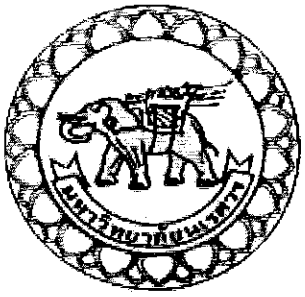


การสร้างระบบอีเมลที่มีการรับรอง

IMPLEMENTING CERTIFIED E-MAIL SYSTEM

นางสาวปวิตรา ฤทธิ์เรืองเดช รหัส 49361119

นางสาวโสภา ห้วยหงษ์ทอง รหัส 49362369

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

สาขาวิชาวิศวกรรมคอมพิวเตอร์ ภาควิชาวิศวกรรมไฟฟ้าและคอมพิวเตอร์

คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนเรศวร

ปีการศึกษา 2552

ใบรับรองโครงงานวิศวกรรม

หัวข้อโครงงาน การสร้างระบบอีเมลที่มีการรับรอง

ผู้ดำเนินโครงงาน นางสาวปวิตรา ฤทธิ์เรืองเดช รหัส 49361119

นางสาวโสภา ห้วยหงษ์ทอง รหัส 49362369

อาจารย์ที่ปรึกษา อาจารย์ภาณุพงศ์ สอนคม

สาขาวิชา วิศวกรรมคอมพิวเตอร์

ภาควิชา วิศวกรรมไฟฟ้าและคอมพิวเตอร์

ปีการศึกษา 2552

.....

คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนเรศวร อนุมัติให้โครงงานฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมคอมพิวเตอร์

คณะกรรมการสอบโครงงานวิศวกรรม

.....ประธานกรรมการ

(อาจารย์ภาณุพงศ์ สอนคม)

.....กรรมการ

(รองศาสตราจารย์ ดร.ไพศาล มุณีสว่าง)

.....กรรมการ

(อาจารย์เศรษฐา ตั้งค้าวานิช)

หัวข้อโครงงาน	การสร้างระบบอีเมลที่มีการรับรอง		
ผู้ดำเนินโครงงาน	นางสาวปวิตรา	ฤทธิ์เรืองเดช	รหัส 49361119
	นางสาวโสภา	ห้วยหงษ์ทอง	รหัส 49362369
อาจารย์ที่ปรึกษา	อาจารย์ภาณุพงศ์	สอนคม	
สาขาวิชา	วิศวกรรมคอมพิวเตอร์		
ภาควิชา	วิศวกรรมไฟฟ้าและคอมพิวเตอร์		
ปีการศึกษา	2552		

บทคัดย่อ

โครงงานการสร้างระบบอีเมลที่มีการรับรองสร้างขึ้นเพื่อแก้ปัญหาการส่งอีเมล โดยที่ผู้ส่งจะทราบวันที่และเวลาที่ผู้รับได้อ่านอีเมล รวมถึงผู้ส่งสามารถป้องกันการถูกแอบอ่านระหว่างทาง ได้มีการออกแบบโปรโตคอลโดยใช้หลักการบุคคลที่สามที่น่าเชื่อถือ (A Light On-line Trusted Third Party) โดยมีเว็บไซต์ทำหน้าที่เป็นบุคคลที่สามที่น่าเชื่อถือ ใช้ภาษาพีเอชพีในการพัฒนาเวปไซต์ ในส่วนของความปลอดภัยได้ใช้อัลกอริทึมการเข้ารหัส – ถอดรหัสข้อความ AES (Rijndael) และอัลกอริทึมการแปลงข้อความโดยเบส 64

ผลที่ได้จากการทำโครงงานคือ มีระบบการรับรองอีเมลไว้ใช้งานได้จริง โดยที่ผู้ส่งเพียงเพิ่มขั้นตอนในการส่งอีเมลเท่านั้น และผู้ส่งจะได้รับหลักฐานการรายงานผลเป็นสิ่งยืนยันว่าผู้รับได้อ่านอีเมลแล้ว

Project Title	IMPLEMENTING CERTIFIED E-MAIL SYSTEM		
Name	Miss. Pawitra	Ritruangdet	ID. 49361119
	Miss. Sopa	Huayhongtong	ID. 49362369
Project Advisor	Mr. Panupong	Sornkhom	
Major	Computing Engineering		
Department	Electrical and Computing Engineering		
Academic Year	2009		

ABSTRACT

This project is conducted by creating a certified emailing system that will be able to solve problems of email receivers. The receivers will be able to retrieve the email and to know when the email was sent or received. Also, the sender will be able to protect their email from hackers during delivery time. The protocol has been designed by using A Light On-line Trusted Third Party method from a trusted website by using PHP development. For security purposes, the algorithm has been designed by using encryption– decryption on AES (Rijndael cipher) and the algorithm encodes the message in Base64.

The result of this project is a trusted emailing system that will be used on email web base system in the real cyber internet business. Sender needs to just add a step for sending, and he / she will get response from the system to confirm that the receipient has already received the email.

กิตติกรรมประกาศ

การจัดทำโครงงานในครั้งนี้สำเร็จลุล่วงไปด้วยดี คณะผู้จัดทำขอขอบพระคุณอาจารย์ที่ปรึกษาโครงงาน อาจารย์ภาณุพงศ์ สอนคม ผู้ซึ่งกรุณาสละเวลา ความคิด และประสบการณ์ให้ความรู้ คำแนะนำ คำปรึกษาอันมีค่ายิ่ง และเอาใจใส่เป็นอย่างดีระหว่างการดำเนินโครงงาน อีกทั้งยังตรวจสอบข้อบกพร่องต่าง ๆ จนโครงงานนี้เสร็จสมบูรณ์

ขอขอบพระคุณรองศาสตราจารย์ ดร.ไพศาล มุณีสว่างและอาจารย์เศรษฐา ตั้งค้าวานิช ที่ท่านกรุณาสละเวลามารับเป็นกรรมการตรวจสอบโครงงาน อีกทั้งยังให้คำแนะนำและตรวจสอบแก้ไขโครงงานให้สมบูรณ์ยิ่งขึ้น

ในโอกาสนี้ทางคณะผู้จัดทำโครงงานจึงขอขอบคุณทุก ๆ ท่านที่มีส่วนช่วยทำให้โครงงานนี้ประสบความสำเร็จลุล่วงไปได้ด้วยดี

ปวิตรา ฤทธิ์เรืองเดช

โสภา ห้วยหงษ์ทอง

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

ตารางที่ **หน้า**

สารบัญรูป

รูปที่ **หน้า**

บทที่ 1
บทนำ

1.1 ที่มาและความสำคัญ

จดหมายอิเลกทรอนิกส์ (Electronic Mail) หรือเรียกสั้น ๆ ว่า อีเมล (E-mail) เป็นที่นิยมกันอย่างมากในปัจจุบัน อีเมลส่งถึงกันผ่านระบบเครือข่าย ผู้ส่งสามารถที่จะส่งอีเมลไปให้ผู้รับซึ่งเป็นสมาชิกของระบบอินเทอร์เน็ตได้โดยไม่จำกัดสถานที่และเวลา อีเมลจะส่งถึงปลายทางอย่างรวดเร็วภายในไม่กี่วินาที หรืออาจส่งจดหมายฉบับเดียวไปถึงผู้รับหลายคนในเวลาเดียวกันได้ อีกทั้งการส่งอีเมลยังสามารถแนบไฟล์ภาพ ไฟล์โปรแกรม และไฟล์ข้อมูลได้

แต่การส่งจดหมายผ่านทางอีเมลมีข้อเสียคือ ผู้ส่งไม่สามารถทราบได้ว่าจดหมายนั้นถึงผู้รับหรือไม่ หรือผู้รับได้เปิดอ่านจดหมายหรือยัง รวมถึงจดหมายจะถูกเปิดอ่านระหว่างทางหรือไม่ จากปัญหาเหล่านี้โครงงานนี้จึงจะสร้างระบบอีเมลที่มีการรับรอง (Certified E-mail) เพื่อแก้ปัญหาดังกล่าวข้างต้น

1.2 วัตถุประสงค์

1. เพื่อศึกษาระบบอีเมลที่มีการรับรอง
2. เพื่อสร้างระบบอีเมลที่มีการรับรอง

1.3 ขอบข่าย

สร้างระบบอีเมลที่มีการรับรอง โดยที่ผู้ส่งจะทราบวันที่และเวลาที่ผู้รับได้อ่านอีเมล รวมถึงผู้ส่งสามารถป้องกันการถูกแอบอ่านระหว่างทาง

1.4 ขั้นตอนดำเนินการ

1. กำหนดนิยามของระบบอีเมลที่มีการรับรอง
2. ศึกษาวิธีการทำระบบอีเมลที่มีการรับรองที่มีอยู่ในปัจจุบัน
3. เลือกวิธีการทำระบบอีเมลที่มีการรับรองที่สนใจมาปรับปรุงและสร้างระบบ
4. ทดสอบระบบอีเมลที่มีการรับรองที่สร้างขึ้น
5. แก้ไข สรุป และประเมินผล
6. จัดทำคู่มือโครงงาน

1.5 แผนการดำเนินงาน

ตารางที่ 1.1 ขั้นตอนการดำเนินโครงงาน

กิจกรรม	เดือน – ปี									
	มิ.ย. 2552	ก.ค. 2552	ส.ค. 2552	ก.ย. 2552	ต.ค. 2552	พ.ย. 2552	ธ.ค. 2552	ม.ค. 2553	ก.พ. 2553	มี.ค. 2553
1. กำหนดนิยามของระบบอีเมลที่มีการรับรอง	←	→								
2. ศึกษาวิธีการทำระบบอีเมลที่มีการรับรองที่มีอยู่ในปัจจุบัน		←	→							
3. เลือกทำระบบอีเมลที่มีการรับรองที่สนใจมาปรับปรุงและสร้างระบบ				←	→	→				
4. ทดสอบระบบอีเมลที่มีการรับรองที่สร้างขึ้น							←	→		
5. แก้ไข สรุป และประเมินผล								←	→	
6. จัดทำคู่มือโครงงาน									←	→

1.6 ผลที่คาดว่าจะได้รับ

1. สามารถเข้าใจระบบอีเมลที่มีการรับรอง
2. สามารถสร้างระบบอีเมลที่มีการรับรอง

1.7 งบประมาณ

1. ค่าพิมพ์เอกสารและถ่ายเอกสาร	1000	บาท
2. ค่าจัดทำรูปเล่ม	1000	บาท
รวมเป็นเงิน	2000	บาท (สองพันบาทถ้วน)

หมายเหตุ – ถัวเฉลี่ยทุกรายการ

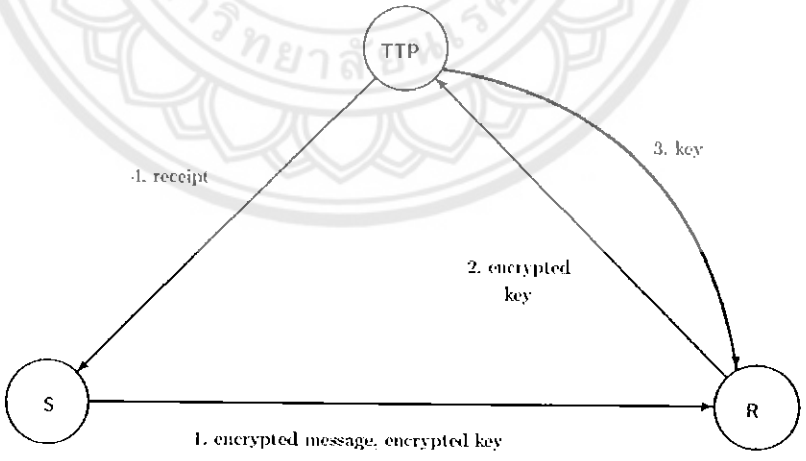
บทที่ 2
หลักการและทฤษฎีเบื้องต้น

2.1 ระบบอีเมลที่มีการรับรอง (Certified E-mail)

ระบบอีเมลที่มีการรับรอง (Certified E-mail) คือ อีเมลที่มีการรับรอง เป็นระบบอีเมลที่ผู้ส่งอีเมลจะทราบวันที่และเวลาที่ผู้รับอีเมลได้เปิดอ่านอีเมล อีกทั้งยังมีการป้องกันการถูกแอบอ่านระหว่างทาง

2.1.1 หลักการ A Light On-line Trusted Third Party

A Light On-line Trusted Third Party (On-line TTP) คือ การรับรองอีเมลโดยมีบุคคลที่สามที่น่าเชื่อถือ (Trusted Third Party : TTP) มาเป็นสื่อกลางระหว่างผู้รับและผู้ส่ง โดยผู้ส่งจะต้องดำเนินการผ่านระบบออนไลน์ โปรโตคอลนี้เป็นวิธีการหนึ่งของระบบอีเมลที่มีการรับรอง มีวัตถุประสงค์มุ่งเน้นในด้านความปลอดภัย การดำเนินการที่ง่าย และสามารถปรับใช้งานได้ โดยที่ผู้รับและผู้ส่งสามารถดำเนินการโดยไม่ต้องใช้ซอฟต์แวร์พิเศษใด ๆ นอกจากอีเมลปกติ และเว็บเบราว์เซอร์ On-line TTP จะมีเซิร์ฟเวอร์รับฝาก สำหรับการแลกเปลี่ยนอีเมลและใบรับรอง ซึ่ง Martin Abadi นักศึกษาภาควิชาวิทยาการคอมพิวเตอร์ มหาวิทยาลัยแห่งแคลิฟอเนีย ได้ศึกษาโปรโตคอลนี้ รวมถึงทำการออกแบบและสร้างระบบขึ้นมา โดยมีโปรโตคอลแสดงดังรูปที่ 2.1 [1]



รูปที่ 2.1 การออกแบบโปรโตคอล [1]

ขั้นตอนการทำงานของโปรโตคอลในรูปที่ 2.1 โดยที่ S คือ ผู้ส่ง, R คือ ผู้รับ, TTP คือ บุคคลที่สามที่น่าเชื่อถือ

1. S ส่งข้อความที่เข้ารหัสและกุญแจที่เข้ารหัสให้ R
2. R ส่งกุญแจที่เข้ารหัสให้ TTP
3. TTP ส่งกุญแจที่ใช้ถอดรหัสข้อความให้ R
4. TTP ส่งใบรับรองให้ S

