บทที่ 3

การออกแบบกุญแจอิเล็กทรอนิกส์

จากความรู้พื้นฐานที่กล่าวถึงในบทที่ 2 นำไปสู่การออกแบบกุญแจอิเล็กทรอนิกส์ในบทนี้ซึ่งจะอธิบายถึงขั้นตอนต่าง ๆ ในการออกแบบและพัฒนากุญแจอิเล็กทรอนิกส์ ความสะดวกของผู้ใช้ ความปลอดภัยที่เชื่อถือได้ รวมถึงต้นทุนที่เหมาะสมในการสร้าง ขั้นตอนกระบวนการในการพัฒนา กุญแจอิเล็กทรอนิกส์ โดยเริ่มจากการออกแบบโครงสร้างโปรโตคอนในการสื่อสารผ่านทางพอร์ต USB การเข้ารหัสลับแบบ RSA การลดทอนแบบ Montgomery และการประยุกต์ใช้งานเพื่อให้ง่ายต่อการทำความเข้าใจกุญแจอิเล็กทรอนิกส์

3.1 ข้อพิจารณาในการออกแบบกุญแจอิเล็กทรอนิกส์

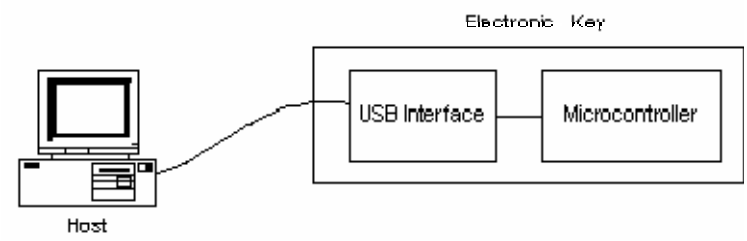
การรักษาความปลอดภัยโปรแกรมประยุกต์ที่ต้องการจำกัดสิทธิ์ผู้ใช้ โดยใช้กุญแจอิเล็กทรอนิกส์ สิ่งที่ต้องพิจารณามีดังนี้

- มีความปลอดภัยสูง ความซับซ้อนของระบบที่ยากต่อการบุกรุก ซึ่งป้องกันโดยการเข้ารหัสลับข้อมูลระหว่างเครื่องแม่ข่ายกับอุปกรณ์ ขณะที่สื่อสารกันทำให้ข้อมูลที่ผ่านสายนำสัญญาณจะเป็นข้อมูลที่เปลี่ยนแปลงทุกครั้งที่เกิดการสื่อสาร เป็นผลให้ยากต่อการคาดเดาของผู้บุกรุก
- กุญแจอิเล็กทรอนิกส์ มีลักษณะเป็นหนึ่งเดียวไม่สามารถทำซ้ำได้ ด้วยเทคโนโลยีของการผลิตชิปไมโครคอนโทรลเลอร์ สามารถป้องกันการอ่านข้อมูลภายในได้ เป็นผลให้ไม่สามารถสร้างไมโครคอนโทรลเลอร์ที่เหมือนกันได้
- สะดวกต่อการใช้งาน มีขนาดเล็ก ไม่จำเป็นต้องใช้แหล่งจ่ายไฟจากภายนอก
- ราคาต้นทุนสร้างเหมาะสม แม้ว่าต้นทุนในการผลิตกุญแจอิเล็กทรอนิกส์ต้นแบบจะสูง แต่เมื่อสร้างกุญแจอิเล็กทรอนิกส์ตัวถัดไปต้นทุนจะต่ำลง โดยจะเสียค่าใช้จ่ายในการสร้างประมาณตัวละ 1,500 บาท ซึ่งคุ้มค่ากับการลงทุนเพราะหากโปรแกรมที่ต้องการจำกัดสิทธิ์ ถูกใช้โดยผู้ที่ไม่ได้รับอนุญาต ความเสียหายทางธุรกิจจะมากกว่านี้หลายเท่า

3.2 ขั้นตอนการออกแบบกุญแจอิเล็กทรอนิกส์

โครงสร้างของกุญแจอิเล็กทรอนิกส์จะประกอบด้วย 2 ส่วนคือส่วนต่อประสานกับพอร์ต USB และ ไมโครคอนโทรลเลอร์แสดงในภาพประกอบ 3-1 โดยที่ส่วนต่อประสานกับพอร์ต USB จะทำหน้าที่ต่อประสานกับพอร์ต USB ของเครื่องคอมพิวเตอร์ และอีกด้านหนึ่งจะสื่อสารกับ

ไมโครคอนโทรลเลอร์ด้วยพอร์ตขนานโดยที่ไมโครคอนโทรลเลอร์ จะทำหน้าที่เข้ารหัสลับและถอดรหัสลับแบบ RSA รวมถึงเก็บค่ารหัสลับ เพื่อตรวจสอบความถูกต้องขณะที่มีการติดต่อสื่อสารระหว่างกุญแจอิเล็กทรอนิกส์กับเครื่องคอมพิวเตอร์



