

สำนักหอสมุดกลาง พระจอมเกล้าลาดกระบัง

ระบบความปลอดภัยในเครือข่ายสำหรับการซื้อขายสินค้าออนไลน์

NETWORK SECURITY SYSTEM FOR E-COMMERCE



ปัญหาพิเศษนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรบัณฑิต

ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์

คณะวิทยาศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2548

เลขหมู่.....

เลขทะเบียน.....

วัน,เดือน,ปี.....

419678
.....
.....

เอกสารนี้สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า

ห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

# **NETWORK SECURITY SYSTEM FOR E-COMMERCE**



**A SPECIAL PROJECT SUBMITTED IN PARTIAL FULFILLMENT  
OF THE REQUIREMENT FOR THE DEGREE OF BACHELOR OF SCIENCE  
DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE  
FACULTY OF SCIENCE  
KING MONGKUT'S INSTITUTE OF TECHNOLOGY LARDKRABANG  
ACADEMIC YEAR 2005**

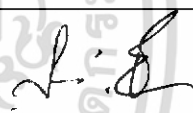


เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

**หัวข้อปัญหาพิเศษ** ระบบความปลอดภัยในเครือข่ายสำหรับการซื้อขายสินค้าออนไลน์  
**NETWORK SECURITY SYSTEM FOR E-COMMERCE**

**ชื่อนักศึกษา** นางสาวดวงกมล อรพินท์พงษ์ 45050475  
 นางสาวนฤมล ปรารักษ์นรินทร์ 45050486  
 นางสาวสุทธิมา สุดสาคร 45050536

**ปริญญา** วิทยาศาสตรบัณฑิต  
**ภาควิชา** คณิตศาสตร์และวิทยาการคอมพิวเตอร์  
**สาขา** วิทยาการคอมพิวเตอร์  
**ปีการศึกษา** 2548  
**อาจารย์ที่ปรึกษา** อ.สังกรศรีณีย์ ล่องชูผล

ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง อนุมัติให้นำปัญหาพิเศษนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์ ประจำปีการศึกษา 2548

คณะกรรมการสอบ	ลายมือชื่อ
ประธานกรรมการ อ. วีระชัย ตันยะสิทธิ์	
กรรมการ ผศ. สิริลักษณ์ อนันต์สถิตย์สิน	
กรรมการและอาจารย์ที่ปรึกษา อ. สังกรศรีณีย์ ล่องชูผล	

(รองศาสตราจารย์ ดร.วีระ บุญจริง)

หัวหน้าภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์

ลิขสิทธิ์ของภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

หัวข้อปัญหาพิเศษ	ระบบความปลอดภัยในเครือข่ายสำหรับการซื้อขายสินค้าออนไลน์
ชื่อนักศึกษา	นางสาวดวงกมล อรพินท์พงษ์ 45050475
	นางสาวนฤมล ปรารักษ์นวัฒน์ 45050486
	นางสาวสุทธิมา สุธสาคร 45050536
ปริญญา	วิทยาศาสตรบัณฑิต
ภาควิชา	คณิตศาสตร์และวิทยาการคอมพิวเตอร์
สาขา	วิทยาการคอมพิวเตอร์
ปีการศึกษา	2548
อาจารย์ที่ปรึกษา	อ.สังกรศรีณย์ ต่องชุมผล

### บทคัดย่อ

ปัญหาพิเศษนี้เป็นการพัฒนาระบบความปลอดภัยในเครือข่ายสำหรับการซื้อขายสินค้าออนไลน์ ที่นำหลักการของการเข้ารหัสและลายมือชื่อดิจิตอลมาใช้ในการระบุตัวผู้ส่งข้อมูล และป้องกันการลักลอบดักจับข้อมูลระหว่างทาง เพื่อทำให้เกิดความปลอดภัยและสร้างความมั่นใจให้กับผู้ใช้งานธุรกรรมผ่านอินเทอร์เน็ต ระบบประกอบด้วย 5 ส่วนคือส่วนลูกค้า ส่วนร้านค้า ส่วนธนาคาร ส่วนบริษัทบัตรเครดิต และส่วนองค์กรพิสูจน์สิทธิ์ ซึ่งทุกๆส่วนสามารถสื่อสารกันเพื่อทำการซื้อขายสินค้าออนไลน์ โดยมีการเข้ารหัสข้อมูลที่จะส่ง เพื่อความปลอดภัยของข้อมูล โดยระบบพัฒนาขึ้นมาโดยใช้ Microsoft Visual C++ .NET บนระบบปฏิบัติการวินโดวส์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

<b>Special Project Title</b>	NETWORK SECURITY SYSTEM FOR E-COMMERCE
<b>Student</b>	Miss Duangkamol Orpinpong 45050475 Miss Narumol Prangnawarat 45050486 Miss Sutthima Sudsakorn 45050536
<b>Degree</b>	Bachelor of Science
<b>Department</b>	Mathematics and Computer Science, Faculty of Science
<b>Programme</b>	Computer Science
<b>Academic Year</b>	2005
<b>Special Project Adviser</b>	Sungkornsarun Longchupole

### ABSTRACT

This special problem is development of network security system for e-commerce. The system uses the principles of cryptography and digital signature to identify users and keep data safe from potential intruders when it is in transit. It consists of 5 parts : client, shop server, bank server, verification server and certificate authority server. All parts communicate using principle of data security. The system is developed using Microsoft Visual C++.NET.

## กิตติกรรมประกาศ

ในการทำปัญหาพิเศษเรื่องระบบความปลอดภัยในเครือข่ายสำหรับการซื้อขายสินค้าออนไลน์ สามารถสำเร็จลุล่วงไปด้วยดี คณะผู้จัดทำต้องขอขอบพระคุณอาจารย์ศังกรศรีณย์ ล่องชูผล อาจารย์ผู้รับผิดชอบปัญหาพิเศษนี้ที่กรุณาให้คำแนะนำและเป็นທີ່ปรึกษาในการแก้ปัญหาต่างๆ รวมทั้งเป็นผู้ตรวจสอบความถูกต้องของปัญหาพิเศษนี้

นอกจากนี้คณะผู้จัดทำต้องขอขอบพระคุณบิดา มารดา สำหรับกำลังใจ, ทุนทรัพย์ และทุกสิ่งทุกอย่าง ขอขอบพระคุณอาจารย์ทุกท่านที่ได้อบรมสั่งสอนให้ความรู้ทั้งทางด้านทฤษฎีและปฏิบัติแก่คณะผู้จัดทำ และขอขอบคุณเพื่อนๆ ทุกคนที่ให้คำแนะนำและคำปรึกษาในด้านต่างๆ เกี่ยวกับปัญหาพิเศษมา ณ ที่นี้ด้วย