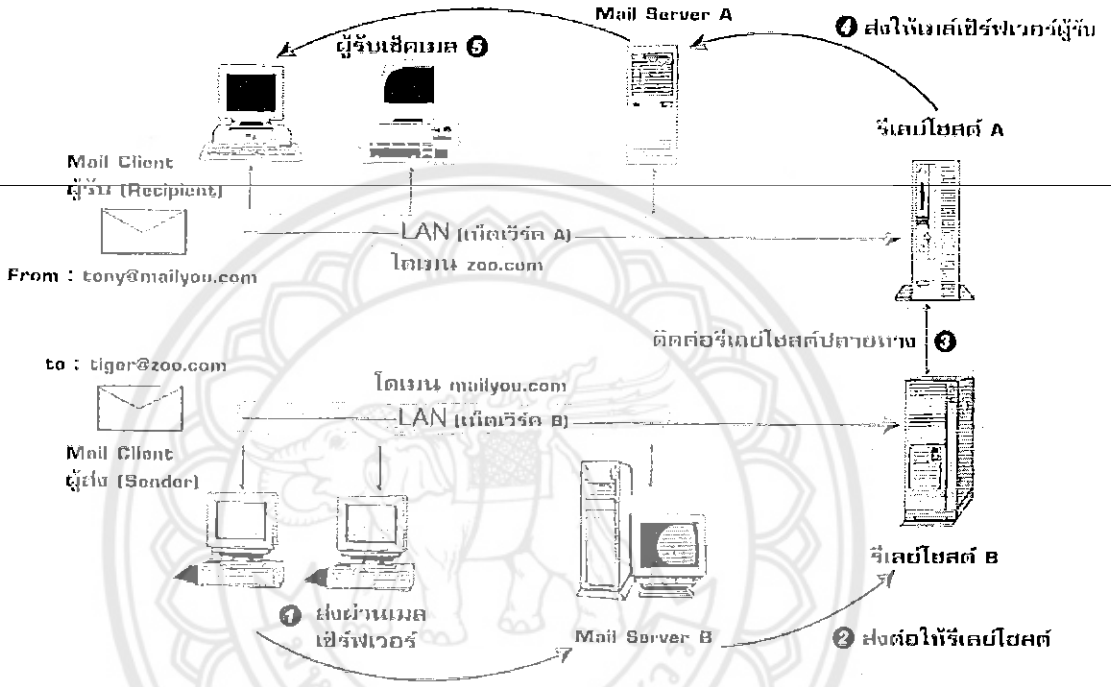
2.2 ระบบอีเมล

อีเมล (E-mail) ย่อมาจาก จดหมายอิเล็กทรอนิกส์หรือไปรษณีย์อิเล็กทรอนิกส์ (Electronic mail) คือวิธีการหนึ่งของการแลกเปลี่ยนข้อความแบบดิจิทัล ซึ่งออกแบบขึ้นเพื่อให้มนุษย์ใช้เป็นหลัก ข้อความนั้นจะต้องประกอบด้วยเนื้อหา ที่อยู่ของผู้ส่ง และที่อยู่ของผู้รับ (ซึ่งอาจมีมากกว่าหนึ่ง) เป็นอย่างน้อย

อีเมลเริ่มใช้กันในปี พ.ศ. 2508 (ค.ศ. 1965) โดยใช้ในการส่งข้อความระหว่างผู้ใช้ภายในเครื่องคอมพิวเตอร์เมนเฟรม ต่อมามีการพัฒนาให้สามารถส่งอีเมลข้ามระหว่างเครื่องคอมพิวเตอร์ได้ โดยระบบแรก ๆ ได้แก่ ระบบ Autodin ซึ่งเป็นระบบเชื่อมโยงข้อมูลของกระทรวงกลาโหมสหรัฐฯ (ปีพ.ศ. 2509) และระบบ Sage ซึ่งใช้ตรวจจับเครื่องบินทิ้งระเบิด ระบบเครือข่ายคอมพิวเตอร์อาร์พาเน็ต (Aapanet) มีส่วนเป็นอย่างมากในการพัฒนาอีเมล มีการทดลองส่งครั้งแรกในเครือข่ายเมื่อปีพ.ศ. 2512 ในปี พ.ศ. 2514 นายเรย์ ทอมลินสัน (Ray Tomlinson) เริ่มใช้เครื่องหมาย @ ในการคั่นระหว่างชื่อผู้ใช้กับชื่อเครื่อง เขายังเขียนโปรแกรมรับส่งอีเมลที่ชื่อ SNDMAIL และ READMAIL อาร์พาเน็ตทำให้อีเมลได้รับความนิยม และอีเมลก็ได้กลายเป็นงานหลักของอาร์พาเน็ต เมื่อประโยชน์ของอีเมลเป็นที่รู้จักมากขึ้น มีการคิดค้นระบบอีเมลที่ติดต่อโดยช่องทางอื่นสำหรับผู้ที่ไม่มีสิทธิ์ใช้เครือข่ายอาร์พาเน็ต เช่น ผ่านเครือข่าย UUCP หรือ VNET ก่อนที่มีการพัฒนาอีเมลที่ค้นหาเส้นทางในการส่งโดยอัตโนมัติ (Auto-routing) การส่งผ่านอีเมลข้ามจากระบบหนึ่งไปยังอีกระบบจำเป็นระบุเส้นทางการส่งโดยใช้เครื่องหมาย ! คั่นชื่อเครื่องระหว่างทาง วิธีนี้สามารถเชื่อมอีเมลจากอาร์พาเน็ต BITNET NSFNET UUCP เข้าด้วยกัน ในช่วงประมาณ พ.ศ. 2520 หน่วยงาน IETF ออกแบบและกำหนดโปรโตคอลในการส่งอีเมลที่มีชื่อว่า SMTP หรือ Simple Mail Transfer Protocol ปัจจุบันโปรโตคอลนี้ถือเป็นมาตรฐานในการรับส่งอีเมลบนอินเทอร์เน็ต [2]

2.2.1 ลักษณะการทำงานของระบบรับส่งอีเมล

ลักษณะการทำงานของระบบอีเมลคล้ายกับระบบไปรษณีย์คือ เริ่มต้นด้วยการเขียนจดหมายขึ้นมา เมื่อเขียนเสร็จจะส่งจดหมายที่ตู้จดหมาย แล้วบุรุษไปรษณีย์จะนำจดหมายไปรวมไว้ที่ทำการไปรษณีย์ เพื่อส่งต่อไปยังที่ทำการไปรษณีย์ปลายทาง แล้วบุรุษไปรษณีย์ปลายทางจะนำส่งถึงผู้รับ



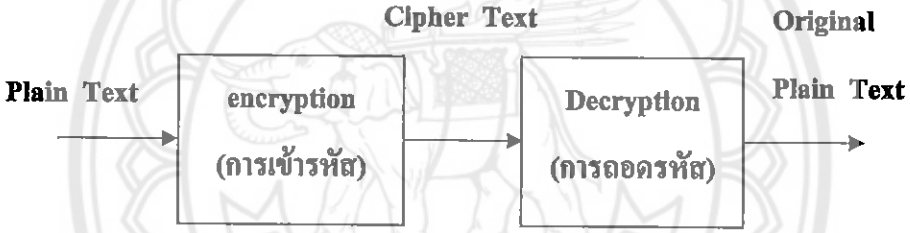
รูปที่ 2.2 ลักษณะการทำงานของระบบอีเมล [3]

ลักษณะการทำงานของระบบอีเมลแสดงดังรูปที่ 2.2 เมื่อผู้ส่งเขียนจดหมายเสร็จก็กดปุ่มส่งผ่านโปรโตคอลส่งไปยังเครื่องอีเมลเซิร์ฟเวอร์ต้นทาง ดังขั้นตอนที่ 1 จากนั้นอีเมลเซิร์ฟเวอร์จะส่งไปยังเครื่องที่เป็นรีเลย์โฮสต์ต้นทาง เนื่องจากรีเลย์โฮสต์เป็นเครื่องที่สามารถติดต่อกับโลกภายนอกได้ ดังขั้นตอนที่ 2 (โดยทั่วไปเครื่องอีเมลเซิร์ฟเวอร์อาจทำหน้าที่เป็นรีเลย์โฮสต์ในเครื่องเดียวกันก็ได้ ดังนั้นก็จะไม่มีขั้นตอนที่ 2 เกิดขึ้น) จากรีเลย์โฮสต์ต้นทางเมื่อได้รับอีเมลมาแล้ว จะติดต่อกับรีเลย์โฮสต์ปลายทางเพื่อส่งอีเมลฉบับนี้ไป ดังขั้นตอนที่ 3 และในกรณีเดียวกันถ้าเครื่องรีเลย์โฮสต์ปลายทางกับเครื่องเมลเซิร์ฟเวอร์ปลายทางเป็นเครื่องเดียวกัน ขั้นตอนที่ 4 จะไม่เกิดขึ้น เมื่ออีเมลถึงอีเมลเซิร์ฟเวอร์ปลายทางเรียบร้อยแล้ว ถือเป็นอันจบกระบวนการส่งอีเมล

เมื่อผู้รับเช็คอีเมลไม่ว่าจะใช้วิธีไหนก็ตามจะต้องติดต่อกับเครื่องอีเมลเซิร์ฟเวอร์ของตนเอง เพื่อนำอีเมลฉบับนั้นมาอ่าน ในที่นี้เครื่องอีเมลเซิร์ฟเวอร์หรือเครื่องรีเลย์โฮสต์จะทำหน้าที่เหมือนกับที่ทำการไปรษณีย์ [3]

2.3 ระบบเข้ารหัส (Cryptography)

ระบบเข้ารหัสโดยพื้นฐานแล้วจะเกี่ยวข้องกับวิธีการทางคณิตศาสตร์เพื่อใช้ในการป้องกันข้อความตั้งต้นที่ต้องการส่งไปถึงผู้รับ ข้อความตั้งต้นจะถูกแปรเปลี่ยนไปสู่ข้อความอีกรูปแบบหนึ่งที่ไม่สามารถอ่านเข้าใจได้โดยใครก็ตามที่ไม่มีกุญแจสำหรับเปิดดูข้อความนั้น เรียกกระบวนการในการแปรรูปของข้อความตั้งต้นว่าการเข้ารหัส (Encryption) และกระบวนการในการแปลงข้อความที่ไม่สามารถอ่าน และทำความเข้าใจให้กลับไปสู่ข้อความดั้งเดิม ว่าการถอดรหัส (Decryption) ดังแสดงในรูปที่ 2.3 [4]



รูปที่ 2.3 ระบบเข้ารหัสโดยทั่วไป

ข้อความที่สามารถอ่านได้ เรียกว่า Plain Text หรือ Clear Text, ข้อความที่เข้ารหัสแล้วเรียกว่า Cipher Text

2.3.1 จุดประสงค์ของระบบเข้ารหัส

1. การทำให้ข้อความเป็นความลับ เพื่อป้องกันไม่ให้ผู้ที่ไม่มีสิทธิ์ในการเข้าถึงข้อความสามารถเข้าถึงข้อความได้

2. การทำให้ข้อความสามารถตรวจสอบความสมบูรณ์ได้ เพื่อป้องกันข้อความให้อยู่ในสภาพเดิมอย่างสมบูรณ์ กล่าวคือในกระบวนการสื่อสารนั้นผู้รับได้รับข้อความที่ถูกต้องตามที่ผู้ส่งส่งมาให้โดยข้อความจะต้องไม่มีการสูญหายหรือถูกเปลี่ยนแปลงแก้ไขใด ๆ

3. การทำให้สามารถพิสูจน์ตัวตนของผู้ส่งข้อความได้ เพื่อให้สามารถตรวจสอบได้ว่าใครคือผู้ส่งข้อความ เพื่อป้องกันการแอบอ้างได้ [4]

2.3.2 ปัจจัยที่ทำให้เกิดความปลอดภัยของข้อความที่เข้ารหัสแล้ว

1. ความยาวของกุญแจเข้ารหัส ปกติกุญแจเข้ารหัสจะมีความยาวเป็นบิต ยิ่งจำนวนบิตของกุญแจยิ่งมาก ยิ่งทำให้การเดาเพื่อสุ่มหากุญแจที่ถูกต้องเป็นไปได้ยากยิ่งขึ้น (เช่น กุญแจขนาด 1 บิต จะสามารถแทนตัวเลขได้ 2 ค่าคือ 0 กับ 1 กุญแจขนาด 2 บิต จะเป็นไปได้ 4 ค่าคือ 0, 1, 2, 3 เป็นต้น)

2. การเก็บกุญแจเข้ารหัสไว้อย่างเป็นความลับ ผู้เป็นเจ้าของกุญแจลับหรือส่วนตัวต้องระมัดระวังไม่ให้กุญแจสูญหายหรือล่วงรู้โดยผู้อื่น [4]

2.3.3 ประเภทของระบบเข้ารหัส

ระบบเข้ารหัสแบ่งออกเป็นได้สองประเภทคือ

2.3.3.1 ระบบเข้ารหัสแบบกุญแจอสมมาตร (Asymmetric-key cryptography or Public Key Technology)

อัลกอริทึมนี้จะใช้กุญแจสองตัวเพื่อทำงาน ตัวหนึ่งใช้ในการเข้ารหัสและอีกตัวหนึ่งใช้ในการถอดรหัสข้อความที่เข้ารหัสมาโดยกุญแจตัวแรก อัลกอริทึมกลุ่มสำคัญในแบบอสมมาตรนี้คือ อัลกอริทึมแบบกุญแจสาธารณะ (Public keys Algorithms) ซึ่งใช้กุญแจที่เรียกกันว่ากุญแจสาธารณะ (Public keys) ในการเข้ารหัสและใช้กุญแจที่เรียกกันว่า กุญแจส่วนตัว (Private keys) ในการถอดรหัสข้อความนั้น กุญแจสาธารณะนี้สามารถส่งมอบให้กับผู้อื่นได้ เช่น เพื่อนร่วมงานที่เราต้องการติดต่อด้วย หรือแม้กระทั่งวางไว้บนเว็บไซต์เพื่อให้ผู้อื่นสามารถดาวน์โหลดไปใช้งานได้ สำหรับกุญแจส่วนตัวนั้นต้องเก็บไว้กับผู้เป็นเจ้าของกุญแจส่วนตัวเท่านั้นและห้ามเปิดเผยให้ผู้อื่นทราบโดยเด็ดขาด

ข้อดีของระบบเข้ารหัสแบบกุญแจอสมมาตร คือ การบริหารจัดการกุญแจทำได้ง่ายกว่า เพราะใช้กุญแจในการเข้ารหัส - ถอดรหัสข้อความต่างกัน และสามารถระบุผู้ใช้โดยการใช้ร่วมกับลายมือชื่ออิเล็กทรอนิกส์ ส่วนข้อเสียคือ ใช้เวลาในการเข้า - ถอดรหัสข้อความค่อนข้างนาน เพราะต้องใช้การคำนวณอย่างมาก

อัลกอริทึมสำหรับการเข้ารหัสแบบกุญแจสาธารณะ (หรือการเข้ารหัสแบบอสมมาตร) ข้างล่างนี้จะนำเสนอเพียงจำนวนหนึ่งเท่านั้น

1. อัลกอริทึม RSA ได้รับการพัฒนาขึ้นที่มหาวิทยาลัย MIT ในปี 1977 โดยศาสตราจารย์ 3 คน ซึ่งประกอบด้วย Ronald Rivest, Adi Shamir และ Leonard Adleman ชื่อของอัลกอริทึมได้รับการตั้งชื่อตามตัวอักษรตัวแรกของนามสกุลของศาสตราจารย์ทั้งสามคน อัลกอริทึมนี้สามารถใช้ในการเข้ารหัสข้อมูลรวมทั้งการลงลายมือชื่ออิเล็กทรอนิกส์ด้วย

2. อัลกอริทึม DSS ย่อมาจาก Digital Signature Standard อัลกอริทึมนี้ได้รับการพัฒนาขึ้นมาโดย National Security Agency ในประเทศสหรัฐอเมริกาและได้รับการรับรองโดย NIST ให้เป็นมาตรฐานกลางสำหรับการลงลายมือชื่ออิเล็กทรอนิกส์ในประเทศสหรัฐอเมริกา [5]

2.3.4.2 ระบบเข้ารหัสแบบกุญแจสมมาตร (Symmetric-key cryptography)

อัลกอริทึมแบบนี้จะใช้กุญแจที่เรียกว่า กุญแจลับ (Secret key) ซึ่งมีเพียงหนึ่งเดียวเพื่อใช้ในการเข้า - ถอดรหัสข้อความที่ส่งไป อัลกอริทึมสามารถแบ่งย่อยออกเป็น 2 ประเภท ได้แก่ แบบบล็อค (Block Algorithms) ซึ่งจะทำการเข้ารหัสทีละบล็อค (1 บล็อคประกอบด้วยหลายไบต์ เช่น 64 ไบต์ เป็นต้น) และแบบสตรีม (Stream Algorithms) ซึ่งจะทำการเข้ารหัสทีละไบต์

