ใช้และรหัสผ่านถูกต้องและระบบตรวจสอบ กุญแจอิเล็กทรอนิกส์ เรียบร้อยแล้วจะสามารถใช้งานโปรแกรมได้ทันทีดังแสดงตามภาพประกอบ 4- 5



ภาพประกอบ 4-5 กรณีผู้ใช้แสดงสิทธิการใช้ได้อย่างถูกต้อง

4.3 การป้องกันการเจาะระบบ

4.3.1 กรณีผู้บุกรุกกระทำการดักจับ (capture) ข้อมูลขณะที่เครื่องแม่ข่ายกำลังสื่อสารกับกุญแจอิเล็กทรอนิกส์ ผู้บุกรุกจะไม่สามารถตีความข้อมูลที่ดักจับได้ เนื่องจากข้อมูลถูกเข้ารหัสแบบ RSA ทำให้ข้อมูลเปลี่ยนแปลงทุกครั้งที่มีการสื่อสาร

4.3.2 กรณีผู้บุกรุกสร้างกุญแจอิเล็กทรอนิกส์ ขึ้นมาเองโดยเลียนแบบกุญแจอิเล็กทรอนิกส์ของระบบ จะไม่สามารถทำได้เนื่องจากภายในกุญแจอิเล็กทรอนิกส์ของระบบมีการฝังค่ารหัสประจำตัวไว้ภายในซึ่งค่านี้จะเก็บไว้เป็นความลับผู้บุกรุกไม่สามารถรู้ได้

4.3.3 กรณีผู้บุกรุกต้องการทำซ้ำ (Copy) กุญแจอิเล็กทรอนิกส์ จะไม่สามารถทำได้เนื่องจากในขณะสร้างกุญแจอิเล็กทรอนิกส์ ผู้วิจัยได้ทำการป้องการการอ่านข้อมูลภายในไว้แล้ว

4.4 ประสิทธิภาพการลดทอนของ Montgomery Reduction Algorithm

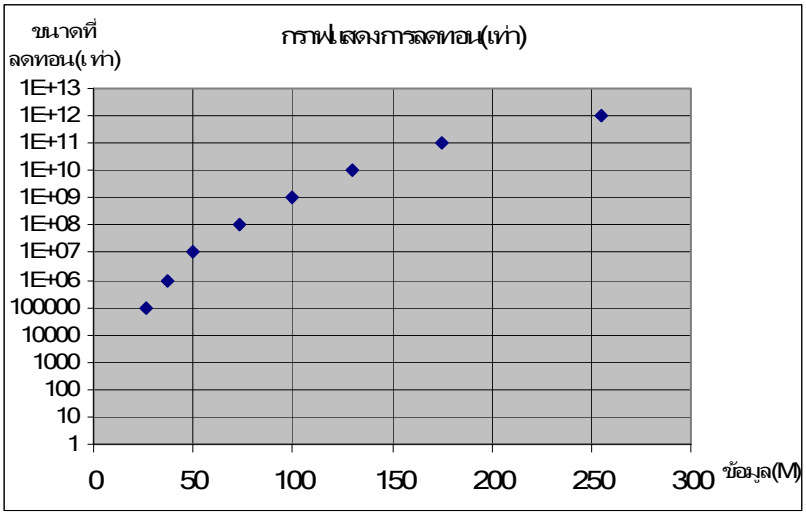
ผู้วิจัยใช้ทฤษฎีการลดทอนแบบ Montgomery ช่วยในการลดทอนสมการการเข้ารหัสแบบ RSA เพื่อให้สามารถเข้ารหัสแบบ RSA บนไมโครคอนโทรลเลอร์ได้ ดังนั้นในการพิจารณาประสิทธิภาพการลดทอน จึงเปรียบเทียบค่าของจำนวนตัวเลขที่เกิดขึ้นจากการคำนวณโดยการใช้ทฤษฎีการลดทอนแบบ Montgomery และการไม่ใช้ทฤษฎีนี้ เมื่อพิจารณาสมการการเข้ารหัส $C= M^e \bmod n$ นี้พบว่าตัวแปรที่มีผลกระทบต่อประสิทธิภาพของทฤษฎีนี้คือ M และ n ซึ่งผู้วิจัยพบว่าเมื่อทั้ง 2 ตัวแปรนี้มีค่าเพิ่มขึ้นจะทำให้ค่าของ t*n′ ในขั้นตอน 2 ของฟังก์ชัน Monpro เพิ่มขึ้นซึ่งค่า t*n′ นี้จะเป็นค่าของตัวเลขที่มากที่สุดในการเข้ารหัสดังภาคผนวก ค การลดทอนแบบ Montgomery จะมีประสิทธิภาพมากที่สุดเมื่อ n มีค่าใกล้เคียงกับ r นั้นหมายความว่าสามารถลดทอนได้มากที่สุดดังแสดงในสมการที่ 4.1 และประสิทธิภาพของการลดทอนแบบ Montgomery จะลดลงจนไม่สามารถลดทอนสมการการเข้ารหัสได้แสดงตามเงื่อนไขของสมการที่ 4.2