คณะผู้จัดทำ  
มีนาคม 2549



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## สารบัญ

	หน้า
บทคัดย่อปัญหาพิเศษภาษาไทย .....	I
บทคัดย่อปัญหาพิเศษภาษาอังกฤษ .....	II
กิตติกรรมประกาศ .....	III
สารบัญ .....	IV
สารบัญตาราง .....	IX
สารบัญรูป .....	X
<b>บทที่ 1 บทนำ .....</b>	<b>1</b>
1.1 ความเป็นมาและความสำคัญของปัญหา .....	1
1.2 วัตถุประสงค์ของปัญหาพิเศษ .....	1
1.3 ขอบเขตของปัญหาพิเศษ .....	1
1.4 ประโยชน์ที่คาดว่าจะได้รับ .....	2
1.5 ขั้นตอนในการดำเนินการ .....	2
<b>บทที่ 2 ทฤษฎีที่เกี่ยวข้อง .....</b>	<b>3</b>
2.1 ความรู้เบื้องต้นเกี่ยวกับการค้าออนไลน์ .....	3
2.1.1 การชำระเงินทางอิเล็กทรอนิกส์ .....	3
2.1.1.1 การชำระเงินผ่านบัตรเครดิต .....	3
2.1.1.2 การชำระเงินผ่าน เซ็คอีเล็กทรอนิกส์ .....	4
2.1.1.3 การชำระเงินโดย เงินสดดิจิทัล .....	4
2.1.2 ความปลอดภัยของข้อมูล .....	4
2.1.2.1 หลักการของระบบความปลอดภัยในระบบ .....	5
2.1.2.2 สิ่งจำเป็นที่ต้องมีในระบบรักษาความปลอดภัย .....	5
2.1.2.3 การเข้ารหัสข้อมูล .....	5
2.1.2.3.1 การเข้ารหัสแบบสมมาตร .....	5
2.1.2.3.2 การเข้ารหัสแบบไม่สมมาตร .....	6
2.1.2.4 การเข้ารหัสแบบผสมกุญแจสมมาตรและกุญแจไม่สมมาตร .....	7
2.1.2.5 ลายมือชื่อดิจิทัล .....	7

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## สารบัญ (ต่อ)

	หน้า
2.1.2.6 ไบรร์รองคิจิตอล.....	8
2.1.2.7 องค์กรร์รับรองความถูกต้อง.....	9
2.2 อัลกอริทึมในการเข้ารหัส.....	9
2.2.1 ตัวอย่างอัลกอริทึมในการเข้ารหัส.....	9
2.2.1.1 ตัวอย่างอัลกอริทึมการเข้ารหัสแบบสมมาตร.....	9
2.2.1.1.1 อัลกอริทึม DES.....	9
2.2.1.1.2 อัลกอริทึม Triple-DES.....	9
2.2.1.1.3 อัลกอริทึม IDEA.....	9
2.2.1.1.4 อัลกอริทึม AES.....	10
2.2.1.2 ตัวอย่างอัลกอริทึมการเข้ารหัสแบบไม่สมมาตร.....	10
2.2.1.2.1 อัลกอริทึม RSA.....	10
2.2.1.3 ตัวอย่างอัลกอริทึมการสร้างเมสเชจไคเจสค์.....	10
2.2.1.3.1 อัลกอริทึม MD2.....	10
2.2.1.3.2 อัลกอริทึม MD4.....	10
2.2.1.3.3 อัลกอริทึม MD5.....	10
2.2.1.3.4 อัลกอริทึม SHA.....	10
2.2.1.3.5 อัลกอริทึม SHA-1.....	11
2.2.1.3.6 อัลกอริทึม SHA-256, SHA-384 และ SHA-512.....	11
2.2.2 อัลกอริทึมในการเข้ารหัสโดยละเอียด.....	11
2.2.2.1 อัลกอริทึมการเข้ารหัสแบบสมมาตร.....	11
2.2.2.1.1 อัลกอริทึม DES (Data Encryption Standard).....	11
2.2.2.1.2 อัลกอริทึม AES (Advanced Encryption Standard).....	20
2.2.2.2 อัลกอริทึมในการเข้ารหัสแบบไม่สมมาตร.....	22
2.2.2.2.1 อัลกอริทึม RSA.....	22
2.2.2.3 อัลกอริทึมสำหรับสร้างเมสเชจไคเจสค์.....	23
2.2.2.3.1 MD5 Algorithm.....	23
2.2.2.3.2 อัลกอริทึม SHA-1.....	26

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## สารบัญ (ต่อ)

	หน้า
<b>บทที่ 3 การทำงานของระบบ.....</b>	<b>28</b>
3.1 ขอบเขตการทำงาน .....	28
3.1.1 ส่วนการซื้อขายสินค้าออนไลน์.....	28
3.1.2 ส่วนการชำระเงินออนไลน์.....	28
3.1.3 ส่วนการบริการออกไปรับรองอิเล็กทรอนิกส์และการพิสูจน์สิทธิ์ .....	28
3.2 การแบ่งส่วนโปรแกรม .....	28
3.2.1 ส่วนของลูกค้า.....	28
3.2.2 ส่วนของร้านค้า .....	29
3.2.3 ส่วนของธนาคาร .....	29
3.2.4 ส่วนของบริษัทบัตรเครดิต .....	29
3.2.5 ส่วนขององค์กรพิสูจน์สิทธิ์.....	29
3.3 การสื่อสารกันภายในระบบ.....	29
3.3.1 การสื่อสารระหว่างลูกค้ากับร้านค้า .....	30
3.3.2 การสื่อสารระหว่างลูกค้ากับธนาคาร .....	31
3.3.3 การสื่อสารระหว่างลูกค้ากับบริษัทบัตรเครดิต .....	31
3.3.4 การสื่อสารระหว่างลูกค้ากับองค์กรพิสูจน์สิทธิ์.....	31
3.3.5 การสื่อสารระหว่างร้านค้ากับองค์กรพิสูจน์สิทธิ์.....	31
3.3.6 การสื่อสารระหว่างร้านค้ากับธนาคาร .....	31
3.3.7 การสื่อสารระหว่างบริษัทบัตรเครดิตกับธนาคาร .....	31
3.4 ขั้นตอนการทำงานในระบบ.....	32
3.4.1 ขั้นตอนการสั่งซื้อสินค้า .....	32
3.4.2 ขั้นตอนการชำระเงิน โดยบัตรเครดิต .....	33
3.4.3 ขั้นตอนการยืนยันตัวตนสำหรับบัตรเครดิตกรณีไม่ลงลายมือชื่อดิจิทัล .....	34
3.4.4 ขั้นตอนการยืนยันตัวตนสำหรับบัตรเครดิตกรณีลงลายมือชื่อดิจิทัล.....	35
3.4.5 ขั้นตอนการตรวจสอบเครดิตและ โอนเงิน .....	36
3.4.6 ขั้นตอนการชำระเงินโดยการตัดบัญชีชำระล่วงหน้า .....	37