ข้อดีของระบบเข้ารหัสแบบกุญแจสมมาตรคือ มีความรวดเร็ว เพราะใช้เวลาในการคำนวณที่น้อย และสามารถสร้างได้ง่าย ส่วนข้อเสียคือ การบริหารจัดการกุญแจทำได้ยากเพราะกุญแจในการเข้า - ถอดรหัสข้อความเหมือนกัน

อัลกอริทึมสำหรับการเข้ารหัสแบบสมมาตรในปัจจุบันมีเป็นจำนวนมาก ข้างล่างนี้นำเสนอเพียงจำนวนหนึ่งเท่านั้น

1. อัลกอริทึม DES ย่อมาจาก Data Encryption Standard อัลกอริทึมนี้ได้รับการรับรองโดยรัฐบาลสหรัฐอเมริกาในปี ค.ศ. 1977 ให้เป็นมาตรฐานการเข้ารหัสข้อความสำหรับหน่วยงานของรัฐทั้งหมด ในปี 1981 อัลกอริทึมยังได้รับการกำหนดให้เป็นมาตรฐานการเข้ารหัสข้อความในระดับนานาชาติตามมาตรฐาน ANSI (American National Standards) อีกด้วย DES เป็นอัลกอริทึมแบบบล็อคซึ่งใช้กุญแจที่มีขนาดความยาว 56 บิตและเป็นอัลกอริทึมที่มีความแข็งแกร่ง แต่เนื่องด้วยขนาดความยาวของกุญแจที่มีขนาดเพียง 56 บิต ซึ่งในปัจจุบันถือได้ว่าสั้นเกินไป ผู้บุกรุกอาจใช้วิธีการลองผิดลองถูกเพื่อค้นหากุญแจที่ถูกต้องสำหรับการถอดรหัสได้ ในปี 1998 ได้มีการสร้างเครื่องคอมพิวเตอร์พิเศษขึ้นมาซึ่งมีมูลค่า 250,000 เหรียญสหรัฐ เพื่อใช้ในการค้นหากุญแจ

ที่ถูกต้องของการเข้ารหัสข้อมูลหนึ่ง ๆ ด้วย DES และพบว่าเครื่องคอมพิวเตอร์นี้สามารถค้นหากุญแจที่ถูกต้องได้ภายในระยะเวลาไม่ถึงหนึ่งวัน

2. อัลกอริทึม Triple-DES เป็นอัลกอริทึมที่เสริมความปลอดภัยของ DES ให้มีความแข็งแกร่งมากขึ้น โดยใช้อัลกอริทึม DES เป็นจำนวนสามครั้งเพื่อทำการเข้ารหัส แต่ละครั้งจะใช้กุญแจในการเข้ารหัสที่แตกต่างกัน ดังนั้นจึงเปรียบเสมือนการใช้กุญแจเข้ารหัสที่มีความยาวเท่ากับ 56*3 = 168 บิต Triple-DES ได้ถูก ใช้งานกับสถาบันทางการเงินอย่างแพร่หลาย รวมทั้งใช้งานกับโปรแกรม Secure Shell (ssh) ด้วย การใช้อัลกอริทึม DES เพื่อเข้ารหัสเป็นจำนวนสองครั้งด้วยกุญแจสองตัว (56*2=112 บิต) ยังถือได้ว่าไม่ปลอดภัยอย่างพอเพียง

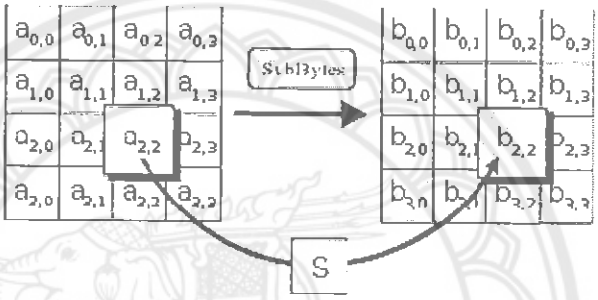
3. อัลกอริทึม Blowfish เป็นอัลกอริทึมที่มีความรวดเร็วในการทำงาน มีขนาดเล็กกระทัดรัด และใช้การเข้ารหัสแบบบล็อค ผู้พัฒนาคือ Bruce Schneier อัลกอริทึมสามารถใช้กุญแจที่มีขนาดความยาวตั้งแต่ไม่มากนักไปจนถึงขนาด 448 บิต ซึ่งทำให้เกิดความยืดหยุ่นสูงในการเลือกใช้กุญแจ รวมทั้งอัลกอริทึมยังได้รับการออกแบบมาให้ทำงานอย่างเหมาะสมกับหน่วยประมวลผลขนาด 32 หรือ 64 บิต Blowfish ได้เปิดเผยสู่สาธารณะและไม่ได้มีการจดสิทธิบัตรใด ๆ นอกจากนั้นยังใช้ในโปรแกรม SSH และอื่น ๆ

4. อัลกอริทึม RC4 อัลกอริทึมนี้เป็นอัลกอริทึมแบบสตรีม ซึ่งได้รับการพัฒนาขึ้นมาโดย Ronald Riverst และถูกเก็บเป็นความลับทางการค้าโดยบริษัท RSA Data Security ในภายหลังอัลกอริทึมนี้ได้รับการเปิดเผยใน Usenet เมื่อปี ค.ศ. 1994 และเป็นที่ทราบกันว่าเป็นอัลกอริทึมที่มีความแข็งแกร่งโดยสามารถใช้ขนาดความยาวของกุญแจที่มีขนาดตั้งแต่ 1 บิตไปจนกระทั่งถึงขนาด 2048 บิต

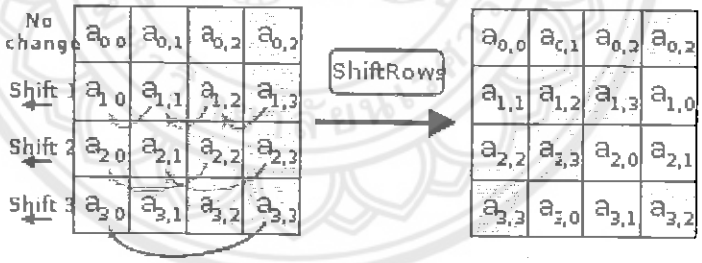
5. อัลกอริทึม AES (Rijndael) อัลกอริทึมนี้ได้รับการพัฒนาโดย Joan Daemen และ Vincent Rijmen ในปี 2000 อัลกอริทึมได้รับการคัดเลือกโดยหน่วยงาน National Institute of Standard and Technology (NIST) ของสหรัฐอเมริกาให้เป็นมาตรฐานในการเข้ารหัสชั้นสูงของประเทศ อัลกอริทึมมีความเร็วสูงและมีขนาดกะทัดรัดโดยสามารถใช้กุญแจที่มีความยาวขนาด 128, 192 และ 256 บิต [5]

การเข้ารหัสของ AES (Rijndael) ในแต่ละรอบนั้น จะใช้เทคนิค 4 ขั้นตอนคือ

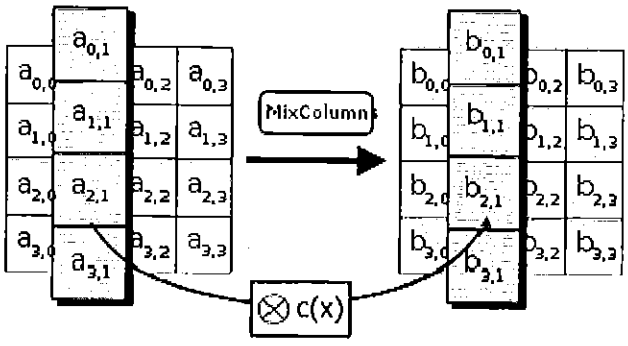
1. SubBytes คือ การใช้ S – box ในการสลับข้อมูลระหว่างสองบล็อก ดังแสดงในรูปที่ 2.4
2. ShiftRows คือ การเลื่อนข้อมูลระหว่างแถว ดังแสดงในรูปที่ 2.5
3. MixColumns คือ การรวมข้อมูลในแต่ละคอลัมน์ ดังแสดงในรูปที่ 2.6
4. AddRoundKey คือ การนำข้อมูลแต่ละไบต์มาบวกกับคีย์โดยใช้ XOR ดังแสดงในรูปที่ 2.7



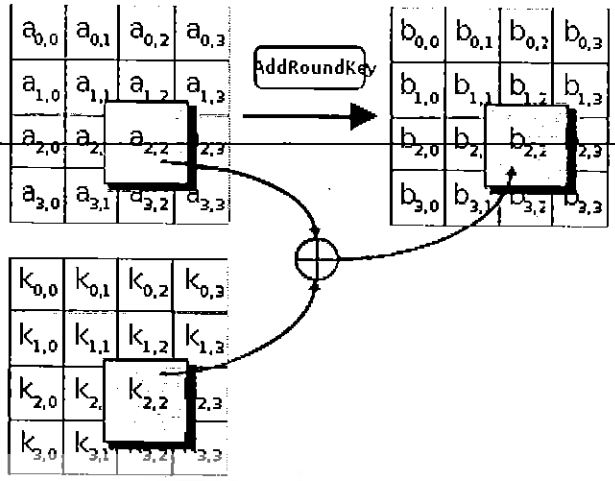
รูปที่ 2.4 ขั้นตอน SubBytes [6]



รูปที่ 2.5 ขั้นตอน ShiftRows [6]



รูปที่ 2.6 ขั้นตอน MixColumns [6]



รูปที่ 2.7 ขั้นตอน AddRoundKey [6]

2.4 เบส 64 (Base 64)

เบส 64 เป็นวิธีแปลงข้อความที่เป็นไบนารีหรือข้อความที่มีตัวอักษรพิเศษไปเป็นข้อความที่เป็นตัวอักษร 64 ตัว เป็นที่มาของชื่อเบส 64 คือ หนึ่งหลักมีเลขอยู่ 64 ตัว ประกอบไปด้วย 0-9 (10 ตัว) A-Z (26 ตัว) a-z (26 ตัว) รวมเป็น 62 ตัวบวกกับ symbol อีกสองตัว

การแปลงข้อความ (Encode) ไปเป็นเบส 64 มีหลักอยู่ว่า ข้อความปลายทางแต่ละตัว มีความเป็นไปได้ 64 ตัวอักษร 64 คือ 2 ยกกำลัง 6 ดังนั้นเราต้องการข้อความต้นทางแค่ 6 บิต สำหรับข้อความปลายทางแต่ละตัว (8 บิต) หรือคือ เอาข้อความต้นทางมาทีละ 6 บิต กลับเป็นข้อมูลปลายทาง 8 บิต ตอนทำกลับ (Decode) ก็เอาข้อความมาทีละตัว (8 บิต) แล้วกลับเป็น 6 บิต ใส่กลับไปเป็นผลลัพธ์

ข้อเสียของเบส 64 คือ ขนาดของข้อความไบนารีที่ถูก Encode ด้วยเบส 64 จะมีขนาดของข้อความที่ใหญ่ขึ้นกว่าขนาดเดิมที่เป็นไฟล์ไบนารีพอสมควร [7]

2.4.1 ขั้นตอนการ Encode เบส64

1. เปลี่ยน "Chaiyanan" ให้อยู่ในรูปของเลขฐาน 2 โดยแอสกี เติมบิต 0 เข้าไป บิตแรกสุดให้ครบ 8 บิตจะได้

01000011 01101000 01100001 01101001 01111001 01100001 01101110 01100001 01101110

2. จากนั้นจัดเรียงบิตใหม่จากด้านซ้ายให้เป็นกลุ่มละ 6 บิตจะได้

010000 110110 100001 100001 011010 010111 100101 100001 011011 100110 000101 101110

3. เปลี่ยนเลขฐาน 2 แบบ 6 บิตที่ได้ให้เป็นเลขฐาน 10 จะได้

เลขฐาน 2 = *010000 110110 100001 100001 011010 010111 100101 100001 011011 100110 000101 101110*

เลขฐาน 10 = *16 52 33 33 26 23 37 33 27 38 5 46*

4. นำไปเปรียบเทียบกับตารางเบส64 จะได้อักษร คือ *Q2hhaXlhbmFu*

กรณีที่เมื่อมีการจัดกลุ่มเลขฐาน 2 กลุ่มละ 6 บิต ถ้าบิตกลุ่มสุดท้ายมี 2 หรือ 4 บิตให้เพิ่มบิต 0 เข้าไปให้ครบ 6 บิตโดยในเบส 64 จะนับบิตสุดท้ายที่เป็น 00 แทนด้วย = เช่น xxxxxx xxxxxx ... ... 011101 11*0000* เมื่อเปลี่ยนเป็นรหัสเบส64 จะได้ ... d**w==**

2.4.2 ขั้นตอนการ Decode เบส64

1. นำเอาชุดของตัวอักษรเปลี่ยนเป็นเลขฐาน 2 ตามตารางเบส 64
2. จัดกลุ่มของเลขฐาน 2 เป็นกลุ่มละ 8 บิต
3. นำตัวเลขกลุ่มละ 8 บิตไปเทียบกับตารางแอสกี
4. จะได้ชุดของตัวอักษรของแอสกี [8]

ตารางที่ 2.1 ตารางรหัสเบส 64 [8]

เลขฐาน 10	ตัวอักษร	เลขฐาน 10	ตัวอักษร	เลขฐาน 10	ตัวอักษร	เลขฐาน 10	ตัวอักษร
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

ตารางที่ 2.2 ตารางรหัสแอสกี [9]

b7	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
b6	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
b5	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
b4	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
b3	b2	b1	b0													
0	0	0	0					@	P	`	p			ฐ	ภ	ะ	เ	๐
0	0	0	1					!	A	Q	a	q		ก	ฑ	ม	ั	แ	๑
0	0	1	0					"	B	R	b	r		ข	ฒ	ย	า	โ	๒
0	0	1	1					#	C	S	c	s		ฃ	ณ	ร	ำ	ใ	๓
0	1	0	0					$	D	T	d	t		ค	ด	ฤ	ิ	ไ	๔
0	1	0	1					%	E	U	e	u		ฅ	ต	ล	ี	ๅ	๕
0	1	1	0					&	F	V	f	v		ฆ	ถ	ฦ	ึ	ๆ	๖
0	1	1	1					'	G	W	g	w		ง	ท	ว	ื	็	๗
1	0	0	0					(	H	X	h	x		จ	ธ	ศ	ุ	่	๘
1	0	0	1					)	I	Y	i	y		ฉ	น	ษ	ู	้	๙
1	0	1	0					*	J	Z	j	z		ช	บ	ส	ฺ	๊	๚
1	0	1	1					+	K	[	k	{		ซ	ป	ห		๋	๛
1	1	0	0					,	L	\	l	|		ฌ	ผ	ฬ		์	
1	1	0	1					-	M	]	m	}		ญ	ฝ	อ		๎	
1	1	1	0					.	N	^	n	~		ฎ	พ	ฮ		๏	
1	1	1	1					/	O	_	o			ฏ	ฟ	ฯ	฿	๏	

2.5 มาโครมีเดีย ดรีมวีฟเวอร์ 8 (Macromedia Dreamweaver 8)

มาโครมีเดียว ดรีมวีฟเวอร์ 8 เป็นโปรแกรมสำหรับการสร้างเว็บเพจ บริหารจัดการเว็บไซต์ รวมไปถึงการพัฒนาเว็บแอปพลิเคชัน เนื่องจากโปรแกรมดรีมวีฟเวอร์มีความสามารถที่โดดเด่น ดังนี้

