บทที่ 1
บทนำ

1.1 ความสำคัญและที่มาของโครงงาน

โปรแกรมรับส่งสารด่วน เป็นอีกตัวอย่างหนึ่งของความนิยมบนอินเทอร์เน็ตในขณะนี้ ซึ่งโปรแกรมดังกล่าวตอบสนองการให้บริการรับส่งสารได้อย่างทันท่วงทีได้ทุกเวลาและทุกที่ เพื่อการบันเทิงหรือทางธุรกิจโดยเป็นรูปแบบของการสื่อสารที่มีความประหยัดเป็นอย่างมากซึ่งนับได้ว่าเป็นคลื่นลูกใหม่ที่มาแรงแทนที่ความนิยมของ จดหมายอิเล็กทรอนิกส์ อย่างสมบูรณ์แต่เมื่อมองในเรื่องความปลอดภัยเป็นหลักโปรแกรมนี้มิได้คำนึงถึงเรื่องความปลอดภัยไม่ว่าจะเป็นเรื่องการเข้าและถอดรหัสหรือแม้กระทั่งการพิสูจน์ตนของผู้ใช้รวมถึงการขาดความเข้าใจในโปรแกรมของผู้ใช้งานยิ่งพิจารณาถึงปัญหาอาชญากรบนอินเทอร์เน็ตรวมด้วยแล้วจะเห็นได้ว่าปัญหาเรื่องความปลอดภัยเป็นอีกมุมมองหนึ่งที่ควรคำนึงถึงอย่างมากเพื่อสนองความต้องการของผู้ใช้งานได้อย่างครบครัน

ทางผู้พัฒนาจึงได้พัฒนาโครงงาน 2 โครงงานขึ้นมาซึ่งโครงงานแรกเป็นส่วนของการสร้างโปรแกรมแม่ข่ายสำหรับรับส่งสารด่วนแบบปลอดภัย (Secure Instant Messaging Server: IsagMQ) พัฒนาด้วยภาษาซีบนระบบปฏิบัติการตระกูลยูนิกซ์เพื่อทำการออกใบรับรองให้แก่โปรแกรมลูกข่ายและโครงงานที่สองเป็นส่วนของการสร้างโปรแกรมปลั๊กอิน (Secure Instant Messenger: IsagQ) เพื่อความปลอดภัยให้กับโปรแกรมลูกข่ายเกี๊ยม (GAIM) ซึ่งพัฒนาด้วยภาษาซี เพื่อตอบสนองด้านความปลอดภัย 2 ประการหลัก คือ การพิสูจน์ตน เพื่อสร้างความมั่นใจให้กับผู้ใช้ว่ากำลังติดต่ออยู่กับบุคคลที่ต้องการจริงๆและการเข้าและถอดรหัสเพื่อปิดบังข้อมูลที่ถูกส่งผ่านเครือข่าย

1.2 วัตถุประสงค์ของโครงงาน

1.1.1. เพื่อศึกษาการทำงานของระบบรับส่งสารด่วน

1.1.2. เพื่อเพื่อปรับปรุงระบบรับส่งสารด่วนให้มีความปลอดภัยยิ่งขึ้น

1.1.3. เพื่อสร้างโปรแกรมที่สามารถเข้าและถอดรหัสลับข้อความเพื่อทำให้ผู้ใช้มั่นใจได้ว่าข้อความที่ส่งถูกปกปิดเป็นความลับ

1.1.4. เพื่อสร้างโปรแกรมที่สามารถใช้ระบบพิสูจน์ตนเพื่อทำให้ผู้ใช้มั่นใจได้ว่ากำลังติดต่อกับบุคคลที่ต้องการติดต่อจริง

1.1.5. เพื่อสร้างการเชื่อมต่อระหว่างโปรแกรมฝั่งเซิร์ฟเวอร์และฝั่งไคลเอ็นต์โดยสร้างเป็นส่วนขยายของโปรแกรมGaim โดยยังคงความสามารถตามข้อ 1.2.3และ1.2.4

1.3 ขอบเขตของโครงงาน

ในปริญญานิพนธ์ฉบับนี้ได้นำเสนอวิธีการเพิ่มความปลอดภัยในด้านการรักษาความลับของข้อมูล และ การพิสูจน์ตัวตน โดยพัฒนา 2 ส่วนคือ ส่วนขยายของโปรแกรม Gaim (IsagQ)และโปรแกรมแม่ข่าย (IsagMQ) ซึ่งระบบสามารถทำงานได้บนทุกระบบปฏิบัติการโดย IsagMQ สามารถให้บริการพื้นฐานของ Certificate Authority ได้เช่น การออกใบรับรองสิทธิ์ให้กับผู้ใช้ การจัดทำฐานข้อมูลของผู้ใช้ที่ลงทะเบียนแล้ว การเรียกดูใบรับรองสิทธิ์ได้ และ สามารถถอดถอนใบรับรองสิทธิ์ได้ ส่วนIsagQ สามารถลงทะเบียนกับIsagMQอัตโนมัติ โดยสามารถกำหนดขนาดกุญแจส่วนตัวได้เมื่อขอใบรับรองสิทธิ์สามารถพิสูจน์ใบรับรองสิทธิ์ของผู้สนทนาที่ติดตั้ง IsagQได้ สามารถเข้ารหัสข้อมูลแบบกุญแจสาธารณะระหว่างไคลเอนต์ด้วยกัน สามารถขอใบรับรองสิทธิ์ได้เมื่อใบรับรองสิทธิ์หมดอายุและสามารถยกเลิกการลงทะเบียนได้