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## สารบัญ (ต่อ)

	หน้า
<b>บทที่ 4 การออกแบบระบบและพัฒนาระบบ.....</b>	<b>38</b>
4.1 โครงสร้างของโปรแกรม .....	38
4.1.1 โครงสร้างของโปรแกรมส่วนร้านค้า.....	38
4.1.2 โครงสร้างของโปรแกรมส่วนธนาคาร .....	40
4.1.3 โครงสร้างของโปรแกรมส่วนบริษัทบัตรเครดิต .....	41
4.1.4 โครงสร้างของโปรแกรมส่วนองค์กรพิสูจน์สิทธิ์.....	43
4.2 การเก็บข้อมูล .....	44
4.2.1 ฐานข้อมูลของร้านค้า.....	44
4.2.2 ฐานข้อมูลของธนาคาร .....	44
4.2.3 ฐานข้อมูลของบริษัทบัตรเครดิต .....	45
4.2.4 ฐานข้อมูลขององค์กรพิสูจน์สิทธิ์.....	45
4.3 หน้าจอของระบบ.....	45
4.3.1 หน้าจอส่วนของลูกค้า.....	45
4.3.2 หน้าจอส่วนของร้านค้า.....	52
4.3.3 หน้าจอส่วนของธนาคาร .....	53
4.3.4 หน้าจอส่วนของบริษัทบัตรเครดิต.....	54
4.3.5 หน้าจอส่วนขององค์กรพิสูจน์สิทธิ์.....	55
<b>บทที่ 5 สรุปผลและข้อเสนอแนะ.....</b>	<b>56</b>
5.1 สรุปผลปัญหาพิเศษ.....	56
5.2 ข้อจำกัดของปัญหาพิเศษ.....	56
5.3 ข้อเสนอแนะและแนวทางการศึกษาต่อ.....	57
<b>ภาคผนวก.....</b>	<b>58</b>
<b>ภาคผนวก ก การติดตั้งโปรแกรมที่ใช้ในการพัฒนาระบบ.....</b>	<b>59</b>
<b>ภาคผนวก ข คู่มือการติดตั้งโปรแกรม .....</b>	<b>67</b>
<b>ภาคผนวก ค การใช้งานโปรแกรม.....</b>	<b>79</b>
<b>ภาคผนวก ง ตัวอย่างรายงาน .....</b>	<b>93</b>

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## สารบัญ (ต่อ)

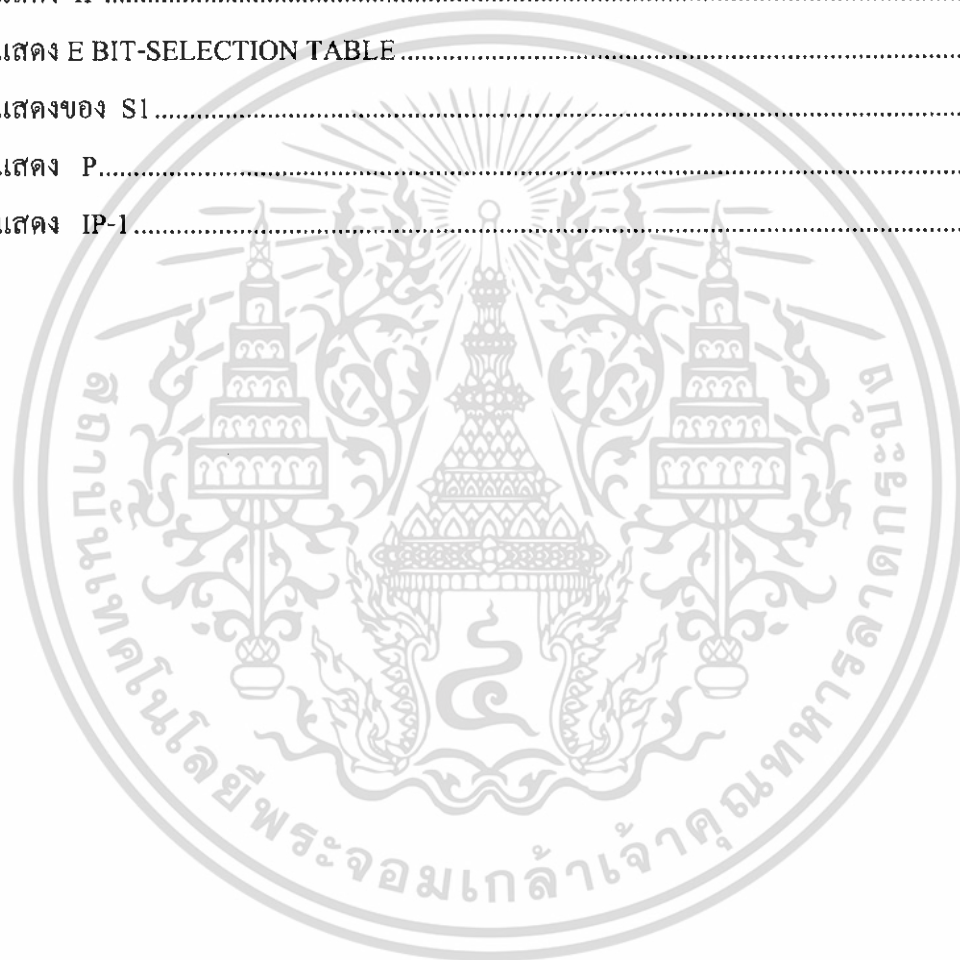
บรรณานุกรม .....	หน้า 102
------------------	----------



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## สารบัญตาราง

ตารางที่	หน้า
2.1 เปรียบเทียบข้อดีข้อเสียของแต่ละแบบ .....	6
2.2 PC-1 .....	12
2.3 แสดงจำนวนการเลื่อนทางซ้าย.....	13
2.4 PC-2.....	14
2.5 แสดง IP .....	15
2.6 แสดง E BIT-SELECTION TABLE .....	16
2.7 แสดงของ S1 .....	17
2.8 แสดง P.....	18
2.9 แสดง IP-1 .....	19