$$\lim_{n \to r} M^e \bmod n \tag{4.1}$$

$$\lim_{n \to r/2} M^e \bmod n \tag{4.2}$$

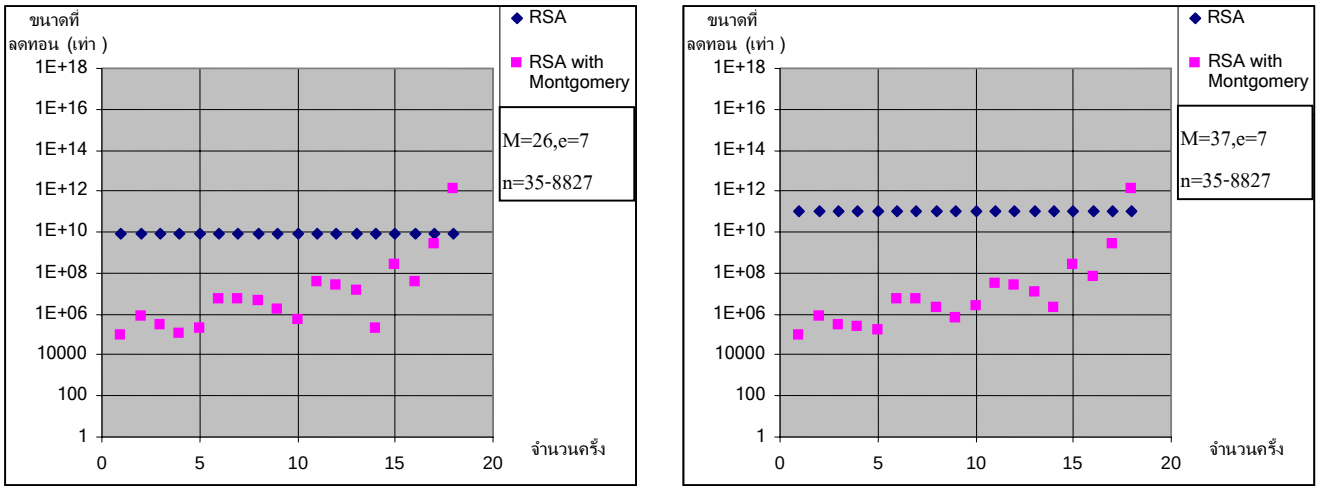
ในทางกลับกันหากไม่ใช้การลดทอนแบบ Montgomery ตัวแปรที่ทำให้ค่าของตัวเลขมากขึ้นเป็นทวีคูณคือ M และ e

ประสิทธิภาพของทฤษฎีนี้ขึ้นอยู่กับค่า M และ n หากค่าตัวแปรทั้ง 2 นี้มีค่ามาก จะสามารถลดทอนได้มากขึ้น ทั้งนี้ขึ้นอยู่กับเงื่อนไขตามสมการ 4.1 และ 4.2 เป็นสำคัญดังแสดงในภาพประกอบ 4-6