ภาพประกอบ 3-1 โครงสร้างภายในกุญแจอิเล็กทรอนิกส์

3.2.1 โปรแกรมติดต่อกับพอร์ต USB

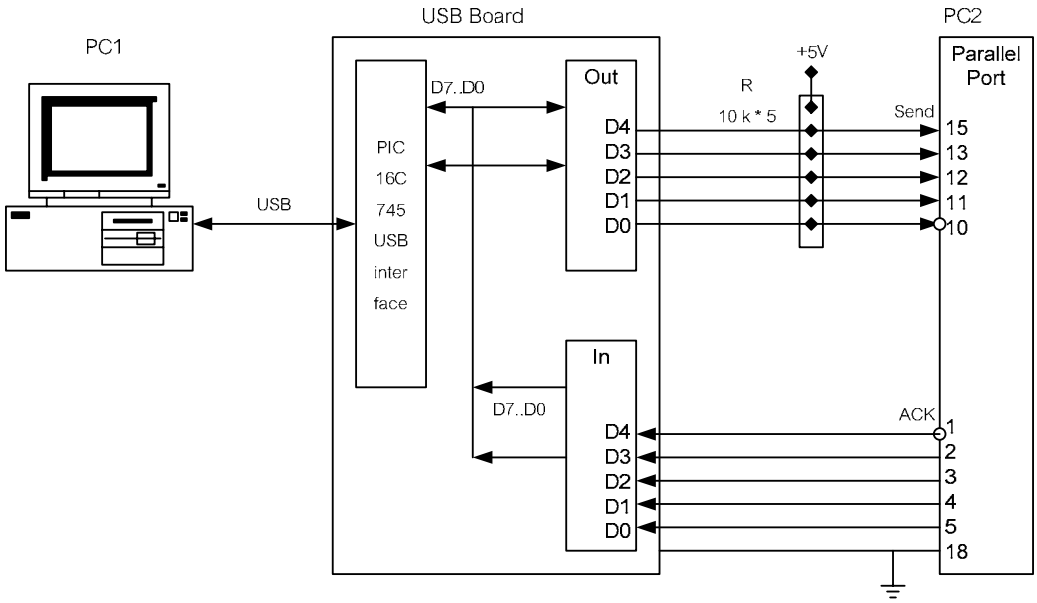
การสื่อสารผ่านพอร์ต USB ของเครื่องคอมพิวเตอร์นั้นแตกต่างจากการติดต่อกับพอร์ตอนุกรมและพอร์ตขนานโดยสิ้นเชิง เนื่องจากพอร์ต USB สามารถรองรับอุปกรณ์ได้หลากหลาย ดังนั้นการเขียนโปรแกรมติดต่อกับพอร์ต USB จะมีขั้นตอนที่ซับซ้อนกล่าวคือก่อนการรับส่งข้อมูลจะต้องมีการตรวจสอบคลาส (Class) ของอุปกรณ์ USB เพื่อให้ USB เครื่องแม่ข่ายทราบถึงอุปกรณ์ที่เสียบเข้ามาในพอร์ตจัดอยู่ในคลาสใดเพื่อให้ USB เครื่องแม่ข่าย กำหนดรูปแบบการถ่ายโอนข้อมูล ได้อย่างถูกต้องตามอุปกรณ์นั้น ๆ เช่น อุปกรณ์ที่เสียบเข้ามาในเครื่องแม่ข่ายคือฮาร์ดดิสก์จัดอยู่ในชั้นการจัดเก็บข้อมูล (Mass Storage Class) จะถ่ายโอนข้อมูลแบบเสมอเวลา (Isochronous Transfer) จุดเด่นของการถ่ายโอนแบบนี้คือความเร็วในการรับส่งข้อมูลจะสูงมาก แต่ในการสร้างกุญแจอิเล็กทรอนิกส์จัดอยู่ใน Human Interface Class (HID) ถ่ายโอนข้อมูลแบบขัดจังหวะ โดยจะส่งข้อมูลทีละน้อย ๆ และเว้นช่วงการส่งเป็นเวลานานคล้ายกับเมาส์และแผงแป้นอักขระ ดังนั้นก่อนที่จะส่งข้อมูลผ่านมายังพอร์ต USB ได้ เครื่องแม่ข่ายต้องอ่านค่าคลาสของอุปกรณ์ รวมถึงค่ารหัสประจำตัวผลิตภัณฑ์และรหัสประจำตัวผู้ผลิตก่อนการส่งข้อมูล เพื่อป้องกันการชนกันของข้อมูลภายในสายนำสัญญาณ ดังนั้นจึงเป็นผลให้ผู้ผลิตชิป ไมโครคอนโทรลเลอร์รายใหญ่เท่านั้น จึงจะสามารถติดต่อสื่อสารกับ USB เครื่องแม่ข่ายได้ โดยผ่านไมโครคอนโทรลเลอร์ที่มีรหัสประจำตัวผลิตภัณฑ์และรหัสประจำตัวผู้ผลิตอยู่ภายใน ดังนั้นในการสร้างกุญแจอิเล็กทรอนิกส์จึงนำ U-Board มาใช้ซึ่งภายในประกอบด้วยไมโครคอนโทรลเลอร์ของบริษัทไมโครชิปเบอร์ PIC16C745 มีรหัสประจำผลิตภัณฑ์และรหัสประจำตัวผู้ผลิตอยู่ภายในและสามารถสื่อสารกับ USB เครื่องแม่ข่าย ได้ ลักษณะเด่นของ U-Board ที่เหมาะกับงานนี้มีดังนี้

- มีส่วนต่อประสานผ่านทางพอร์ต USB
- มีพอร์ตขนานขนาด 8 บิต สำหรับเชื่อมต่อไมโครคอนโทรลเลอร์

- สามารถใช้แรงดันจากพอร์ต USB ได้ไม่จำเป็นต้องใช้แหล่งจ่ายจากภายนอก
- มีขนาดเล็ก

3.2.2 โปรแกรมติดต่อกับ USB ไมโครคอนโทรลเลอร์

เนื่องจากต้องใช้ชิปจากผู้ผลิต ดังนั้นเมื่อนำ U-Board มาใช้งานบริษัทไมโครชิปจึงกำหนดช่องทางในการติดต่อกับ U-Board โดยใช้ส่วนโปรแกรม HIDComm ActiveX Control (.OCX) ซึ่งเป็นไฟล์ที่แนบมาพร้อมกับ U-Board เพื่อให้ผู้ใช้สามารถเขียนโปรแกรมติดต่ออุปกรณ์ผ่านทาง PIC16C745 ได้โดยใช้โปรแกรมวิชวลเบสิก 6.0 ในการติดต่อ จากนั้นออกแบบอุปกรณ์ตามภาพประกอบ 3-2 สังเกตได้ว่าระหว่าง PC กับ U-Board จะติดต่อผ่านพอร์ต USB ระหว่าง U-Board กับ PC2 ใช้สำหรับแสดงผลส่วนอินพุตจะติดต่อผ่านทางพอร์ตขนาน