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## สารบัญรูป

รูปที่	หน้า
2.1 แสดงการเข้ารหัสแบบสมมาตร .....	5
2.2 แสดงการเข้ารหัสแบบไม่สมมาตร.....	6
2.3 แสดงการเข้ารหัสแบบผสม.....	7
2.4 แสดงการลงลายมือชื่อดิจิทัล.....	8
2.5 แสดงคีย์ 56 บิต ที่เรียงลำดับแล้วถูกแบ่งเป็น 2 ส่วน .....	11
2.6 แสดงบล็อกของข้อมูลขนาด 64 บิต ถูกแบ่งเป็น 2 บล็อก.....	12
2.7 แสดงการทำ SubBytes.....	20
2.8 แสดงการทำ ShiftRows .....	21
2.9 แสดงการทำ MixColumns .....	21
2.10 แสดงการทำ AddRoundKey.....	21
3.1 การสื่อสารกันระหว่างลูกค้า ร้านค้า ธนาคาร บริษัทบัตรเครดิต และองค์กรพิสูจน์สิทธิ์.....	29
3.2 ตัวอย่างแคตตาล็อกสินค้า .....	30
3.3 ขั้นตอนการสั่งซื้อสินค้า.....	32
3.4 ขั้นตอนการชำระเงินโดยบัตรเครดิต.....	33
3.5 ขั้นตอนการยืนยันตัวตนสำหรับบัตรเครดิตกรณีไม่ลงลายมือชื่อดิจิทัล.....	34
3.6 ขั้นตอนการยืนยันตัวตนสำหรับบัตรเครดิตกรณีลงลายมือชื่อดิจิทัล.....	35
3.7 ขั้นตอนการตรวจสอบเครดิตและ โอนเงิน .....	36
3.8 ขั้นตอนการชำระเงินโดยการตัดบัญชีร้านค้า .....	37
4.1 โครงสร้างของโปรแกรมส่วนร้านค้า.....	38
4.2 โครงสร้างของโปรแกรมส่วนธนาคาร .....	40
4.3 โครงสร้างของโปรแกรมส่วนบริษัทบัตรเครดิต.....	41
4.4 โครงสร้างของโปรแกรมส่วนองค์กรพิสูจน์สิทธิ์.....	43
4.5 แผนผังแสดงความสัมพันธ์ในฐานข้อมูลร้านค้า .....	44
4.6 แผนผังแสดงความสัมพันธ์ในฐานข้อมูลธนาคาร .....	44
4.7 แผนผังแสดงความสัมพันธ์ในฐานข้อมูลบริษัทบัตรเครดิต .....	45
4.8 แผนผังแสดงฐานข้อมูลองค์กรพิสูจน์สิทธิ์ .....	45
4.9 หน้าจอต้อนรับเมื่อเข้าสู่โปรแกรม .....	46
4.10 หน้าจอหลักของส่วนลูกค้า .....	46

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## สารบัญรูป (ต่อ)

รูปที่	หน้า
4.11 หน้าจอการสมัครสมาชิก.....	47
4.12 หน้าจอการลงทะเบียนบัตรเครดิต.....	47
4.13 หน้าจอการลงทะเบียนขอใบรับรองดิจิทัล.....	48
4.14 หน้าจอแสดงการแสดงผลคีย์.....	48
4.15 หน้าจอการลงทะเบียนบัญชีชำระเงินล่วงหน้ากับทางร้านค้า.....	49
4.16 หน้าจอการเข้าสู่ระบบ.....	49
4.17 หน้าจอการสั่งซื้อสินค้า.....	50
4.18 หน้าจอกรอกจำนวนสินค้า.....	50
4.19 หน้าจอแสดงการสั่งซื้อสินค้า.....	51
4.20 หน้าจอการชำระเงิน.....	51
4.21 หน้าจอการชำระเงินแสดงรายละเอียดการชำระเงิน.....	52
4.22 หน้าจอส่วนของร้านค้า.....	52
4.23 หน้าจอหลักส่วนการแสดงรายงานของร้านค้า.....	53
4.24 หน้าจอส่วนของธนาคาร.....	53
4.25 หน้าจอหลักส่วนการแสดงรายงานของธนาคาร.....	54
4.26 หน้าจอส่วนของบริษัทบัตรเครดิต.....	54
4.27 หน้าจอส่วนขององค์กรพิสูจน์สิทธิ์.....	55
ก-1 หน้าจอเริ่มต้นการติดตั้งโปรแกรม Oracle Database 10g.....	59
ก-2 แสดงการตรวจความพร้อมของเครื่องที่ทำการติดตั้งโปรแกรม.....	60
ก-3 แสดงรูปแบบการติดตั้งโปรแกรม Welcome to the Oracle Database 10g.....	60
ก-4 Oracle Universal Installer เตรียมการติดตั้ง.....	61
ก-5 แสดงผลสรุปรายละเอียดของการติดตั้งโปรแกรม.....	62
ก-6 แสดงการติดตั้งโปรแกรม.....	62
ก-7 แสดงการ Configuration Assistants.....	63
ก-8 แสดงการสร้างฐานข้อมูล.....	64
ก-9 แสดงรายละเอียดของฐานข้อมูล.....	64
ก-10 แสดงการจัดการ Password Management.....	65
ก-11 แสดงสรุปวิธีการจัดการและใช้ข้อมูล.....	65

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## สารบัญรูป (ต่อ)

รูปที่	หน้า
ก-12 แสดงการยืนยันการเสร็จสิ้นการติดตั้งโปรแกรม.....	66
ก-13 แสดงการติดตั้งโปรแกรมสำเร็จ.....	66
ข-1 ไฟล์ที่ใช้ในการติดตั้งโปรแกรมสำหรับลูกค้า.....	67
ข-2 หน้าต่างต้อนรับ.....	68
ข-3 หน้าต่างลิขสิทธิ์.....	69
ข-4 หน้าต่างระบุผู้ใช้งาน.....	70
ข-5 หน้าต่างเลือกโฟลเดอร์ในการติดตั้งโปรแกรม.....	71
ข-6 หน้าต่างแสดงโฟลเดอร์ที่ต้องการสร้างซ็อกเก็ต.....	72
ข-7 หน้าต่างแสดงรายละเอียดการลงโปรแกรม.....	73
ข-8 หน้าต่างเสร็จสิ้นการลงโปรแกรม.....	74
ข-9 ไฟล์ที่ใช้ในการติดตั้งโปรแกรมสำหรับร้านค้า.....	75
ข-10 ไฟล์ที่ใช้ในการติดตั้งโปรแกรมสำหรับธนาคาร.....	76
ข-11 ไฟล์ที่ใช้ในการติดตั้งโปรแกรมสำหรับบริษัทบัตรเครดิต.....	77
ข-12 ไฟล์ที่ใช้ในการติดตั้งโปรแกรมสำหรับองค์กรพิสูจน์สิทธิ์.....	78
ค-1 แสดงหน้าจอเริ่มต้นของ โปรแกรมลูกค้า.....	79
ค-2 แสดงหน้าจอหลักในการทำงานของ โปรแกรมลูกค้า.....	79
ค-3 แสดงหน้าจอการล็อกอินเพื่อทำการสั่งซื้อสินค้า.....	80
ค-4 แสดงหน้าจอการสั่งซื้อสินค้า.....	80
ค-5 แสดงหน้าจอการสั่งซื้อสินค้าเมื่อลูกค้าทำการเลือกประเภทของสินค้า.....	81
ค-6 แสดงหน้าจอการสั่งซื้อสินค้าให้ใส่ปริมาณสินค้า.....	81
ค-7 แสดงหน้าจอการสั่งซื้อสินค้าเมื่อลูกค้าทำการเลือกชื่อรายการสินค้า.....	82
ค-8 แสดงหน้าจอการสั่งซื้อสินค้าเมื่อลูกค้าทำการเลือกชื่อรายการสินค้า.....	82
ค-9 แสดงหน้าจอการชำระเงิน.....	83
ค-10 แสดงการชำระเงินแบบลูกค้าทำการชำระเงินไว้ล่วงหน้า.....	83
ค-11 แสดงการชำระเงินแบบที่ลูกค้ามีใบรับรองอิเล็กทรอนิกส์.....	84
ค-12 แสดงการชำระเงินแบบที่ลูกค้าไม่มีใบรับรองอิเล็กทรอนิกส์.....	84
ค-13 แสดงหน้าจอหลักของ โปรแกรม Shop Report.....	85
ค-14 แสดงหน้าจอการใส่รหัสฐานข้อมูล.....	85