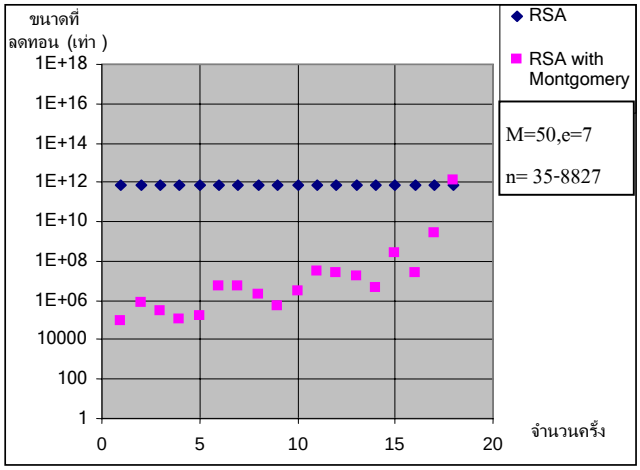
ภาพประกอบ 4-6 ประสิทธิภาพการลดทอน

ผู้วิจัยทำการทดสอบโดยการเพิ่มค่า M จาก 0-255 และเพิ่มค่า n จาก 35-8827 เพื่อหาประสิทธิภาพการลดทอนแบบ Montgomery โดยเปรียบเทียบกับค่าที่ได้จากการยกกำลังสมการการเข้ารหัสแบบ RSA โดยตรงกับค่าที่ได้จาก t*n' ในขั้นตอน 2 ของฟังก์ชัน Monpro ในทฤษฎีการลดทอนแบบ Montgomery พบว่าเมื่อเพิ่มค่า M ให้มากขึ้นประสิทธิภาพการลดทอนจะเพิ่มขึ้นตามไปด้วย ซึ่งเป็นไปตามเงื่อนไขของสมการ 4.1 และ 4.2 ดังแสดงในภาพประกอบ 4-7

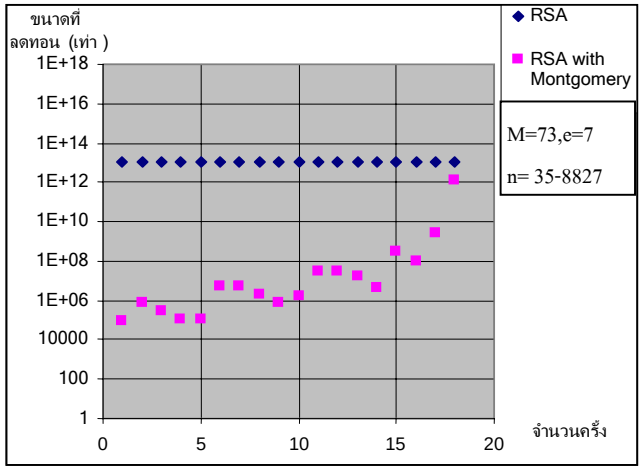


(ก) (ข)

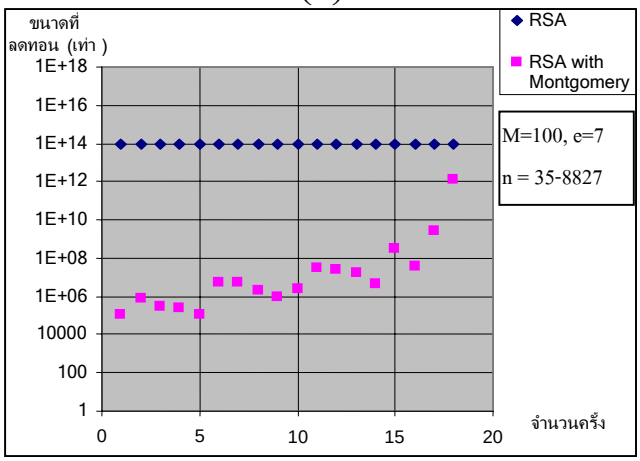
ภาพประกอบ 4-7 เปรียบเทียบตัวเลขที่เกิดจากการเข้ารหัสแบบ RSA โดยใช้ทฤษฎีการลดทอนแบบ Montgomery และการไม่ใช้ทฤษฎีลดทอน