ภาพประกอบ 3-2 ลักษณะการประกอบอุปกรณ์เพื่อรับส่งข้อมูลผ่านพอร์ต USB

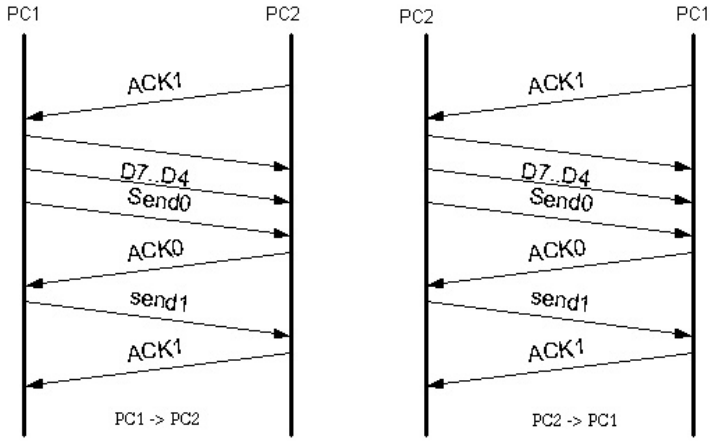
เมื่อออกแบบวงจรตามภาพประกอบ 3-2 และเขียนโปรแกรมด้วยวิชวลเบสิก 6.0 สั่งนำเข้าและส่งออกระหว่าง PC กับ U-Board เรียบร้อยแล้วทดสอบ นำเข้าด้วยการสั่งให้ PC2 ส่งออกสังเกตผลการรับนำเข้าที่หน้าจอ PC1 จากนั้นทดลองส่งข้อมูลออกไปจาก PC1 ผ่าน U-Board ให้แสดงผลตามข้อมูลที่ส่งออกไป ที่ PC2 ซึ่งผลการทดลองปรากฏว่าสามารถรับส่งข้อมูลผ่านพอร์ต USB ได้อย่างถูกต้อง

3.2.3 โปรแกรมรับส่งข้อมูลระหว่าง PC to PC

เนื่องจากในการใช้งานระบบจริงกุญแจอิเล็กทรอนิกส์เปรียบเสมือน PC 1 เครื่อง ดังนั้นจึงจำเป็นต้องจำลอง PC ให้เป็นกุญแจอิเล็กทรอนิกส์ แล้วทำการรับส่งข้อมูลระหว่าง PC โดยผ่านทางพอร์ต USB ดังแสดงในภาพประกอบ 3-3

ภาพประกอบ 3-3 การประกอบอุปกรณ์เพื่อสื่อสารระหว่าง PC 2 เครื่อง

จากภาพประกอบ 3-3 สังเกตได้ว่าการเชื่อมต่อระหว่าง PC1 กับ U-Board จะผ่านทาง USB Port และการเชื่อมต่อระหว่าง PC2 กับ U-Board จะผ่านทางพอร์ตขนานแต่ในการสื่อสารข้อมูลระหว่าง PC 2 เครื่องนั้น นอกจากจะทราบช่องทางในการสื่อสารแล้ว ยังจำเป็นต้องมีข้อตกลงในการสื่อสารหรือเรียกว่าโพรโทคอล ซึ่งได้ออกแบบโพรโทคอลดังแสดงตามภาพประกอบ 3-4