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## สารบัญรูป (ต่อ)

รูปที่	หน้า
ค-15 แสดงหน้าจอรายงานรายละเอียดสมาชิก.....	86
ค-16 แสดงหน้าจอรายงานของการสั่งซื้อ.....	86
ค-17 แสดงหน้าจอรายงานรายละเอียดการสั่งซื้อ.....	87
ค-18 แสดงหน้าจอรายงานรายละเอียดสินค้า.....	87
ค-19 แสดงหน้าจอรายงานบัญชีที่ลูกค้าชำระล่วงหน้า.....	88
ค-20 แสดงหน้าจอหลักของโปรแกรม Bank Report.....	89
ค-21 หน้าจอการใส่รหัสฐานข้อมูล.....	89
ค-22 แสดงหน้าจอรายงานบัญชีของลูกค้า.....	90
ค-23 แสดงหน้าจอรายงานรายละเอียดบัญชีของลูกค้า.....	90
ค-24 แสดงหน้าจอรายงานบัตรเครดิต.....	91
ค-25 แสดงหน้าจอรายงานรายละเอียดการใช้บัตรเครดิต.....	91
ง-1 หน้าจอแสดงรายงานสมาชิก.....	94
ง-2 หน้าจอแสดงรายงานการสั่งซื้อของลูกค้า.....	95
ง-3 หน้าจอแสดงรายงานรายละเอียดการสั่งซื้อสินค้า.....	96
ง-4 หน้าจอแสดงรายงานรายละเอียดสินค้า.....	97
ง-5 หน้าจอแสดงรายงานบัญชีที่ลูกค้าชำระล่วงหน้า.....	98
ง-6 หน้าจอแสดงรายงานบัญชีของลูกค้า.....	99
ง-7 แสดงรายงานรายละเอียดบัญชีของลูกค้า.....	100
ง-8 แสดงรายงานบัตรเครดิต.....	100
ง-9 แสดงรายงานรายละเอียดบัตรเครดิต.....	101

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

# บทที่ 1

## บทนำ

### 1.1 ความเป็นมาและความสำคัญของปัญหา

เนื่องจากปัจจุบันเทคโนโลยีมีผลต่อชีวิตประจำวันมากในทุกๆด้าน โดยธุรกิจแต่ละประเภทก็ต้องปรับตัว และเปลี่ยนแปลงไปพึ่งพาเทคโนโลยีเพื่อนำเทคโนโลยีมาใช้กับธุรกิจการค้าต่างๆ อีกทั้งรูปแบบทางการตลาดก็เปลี่ยนแปลงไปทำให้เกิดธุรกิจรูปแบบใหม่ที่อาศัยอินเทอร์เน็ต และการดำเนินธุรกรรมผ่านเครือข่ายกำลังเป็นที่นิยมอย่างสูง และเพื่อเพิ่มความมั่นใจให้กับผู้ใช้งานธุรกรรมผ่านอินเทอร์เน็ต ระบบจะต้องมีความปลอดภัยที่สูงมากพอ ทั้งการพิสูจน์ตัวตน และความถูกต้องของข้อมูล โดยเฉพาะอย่างยิ่ง ความปลอดภัยทางการเงิน

โครงการนี้จึงจัดทำเพื่อเสนอแนวทางในการสร้างระบบการซื้อขายสินค้าออนไลน์ที่มีความปลอดภัย ทั้งทางด้านการเงินและความปลอดภัยของข้อมูล โดยนำหลักการของการเข้ารหัสและลายมือชื่อดิจิตอลมาใช้ในการระบุตัวผู้ส่งข้อมูล และป้องกันการลักลอบดักจับข้อมูลระหว่างทาง

### 1.2 วัตถุประสงค์ของปัญหาพิเศษ

เพื่อพัฒนาระบบการซื้อขายสินค้าผ่านอินเทอร์เน็ตอย่างปลอดภัย โดยใช้การเข้ารหัสข้อมูล และการตรวจสอบผู้ใช้ โดยผู้ใช้ ไม่จำเป็นต้องมีความรู้ด้านการเข้ารหัสข้อมูล หรือด้านเครือข่าย โดยจะมีการศึกษาระบบรักษาความปลอดภัยในการส่งข้อมูลผ่านระบบเครือข่าย ศึกษาวิธีการเข้ารหัสข้อมูล และตรวจสอบผู้ใช้ ศึกษากระบวนการชำระเงินผ่านอินเทอร์เน็ต และศึกษาระบบการค้าผ่านอินเทอร์เน็ต เพื่อนำมาใช้กับระบบ

### 1.3 ขอบเขตของปัญหา

1.3.1 จัดทำระบบการซื้อขายสินค้าออนไลน์ที่มีความปลอดภัย โดยมีการเข้ารหัสข้อมูล และการลงลายมือชื่อดิจิตอลในการระบุตัวผู้ส่งข้อมูล โดยนำอัลกอริทึมที่มีอยู่แล้วมาใช้

1.3.2 จัดทำระบบการชำระเงินอย่างง่ายเพื่อทดสอบการชำระเงิน ในการซื้อขายสินค้าผ่านอินเทอร์เน็ต

1.3.3 จำลองการให้บริการออกไปรับรองอิเล็กทรอนิกส์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## 1.4 ประโยชน์ที่คาดว่าจะได้รับ

1.4.1 มีความเข้าใจในระบบรักษาความปลอดภัยทางอินเทอร์เน็ตมากขึ้น โดยเฉพาะอย่างยิ่ง การเข้ารหัสข้อมูลและการลงลายมือชื่อดิจิทัล