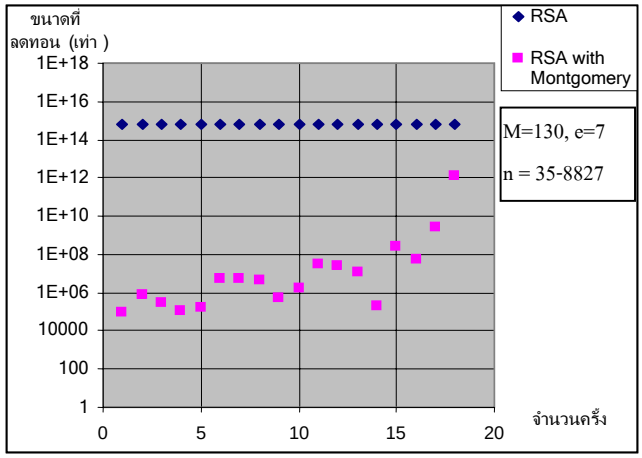
(ค)



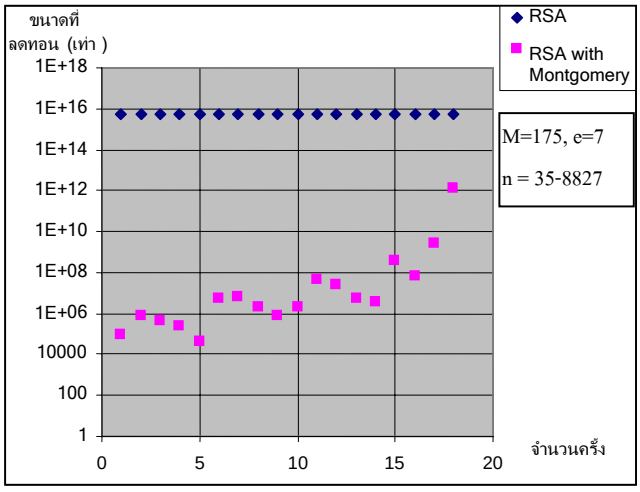
(ง)



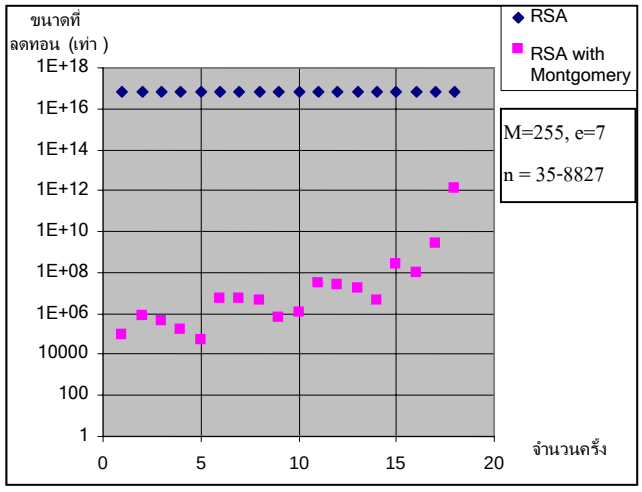
(จ)



(ฉ)



(ช)