- สามารถเขียนโปรแกรมสำหรับเว็บได้ทุกรูปแบบ เช่น ASP, ASP.Net, ColdFusion, bJSP, PHP, XML, XHTML
- มีการปรับปรุงกลไกภายในให้มีประสิทธิภาพสูงขึ้น
- สามารถสร้างแอปพลิเคชันง่ายๆ โดยไม่จำเป็นต้องเขียนโปรแกรม
- สร้างเว็บเพจภาษาไทยได้ทันทีโดยไม่ต้องติดต้องโปรแกรมเสริม เพราะดรีมวีฟเวอร์รองรับตัวอักษรแบบยูนิโค้ด
- โปรแกรมจะทำการแปลงรหัสให้เป็นภาษาเอชทีเอ็มแอล โดยอัตโนมัติดังนั้น ผู้ใช้ที่ไม่มีความรู้ ด้านนี้ก็สามารถทำได้
- มีแถบเครื่องมือ หรือแถบคำสั่ง ที่ใช้ในการควบคุมการทำงาน แบ่งออกเป็นหมวดหมู่จึงช่วยในการทำงานที่ดีขึ้นและรวดเร็วยิ่งขึ้น
- มีคุณสมบัติที่สามารถจัดการกับรูปภาพเคลื่อนไหว โดยไม่ต้องอาศัยปลั๊กอิน
- สามารถเรียกใช้ตารางจากภายนอก โดยการอิมพอร์ทจาก Text File
- เป็นโปรแกรมที่สามารถสนับสนุนการใช้งาน CSS (Cadcading Style Sheet)
- มีความสามารถในการทำ Drop Down Menu รวมไปถึงการทำให้รูปภาพเปลี่ยนเมื่อนำเมาส์ไปชี้ เป็นต้น

2.6 พีเอชพี (PHP)

พีเอชพี เป็นภาษาจำพวกภาษาสคริปต์ (script) คำสั่งต่าง ๆ จะเก็บอยู่ในไฟล์ที่เรียกว่าสคริปต์ และเวลาใช้งานต้องอาศัยตัวแปลชุดคำสั่ง ตัวอย่างของภาษาสคริปต์ เช่น JavaScript , Perl เป็นต้น ลักษณะของพีเอชพีที่แตกต่างจากภาษาสคริปต์แบบอื่น ๆ คือ พีเอชพีได้รับการพัฒนาและออกแบบมาเพื่อใช้งานในการสร้างเอกสารแบบเอชทีเอ็มแอล โดยสามารถสอดแทรกหรือแก้ไขเนื้อหาได้โดยอัตโนมัติ ดังนั้นจึงกล่าวว่าพีเอชพีเป็นภาษาที่เรียกว่า server-side หรือ HTML-embedded scripting language เป็นเครื่องมือที่สำคัญชนิดหนึ่งที่ช่วยให้เราสามารถสร้างเอกสารแบบ Dynamic HTML ได้อย่างมีประสิทธิภาพและมีลูกเล่นมากขึ้น [10]

2.6.1 การประมวลผลไฟล์พีเอชพี

พีเอชพี เอนจิง (PHP Engine) จะแปลและประมวลผลเฉพาะคำสั่งที่อยู่ภายในแท็กของพีเอชพีเท่านั้น การทำงานที่เกิดขึ้นคือ หลังจากพีเอชพี เอนจิง ถูกเว็บเซิร์ฟเวอร์เรียกขึ้นมาประมวลผลไฟล์พีเอชพี แล้วมันจะส่งผ่านเนื้อหาของไฟล์ไปยังเบราวเซอร์โดยไม่ทำอะไรกับเนื้อหานั้น ยกเว้นเมื่อพบกับสัญลักษณ์ (แท็ก) ที่ระบุจุดเริ่มต้นของบล็อคคำสั่งพีเอชพีก็จะแปลและประมวลผลคำสั่งต่าง ๆ ไปตามลำดับ (ภายในบล็อคพีเอชพีนี้จะส่งผลลัพธ์ให้แก่เบราวเซอร์ ต้องเรียกใช้คำสั่ง / ฟังก์ชั่นของพีเอชพี เช่น print) โดยเมื่อพบสัญลักษณ์ปิดท้ายบล็อคคำสั่งพีเอชพี เอนจิง ก็จะหันกลับไปส่งผ่านเนื้อหาของไฟล์ต่อไปเช่นเดิม จนกว่าจะพบสัญลักษณ์ระบุจุดเริ่มต้นของบล็อคคำสั่งของพีเอชพีอีกและเป็นอย่างนี้เรื่อยไปจนจบไฟล์ [10]

2.6.2 ตัวแปรเซสชัน (Session)

ตัวแปรเซสชันคือ การเก็บค่าจากเว็บเซิร์ฟเวอร์ลงในหน่วยความจำของเครื่อง Client แต่ละราย เซิร์ฟเวอร์จะกำหนดเวลาและติดตามการใช้งานของเครื่อง Client Session ID คืออะไร Session ID คือ หมายเลขประจำตัวที่เว็บเซิร์ฟเวอร์ส่งมายัง Client ค่า Session จะไม่มีทางซ้ำกัน Session ID มีประโยชน์ไรการอ้างอิงเกี่ยวกับการใช้งานของ Client

1. รูปแบบการอ่านค่า Session ID

   Session_ID () ;

2. รูปแบบการใช้งาน Session อื่น ๆ

   Session_Type ("Session-name")

   เมื่อ Type คือ ชนิดของ Session

3. การสร้าง session

Session_Start ()

$session-name = value ;

Session_registe r("session-name") ;

4. การอ่านค่าจาก Session

Session_Start () ;

$session-name ;

Echo "$session-name" ;

5. การตรวจสอบตัวแปร Session

```
Session_Start () ;
$session-name ;
If (Session_is_registered ("$session-name") )
{
 Echo "ตัวแปรนี้มีค่าอยู่" ;
}
 Else
{
 Echo "ตัวแปรนี้ไม่มีค่าอยู่" ;
}
```

6. การลบค่าใน Session

- การลบ Session เฉพาะตัวแปร

Session_unregister ("session-name ") ;

- การลบ Session ทั้งหมด

Session_destroy () ;[10]

2.6.3 การติดต่อฐานข้อมูลมายเอสคิวแอล (MySQL) ด้วยพีเอชพี

1. ฟังก์ชั่น mysql_connect () เป็นฟังก์ชั่นที่ใช้เปิดการเชื่อมต่อกับมายเอสคิวแอล

รูปแบบ mysql_connect (ชื่อโฮสต์, ชื่อผู้ใช้, รหัสผ่าน) ;

ถ้าสามารถติดต่อกับมายเอสคิวแอลได้ ฟังก์ชั่นนี้จะส่งหมายเลขการเชื่อมต่อ (link identifier) กลับคืนมา ซึ่งเราจะนำหมายเลขการเชื่อมต่อนี้ไประบุให้กับฟังก์ชั่นอื่น ๆ ต่อไป แต่ถ้าการติดต่อกับมายเอสคิวแอลไม่สำเร็จจะส่งค่า False กลับมา

2. ฟังก์ชั่น mysql_close () เป็นฟังก์ชั่นที่ใช้ในการปิดการเชื่อมต่อมายเอสคิวแอล

รูปแบบ mysql_close (หมายเลขการเชื่อมต่อ) ;

โดยหมายเลขการเชื่อมต่อคือ ค่าที่ได้รับมาจากฟังก์ชั่น mysql_connect ()

3. ฟังก์ชั่น mysql_select_db () เป็นฟังก์ชั่นที่ส่งหมายเลขการเชื่อมต่อไปยังมายเอสคิวแอล เพื่อที่จะเลือกดาต้าเบสที่จะใช้

รูปแบบ mysql_select_db (ชื่อดาต้าเบส,หมายเลขการเชื่อมต่อ) ;

4. ฟังก์ชั่น mysql_query () เป็นฟังก์ชั่นที่ใช้ส่งคำสั่งเอสคิวแอลไปยังมายเอสคิวแอล

รูปแบบ mysql_query (คำสั่งเอสคิวแอล) ;

5. ฟังก์ชั่น mysql_num_rows () เป็นฟังก์ชั่นที่ใช้ในการนับเรคคอร์ด

รูปแบบ mysql_num_rows (ผลลัพธ์ของคำสั่งเอสคิวแอล) ;

ผลลัพธ์ของคำสั่งเอสคิวแอลคือ ข้อมูลชนิดรีซอร์ซ (Resource) ที่ฟังก์ชั่น mysql_query () ส่งคืนมาให้หลังจากที่เราส่งคำสั่ง SELECT ของเอสคิวแอลผ่านทางฟังก์ชั่นดังกล่าวไปยังมายเอสคิวแอล

6. ฟังก์ชั่น mysql_result () เป็นฟังก์ชั่นที่ใช้เรียกดูข้อมูลของเรคคอร์ดที่กำหนด

รูปแบบ mysql_result (ผลลัพธ์ของคำสั่งเอสคิวแอล, ลำดับของเรคคอร์ด, ชื่อฟิลด์) ;

ผลลัพธ์ของคำสั่งเอสคิวแอลคือ ข้อมูลชนิดรีซอร์ซที่ฟังก์ชั่น mysql_query () ส่งคืนมาให้หลังจากที่เราส่งคำสั่ง SELECT ของเอสคิวแอลผ่านทางฟังก์ชั่นดังกล่าวไปยังมายเอสคิวแอล

7. ฟังก์ชั่น mysql_fetch_array () เป็นฟังก์ชั่นที่สามารถใช้เรียกดูข้อมูลได้ โดยฟังก์ชั่นนี้คืนมาให้จะเป็นตัวแปรชนิดอาเรย์ซึ่งมีสมาชิกเป็นฟิลด์ต่าง ๆ ของเรคคอร์ดปัจจุบัน โดยในการใช้นั้นเราต้องเรียกฟังก์ชั่นนี้ซ้ำ ๆ จนกว่าค่าที่ส่งคืนกลับมาจะเป็นเท็จ จึงจะได้ข้อมูลเรคคอร์ดต่าง ๆ (ซึ่งเป็นผลลัพธ์ของคำสั่งมายเอสคิวแอลที่เราส่งผ่านฟังก์ชั่น mysql_query () ไป) ครบทุกเรคคอร์ด

รูปแบบ mysql_fetch_array (ผลลัพธ์ของคำสั่ง SQL) ;

ผลลัพธ์ของคำสั่ง SQL คือ ข้อมูลชนิดรีซอร์ซที่ฟังก์ชั่น mysql_query () ส่งคืนมาให้ [10]

2.7 มายเอสคิวแอล (MySQL)

มายเอสคิวแอลคือ โปรแกรมระบบจัดการฐานข้อมูล มีหน้าที่เก็บข้อมูลอย่างเป็นระบบ รองรับคำสั่งเอสคิวแอล (SQL = Structured Query Language) เป็นเครื่องมือสำหรับเก็บข้อมูลที่ต้องใช้ร่วมกับเครื่องมือหรือโปรแกรมอื่นอย่างบูรณาการ เพื่อให้ได้ระบบงานที่รองรับความต้องการของผู้ใช้ เช่น ทำงานร่วมกับเว็บเซิร์ฟเวอร์ เพื่อให้บริการแก่ภาษาสคริปต์ที่ทำงานฝั่งเครื่องบริการ (Server-Side Script) เช่น PHP, ASP, JSP เป็นต้น หรือทำงานร่วมกับโปรแกรมประยุกต์ เช่น Visual basic, JAVA, C เป็นต้น

มายเอสคิวแอลเป็นระบบฐานข้อมูลแบบโอเพนซอร์ทสำหรับจัดการระบบดาต้าเบส ผ่านเอสคิวแอล โปรแกรมนี้ถูกพัฒนาโดย บริษัท MySQL AB ในประเทศสวีเดน

2.7.1 คำสั่งพื้นฐาน

1. การสร้างฐานข้อมูล

   รูปแบบ Create database [database-name] ;

2. การลบฐานข้อมูล

   รูปแบบ Drop database [database-name] ;

3. การเลือกใช้ฐานข้อมูล

   รูปแบบ Use [database-name] ;

4. การสร้างตาราง

รูปแบบ Create Table Table-name (

filed1 tpye [not null / null],

filed2 tpye [not null / null],

filed3 tpye [not null / null],

.....

.....

.....

filedN tpye [not null / null]

primary key (filed) //ไม่กำหนดคีย์ได้

) ;

5. คำสั่งลบตาราง

รูปแบบ Drop Table Table-name ;

6. คำสั่งเรียกดูโครงสร้างของตาราง

รูปแบบ describe Table-name ;

7. คำสั่งการเพิ่มข้อมูลลงในตาราง

รูปแบบ Insert Into Table-name (filed1, filed2, filed3, ..., filedN)

Values ('Value1', 'Value2', 'Value3' ,... , 'ValueN') ;

8. คำสั่งการแก้ไขข้อมูลลงในตาราง

รูปแบบ Update Table-name Set filed1 = 'Value1', filed2' = Value2'

Where filed = 'Value' ;

9. คำสั่งการลบข้อมูลลงในตาราง

รูปแบบ DELETE FROM Table-name WHERE (filed = ' Value') ;

10. คำสั่งแสดงข้อมูลในตาราง

รูปแบบ Select filed1, filed2, filed3, filedN

From Table-name Where filed = 'Value' ;

บทที่ 3
วิธีการดำเนินงานโครงงานวิศวกรรม

ในส่วนของบทนี้ได้แบ่งวิธีการดำเนินงานของโครงงานออกเป็นสองส่วนคือ ส่วนแรกคือการศึกษาวิธีการและเครื่องมือที่ใช้สำหรับการสร้างระบบอีเมลที่มีการรับรอง ส่วนที่สองคือ การออกแบบสำหรับการสร้างระบบอีเมลที่มีการรับรอง

3.1 การศึกษา

1. หลักการบุคคลที่สามที่น่าเชื่อถือ (A Light On-line Trusted Third Party : On-line TTP) ระบบอีเมลที่มีการรับรองนั้นมีหลากหลายรูปแบบ มีการรับรองด้วยขั้นตอนที่แตกต่างกันไป ทางผู้จัดทำได้เลือกใช้หลักการ On-line TTP เนื่องจากหลักการนี้สามารถนำไปปรับใช้งานได้ง่าย มีวัตถุประสงค์ที่มุ่งเน้นในด้านความปลอดภัยของข้อมูล และระบบไม่จำเป็นต้องเกี่ยวข้องทุกกระบวนการ จึงทำให้สามารถใช้บริการระบบอีเมลได้ตามปกติ อีกทั้งโปรโตคอลยังตรงกับจุดประสงค์ของการทำโครงงานที่ต้องการเป็นสื่อกลางระหว่างผู้ส่งและผู้รับ

2. การเข้ารหัส – ถอดรหัสข้อความและการแปลงข้อความ เนื่องจากหลักการ On-line TTP มุ่งเน้นในด้านความปลอดภัยของข้อความ เพื่อที่จะป้องกันไม่ให้ผู้อื่นสามารถอ่านข้อความได้ จึงจำเป็นต้องมีการเข้ารหัส – ถอดรหัสข้อความ จากอัลกอลิทึมการเข้ารหัส - ถอดรหัสข้อความ มีอยู่หลายอัลกอลิทึม แต่อัลกอลิทึม AES (Rijndael) โดยรวมแล้วมีความเหมาะสมที่จะนำมาใช้งานมากที่สุด เนื่องจากเป็นอัลกอริทึมที่มีความเร็วสูงและมีขนาดกะทัดรัด โดยสามารถใช้กุญแจที่มีความยาวขนาด 128, 192 และ256 บิต