1.4.2 มีความเข้าใจในระบบการค้าทางอินเทอร์เน็ต

1.4.3 สามารถสร้างโปรแกรมการซื้อขายสินค้าออนไลน์ที่มีความปลอดภัยสูงอย่างง่ายได้

1.4.4 สามารถนำระบบไปใช้จริง ในการซื้อขายสินค้าออนไลน์ได้

## 1.5 ขั้นตอนในการดำเนินงาน

1.5.1 ศึกษาความจำเป็นที่ต้องใช้ในระบบความปลอดภัยสำหรับการซื้อขายสินค้าออนไลน์

1.5.2 ศึกษาการรักษาความปลอดภัยทางอินเทอร์เน็ต

1.5.3 ศึกษาการเข้ารหัสโดยใช้อัลกอริทึมแบบต่างๆ รวมถึงการลงลายมือชื่อดิจิทัลและ ใบรับรองอิเล็กทรอนิกส์

1.5.4 ศึกษาเครื่องมือที่ใช้ในการพัฒนาระบบ

1.5.5 ออกแบบและพัฒนาระบบ

1.5.6 ทดสอบการทำงานของระบบและปรับปรุงแก้ไขข้อผิดพลาดที่เกิดขึ้น

1.5.7 จัดทำคู่มือและรายงาน

## บทที่ 2

### ทฤษฎีที่เกี่ยวข้อง

#### 2.1 ความรู้เบื้องต้นเกี่ยวกับการค้าออนไลน์

การค้าออนไลน์เริ่มจากการสั่งซื้อสินค้าผ่านทางเครือข่าย และพัฒนาขึ้นเรื่อยๆ กระทั่งเป็นการซื้อขายหรือแลกเปลี่ยนสินค้าสำหรับบุคคลทั่วไป โดยการค้าออนไลน์นั้นอาจเป็นสินค้าที่เป็นรูปธรรมจับต้องได้ หรืออาจอยู่ในรูปแบบข้อมูลอิเล็กทรอนิกส์ เช่น ภาพ เสียง มัลติมีเดีย โดยมีขั้นตอนคือ

- ประชาสัมพันธ์สินค้าหรือบริการ เพื่อให้ลูกค้าทราบ ขั้นตอนนี้อาจรวมทั้งการประชาสัมพันธ์สินค้าต่างๆ รวมถึงการให้ข้อมูลต่างๆ หรือตอบคำถามที่ลูกค้าสนใจ
- ลูกค้าจะสั่งซื้อสินค้าหลังจากที่เลือกรายการสินค้าแล้ว โดยอาจทำการสั่งซื้อผ่านทางหน้าเว็บ หรือผ่านทาง โปรแกรมเฉพาะของร้านค้า
- การชำระเงิน เช่น การชำระด้วยบัตรเครดิต เงินสดดิจิทัลและเช็คอิเล็กทรอนิกส์
- การจัดส่งสินค้า หากข้อมูลเป็นข้อมูลดิจิทัล อาจส่งผ่านเครือข่ายเลยได้ หรือหากข้อมูลเป็นสินค้า ทางบริษัทอาจมีบริการจัดส่งเอง หรือจ้างบริษัทรับส่งสินค้าได้
- การให้บริการ อาจอยู่ในรูปแบบการตอบคำถามทางอีเมลล์ หรือทางเว็บไซต์ก็ได้

##### 2.1.1 การชำระเงินทางอิเล็กทรอนิกส์

การชำระเงินผ่านเครือข่ายอินเทอร์เน็ตโดยทั่วไปจะผ่าน โพรโทคอล SET(Secured Electronic Transaction) ซึ่งเป็นโพรโทคอลที่พัฒนาร่วมกันระหว่างบริษัท Visa และ MasterCard โดยการทำการชำระเงินนี้ ผู้ที่เกี่ยวข้องกับการทำการค้าทั้งผู้ซื้อและผู้ขายจะต้องมีใบรับรองดิจิทัล และการทำการค้าจะมีการเข้ารหัสข้อมูลด้วย

##### 2.1.1.1 การชำระเงินผ่านบัตรเครดิต

เนื่องจากการชำระเงินด้วยบัตรเครดิตผ่านทางเครือข่ายอินเทอร์เน็ตนั้น ไม่สามารถยืนยันได้จากลายมือชื่อหลังบัตรของเจ้าของบัตรว่าเป็นเจ้าของบัตรตัวจริงหรือไม่ จึงต้องมีการเพิ่มความปลอดภัยโดยการ ใช้ลายมือชื่อดิจิทัลเพื่อเป็นการยืนยันตัวบุคคล และการเข้ารหัสข้อมูลเพื่อเป็นความลับไม่ให้ผู้ที่มาบุกรุกระบบนำข้อมูลไปใช้ได้ โดยการเข้ารหัสนั้น ร้านค้าจะไม่สามารถถอดรหัสข้อมูลของบัตรเครดิตได้ ร้านค้าจะอ่านได้เพียงรายละเอียดของการสั่งซื้อเท่านั้น โดยข้อมูลของบัตรเครดิตจะถูกส่งไปให้ธนาคารหรือบริษัทบัตรเครดิตโดยตรงเพื่อตรวจสอบความถูกต้อง และทำการตัดบัญชีต่อไป

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

นอกจากนี้ ทางบริษัท First Virtual ได้คิดค้นระบบการชำระเงินผ่านบัตรเครดิตโดยใช้หมายเลขประจำตัว ที่เรียกว่า VirtualPin ให้ลูกค้าใช้แทนหมายเลขบัตรเครดิต โดยในการสั่งซื้อลูกค้าจะใช้หมายเลข VirtualPin แทนหมายเลขบัตรเครดิต ร้านค้าจะส่ง VirtualPin ไปยังบริษัท บริษัทจะทำการแปลงหมายเลขนี้ให้เป็นหมายเลขบัตรเครดิต และ นำข้อมูลไปชำระเงินกับบริษัทบัตรเครดิตของลูกค้า

### 2.1.1.2 การชำระเงินผ่าน เช็คอิเล็กทรอนิกส์

มีลักษณะคล้ายเช็คกระดาษทั่วไป แต่ในการส่งข้อมูลเลขที่บัญชีจะต้องมีการเข้ารหัส โดยที่ร้านค้าจะสามารถถอดรหัสรายละเอียดของการสั่งซื้อเท่านั้น ไม่สามารถรู้ข้อมูลเลขที่บัญชีได้ แต่จะต้องส่งไปให้กับธนาคารเพื่อทำการตัดบัญชีชำระเงินต่อไป

### 2.1.1.3 การชำระเงินโดย เงินสดดิจิทัล

ธนาคารจะออกชุดข้อมูลแล้วตัดเงินในบัญชีลูกค้า จากนั้นจึงส่งเงินสดดิจิทัลมายังเครื่องของลูกค้า เมื่อลูกค้าต้องการสั่งซื้อสินค้า ก็จะส่งเงินสดดิจิทัลไปยังร้านค้า ร้านค้าจะทำการตรวจสอบกับธนาคารว่าเงินสดดิจิทัลนี้ถูกใช้แล้วหรือไม่ นอกจากนี้การใช้เงินสดดิจิทัลอาจใช้กับการซื้อขายสินค้าที่มีมูลค่าเพียงเล็กน้อยได้ ซึ่งเรียกว่าไมโครแคช โดยจะรวบรวมรายการการซื้อขายแต่ละครั้งเข้าด้วยกัน กระทั่งมีมูลค่าพอสมควร แล้วจึงเรียกเก็บเงินจากลูกค้า ซึ่งอาจชำระโดยบัตรเครดิตหรืออื่นๆ