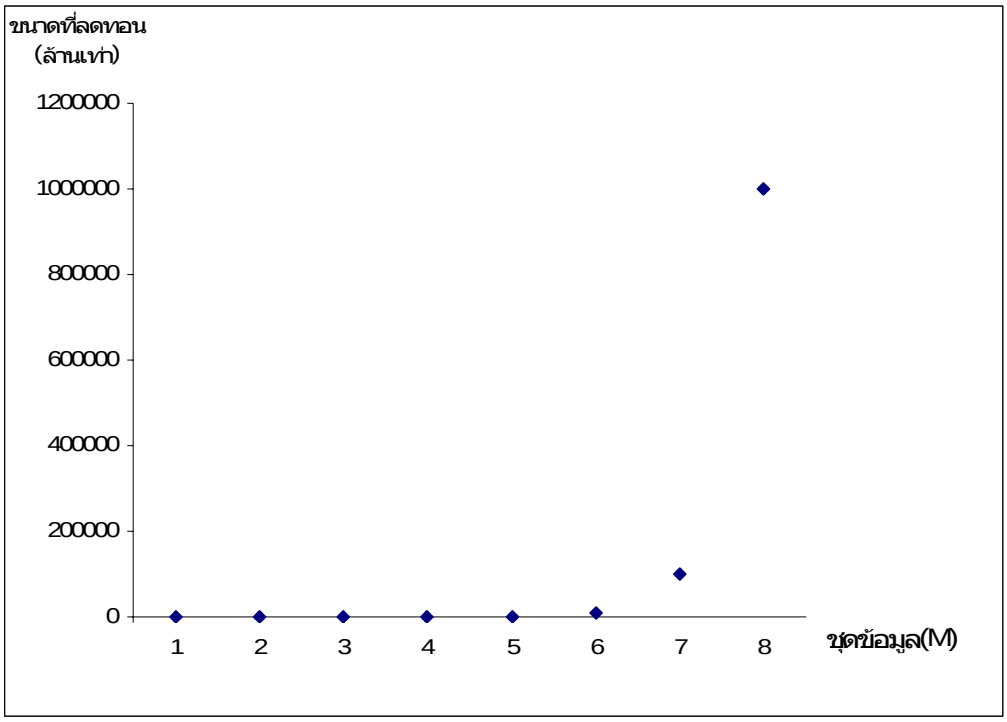
(ซ)

ภาพประกอบ 4-7 (ต่อ)

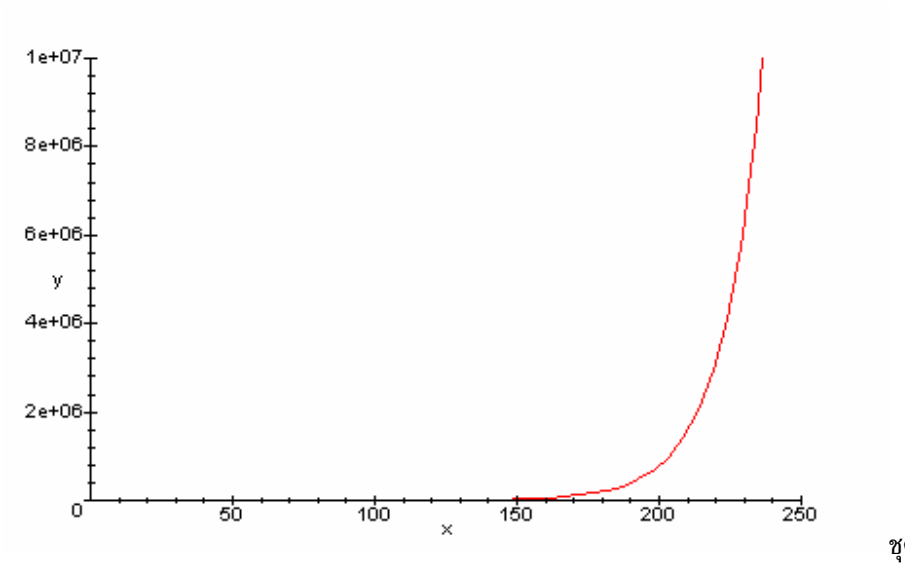
จากภาพประกอบ 4-7 (ก) แสดงให้เห็นว่าเมื่อค่า M คงที่และเพิ่มค่า n จาก 35-8827 สามารถลดทอนได้สูงสุดประมาณ 100,000 เท่าและเมื่อเพิ่มค่า n เพิ่มมากขึ้นจน n เข้าใกล้ r/2 ทำให้ไม่สามารถลดทอนได้ซึ่งเป็นไปตามเงื่อนไงในสมการ 4.2 สำหรับภาพประกอบอื่น ๆ แสดงให้เห็นถึงการเพิ่มค่า M จะทำให้การลดทอนมีประสิทธิขึ้น นั้นคือสามารถลดทอนได้เพิ่มมากขึ้นหลายเท่า ดังนั้นจึงกล่าวได้ว่าประสิทธิภาพการลดทอนโดยใช้การลดทอนแบบ Montgomery ขึ้นอยู่กับค่าของ M และ n ทั้งนี้ต้องอยู่ภาคใต้เงื่อนไขตามสมการ 4.1 และ 4.2