เมื่อเข้ารหัสแล้วจะได้ข้อความที่เป็นตัวอักษรพิเศษ ทำให้ไม่สามารถส่งข้อความผ่านระบบเครือข่ายได้ เพราะการส่งข้อความผ่านระบบเครือข่ายนั้นสามารถส่งได้แต่แบบไบนารี จึงจำเป็นต้องใช้การแปลงข้อความด้วยอัลกอริทึมเบส 64 โดยทำการแปลงข้อความหลังการเข้ารหัสและก่อนการถอดรหัส เพื่อที่จะได้ข้อความที่สามารถส่งผ่านระบบเครือข่ายได้

3. เครื่องมือที่ใช้ จากหลักการ On-line TTP ที่ต้องการเป็นบุคคลที่สามที่น่าเชื่อถือหรือเป็นสื่อกลางระหว่างผู้รับและผู้ส่ง ผู้จัดทำจึงได้ทำการสร้างเว็บไซต์ขึ้นมาเพื่อเป็นบุคคลที่สามที่น่าเชื่อถือ (TTP) และได้เลือกใช้ภาษาสคริปต์พีเอชพีในการพัฒนาเว็บไซต์ เนื่องจากเป็นภาษาที่เข้าใจง่าย สามารถเรียนรู้ได้เร็ว เป็นที่นิยมใช้กันอย่างแพร่หลาย มีประสิทธิภาพ และสามารถติดต่อกับฐานข้อมูลได้ง่าย ในด้านของฐานข้อมูลใช้มายเอสคิวแอล เป็นโปรแกรมระบบจัดการฐานข้อมูลของเว็บไซต์ และใช้โปรแกรมมาโครมีเดีย ดรีมวีฟเวอร์ 8 เป็นโปรแกรมสร้างโฮมเพจแบบเสมือนจริงโดยไม่ต้องเขียนภาษาเอชทีเอ็มแอลเอง

3.2 การออกแบบ

การออกแบบได้แบ่งออกเป็นสี่ส่วนคือ การออกแบบโปรโตคอล, การออกแบบหน้าเวปไซต์, การออกแบบการเข้ารหัส – ถอดรหัสข้อความ และการออกแบบดาต้าเบส

3.2.1 การออกแบบโปรโตคอล

จากโปรโตคอลของหลักการ On-line TTP จะมีบุคคลที่เกี่ยวข้องกันสามบุคคลคือ ผู้ส่ง, ผู้รับ, และTTP แต่ขั้นตอนการทำงานของโปรโตคอลนี้ไม่สามารถนำมาใช้กับเว็บไซต์ที่ต้องการสร้างได้ ผู้จัดทำจึงได้ออกแบบขั้นตอนการทำงานของโปรโตคอลใหม่ เพื่อให้เหมาะสมแก่การใช้งานในส่วนของเว็บไซต์โดยที่ยังใช้หลักการ On-line TTP เช่นเดิม

จากการออกแบบโปรโตคอลใหม่ การทำงานของโปรโตคอลมีขั้นตอนดังนี้

1. S ---> TTP : R, M
2. TTP ---> S : E_k (M), N
3. S ---> R : E_k (M), N
4. R ---> TTP : S, R, N, E_k (M)
5. TTP ---> R : M
6. TTP ---> S : Timestamp

โดยที่ S คือ ผู้ส่ง

R คือ ผู้รับ

TTP คือ เว็บไซต์ที่ทำหน้าที่เป็นบุคคลที่สามที่น่าเชื่อถือ

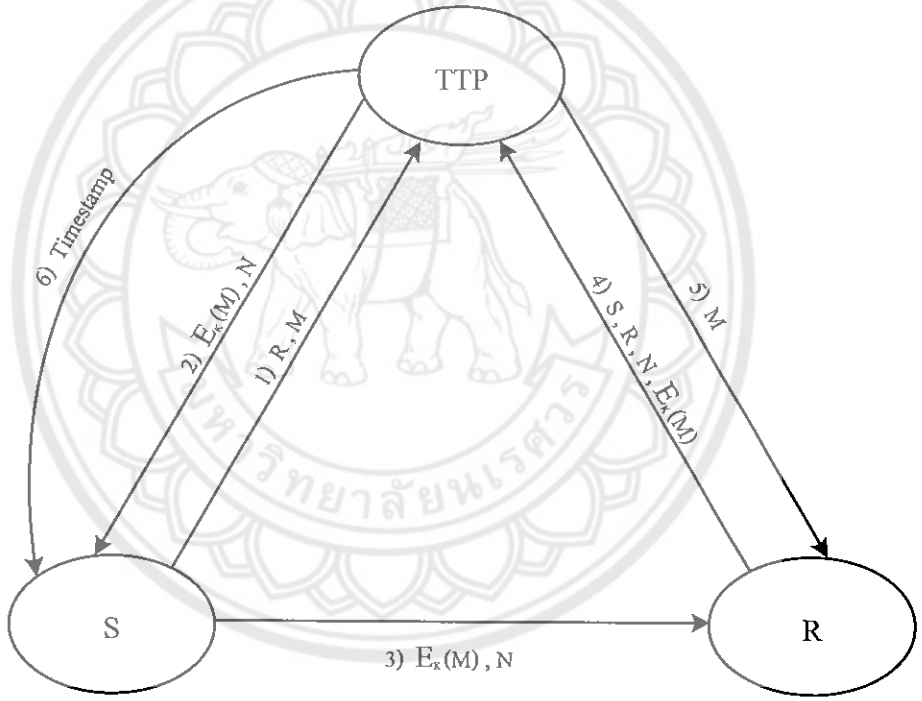
M คือ ข้อความที่ S ต้องการส่งให้ R

E_k (M) คือ การเข้ารหัสข้อความ

k คือ กุญแจที่ใช้ในการเข้ารหัส – ถอดรหัสข้อความ

N คือ ฟังก์ชันที่ TTP สร้างให้ S เพื่อตรวจสอบ R

Timestamp คือ หลักฐานการยืนยันเวลาเมื่อมีการกระทำบน TTP



รูปที่ 3.1 การออกแบบโปรโตคอล

จากรูปที่ 3.1 สามารถอธิบายขั้นตอนการทำงานของโปรโตคอลได้ดังนี้

1. เมื่อผู้ส่งต้องการร้องขอระบบอีเมลที่มีการรับรอง ผู้ส่งต้องทำการเขียนข้อความและชื่อผู้รับให้กับเวปไซต์ที่เป็นบุคคลที่สามที่น่าเชื่อถือ

2. เมื่อเวปไซต์ได้รับการร้องขอระบบอีเมลที่มีการรับรองจากผู้ส่ง เวปไซต์จะทำการเข้ารหัสข้อความ จากนั้นจะแสดงข้อความที่เข้ารหัสและฟังก์ชันที่ทางเวปไซต์สร้างให้ผู้ส่งเพื่อตรวจสอบผู้รับให้กับผู้ส่ง

3. ผู้ส่งทำการส่งข้อความที่เข้ารหัสและฟังก์ชันที่ทางเวปไซต์สร้างให้ผู้ส่งเพื่อตรวจสอบผู้รับ ให้กับผู้รับทางระบบอีเมลของผู้ส่งปกติ

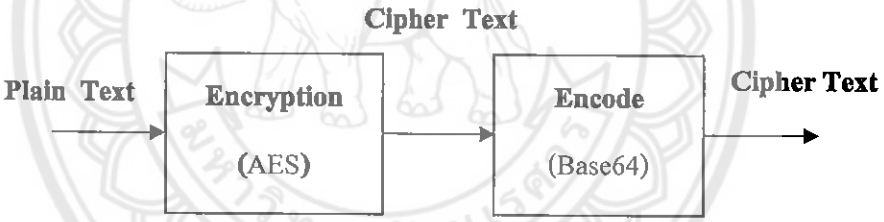
4. เมื่อผู้รับต้องการอ่านข้อความ ต้องทำการร้องขอระบบอีเมลที่มีการรับรอง โดยกระทำการกับฟังก์ชันที่ทางผู้ส่งส่งให้ทางระบบอีเมล พร้อมทั้งบอกชื่อผู้รับ ชื่อผู้ส่ง และข้อความที่เข้ารหัส ให้กับทางเวปไซต์

5. เมื่อเวปไซต์ได้รับการร้องขอระบบอีเมลที่มีการรับรองจากผู้รับ เวปไซต์จะทำการตรวจสอบว่าผู้รับสามารถอ่านข้อความได้หรือไม่ ถ้าผ่านการตรวจสอบเวปไซต์จะแสดงข้อความที่ถอดรหัสให้กับผู้รับ แต่ถ้าผู้รับไม่ผ่านการตรวจสอบจะไม่สามารถอ่านข้อความที่ถอดรหัสได้

6. เมื่อผู้รับได้ทำการอ่านข้อความเรียบร้อยแล้ว เวปไซต์จะส่งหลักฐานการยืนยันเวลาเมื่อผู้รับเปิดอ่านอีเมลแล้วทางอีเมลของผู้ส่ง

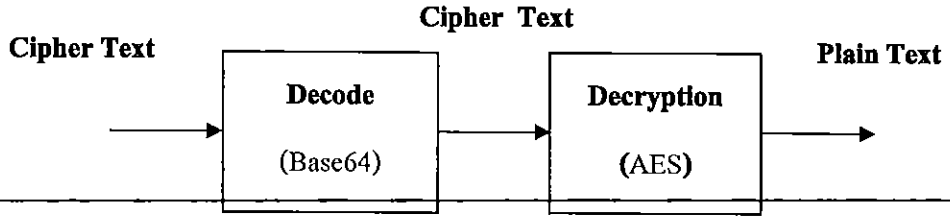
3.3.2 การออกแบบขั้นตอนการเข้ารหัส – ถอดรหัสข้อความ

Plain text คือ ข้อความที่สามารถอ่านได้, Cipher text คือ ข้อความที่เข้ารหัสแล้ว



รูปที่ 3.2 ขั้นตอนการเข้ารหัสข้อความ

จากรูปที่ 3.2 สามารถอธิบายขั้นตอนการเข้ารหัสข้อความได้ดังนี้ ขั้นแรกเข้ารหัสข้อความที่สามารถอ่านได้ด้วยอัลกอริทึม AES จะได้ข้อความที่เข้ารหัสจาก AES ขั้นที่สองแปลงข้อความที่เข้ารหัสด้วยอัลกอริทึม AES ในขั้นแรกด้วยอัลกอริทึมเบส64 จะได้ข้อความที่เข้ารหัสด้วยอัลกอริทึม AES ที่ทำการแปลงข้อมูลด้วยอัลกอริทึมเบส64 เรียบร้อย

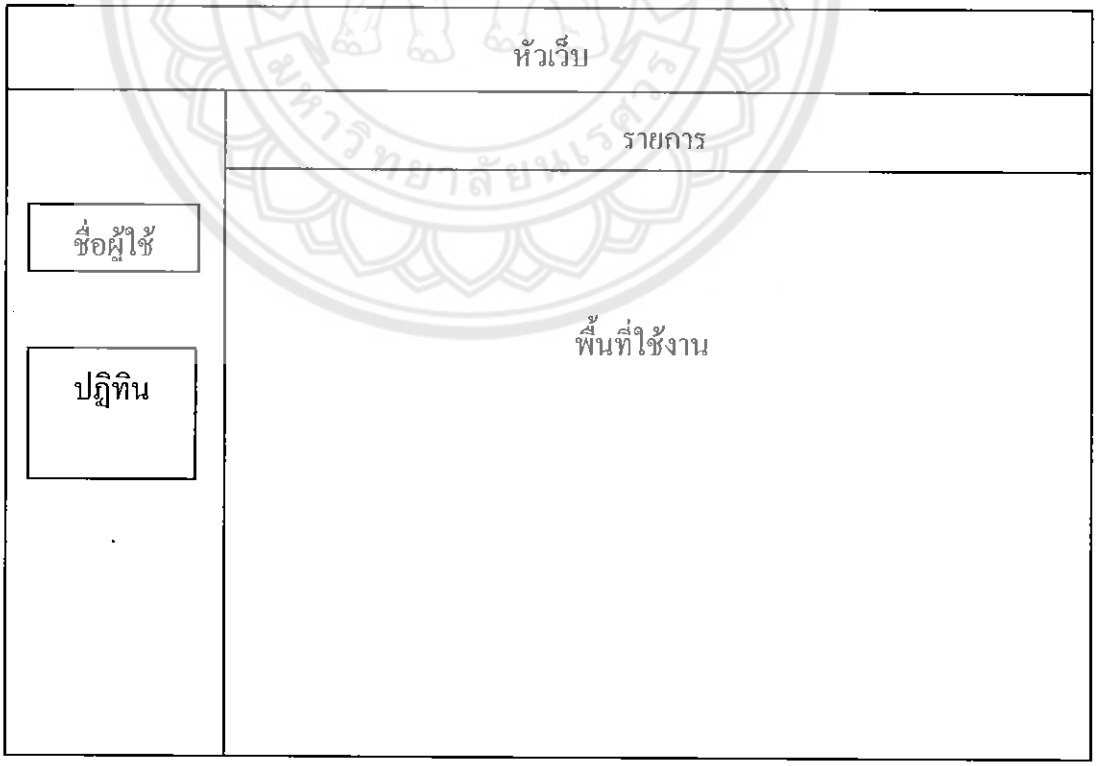


รูปที่ 3.3 ขั้นตอนการถอดรหัสข้อความ

จากรูปที่ 3.3 สามารถอธิบายขั้นตอนการถอดรหัสข้อความได้ดังนี้ ขั้นแรกแปลงข้อความที่เข้ารหัสด้วยอัลกอริทึม AES ที่ทำการแปลงข้อมูลด้วยอัลกอริทึมเบส64 เรียบร้อยแล้วด้วยอัลกอริทึมเบส64 จะได้ข้อความที่เข้ารหัสด้วยอัลกอริทึม AES ขั้นที่สองถอดรหัสข้อความด้วยอัลกอริทึม AES ในขั้นแรกด้วยอัลกอริทึม AES จะได้ข้อความที่สามารถอ่านได้

3.3.3 การออกแบบหน้าเว็บไซต์

ในส่วนของเว็บไซต์ที่ทำหน้าที่เป็นบุคคลที่สามที่น่าเชื่อถือ ได้ทำการแบ่งหน้าเวปไซต์ดังแสดงในรูปที่ 3.4



รูปที่ 3.4 การออกแบบหน้าเว็บไซต์

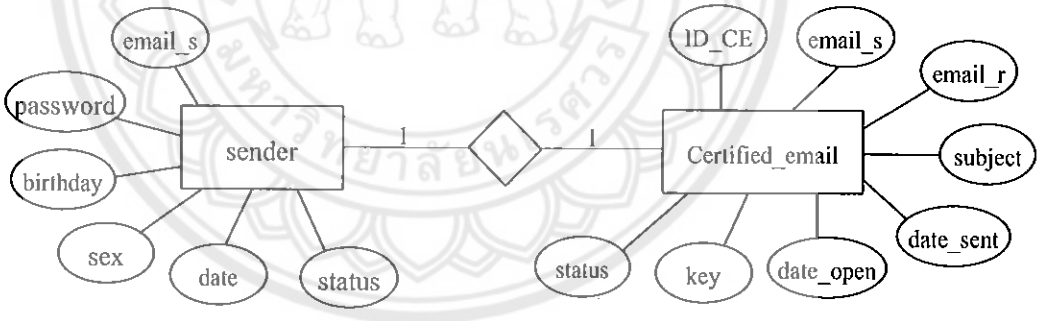
หน้าเว็บไซต์จะแบ่งเป็น 5 ส่วนดังนี้

1. หัวเว็บ ส่วนของหัวเว็บแสดงชื่อเว็บไซต์
2. ชื่อผู้ใช้ ส่วนของเมนูที่แสดงชื่อผู้ใช้งานปัจจุบัน
3. ปฏิทิน ส่วนของเมนูที่แสดงวันและเวลาปัจจุบัน
4. รายการ ส่วนของเมนูที่ให้เลือกทำรายการ
5. พื้นที่ใช้งาน ส่วนของพื้นที่ที่ให้ทำรายการต่าง ๆ