1.4 วิธีการดำเนินการ

1. วิเคราะห์และออกแบบระบบ
2. ศึกษาโครงสร้างโปรแกรมสนทนา
3. ศึกษาโปรโตคอลเอสเอสแอล ซึ่งนำมาใช้เพิ่มความปลอดภัยให้กับระบบ
4. ศึกษาโครงสร้างกุญแจสาธารณะและการออกใบรับรองสิทธิ์
5. ศึกษาไลบราลี่โอเพนเอสเอสแอล
6. ศึกษาโปรแกรมเกี๊ยม
7. ศึกษาการเขียนจีทีเคพลัส
8. ติดตั้งระบบปฏิบัติการและสภาพแวดล้อมที่จำเป็นต้องใช้ในการพัฒนา
9. พัฒนาส่วนขยายของโปรแกรมเกี๊ยม
10. พัฒนาเซิร์ฟเวอร์และสร้างผู้ออกใบรับรองสิทธิ์
11. สร้างการเชื่อมต่อบนโปรโตคอลเอสเอสแอล ติดตั้งการเข้ารหัสและการพิสูจน์ตัวตน
12. วิเคราะห์ผลของระบบที่ได้ทำการพัฒนาขึ้นและแก้ไขส่วนที่ผิดพลาดเพื่อให้สามารถสร้างระบบที่ใช้งานได้อย่างมีประสิทธิภาพมากที่สุด

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1. ได้รับความรู้ความเข้าใจเกี่ยวกับการเข้ารหัสและถอดรหัส
2. ได้รับความรู้ความเข้าใจเกี่ยวกับการระบุตัวตน
3. ได้รับความรู้ความเข้าใจเกี่ยวกับการเขียนโปรแกรมด้วยภาษาซี
4. ได้รับความรู้ความเข้าใจเกี่ยวกับการใช้งานระบบปฏิบัติการตระกูลยูนิกซ์
5. ระบบไคลเอ็นต์และเซิร์ฟเวอร์ที่ติดต่อกันโดยใช้ระบบพิสูจน์ตัวตนรวมถึงการเข้าและถอดรหัส

1.6 ส่วนประกอบของปริญญานิพนธ์

ปริญญานิพนธ์ฉบับนี้ได้แบ่งเนื้อหาออกเป็น 5 บทด้วยกันคือ

บทที่ 1 กล่าวถึงความสำคัญและที่มาของโครงงาน วัตถุประสงค์ของโครงงาน ขอบเขตของโครงงาน วิธีการดำเนินการ ประโยชน์ที่คาดว่าจะได้รับ และส่วนประกอบของปริญญานิพนธ์

บทที่ 2 กล่าวถึงทฤษฎีพื้นฐานที่ใช้ในการพัฒนาโครงงาน ประกอบด้วย โครงสร้างระบบไคลเอนท์และเซิร์ฟเวอร์สำหรับรับส่งสารด่วน นิยามความมั่นคงปลอดภัยคอมพิวเตอร์ ทฤษฎีสำหรับการส่งข้อมูลบนอินเตอร์เนทให้ปลอดภัยด้วย SSL ทฤษฎีใบรับรองสิทธิ์และทฤษฎีการสร้างผู้ให้บริการใบรับรองสิทธิ์

บทที่ 3 กล่าวถึงการออกแบบซอฟต์แวร์IsagQ และIsagMQ ในปี2547 และ ปี2548 และความแตกต่างระหว่าง IsagMQ และ IsagQ ปีการศึกษา 2547 กับ 2548

บทที่ 4 กล่าวถึงการพัฒนาชิ้นงานของโครงงาน ตั้งแต่การเตรียมสภาพแวดล้อมของทั้งส่วนเซิร์ฟเวอร์ IsagMQ และส่วนไคลเอนต์ IsagQ (ส่วนขยายบน Gaim) การนำโอเพนเอสแอลไลบรารี (OpenSSL Library) มาใช้ในโครงงาน การพัฒนาส่วนขยาย IsagQ กระบวนการรับ-ส่งข้อความของ IsagQ การสร้างผู้ออกใบรับรองสิทธิ์และกระบวนการจัดการใบรับรองสิทธิ์

บทที่ 5 กล่าวถึงการทดลองและผลการทดลองของระบบไคลเอนท์และเซิร์ฟเวอร์ โดยมีการทดสอบการส่งการร้องขอใบรับรองสิทธิ์ระหว่าง IsagQ และ IsagMQ ได้แก่การทดสอบ IsagQ สร้างใบร้องขอใบรับรองสิทธิ์ การทดสอบIsagQ และ IsagMQ สร้างการเชื่อมต่อแบบSSL การทดสอบ IsagMQ สร้างใบรับรองสิทธิ์ และการทดสอบให้ IsagMQ การตรวจใบรับรองสิทธิ์

บทที่ 6 บทนี้กล่าวถึงบทวิจารณ์และบทสรุปของโครงงานนี้ ปัญหาอุปสรรคและแนวทางแก้ไขและแนวทางการพัฒนาต่อ