เมื่อนำประสิทธิภาพการลดทอนมาปรับเส้นโค้ง (Curve fitting) เพื่อให้ทราบถึงค่าที่ลดทอนได้ โดยที่ค่าเหล่านี้ไม่จำเป็นต้องทดลองแต่สามารถหาได้จากสมการที่ 4.3 และสามารถเขียนเป็นภาพประกอบ 4-9

$$y = e^{0.069x+0.211} \tag{4.3}$$



ภาพประกอบ 4-8 ประสิทธิภาพการลดทอนจากการทดลอง

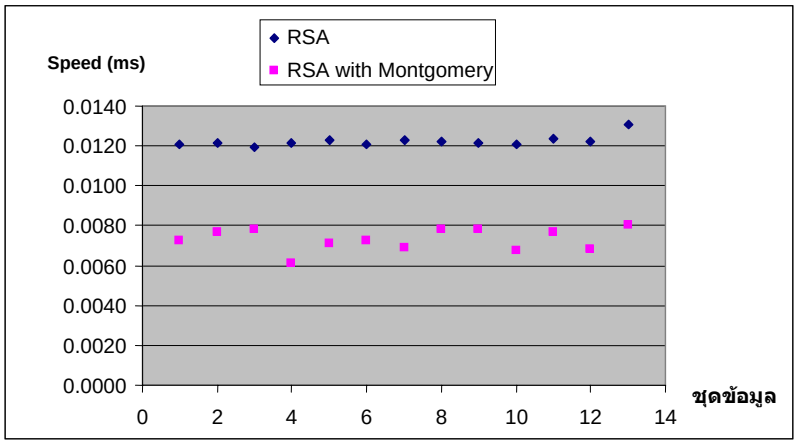


ภาพประกอบ 4-9 ประสิทธิภาพการลดทอนจากการปรับเส้นโค้ง

4.5 ความเร็วในการประมวลผลการเข้ารหัสแบบ RSA

4.5.1 ความเร็วในการประมวลผลบน CPU

การพิจารณาความเร็วในการประมวลผลบน CPU ผู้วิจัยได้ทำการทดลองวัดความเร็วในการประมวลผลของโปรแกรมเข้ารหัสโดยเปรียบเทียบกันระหว่างการเข้ารหัสแบบ RSA และการใช้ทฤษฎีการลดทอนการเข้ารหัสแบบ RSA ในการทดลองนี้ผู้วิจัยใช้โปรแกรม Borland C โปรแกรมจะได้เป็นไฟล์ .EXE จากนั้นใช้โปรแกรม Turbo Profiler วัดความเร็วในการทำงานของโปรแกรม