## 2.1.2 ความปลอดภัยของข้อมูล

ความปลอดภัยในธุรกิจพาณิชย์อิเล็กทรอนิกส์ ต้องการความมั่นใจในความปลอดภัยของการทำธุรกรรม โดยเฉพาะความปลอดภัยของข้อมูล (Information Security) เนื่องจากข้อมูลที่ทำการรับส่ง หรือแลกเปลี่ยนกันนั้น เป็นการดำเนินการผ่านเครือข่าย ซึ่งอาจถูกคุกคามได้ในหลายรูปแบบ เช่น การเข้าถึงโดยผู้ไม่มีสิทธิ์ การแก้ไข เปลี่ยนแปลง หรือทำลายข้อมูล การปฏิเสธความรับผิดชอบในการทำธุรกรรม เป็นต้น จึงจำเป็นต้องมีการสร้างระบบรักษาความปลอดภัยของข้อมูลขึ้น โดยครอบคลุมในประเด็นสำคัญ คือ การรักษาความปลอดภัยของข้อมูลในการทำธุรกรรม อิเล็กทรอนิกส์ ให้มีความครอบคลุมในเรื่องของการระบุตัวตน (Authentication) การควบคุมการเข้าถึง (Access Control) การรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วนของข้อมูล (Integrity) และการป้องกันการปฏิเสธความรับผิดชอบ (Non - repudiation) นั้น จำเป็นต้องอาศัยเทคโนโลยีเข้ามาช่วยในการรักษาความปลอดภัย ซึ่งเทคโนโลยีที่นิยมในปัจจุบัน ได้แก่ เทคโนโลยีการเข้ารหัส

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

### 2.1.2.1 หลักการของระบบความปลอดภัยในระบบ

- Confidentiality : รักษาความลับให้เฉพาะบุคคลที่ควรรู้
- Integrity : รักษาความถูกต้องของข้อมูล
- Availability : สามารถใช้งานได้เมื่อต้องการ

### 2.1.2.2 สิ่งจำเป็นที่ต้องมีในระบบรักษาความปลอดภัย

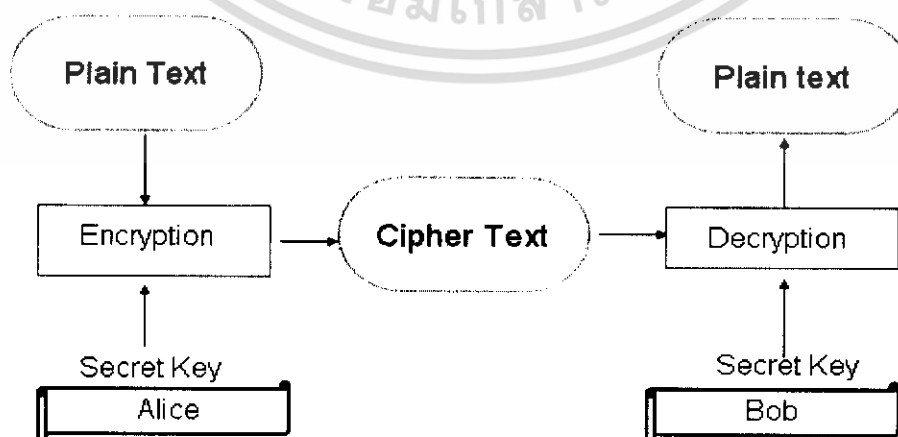
- Authentication : การพิสูจน์ตัวตน
- Authorization : การพิสูจน์สิทธิ์
- Auditing : การตรวจสอบการทำงาน

### 2.1.2.3 การเข้ารหัสข้อมูล

หมายถึง การทำให้ข้อมูล (Plain Text) ที่จะส่งผ่านไปทางเครือข่ายอยู่ในรูปแบบที่ไม่สามารถอ่านได้ (Cipher Text) โดยใช้การเข้ารหัส ผู้มีสิทธิ์จริงเท่านั้นจะสามารถอ่านข้อมูลได้ด้วยการถอดรหัส (Decryption) ซึ่งการเข้ารหัสและถอดรหัสนั้นจะอาศัยสมการทางคณิตศาสตร์ที่ซับซ้อน และต้องอาศัยกุญแจในการเข้ารหัสและถอดรหัส สามารถแบ่งเป็น 2 ประเภท คือ

#### 2.1.2.3.1 การเข้ารหัสแบบสมมาตร (Symmetric Encryption)

คือการเข้ารหัสโดยใช้กุญแจลับที่เหมือนกัน มีข้อดีคือสามารถเข้ารหัสและถอดรหัสข้อมูลได้อย่างรวดเร็ว ไม่ซับซ้อน แต่ข้อเสียคือการส่งกุญแจลับให้อีกฝ่ายยากที่จะทำให้มีความปลอดภัยสูงหากส่งผ่านเครือข่าย เนื่องจากอาจมีผู้ที่ดักจับข้อมูลอยู่ และหากมีการติดต่อกันเป็นจำนวนมากก็จะเป็นการสิ้นเปลืองกุญแจลับ เนื่องจากจะต้องใช้กุญแจลับ 1 รหัส ต่อการติดต่อสื่อสาร 1 คู่

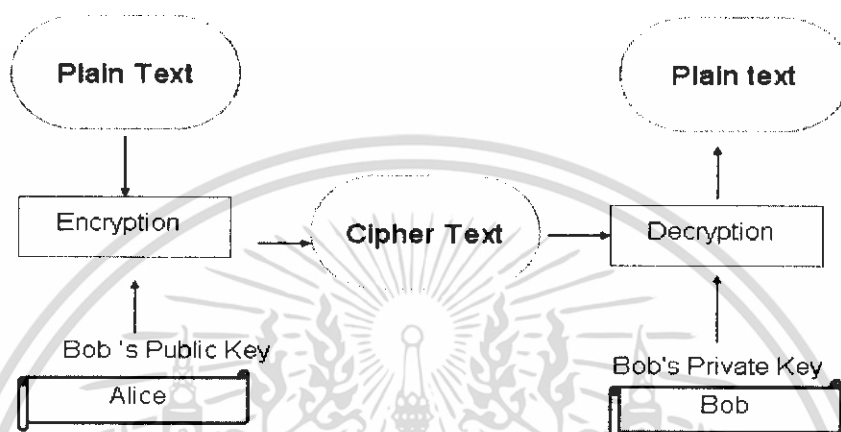


รูปที่ 2.1 แสดงการเข้ารหัสแบบสมมาตร

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

### 2.1.2.3.2 การเข้ารหัสแบบไม่สมมาตร (Asymmetric Encryption)

คือการเข้ารหัสและถอดรหัสโดยใช้กุญแจต่างกัน ที่เข้าคู่กัน โดยการเข้ารหัสจะใช้คีย์สาธารณะส่วนการถอดรหัสจะใช้คีย์ส่วนตัว ซึ่งมีข้อดีคือ คีย์ส่วนตัวจะถูกเก็บไว้กับเจ้าของเพียงคนเดียวจึงไม่มีปัญหาเรื่องความปลอดภัยในการส่งกุญแจผ่านเครือข่าย ไม่ว่าผู้อื่นจะรู้คีย์สาธารณะก็ไม่สามารถที่จะถอดรหัสข้อความได้ ดังนั้นจะมีเพียงเจ้าของคีย์ส่วนตัวเท่านั้นที่จะอ่านข้อความได้