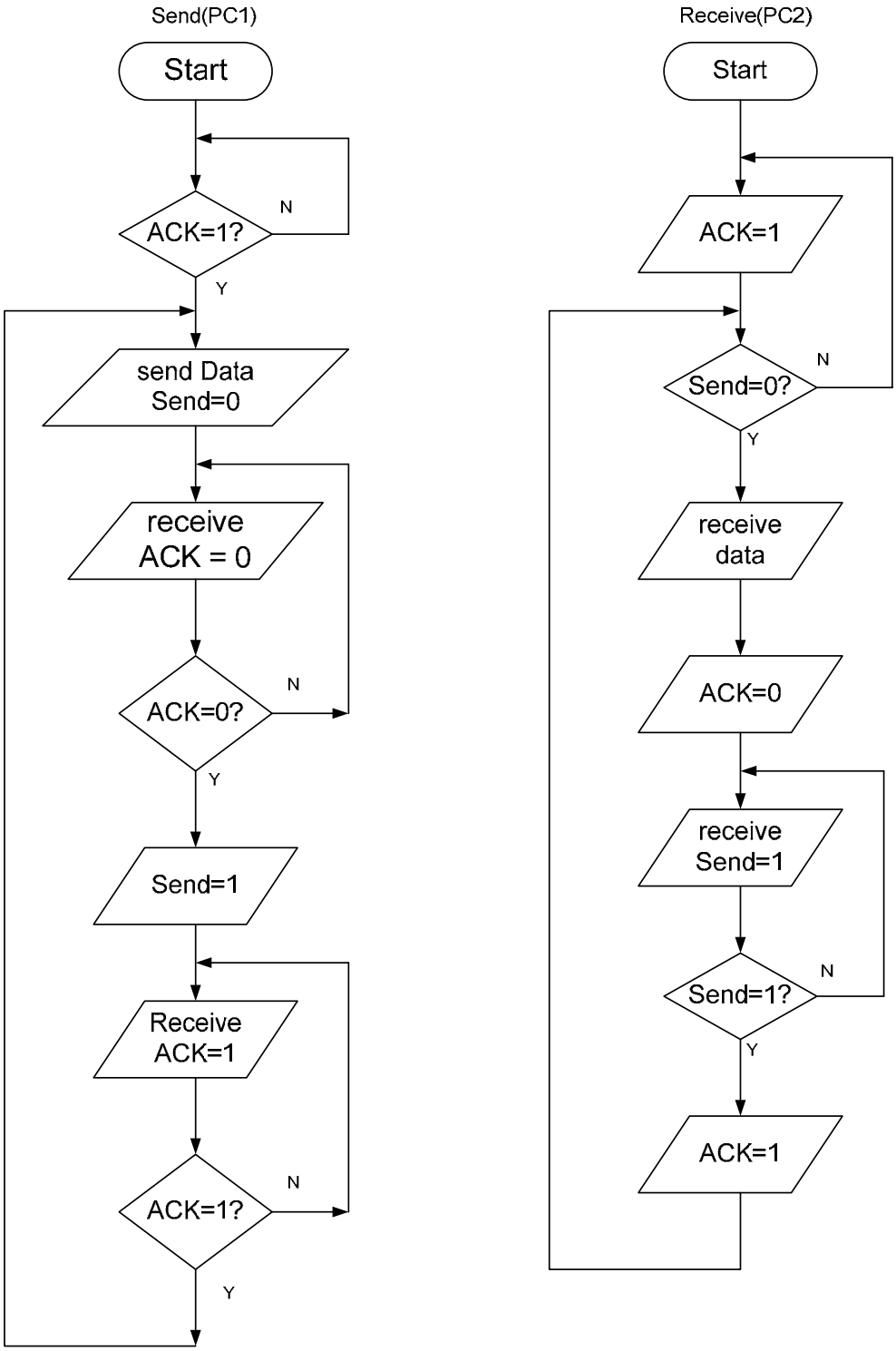
ภาพประกอบ 3-4 โพรโทคอลในการสื่อสารแบบ Stop and Wait

โพรโทคอลคือข้อตกลงในการสื่อสารระหว่างเครื่องคอมพิวเตอร์ 2 เครื่องหรือมากกว่าเพื่อให้สามารถรับส่งข้อมูลระหว่างกันได้อย่างถูกต้องโพรโทคอลจะถูกออกแบบมา เพื่อใช้กับงานแต่ละอย่างเช่น TCP/IP FTP เป็นต้น นอกจากนี้ หากมีข้อผิดพลาดระหว่างการสื่อสารโพรโทคอลสามารถที่จะสื่อให้ปลายทางรับทราบได้หากเกิดข้อผิดพลาดขึ้นภายในระบบ และจะยกเลิกการสื่อสารครั้งนั้น ทั้งนี้ขึ้นอยู่กับผู้ออกแบบโพรโทคอล ทำให้การสื่อสารมีประสิทธิภาพและระบบเกิดความน่าเชื่อถือ

ในการรับส่งข้อมูลทางฝ่ายรับกับฝ่ายส่งต้องใช้โพรโทคอลที่เหมือนกัน ดังนั้น ก่อนที่จะมีการส่งข้อมูลระหว่าง PC ต้องกำหนดให้ PC1 รอสัญญาณ ACK1 จาก PC2 ก่อน นั้นหมายความว่าหาก PC2 พร้อมรับข้อมูล PC2 จะส่ง ACK1 มาให้ PC1 เมื่อ PC1 ได้รับ ACK1 กลับมา PC2 จะส่งข้อมูลที่มีขนาด 4 บิตคือ D7..D4 ขณะนี้ PC2 ยังไม่รับข้อมูล โดยจะรับข้อมูลเมื่อได้รับ Send0 จาก PC1 แล้วเท่านั้น เมื่อ PC2 รับข้อมูลเรียบร้อยแล้วจะส่ง ACK0 ออกไปที่ PC1 เพื่อแจ้งให้ PC1 ทราบว่าขณะนี้ได้รับข้อมูลเรียบร้อยแล้วและ PC1 จะส่ง send1 เพื่อแจ้งให้ PC2 ทราบว่าขณะนี้ PC1 ได้รับทราบแล้วว่า PC2 ได้รับข้อมูลแล้ว ดังนั้น PC2 จะ ACK1 กลับไปที่ PC1 ว่าพร้อมที่จะรับข้อมูลในชุดต่อไปแล้ว ซึ่งข้อมูลในชุดต่อไปก็จะเป็นไปตามทำนองเดียวกันนี้ ดังแสดงในภาพประกอบ 3-4 ในระหว่างการสื่อสารอาจเกิดผิดพลาดได้ ซึ่งเมื่อเกิดความผิดพลาดขึ้นจะต้องรอฝ่ายตรงข้ามเป็นช่วงเวลาหนึ่งจึงหมดเวลา (Time Out) เพื่อเริ่มการสื่อสารใหม่อีกครั้ง

จากภาพประกอบ 3-4 ต้องเขียนโปรแกรมสื่อสารข้อมูลระหว่าง PC ซึ่งก่อนเริ่มต้นเขียนโปรแกรมสามารถนำผังงานมาแยกลำดับงานได้ดังนี้