ภาพประกอบ 4-10 ความเร็วในการประมวลผลบน CPU

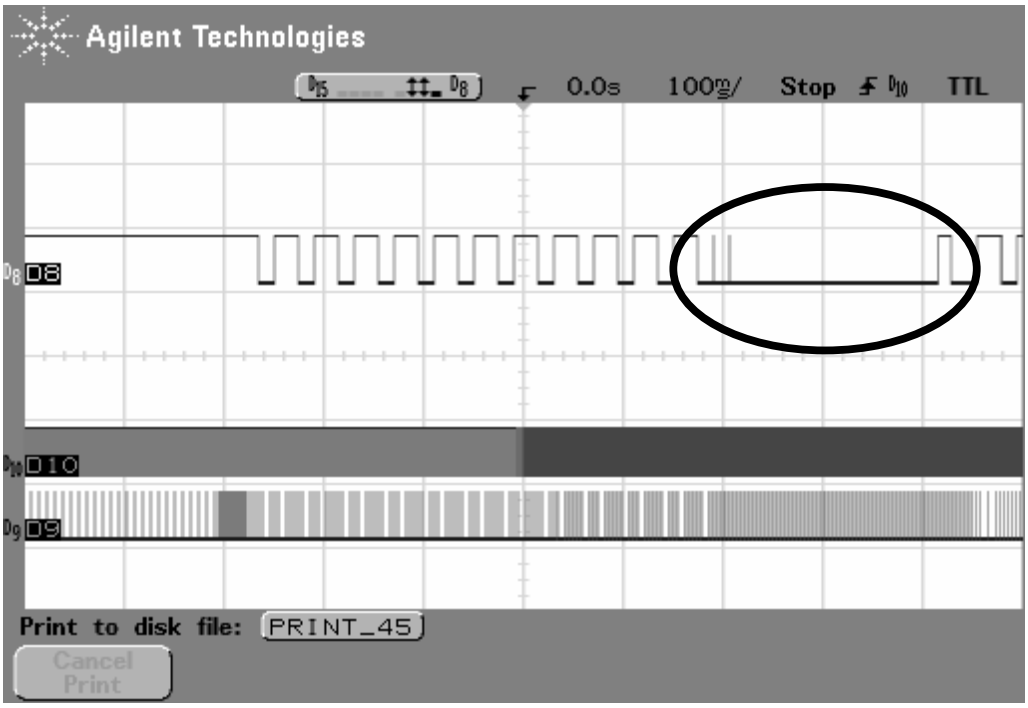
จากภาพประกอบ 4-10 พบว่าเมื่อใช้ทฤษฎีการลดทอนจะทำให้เวลาในการประมวลผลการเข้ารหัสหนึ่งครั้งจะลดลงอย่างเห็นได้ชัด ซึ่งมีค่าประมาณ 0.004 ms หรือคิดเป็นร้อยละ 30 ซึ่งผลของเวลาที่ลดลงนี้สืบเนื่องมาจากการใช้ทฤษฎีการลดทอน โดยวิธีการประมวลผลที่เกิดขึ้นจะไม่ยกกำลังสมการโดยตรง แต่จะนำสมการเข้ารหัสมาประมวลผลบนพื้นฐานของวิธีการเลขฐานสอง ซึ่งได้กล่าวรายละเอียดแล้วในบทที่ 2 โดยที่โค้ดโปรแกรมจะมีขนาดตามตารางที่ 4-1 ซึ่งผู้วิจัยทดสอบโดยใช้ CPU Pentium II 400 MHz

ตารางที่ 4-1 ขนาดของโค้ดโปรแกรมและไฟล์ exe

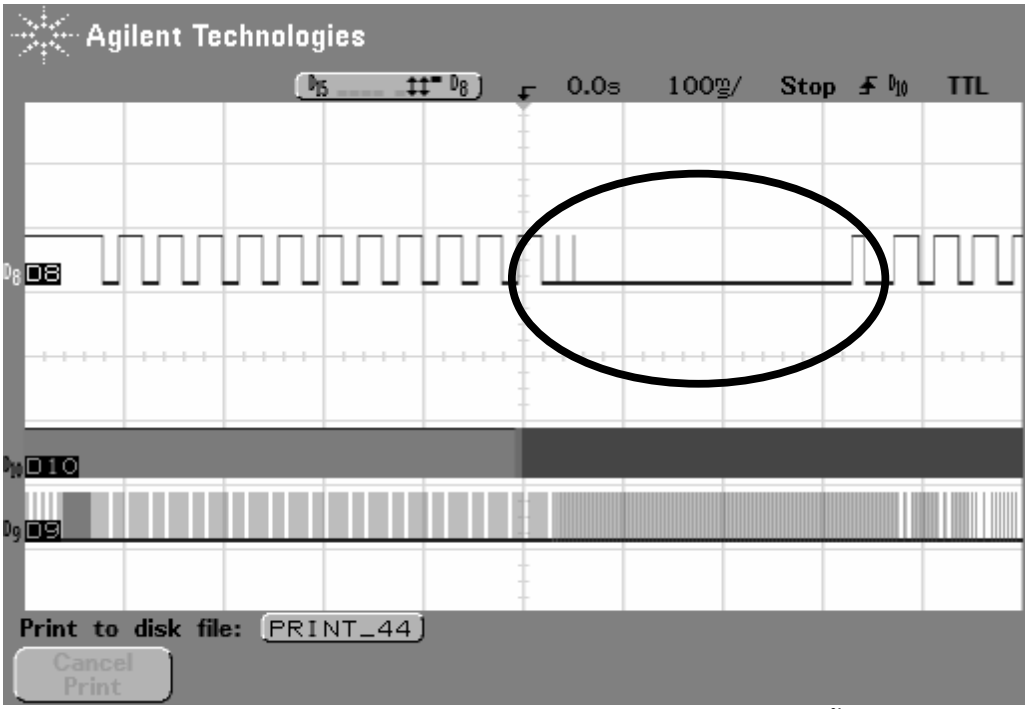
	ขนาดโค้ดโปรแกรม	ขนาด .EXE
RSA	1 Kbyte	26 Kbyte
RSA with Montgomery	4 Kbyte	14 Kbyte