3.3.4 การออกแบบดาต้าเบส

การสร้างเวปไซต์จำเป็นต้องมีฐานข้อมูล เพื่อเก็บข้อมูลต่าง ๆ การใช้บริการเว็บไซต์จะต้องทำการสมัครสมาชิกก่อนจึงจะสามารถใช้บริการได้ จึงได้ออกแบบตาราง sender สำหรับเก็บข้อมูลสมาชิก และเมื่อผู้ส่งทำการร้องขอระบบอีเมลที่มีการรับรอง จำเป็นต้องเก็บข้อมูลบางส่วน เพื่อใช้ในการตรวจสอบความถูกต้อง จึงได้ออกแบบตาราง Certified_email ขึ้นมาอีกหนึ่งตาราง

1. โมเดลความสัมพันธ์ระหว่างข้อมูล (ER – Diagram)



รูปที่ 3.5 ER – Diagram

จาก ER – Diagram แสดงความสัมพันธ์ระหว่างผู้ส่งกับการร้องขอรับรองอีเมล โดยที่ผู้ส่งหนึ่งคนสามารถร้องขอระบบอีเมลที่มีการรับรอง ได้เพียงครั้งละหนึ่งคำร้องเท่านั้น ไม่สามารถร้องขอครั้งละหลายคำร้องได้และการร้องขอแต่ละครั้งจะรับรองให้ผู้ส่งเพียงคนเดียวเท่านั้น ความสัมพันธ์จึงเป็นแบบหนึ่งต่อหนึ่ง (One to One Relationships)

2. พจนานุกรมข้อมูล (Data Dictionary)

พจนานุกรมข้อมูลเป็นที่เก็บรวบรวมข้อมูลทั้งหมดและเป็นที่ค้นหาข้อมูลที่ต้องการเกี่ยวกับข้อมูลของระบบทั้งหมดได้ โดยนำข้อมูลเหล่านี้มาจาก ER – Diagram พจนานุกรมข้อมูลของระบบแสดงดังตารางที่ 3.1 และตารางที่ 3.2

ตารางที่ 3.1 ตาราง sender

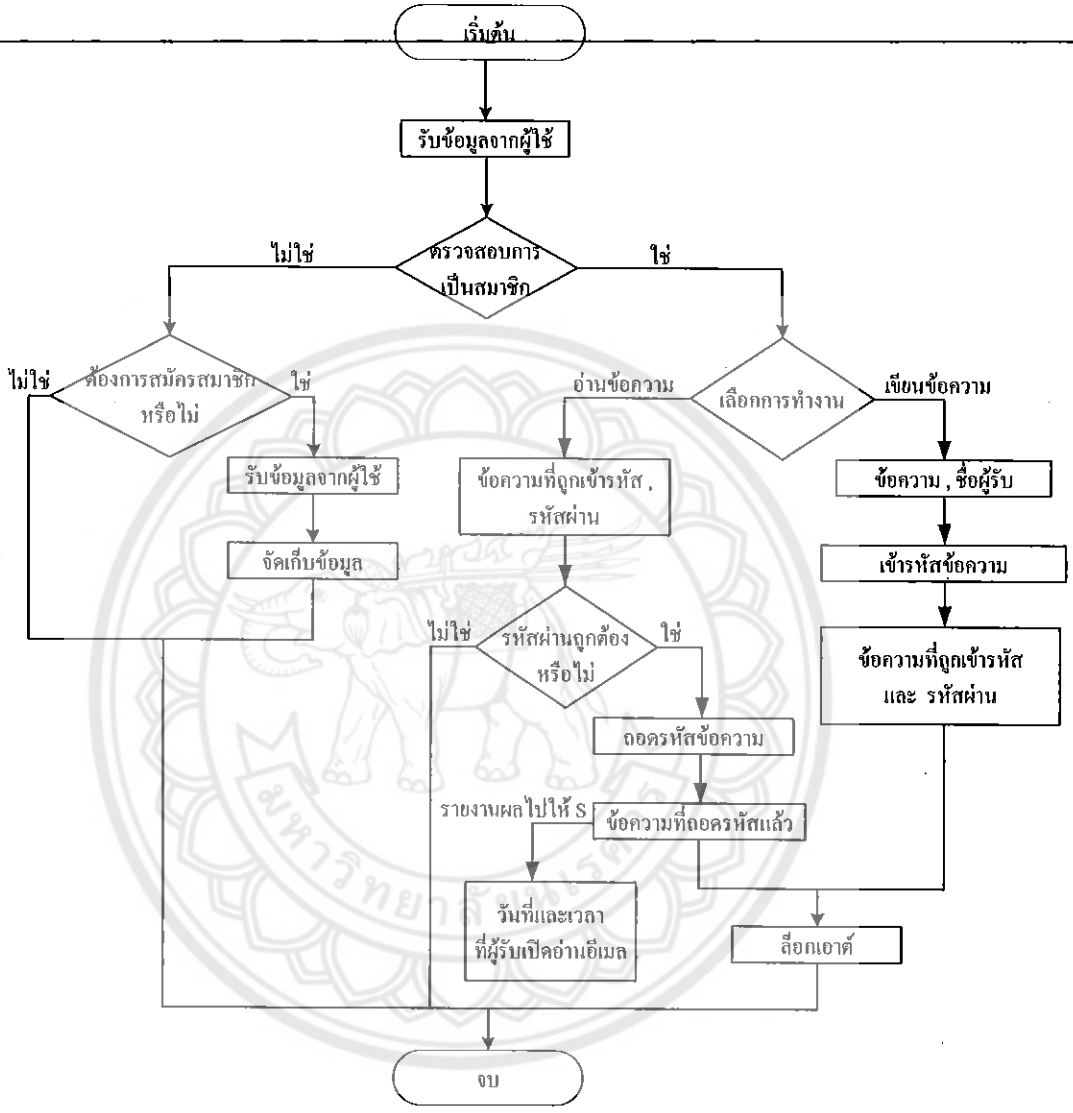
ฟิลด์	ชนิด	สถานะ	รายละเอียด
email_s	varchar (50)	PK	อีเมล
password	varchar (8)	-	รหัสผ่าน
birthday	date	-	วันเกิด
sex	varchar (10)	-	เพศ
date	datetime	-	วันที่สมัคร
status	text	-	การยืนยันสมาชิก

ตารางที่ 3.2 ตาราง Certified_email

ฟิลด์	ชนิด	สถานะ	รายละเอียด
ID_ce	int	PK	หมายเลขการทำรายการ
email_s	varchar (50)	-	อีเมล
email_r	varchar (50)	-	อีเมล
subject	varchar (100)	-	หัวข้อ
date_sent	datetime	-	วันที่ส่ง
key	varchar (8)	-	กุญแจ
status	text	-	สถานะการถอดรหัสข้อความ
date_open	datetime	-	วันที่เปิดข้อความ

3.3.5 ขั้นตอนการทำงานของเวปไซต์

ขั้นตอนการทำงานของเวปไซต์สามารถแสดงได้ดังรูปที่ 3.6



รูปที่ 3.6 ระบบการทำงานของเว็บไซต์

จากรูปที่ 3.6 อธิบายได้ว่าเวปไซต์จะเริ่มจากรับข้อมูลจากผู้ใช้ แล้วทำการตรวจสอบว่าผู้ใช้นั้นได้เป็นสมาชิกหรือไม่

1. ถ้าเป็นสมาชิกแล้ว ทำการเลือกการทำงานระหว่างเขียนข้อความ (ผู้ส่ง) และอ่านข้อความ (ผู้รับ)

1.1 ถ้าเลือกเขียนข้อความ ต้องทำการกรอกข้อความและชื่อผู้รับ จากนั้นเวปไซต์จะทำการเข้ารหัสข้อความ แล้วแสดงข้อความที่ถูกเข้ารหัสและรหัสผ่าน เมื่อผู้ใช้ล็อกเอาต์จะจบการทำงาน

1.2 ถ้าเลือกอ่านข้อความ ต้องทำการกรอกรหัสผ่านและข้อความที่ถูกเข้ารหัส ทางเวปไซต์จะทำการตรวจสอบรหัสผ่านว่าถูกต้องหรือไม่

1.2.1 ถ้ารหัสผ่านถูกต้องเวปไซต์จะทำการถอดรหัสข้อความ และแสดงข้อความที่ถอดรหัสแล้ว พร้อมทั้งส่งหลักฐานการยืนยันวันที่และเวลาที่ผู้รับเปิดอ่านอีเมลรายงานผลไปให้ผู้ส่ง เมื่อผู้ใช้ล็อกเอาต์จะจบการทำงาน

1.2.2 ถ้ารหัสผ่านไม่ถูกต้อง จะไม่สามารถเปิดอ่านข้อความได้และจบการทำงาน

2. ถ้าไม่ได้เป็นสมาชิก ทำการเลือกว่าต้องการสมัครสมาชิกหรือไม่

2.1 ถ้าต้องการสมัครสมาชิก เวปไซต์จะรับข้อมูลจากผู้ใช้แล้วจัดเก็บข้อมูลและจบการทำงาน

2.2 ถ้าไม่ต้องการสมัครสมาชิก จะจบการทำงาน

บทที่ 4

ผลการทำงานของระบบ

ในบทนี้จะแบ่งออกเป็นสองส่วนคือ ส่วนแรกเป็นการวิเคราะห์โปรโตคอล ซึ่งเป็นการวิเคราะห์การทำงานของโปรโตคอลที่ได้ออกแบบไว้ในข้างต้น ส่วนที่สองเป็นการใช้งานหน้าเวปไซต์ทั่วไปและการใช้งานหน้าเวปไซต์เมื่อมีการร้องขอระบบอีเมลที่มีการรับรอง

4.1 การวิเคราะห์โปรโตคอล

การวิเคราะห์โปรโตคอลนั้นแบ่งออกเป็นสองส่วนคือ เป้าหมายของโปรโตคอล เป็นการกล่าวถึงว่าระบบอีเมลที่มีการรับรองสามารถรับรองอีเมลได้ และจากโปรโตคอลที่ออกแบบ เป็นการกล่าวถึงเวปไซต์ที่ทำหน้าที่เป็นบุคคลที่สามที่น่าเชื่อถือว่ามีความน่าเชื่อถือจริง

4.1.1 เป้าหมายของโปรโตคอล

- ระบบอีเมลที่มีการรับรองสามารถรับรองอีเมลได้ ถ้าผู้ส่งได้รับหลักฐานการยืนยันวันที่และเวลาที่ผู้รับได้เปิดอ่านข้อความ ก็ต่อเมื่อผู้รับได้รับข้อความแล้วเท่านั้น

- ระบบอีเมลที่มีการรับรองไม่สามารถรับรองได้ ถ้าผู้ส่งได้รับหลักฐานการยืนยันวันที่และเวลาที่ผู้รับได้เปิดอ่านข้อความ แต่ในความเป็นจริงนั้นผู้รับไม่ได้รับข้อความ

- ระบบอีเมลที่มีการรับรองไม่สามารถรับรองได้ ถ้าผู้ส่งไม่ได้รับหลักฐานการยืนยันวันที่และเวลาที่ผู้รับได้เปิดอ่านข้อความ แต่ในความเป็นจริงนั้นผู้รับได้รับข้อความ

4.1.2 จากโปรโตคอลที่ออกแบบ

- ผู้รับจะได้รับข้อความก็ต่อเมื่อสามารถถอดรหัสข้อความบนเวปไซต์ที่ทำหน้าที่เป็นบุคคลที่สามที่น่าเชื่อถือได้ ซึ่งผู้ที่ทำหน้าที่ถอดรหัสข้อความมีเพียงเวปไซต์ที่เป็นบุคคลที่สามที่น่าเชื่อถือเท่านั้น

- ผู้ส่งจะได้รับหลักฐานการยืนยันวันที่และเวลาที่ผู้รับได้เปิดอ่านข้อความก็ต่อเมื่อเวปไซต์ที่ทำหน้าที่เป็นบุคคลที่สามที่น่าเชื่อถือส่งให้เท่านั้น

ดังนั้นถ้าเวปไซต์ที่ทำหน้าที่เป็นบุคคลที่สามที่น่าเชื่อถือมีความน่าเชื่อถือได้ โปรโตคอลที่ออกแบบสามารถนำไปใช้งานในระบบอีเมลที่มีการรับรองได้

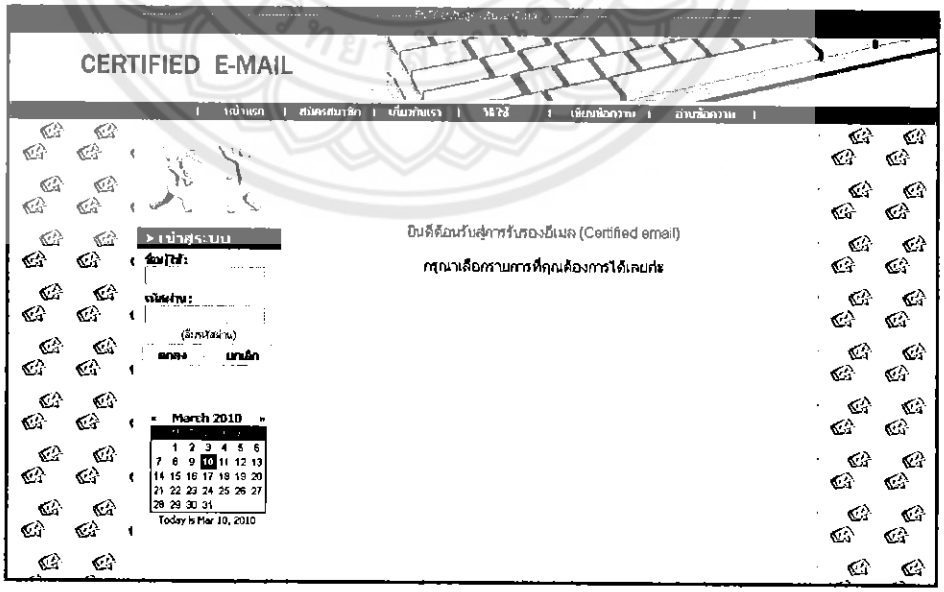
4.2 การใช้งานหน้าเวปไซต์

เวปไซต์ได้แบ่งการใช้งานเป็นสามส่วนคือ การใช้งานหน้าเวปไซต์ทั่วไป การใช้งานหน้าเวปไซต์เมื่อมีการร้องขอระบบอีเมลที่มีการรับรองในกรณีที่เป็นผู้ส่ง และการใช้งานหน้าเวปไซต์เมื่อมีการร้องขอระบบอีเมลที่มีการรับรองในกรณีที่เป็นผู้รับ

