ชื่อวิทยานิพนธ์ การพัฒนากุญแจอิเล็กทรอนิกส์โดยใช้ RSA ด้วยอัลกอริทึมการลดทอนของ Montgomery ในไมโครคอนโทรลเลอร์
ผู้เขียน นายชลากร ครุพงศ์สิริ
สาขาวิชา วิศวกรรมไฟฟ้า
ปีการศึกษา 2548

บทคัดย่อ

การเข้ารหัสลับแบบ RSA มีใช้กันอย่างแพร่หลายในปัจจุบัน เนื่องจากเป็นระบบรหัสลับที่ยากในการวิเคราะห์ย้อนกลับ งานวิจัยนี้มีวัตถุประสงค์ที่จะสร้างระบบรหัสลับ RSA แบบซอฟต์แวร์บนไมโครคอนโทรลเลอร์และใช้ทฤษฎีการลดทอนแบบ Montgomery ในการลดทอนสมการรูปแบบชี้กำลังมอดุลาร์ (Modular Exponentiation) ทำให้ลดความซับซ้อนของการเข้ารหัสลับ RSA จึงเหมาะสมที่จะสร้างระบบรหัสลับนี้บนไมโครคอนโทรลเลอร์และสามารถนำไปประยุกต์เป็นกุญแจอิเล็กทรอนิกส์ที่สร้างจากไมโครคอนโทรลเลอร์ได้ กุญแจอิเล็กทรอนิกส์ที่สร้างขึ้นนี้ประกอบด้วย 2 ส่วนคือ ส่วนแรกทำหน้าที่เชื่อมต่อกับพอร์ต USB โดยใช้ USB ไมโครคอนโทรลเลอร์เบอร์ PIC16C745 และส่วนที่ 2 ทำหน้าที่ประมวลผลรหัสลับ RSA โดยใช้ไมโครคอนโทรลเลอร์เบอร์ PIC18F242 ผลการวิจัยพบว่าเมื่อประยุกต์ใช้ทฤษฎีการลดทอนแบบ Montgomery ในต้นแบบกุญแจอิเล็กทรอนิกส์บนไมโครคอนโทรลเลอร์ และเปรียบเทียบกับการเข้ารหัสลับแบบ RSA ทั่ว ๆ ไปพบว่าสามารถลดทอนค่าตัวเลขที่เกิดจากการประมวลผลได้มากกว่า 100,000 เท่า โดยมีความเร็วที่เร็วกว่า 0.04 มิลลิวินาที และมีขนาดของไฟล์การกระทำเล็กกว่า 46 %

ผลของการวิจัยสามารถนำกุญแจอิเล็กทรอนิกส์ไปประยุกต์ใช้งาน เพื่อจำกัดสิทธิ์การใช้ โปรแกรมประยุกต์ได้ โดยการนำไปประยุกต์ใช้งานนี้ โปรแกรมประยุกต์สามารถเรียกใช้งานระบบรหัสลับ RSA โดยผ่านไดนามิกส์ลิงค์ไลบรารี่ซึ่งโปรแกรมประยุกต์ นี้ต้องเขียนด้วยโปรแกรมวิชวลเบสิก 6.0 เท่านั้น

คำสำคัญ : กุญแจอิเล็กทรอนิกส์, การเข้ารหัสลับแบบ RSA, Montgomery reduction algorithm, Microcontroller

Thesis Title	Implementation of an Electronic Key Using RSA with Montgomery Reduction Algorithm in a Microcontroller
Author	Mr. Chalakorn Karupongsiri
Major Program	Electrical Engineering
Acadecmic Year	2005

ABSTRACT

RSA cryptography has been widely used in data security implementation because of its effectiveness and hardship cryptanalysis. This thesis aims to design and implement an electronic key in software using the Montgomery algorithm. The Montgomery algorithm is able to reduce large integers in modular exponentiation expression and complexity in a RSA process. The proposed electronic key consists of 2 units: an USB interface unit using a PIC microcontroller 16C745 and a RSA processing unit using a PIC microcontroller 18F242. In comparison to native RSA, the prototype electronic key on a microcontroller can reduce upper bound of intermediate values in processing more than 100,000 times. The processing speed is less than 0.04 milliseconds and the size of executable file is less than 46 %.

The electronic key can be successfully applied for authentication application software written in Visual Basic 6.0 using a Dynamics Link Library.

Keywords: Electronic Key, RSA Cryptography, Montgomery reduction algorithm, Microcontroller