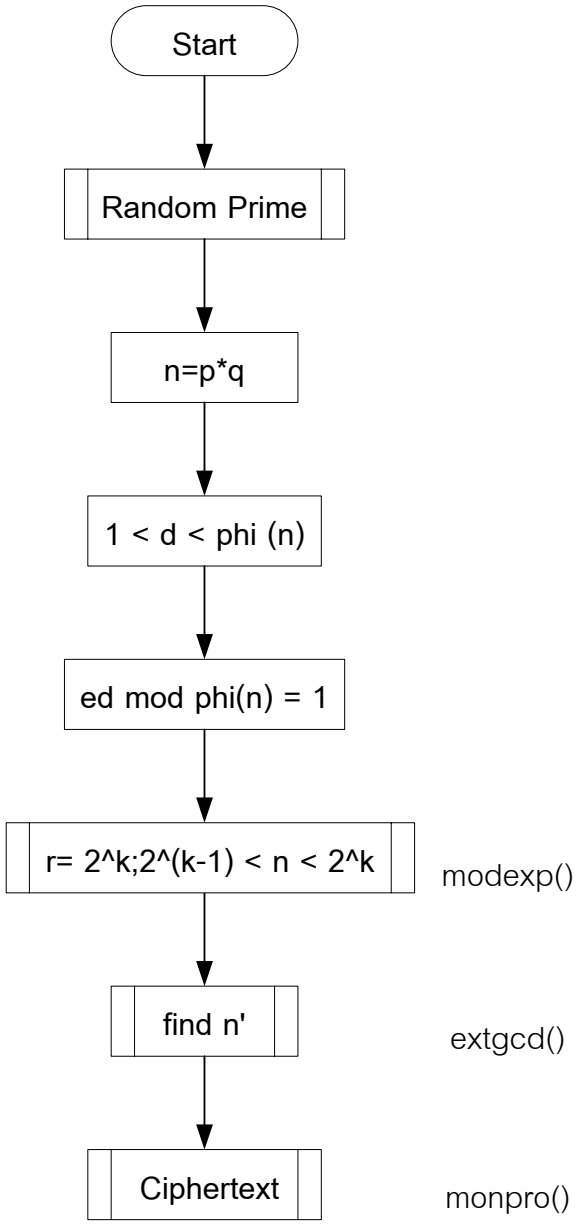
เนื่องจากข้อจำกัดทางด้านพอร์ตขนานของเครื่อง PC ทำให้การรับส่งข้อมูลทำได้ครั้งละ 4 บิตคือ D3…D0 ดังนั้นในการส่งข้อมูลออกทางพอร์ตของ U-Board จึงส่งได้ครั้งละ 4 บิต สำหรับ D4 เป็นบิตที่ใช้ในการตรวจสอบการส่งนั้นคือ send ในภาพประกอบ 3-2 และที่ขา 10 ของพอร์ตขนานจะเป็นส่วนกลับส่วน ACK จะใช้ขา 1 ของพอร์ตขนานในการส่ง เพื่อแจ้งให้ทราบถึงการได้รับข้อมูลแล้วโดยต่อเข้าทางด้าน D4 ของพอร์ตเมื่อประกอบวงจรได้ตามที่ต้องแล้วที่ PC1 เขียนโปรแกรมรับส่งข้อมูลด้วยโปรแกรมวิชวลเบสิกและที่ PC2 เขียนโปรแกรมรับส่งด้วยโปรแกรม Borland C ตามโพรโทคอลที่ออกแบบไว้ซึ่งสามารถรับส่งข้อมูลได้ถูกต้อง



ภาพประกอบ 3-5 ผังงานการสื่อสารระหว่าง PC 2 เครื่อง

3.2.4 โปรแกรมรับส่งข้อมูล โดยเข้ารหัสลับแบบ RSA

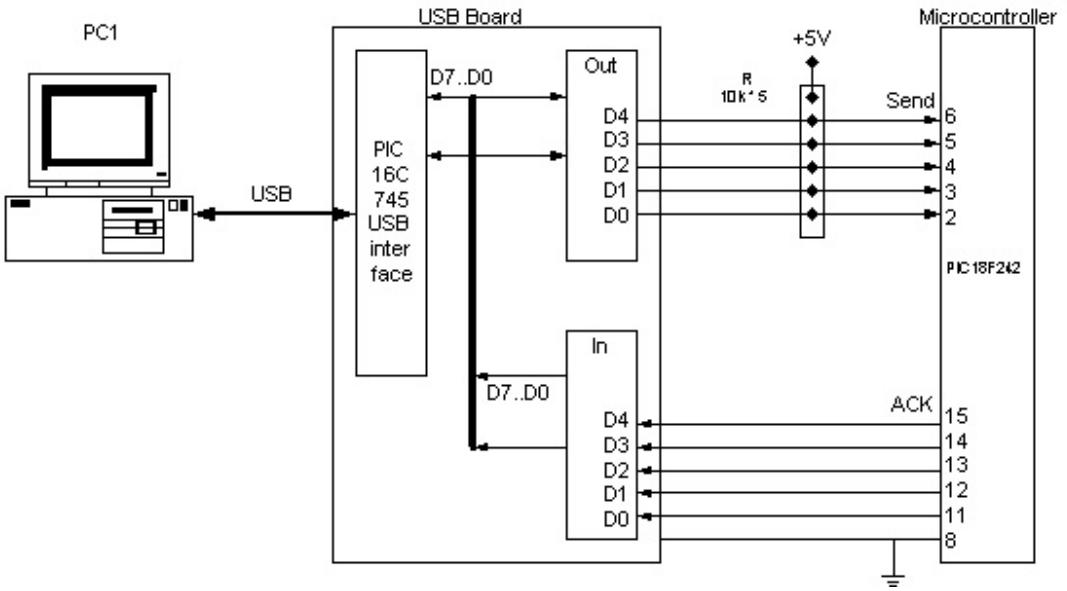
การเขียนโปรแกรมเข้ารหัสลับแบบ RSA เพื่อรับส่งข้อมูลระหว่าง PC 2 เครื่องนั้น จำเป็นต้องเรียนรู้และเข้าใจการเข้ารหัสลับแบบ RSA อย่างครบถ้วน รวมถึงความเข้าใจการลดทอนของ Montgomery จึงจะสามารถเขียนโปรแกรมเข้ารหัสลับข้อมูลและนำไปใช้งานกับระบบจริงได้ ซึ่งทฤษฎีต่าง ๆ ที่กล่าวนี้ สามารถทำความเข้าใจได้ในบทที่ 2 โดยในการเขียนโปรแกรมจริง ต้องวางแผนการเขียนโปรแกรม โดยแยกส่วนต่าง ๆ ออกเป็นฟังก์ชั้นเพื่อใช้สำหรับเข้าและถอดรหัสลับ เนื่องจากฟังก์ชันในการเข้ารหัสลับและถอดรหัสลับเป็นฟังก์ชันเดียวกัน หากวางแผนได้ดีจะทำให้ลดทรัพยากรได้เป็นอย่างมาก รวมถึงสะดวกในการพัฒนาในขั้นต่อไป เพราะหากพิจารณาที่ภาพประกอบ 3-2 ต้อง แปลโค้ดโปรแกรมในภาษา C ทั้งหมดให้เป็น hex ไฟล์จากนั้นโปรแกรมลงในไมโครคอนโทรลเลอร์ ซึ่งมีทรัพยากรที่จำกัดอย่างยิ่ง จึงต้องตระหนักส่วนนี้เป็นพิเศษ และหลังจากเขียนโปรแกรมเรียบร้อยแล้วต้องทดสอบโปรแกรมให้มากที่สุดเท่าที่จะเป็นไปได้ เนื่องจากค่าจำนวนเฉพาะที่สุ่มได้แต่ละครั้งไม่เหมือนกัน รวมถึงค่า e ที่แตกต่างกันไปตามค่าจำนวนเฉพาะ เพื่อให้ทราบถึงเสถียรภาพและเพิ่มความน่าเชื่อถือในระบบ ให้มีประสิทธิภาพสูงสุด การเขียนโปรแกรมเข้าและถอดรหัสลับแบบ RSA และใช้ การลดทอนแบบ Montgomery เป็นไปตามภาพประกอบ 3-6