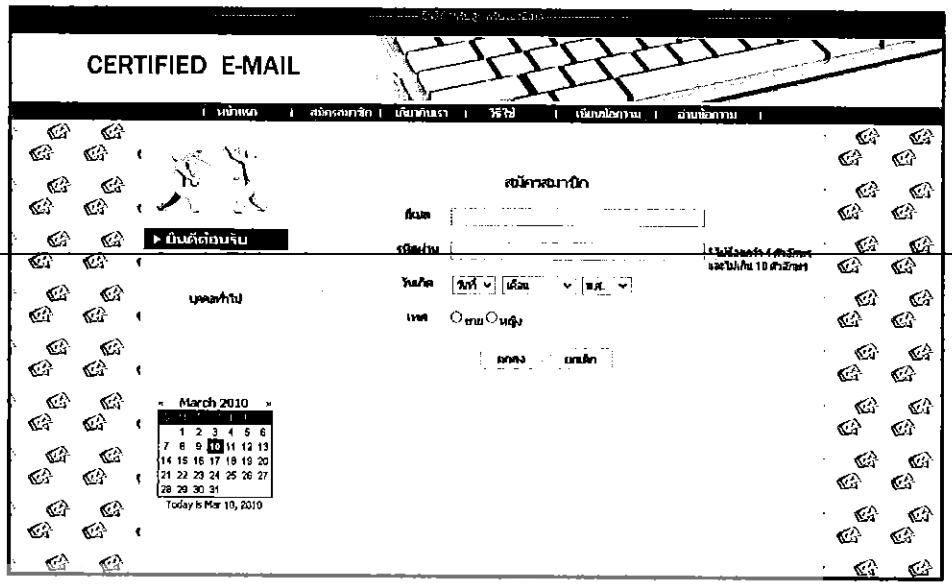
4.2.1 การใช้งานหน้าเว็ปไซต์ทั่วไป

การใช้งานหน้าเว็ปไซต์ทั่วไป เป็นดังต่อไปนี้

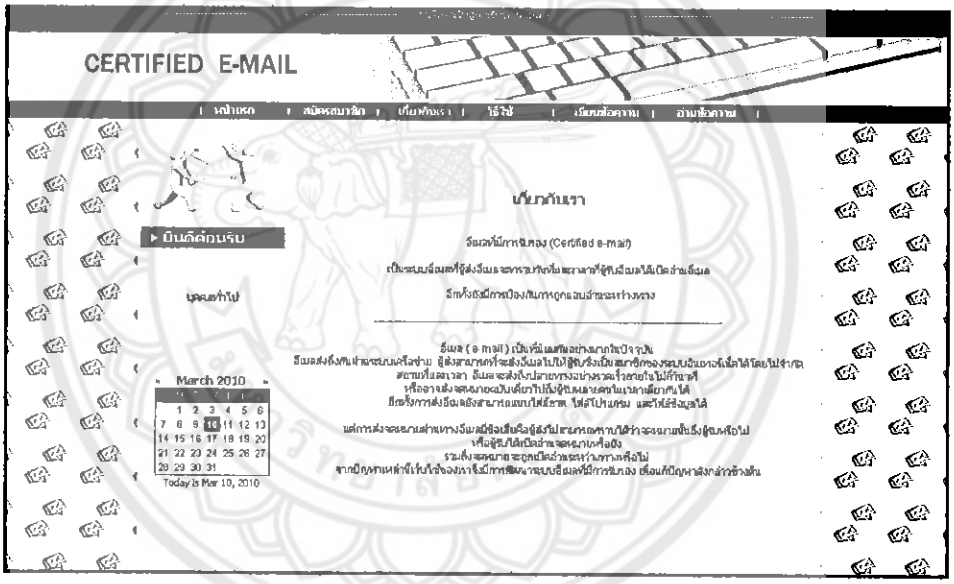
1. หน้าแรกของเวปไซต์ www.ttp.cpenu.com ดังแสดงในรูปที่ 4.1
2. หน้าสมัครสมาชิก หากต้องการทำรายการของเว็บไซต์ต้องทำการสมัครสมาชิก ดังแสดงในรูปที่ 4.2
3. หน้าเกี่ยวกับเรา แสดงข้อมูลและที่มาของการรับรองอีเมล ดังแสดงในรูปที่ 4.3
4. หน้าวิธีใช้ อธิบายถึงขั้นตอนการเขียนข้อความและการอ่านข้อความ ดังแสดงในรูปที่ 4.4
5. หน้าลืมรหัสผ่าน ใช้ในกรณีที่สมาชิกลืมรหัสผ่านที่ใช้ในการเข้าระบบ ดังแสดงในรูปที่ 4.5
6. หน้าประวัติการใช้ แสดงถึงประวัติการใช้งานที่สมาชิกทำการเขียนข้อความ รวมถึงแสดงวันที่และเวลาที่ผู้รับได้เปิดอ่านข้อความด้วย ดังแสดงในรูปที่ 4.6



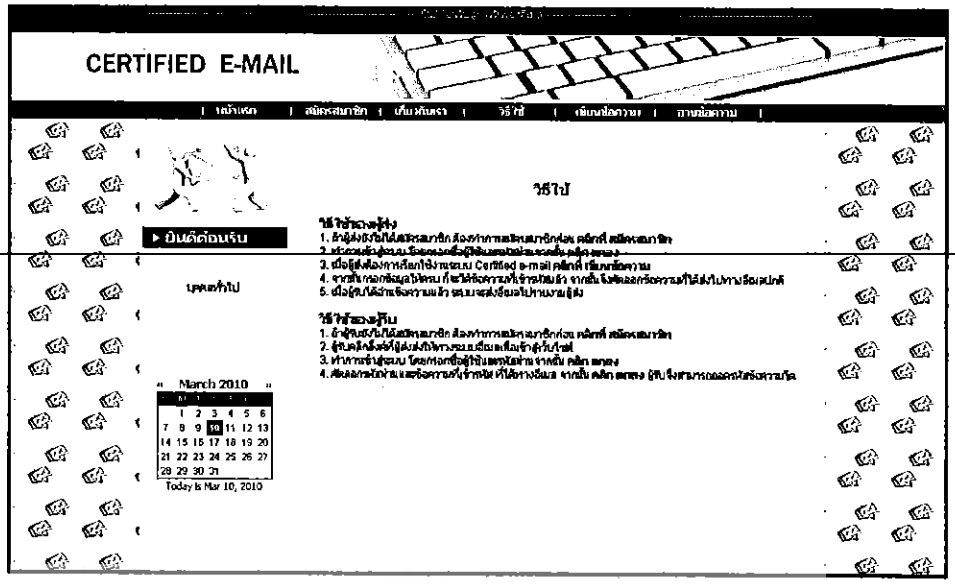
รูปที่ 4.1 หน้าแรก



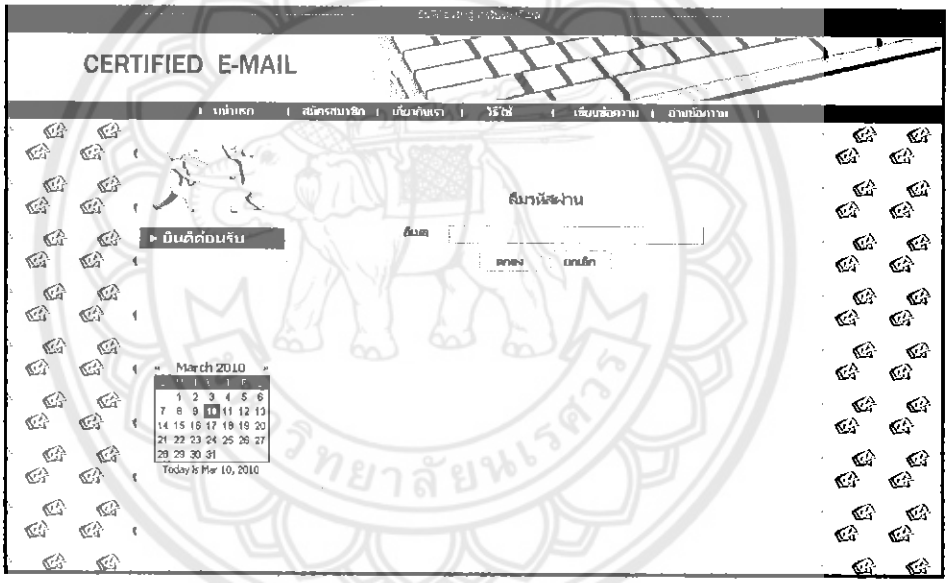
รูปที่ 4.2 หน้าการสมัครสมาชิก



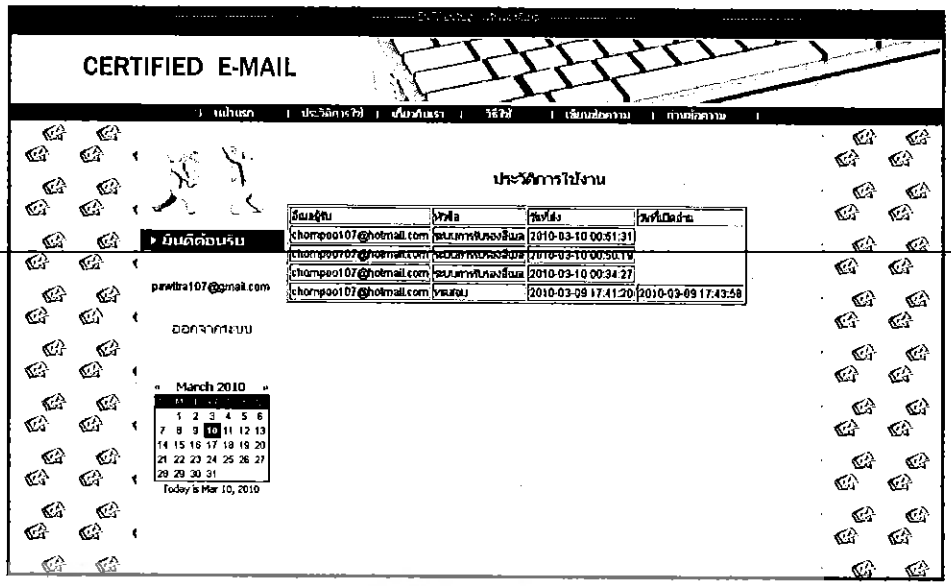
รูปที่ 4.3 หน้าเกี่ยวกับเรา



รูปที่ 4.4 หน้าวิธีใช้



รูปที่ 4.5 หน้าลืมรหัสผ่าน



รูปที่ 4.6 หน้าประวัติการใช้

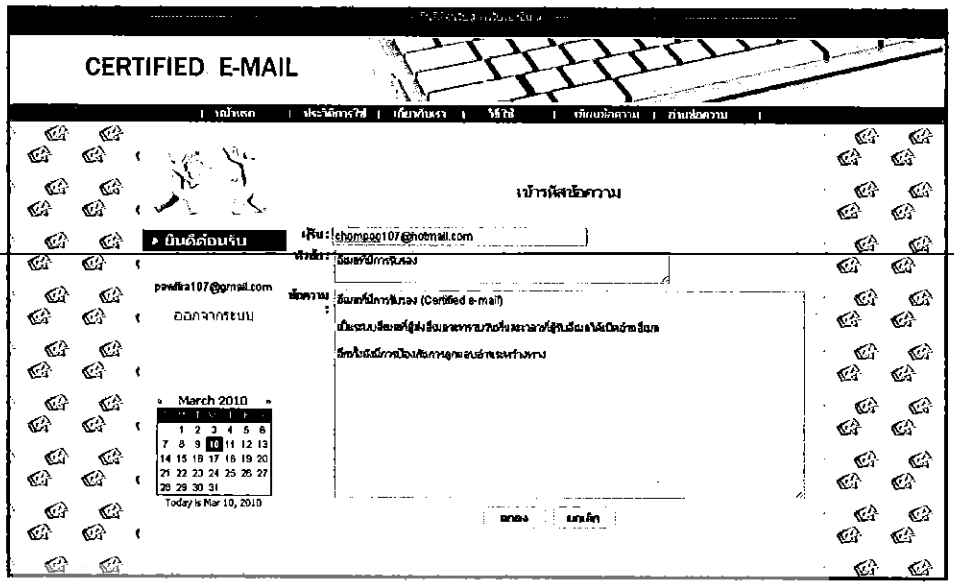
4.2.2 การใช้งานหน้าเวปไซต์เมื่อมีการร้องขอระบบอีเมลที่มีการรับรอง (ผู้ส่ง)

ก่อนที่ผู้ส่งจะทำการเขียนข้อความต้องเข้าสู่ระบบก่อน ด้วยการกรอก**ชื่อผู้ใช้และรหัสผ่าน**ที่หน้าแรกของเว็บไซต์ หลังจากนั้นจะมีการใช้งานดังต่อไปนี้

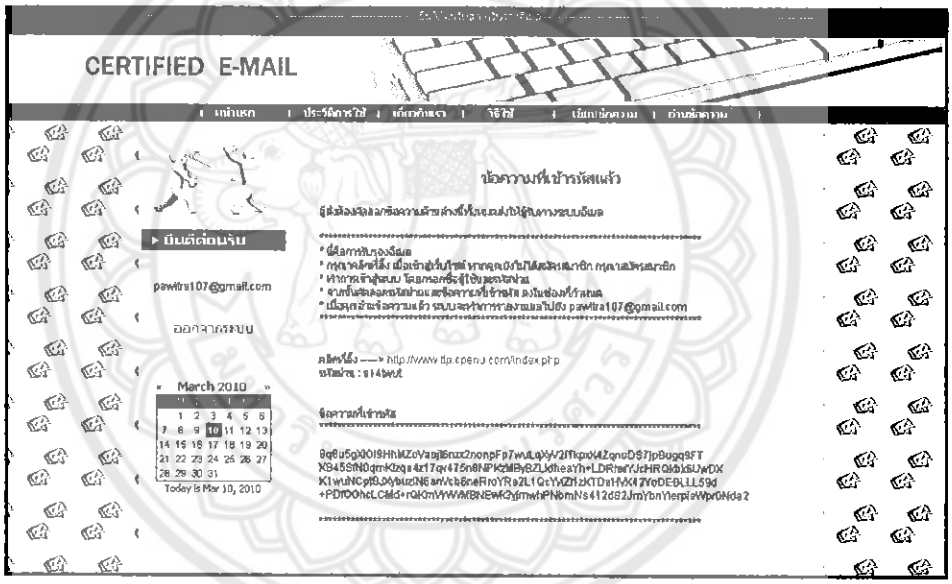
1. หน้าเขียนข้อความ ผู้ส่งจะต้องกรอกข้อมูลให้ครบถ้วน ดังแสดงใน**รูปที่** 4.7

2. เมื่อคลิกตกลงแล้ว ระบบจะเก็บข้อมูลลงฐานข้อมูลและทำการเข้า**รหัสข้อความ ผู้ส่งต้องคัดลอก**ข้อความที่ได้จากหน้าเว็บไซต์ส่งอีเมลไปหาผู้รับด้วยอีเมลปกติ ดังแส**ดงในรูปที่** 4.8

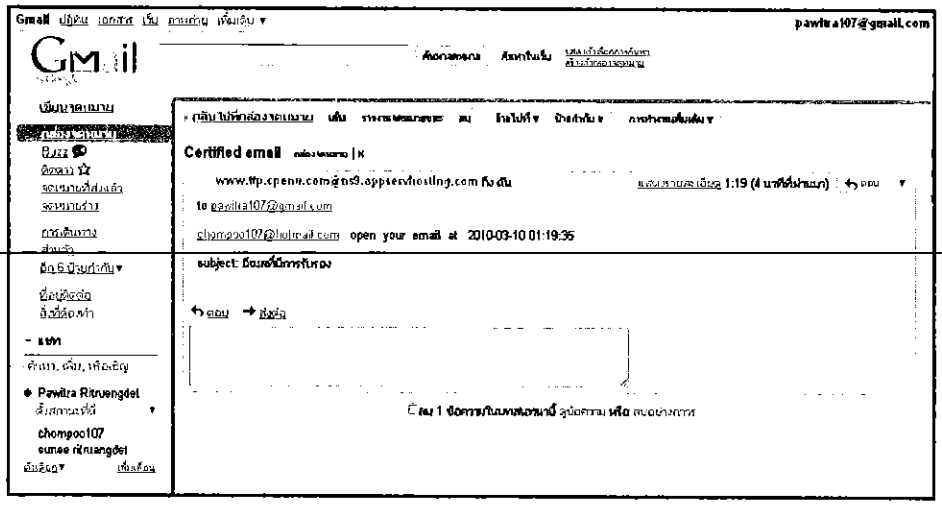
3. เมื่อผู้รับได้เปิดอ่านข้อความแล้ว ระบบจะส่งหลักฐานการยืนยันวัน**ที่และเวลาที่ผู้รับเปิดอ่าน**อีเมลไปให้ผู้ส่งทางระบบอีเมล ดังแสดงในรูปที่ 4.9