4.5.2 ความเร็วในการประมวลผลบน Microcontroller

จุดมุ่งหมายอีกประการหนึ่งของงานวิจัยนี้ คือการเข้ารหัสลับแบบ RSA บนไมโครคอนโทรลเลอร์ซึ่งมีสภาพแวดล้อมที่จำกัดเมื่อเปรียบเทียบกับ CPU ที่มีขีดความสามารถสูงและอยู่ในสภาวะแวดล้อมที่เหมาะสมกว่าไมโครคอนโทรลเลอร์เช่น การทำงานของ CPU ที่ความเร็วของสัญญาณนาฬิกาสูงกว่าไมโครคอนโทรลเลอร์, CPU มีหน่วยความจำที่มากกว่าไมโครคอนโทรลเลอร์ เวลาในการประมวลผลการเข้าหรัสไม่สามารถวัดได้โดยใช้โปรแกรม ดังนั้นผู้วิจัยจึงวัดความเร็วการประมวลผลของ ไมโครคอนโทรลเลอร์ ด้วยรูปสัญญาณดังแสดงในภาพประกอบ 4-11



ภาพประกอบ 4-11 (ก) สัญญาณเมื่อเข้าและถอดรหัส 20 ครั้ง



ภาพประกอบ 4-11 (ข) สัญญาณเมื่อเข้าและถอดรหัส 30 ครั้ง

ภาพประกอบ 4-11 การวัดความเร็วในการประมวลผลบนไมโครคอนโทรลเลอร์

จากภาพประกอบ 4-11 (ก) และ (ข) พบว่าเมื่อสั่งให้ไมโครคอนโทรลเลอร์เข้ารหัส 20 และ 30 ครั้งตามลำดับ สัญญาณของรูปคลื่นจะแตกต่างกัน ตามจำนวนเวลาที่ไมโครคอนโทรลเลอร์ใช้ในการประมวลผลคำสั่ง ซึ่งเมื่อพิจารณาจากภาพประกอบแล้ว ไมโครคอนโทรลเลอร์จะทำงานโดยใช้เวลา 5 มิลลิวินาทีต่อการเข้ารหัส 1 ครั้ง โดยใช้สัญญาณนาฬิกา 20 MHz อนึ่งการวิเคราะห์ความเร็วนี้ ยังไม่มีงานวิจัยใดที่สามารถระบุเวลาที่ชัดเชนในการประมวลผลสมการเลขชี้กำลังมอดุลาร์ ด้วยการลดทอนแบบ Montgomery

4.6 สรุปท้ายบท

จากการทดสอบต่าง ๆ จะเห็นได้ว่าในการทดสอบกุญแจอิเล็กทรอนิกส์มีการทดสอบตลอดการสร้างเพื่อให้แน่ใจถึงความถูกต้องในการตรวจสอบค่ารหัสประจำตัว และการสื่อสารระหว่างเครื่องแม่ข่ายกับกุญแจอิเล็กทรอนิกส์ รวมถึงการป้องกันการถูกคุกคามจากผู้บุกรุกด้วยการเข้ารหัสข้อมูลระหว่างการสื่อสาร ทำให้ระบบมีความเข้มแข็ง ยากต่อการบุกรุก แต่ระบบยังมีข้อจำกัดบางประการซึ่งจะกล่าวในบทต่อไป