ภาพประกอบ 3-6 การเข้ารหัสลับแบบ RSA โดยใช้วิธีการลดทอน Montgomery

3.2.5 โปรแกรมบนไมโครคอนโทรลเลอร์

จากการทดลองที่ผ่านมา เป้าหมายของผู้วิจัยคือต้องการเปลี่ยน PC2 ให้เป็นไมโครคอนโทรลเลอร์ เพื่อสร้างเป็นกุญแจอิเล็กทรอนิกส์ โดยใช้ทฤษฎีการลดทอน Montgomery เข้าช่วยในการคำนวณเลขกำลังดังนั้นจึงเลือกไมโครคอนโทรลเลอร์ เบอร์ PIC18F242 ซึ่งเป็นของบริษัทไมโครชิปมาแทนตำแหน่งของ PC2 สามารถประกอบวงจรได้ตามภาพประกอบ 3-7



ภาพประกอบ 3-7 ลักษณะการจัดวงจรเพื่อสื่อสารระหว่าง PC กับไมโครคอนโทรลเลอร์

จุดเด่น PIC18F242 ที่เหมาะกับการนำมาสร้างเป็นกุญแจอิเล็กทรอนิกส์ มีดังนี้

- มีหน่วยความจำโปรแกรมขนาด16 กิโลไบต์
- มีหน่วยความจำชั่วคราวขนาด 768 ไบต์
- ใช้แหล่งจ่ายไฟจากพอร์ต USB ได้
- ต้องการกระแสในการทำงานน้อยกว่า 1 มิลลิแอมแปร์
- มีขนาดเล็ก