รูปที่ 4.7 หน้าเขียนข้อความ



รูปที่ 4.8 หน้าข้อความที่เข้ารหัสแล้ว



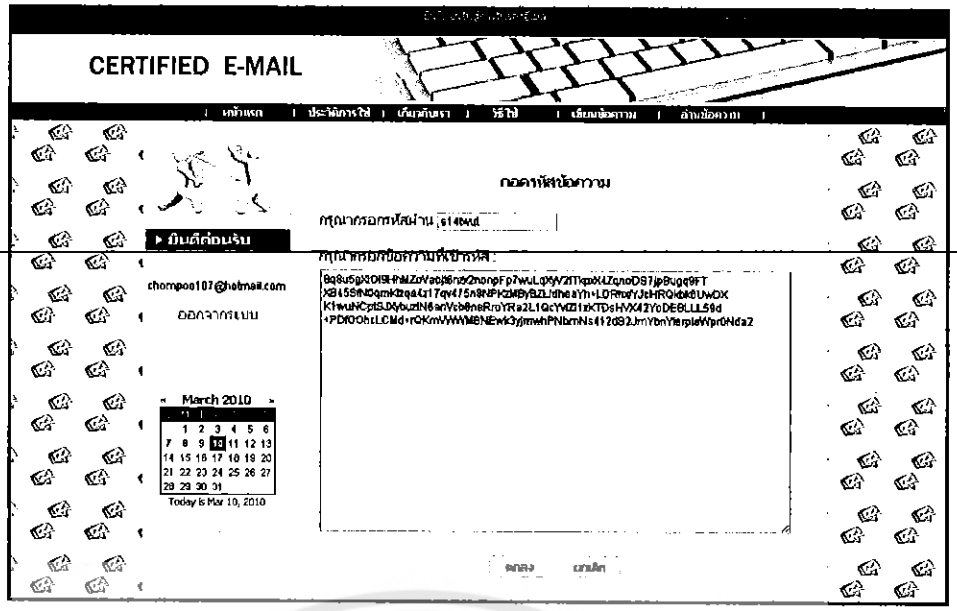
รูปที่ 4.9 ระบบรายงานผลไปยังอีเมลผู้ส่ง

4.2.3 การใช้งานหน้าเวปไซต์เมื่อมีการร้องขอระบบอีเมลที่มีการรับรอง (ผู้รับ)

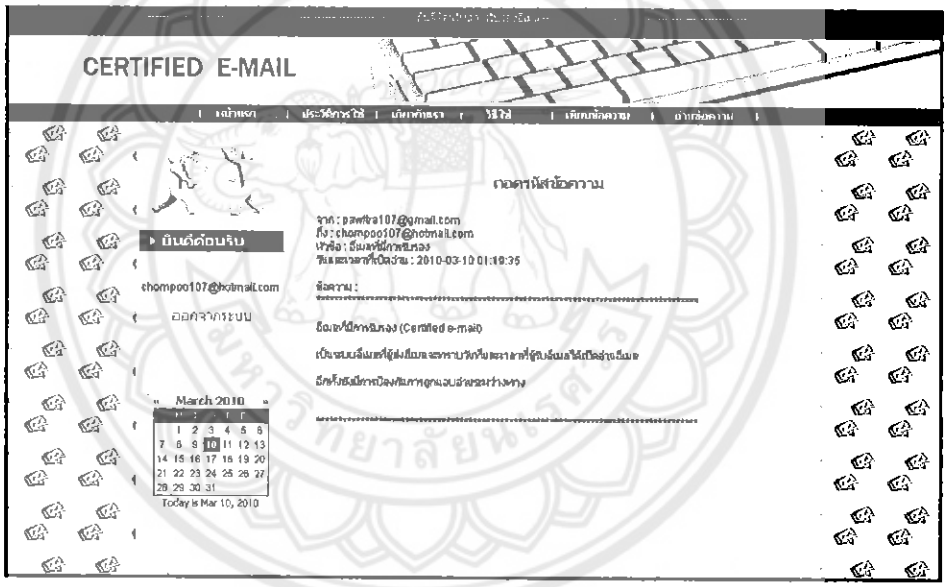
ก่อนที่ผู้รับจะทำการอ่านข้อความต้องเข้าสู่ระบบก่อน ด้วยการกรอกชื่อผู้ใช้และรหัสผ่านที่หน้าแรกของเว็ปไซต์ หลังจากนั้นจะมีขั้นตอนดังต่อไปนี้

1. เมื่อผู้รับได้รับข้อความทางอีเมลจากผู้ส่ง ให้ทำการคลิกที่ลิ้งค์เพื่อเข้าสู่เว็ปไซต์แล้วทำการเข้าสู่ระบบ จากนั้นไปที่หน้าอ่านข้อความ กรอกรหัสผ่านและข้อความที่ได้ในอีเมล ดังแสดงในรูปที่ 4.10

2. เมื่อคลิกตกลง จะได้ข้อความที่ถอดรหัสแล้ว ผู้รับจึงสามารถอ่านข้อความได้ ดังแสดงในรูปที่ 4.11



รูปที่ 4.10 หน้าอ่านข้อความ



รูปที่ 4.11 หน้าข้อความที่ถอดรหัสแล้ว

บทที่ 5
สรุปผลการทำงานของระบบ

โครงงานนี้ได้ทำการสร้างระบบอีเมลที่มีการรับรอง ซึ่งเป็นระบบที่ช่วยสร้างความมั่นใจให้แก่ผู้ส่งอีเมลว่าข้อความนั้นถึงผู้รับและสามารถป้องกันการถูกแอบอ่านระหว่างทางได้ เพราะข้อความจะถูกเข้ารหัสไว้ โครงงานนี้ใช้ภาษาพีเอชพีและฐานข้อมูลมายเอสคิวแอลเป็นหลัก เนื่องจากเป็นภาษาที่พัฒนาได้ง่ายและมีความยืดหยุ่นในด้านการเขียนโปรแกรมค่อนข้างสูง ทำให้ง่ายต่อการสร้างระบบ

5.1 สรุปผลการทำงานของระบบอีเมลที่มีการรับรอง

จากการสร้างระบบอีเมลที่มีการรับรองสามารถสรุปผลการดำเนินงานได้ดังนี้

1. ได้ระบบอีเมลที่มีการรับรองที่สามารถนำไปใช้งานได้จริง
2. ผู้ส่งสามารถทราบวันที่และเวลาที่ผู้รับได้อ่านอีเมล จากหลักฐานการยืนยันวันที่และเวลาที่ผู้รับได้เปิดอ่านข้อความที่ทางเวปไซต์ที่ทำหน้าที่เป็นบุคคลที่สามที่น่าเชื่อถือส่งให้
3. ผู้ส่งสามารถป้องกันการถูกแอบอ่านระหว่างทาง จากการเข้ารหัส – ถอดรหัสข้อความ

5.2 ปัญหาและแนวทางแก้ไขจากการสร้างระบบ

จากการสร้างระบบอีเมลที่มีการรับรองพบปัญหาและอุปสรรคต่าง ๆ ดังนี้

1. ในช่วงแรกผู้จัดทำยังไม่มีความเข้าใจในเรื่องของโปรโตคอลในระบบอีเมลที่มีการรับรอง เนื่องจากเอกสารที่เกี่ยวข้องนั้นเป็นภาษาอังกฤษทำให้ยากต่อการทำความเข้าใจ จึงทำให้การออกแบบโปรโตคอลล่าช้าและมีการแก้ไขหลายครั้ง เพื่อให้ได้โปรโตคอลที่ดีที่สุด
2. เนื่องจากผู้จัดทำไม่มีความรู้ในการเขียนภาษาสคริปต์พีเอชพีและการใช้โปรแกรมดรีมวีฟเวอร์จึงทำให้การสร้างระบบมีความล่าช้า เมื่อเกิดปัญหาทำให้ต้องใช้เวลานานในการแก้ไขปัญหา เพื่อที่จะให้การสร้างระบบเป็นไปด้วยดีควรที่จะทำการศึกษาภาษาและเครื่องมือที่จะต้องใช้ไว้ล่วงหน้า

5.3 ข้อจำกัดของระบบ

1. ระบบอีเมลที่มีการรับรองสามารถส่งข้อความแบบตัวอักษรได้เท่านั้น เนื่องจากระบบอีเมลที่มีการรับรองที่สร้างขึ้นนั้นยังไม่รองรับการส่งข้อความแบบแนบไฟล์

2. ระบบอีเมลที่มีการรับรองสามารถส่งข้อความถึงผู้รับได้เพียงครั้งละหนึ่งคนเท่านั้น เนื่องจากระบบอีเมลที่มีการรับรองที่สร้างขึ้นนั้นยังไม่รองรับการส่งข้อความถึงผู้รับได้ทีละหลาย ๆ คน

5.4 ข้อเสนอแนะในการพัฒนาต่อไป

จากการสร้างระบบอีเมลที่มีการรับรองผู้จัดทำได้มีแนวคิดและคำแนะนำจากบุคคลอื่น ๆ และจากข้อจำกัดของระบบ ซึ่งอาจเป็นประโยชน์ต่อผู้ที่ต้องการพัฒนาระบบต่อไป

1. สร้างระบบอีเมลที่มีการรับรองที่สามารถส่งข้อความแบบแนบไฟล์ได้ เพื่อที่ทำให้ระบบมีประโยชน์ต่อผู้ที่ต้องการร้องขอระบบอีเมลที่มีการรับรองมากยิ่งขึ้น

2. สร้างระบบอีเมลที่มีการรับรองที่สามารถส่งถึงผู้รับได้ทีละหลาย ๆ คน เพื่อเป็นการประหยัดเวลาและช่วยให้ผู้ที่ต้องการร้องขอระบบอีเมลที่มีการรับรองมีความสะดวกมากยิ่งขึ้น

เอกสารอ้างอิง

[1] Mart'ın Abadi. (May 7-11, 2002). **Certified Email with a Light Online Trusted Third Party: Design and Implementation.** Retrieved July 1, 2009, from http://www2002.org/CDROM/refereed/488/.

[2] อาสาสมัครผู้เขียนวิกิพีเดีย. (26 เมษายน 2550). อีเมล. **วิกิพีเดีย สารานุกรมเสรี.** สืบค้นเมื่อ 9 มีนาคม 2553, จาก http://th.wikipedia.org/wiki/อีเมล

[3] **ระบบเมล์ (Mail System).** สืบค้นเมื่อ 20 กันยายน 2552, จาก http://www.skh.moph.go.th/itwizard/technology/general/Mail%20System.htm.

[4] ดร. บรรจง หะรังษี. (6 สิงหาคม 2547). **ความรู้เบื้องต้นของการเข้ารหัสข้อมูล (Introduction to Cryptography). ThaiCERT : Thai Computer Emergency Response Team ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย.** สืบค้นเมื่อ 20 กันยายน 2552, จาก http://www.thaicert.org/paper/encryption/intro_crypt.php

[5] **tawanaugust. (**15 มีนาคม 2552**).** การเข้ารหัสข้อมูล (Encryption). **Bloggang.com.** สืบค้นเมื่อ 20 กันยายน 2552, จาก http://www.bloggang.com/viewdiary.php?id=itm0073&month=03-2009&date=15&group=6&gblog=1

[6] Wikipedia contributors. (November 10,2001). Advanced Encryption Standard. **Wikipedia, the free encyclopedia. Retrieved March 5, 2010, from** http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

[7] MiZaKi. (12 กันยายน 2550). Base64. **HEKKERGAMES.** สืบค้นเมื่อ 22 กันยายน 2552, จาก http://hekkergames.blogspot.com/search?updated-max=2007-09-12T12:43:00%2B07:00&max-results=7

[8] อาจารย์ชัยนันท์ สมพงษ์. (3 มิถุนายน 2551). การเข้ารหัสข้อมูล. **เอกสารประกอบการเรียน.** สืบค้นเมื่อ 26 กุมภาพันธ์ 2553, จาก teacher.snru.ac.th/chaiyanan/admin/document/.../Code.ppt

เอกสารอ้างอิง (ต่อ)

[9] ครูสุนันตา สะราคำ. (17 พฤศจิกายน 2552). ข้อมูลในคอมพิวเตอร์. **บทเรียนเครือข่าย Web Base Instruction.** สืบค้นเมื่อ 26 กุมภาพันธ์ 2553, จาก http://krusunanta.net/main/chapter2/chapter2-sub3

[10] บัญชา ปะสีละเตสัง. (2550). **PHP5 และ MySQL5.** กรุงเทพมหานคร : บริษัท ซีเอ็ดยูเคชั่น จำกัด (มหาชน).

[11] Jim Wigginton. (May 27, 2009). **PHP Secure Communications Library.** Retrieved October 7,2009 from http://phpseclib.sourceforge.net/

ภาคผนวก ก.
การใช้งานไลบรารีเข้ารหัส – ถอดรหัสข้อความ

ก.1 การใช้งานไลบรารีของอัลกอริทึม AES (Rijndael)

ดาวน์โหลดไลบรารีที่ http://phpseclib.sourceforge.net/ จะได้ไฟล์ phpseclib0.2.0.zip จากนั้น Extract ไฟล์ ได้ออกมาทั้งหมด 4 โฟล์เดอร์ นำโฟล์เดอร์ทั้งหมดไปไว้ที่ C:\AppServ\www\ชื่อโฟล์เดอร์ที่เก็บไฟล์.php [11]

1. โค้ดการเรียกใช้ไลบรารี

```
include('Crypt/Rijndael.php');
$rijndael = new Crypt_Rijndael();
$size = 1;
$rijndael->setKey('abcdefghijklmnopqrstuvwxyz012345');
$ciphertext3 = '';
for ($i = 0; $i < $size; $i++)
{
        $ciphertext3.= $rijndael->decrypt($ciphertext);
}
```

ประวัติผู้เขียนโครงงาน

ชื่อ นางสาวปวิตรา ฤทธิ์เรืองเดช

ภูมิลำเนา 381 ม.8 ต.หนองไม้กอง อ.ไทรงาม จ.กำแพงเพชร

ประวัติการศึกษา

- จบระดับมัธยมศึกษาจากโรงเรียนไทรงามพิทยาคม
- ปัจจุบันกำลังศึกษาในระดับปริญญาตรีชั้นปีที่ 4

สาขาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์

มหาวิทยาลัยนเรศวร

E-mail : chompoo107@hotmail.com

ชื่อ นางสาวโสภา ห้วยหงษ์ทอง

ภูมิลำเนา 141/2 ม.4 ต.ระหาน อ.บึงสามัคคี จ.กำแพงเพชร

ประวัติการศึกษา

- จบระดับมัธยมศึกษาจากโรงเรียนระหานวิทยา
- ปัจจุบันกำลังศึกษาในระดับปริญญาตรีชั้นปีที่ 4

สาขาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์

มหาวิทยาลัยนเรศวร

E-mail : kum_kum0707@hotmail.com