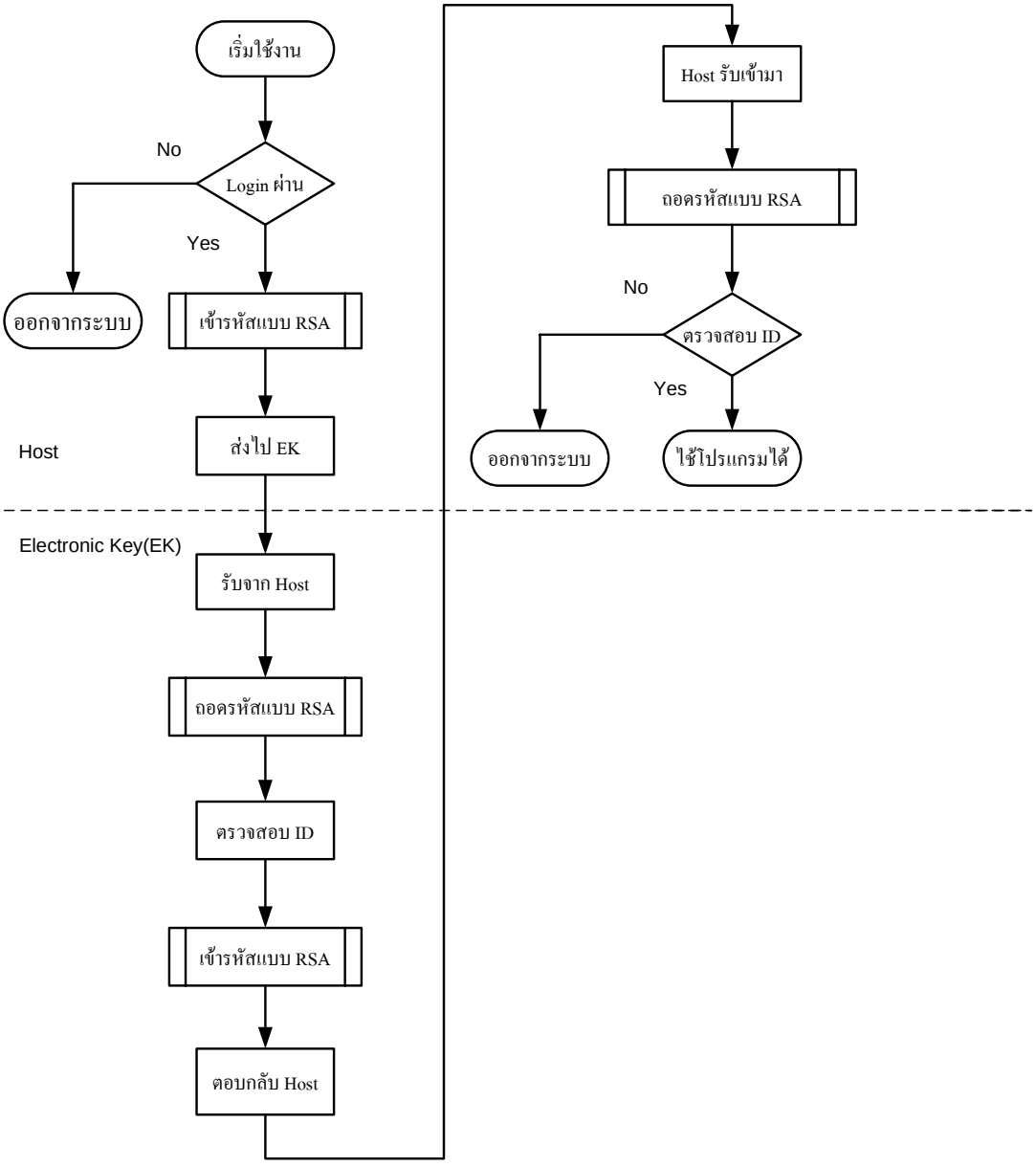
การเขียนโปรแกรมบนไมโครคอนโทรลเลอร์ แตกต่างกับการเขียนโปรแกรมบนเครื่องคอมพิวเตอร์เล็กน้อยขึ้นอยู่กับตัวแปลภาษา (Compiler) ที่ใช้ แต่โดยรวมแล้วลักษณะจะคล้าย ๆ กันกับ Borland C Compiler ซึ่งในงานวิจัยนี้ใช้โปรแกรม PIC C Compiler เมื่อแปลภาษาแล้วจะได้ไฟล์นามสกุล .hex พร้อมที่จะเขียนโปรแกรมลงไมโครคอนโทรลเลอร์

ในการสร้างระบบจริงอาจเกิดการผิดพลาดขึ้นได้ แม้ว่าระบบถูกจำลองให้ทำงานจนถูกต้องบน PC2 แล้วก็ตาม แต่เมื่อแทนที่ PC2 ด้วย ไมโครคอนโทรลเลอร์ สิ่งที่ไม่คาดคิดก็อาจเกิดขึ้นได้ เนื่องจากสภาพแวดล้อมภายในอุปกรณ์ต่างกัน ดังนั้นการตรวจสอบการทำงานของโปรแกรมบน ไมโครคอนโทรลเลอร์ จึงใช้โปรแกรม MPLAB ของบริษัทไมโครชิปโดยทำการตรวจสอบข้อผิดพลาดเพื่อตรวจสอบการทำงาน รวมถึงค่าตัวแปรต่าง ๆที่เกิดขึ้น

3.3 การประยุกต์ใช้งาน

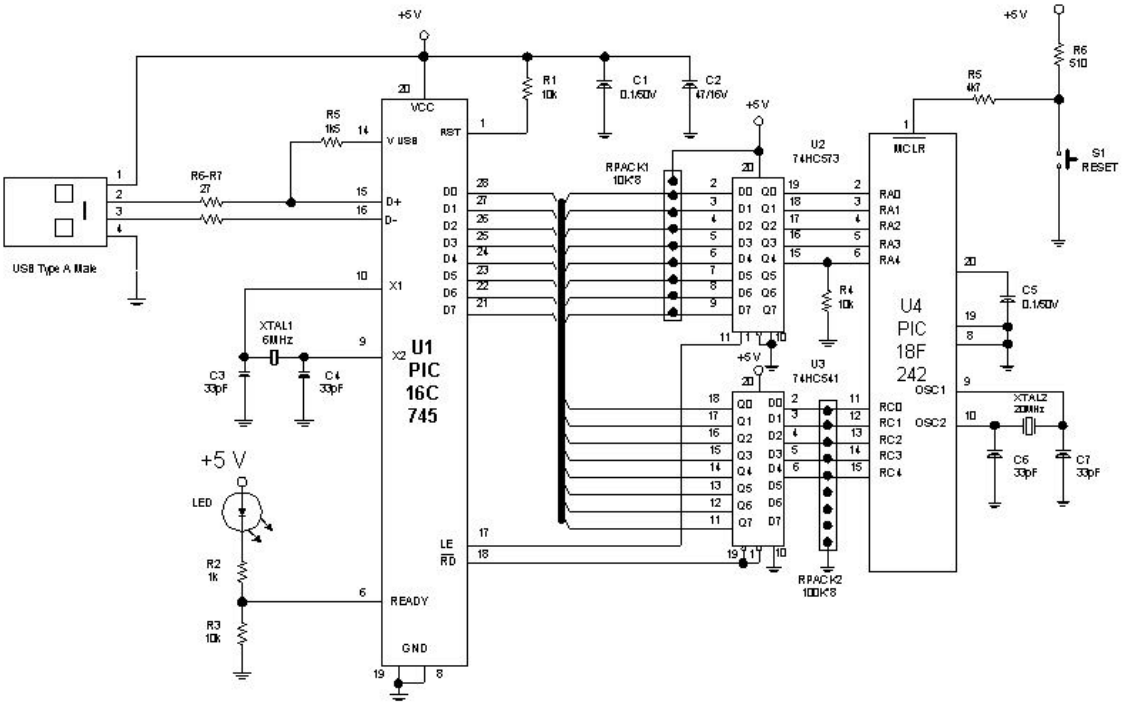
เมื่อดำเนินการออกแบบให้กุญแจอิเล็กทรอนิกส์ทำงานได้ตามที่ต้องการแล้ว สิ่งที่ต้องพิจารณาอีกประการหนึ่งคือความสะดวกในการนำไปประยุกต์ใช้งาน เนื่องจากเมื่อนำไปใช้งานจริง โปรแกรมเมอร์จะต้องนำโค้ดโปรแกรมบางส่วนที่เขียนขึ้นด้วยวิชวลเบสิก 6.0 ของงานวิจัยนี้ไปรวมกับ โค้ดโปรแกรมของโปรแกรมที่ต้องการจำกัดสิทธิ์ ดังนั้นเพื่อความสะดวกในการใช้งานและรักษาความปลอดภัยของโค้ดโปรแกรมในระบบ จึงต้องแยกโค้ดโปรแกรมออกเป็น 2 ส่วนคือ ส่วนที่เป็นไดนามิกส์ลิงค์ไลบรารี่ซึ่งเป็นส่วนที่เข้าและถอดรหัสลับ รวมถึงการตรวจสอบรหัสประจำตัวของกุญแจอิเล็กทรอนิกส์ทำให้โค้ดโปรแกรมมีความปลอดภัยจากผู้นำไปประยุกต์ ส่วนที่ 2 คือโค้ดโปรแกรมที่ใช้ในการติดต่อระหว่างเครื่องแม่ข่ายกับกุญแจอิเล็กทรอนิกส์ จะอยู่ภายนอกไดนามิกส์ลิงค์ไลบรารี่ เมื่อโปรแกรมเมอร์นำไปใช้งานสามารถเขียนโปรแกรมเพื่อตรวจสอบกุญแจอิเล็กทรอนิกส์ได้จากส่วนนี้ โดยผู้วิจัยแสดงตัวอย่าง สำหรับการนำไปประยุกต์ใช้งานจะแสดงไว้ในภาคผนวก ก ภาพรวมของการทำงาน กุญแจอิเล็กทรอนิกส์ ทั้งหมดแสดงในภาพประกอบ 3-8

เมื่อเริ่มต้นใช้งานโปรแกรมที่ต้องการจำกัดสิทธิ์การใช้ โดยผู้ใช้ต้องแสดงสิทธิ์การใช้งานโปรแกรมด้วยการล็อกออน หากล็อกออนได้สำเร็จระบบจะทำการตรวจสอบกุญแจอิเล็กทรอนิกส์ ซึ่งในการตรวจสอบจะส่งข้อมูลที่เข้ารหัสลับแบบ RSA ไปยังกุญแจอิเล็กทรอนิกส์ เมื่อกุญแจอิเล็กทรอนิกส์รับข้อมูลมาจากเครื่องแม่ข่าย ก็จะถอดรหัสลับและประมวลผลจากนั้นกุญแจอิเล็กทรอนิกส์จะเข้ารหัสลับข้อมูลแล้วส่งกลับไปยังเครื่องแม่ข่าย เพื่อให้เครื่องแม่ข่ายรับข้อมูลที่กุญแจอิเล็กทรอนิกส์ตอบกลับมา จะสังเกตได้ว่าในกระบวนการสื่อสารข้อมูลจะถูกเข้ารหัสลับทั้งหมด ซึ่งเมื่อเครื่องแม่ข่ายตรวจสอบการตอบกลับมาของกุญแจอิเล็กทรอนิกส์ ได้ถูกต้องแล้วจึงจะยอมให้ใช้โปรแกรมจำกัดสิทธิ์นี้



ภาพประกอบ 3-8 ผังงานการทำงานของกุญแจอิเล็กทรอนิกส์

ภาพประกอบ 3-9 วงจรของกุญแจอิเล็กทรอนิกส์ โดยที่ U1 ทำหน้าที่ติดต่อกับพอร์ต USB และ U4 ทำหน้าที่ เข้ารหัสลับและถอดรหัสลับแบบ RSA โดยใช้วิธีการลดทอนแบบ Montgomery การติดต่อระหว่าง U1 กับ U4 ผ่านทางพอร์ตขนานโดยมีโพรโทคอลในการสื่อสารดังที่ได้กล่าวมาแล้ว เนื่องจากผู้วิจัยไม่สามารถที่จะแก้ไขโปรแกรมบน U1 ได้ดังนั้น U2 และ U3 ทำหน้าที่เป็น latch ระหว่าง U1 และ U4



ภาพประกอบ 3-9 วงจรของกุญแจอิเล็กทรอนิกส์

3.4 สรุปท้ายบท

เนื้อหาโดยรวมบทนี้ผู้วิจัยจะกล่าวถึงการเริ่มต้นออกแบบและการสร้าง กุญแจอิเล็กทรอนิกส์ ซึ่งเนื้อหาดังกล่าวจะเป็นข้อมูลทางเทคนิคทั้งด้านซอฟแวร์และฮาร์ดแวร์สำหรับรายละเอียดเพิ่มเติมจะกล่าวไว้ที่ภาคผนวก เนื้อหาในบทที่ 4 จะกล่าวถึงการทดสอบการใช้งานกุญแจอิเล็กทรอนิกส์ ซึ่งจะแสดงตามลำดับการทดสอบ เพื่อให้ระบบมีความน่าเชื่อถือสูงสุด