รูปที่ 2.2 แสดงการเข้ารหัสแบบไม่สมมาตร

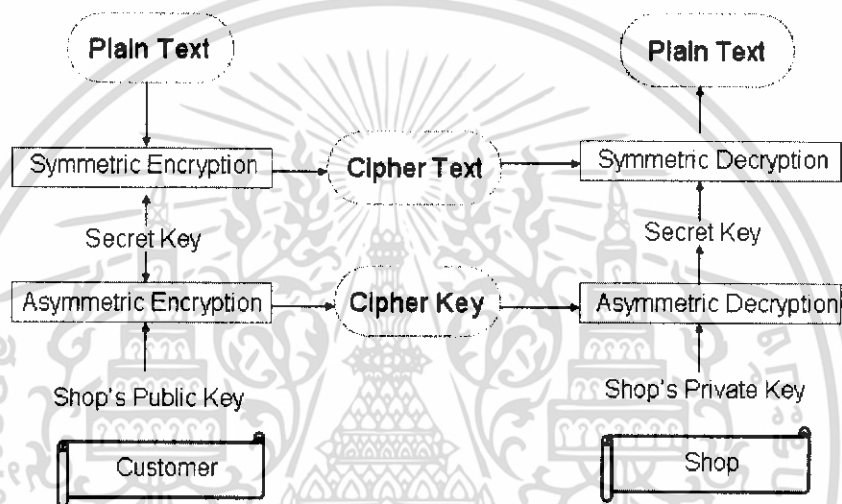
ตารางที่ 2.1 เปรียบเทียบข้อดีข้อเสียของแต่ละแบบ

	กุญแจสมมาตร	กุญแจอสมมาตร
ข้อดี	<ul style="list-style-type: none"> <li>- มีความรวดเร็วเพราะใช้การคำนวณที่น้อยกว่า</li> <li>- สามารถสร้างได้ง่ายโดยใช้ฮาร์ดแวร์</li> </ul>	<ul style="list-style-type: none"> <li>- การบริหารจัดการกุญแจทำได้ง่ายกว่า เพราะ ใช้กุญแจในการเข้ารหัส และถอดรหัสต่างกัน</li> <li>- สามารถระบุผู้ใช้โดยการเข้าร่วมกับลายมือชื่อ อิเล็กทรอนิกส์</li> </ul>
ข้อเสีย	<ul style="list-style-type: none"> <li>- การบริหารจัดการกุญแจทำได้ยาก เพราะ กุญแจในการเข้ารหัสและถอดรหัสเหมือนกัน</li> </ul>	<ul style="list-style-type: none"> <li>- ใช้เวลาในการเข้าและถอดรหัสค่อนข้างนาน เพราะต้องใช้การคำนวณอย่างมาก</li> </ul>

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

#### 2.1.2.4 การเข้ารหัสแบบผสมกุญแจสมมาตรและกุญแจไม่สมมาตร

การเข้ารหัสจะนำข้อดีของการเข้ารหัสทั้งสองรูปแบบมาประยุกต์ คือ นำข้อดีของการเข้ารหัสแบบสมมาตรที่สามารถทำการคำนวณได้อย่างรวดเร็ว มาใช้ในการเข้ารหัสข้อความทั้งหมด แล้วจึงนำคีย์แบบสมมาตรนั้นมาเข้ารหัสแบบไม่สมมาตรส่งไปพร้อมกับข้อความที่เข้ารหัสแล้ว เพื่อให้ผู้รับรู้ว่าใช้คีย์ใดในการเข้ารหัสข้อความ เนื่องจากการเข้ารหัสแบบไม่สมมาตรมีข้อดีในการแลกเปลี่ยนคีย์ที่มีความปลอดภัยสูงกว่า เมื่อผู้รับได้รับข้อมูลซึ่งประกอบด้วยข้อความที่เข้ารหัสโดยคีย์แบบสมมาตร และคีย์แบบสมมาตรที่ถูกเข้ารหัสโดยคีย์แบบไม่สมมาตร ผู้รับจะนำคีย์ส่วนตัวของผู้รับมาใช้ในการถอดรหัสจะได้คีย์แบบสมมาตรเพื่อถอดรหัสข้อความทั้งหมด



รูปที่ 2.3 แสดงการเข้ารหัสแบบผสม

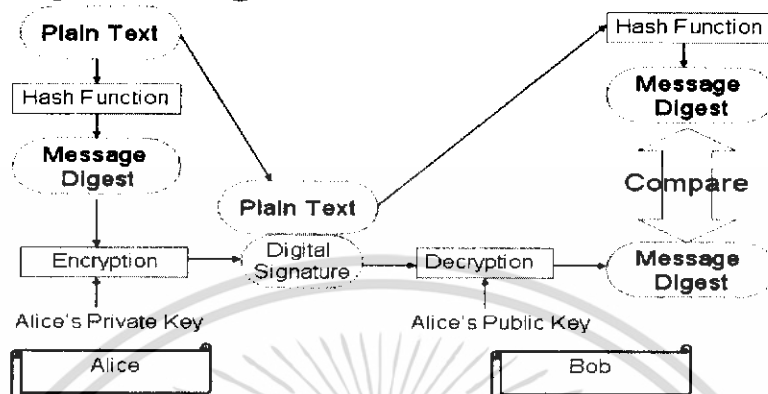
#### 2.1.2.5 ลายมือชื่อดิจิตอล

ลายมือชื่อดิจิตอลถูกสร้างขึ้นเพื่อเป็นการยืนยันตัวบุคคลว่าเป็นเจ้าของเอกสารจริงๆ นอกจากนี้ยังเป็นการตรวจสอบได้ว่าข้อความที่ส่งไปไม่ได้ถูกตัดแปลงแก้ไขแต่อย่างใด

ขั้นตอนการสร้างลายมือชื่อดิจิตอลขั้นแรก ข้อความจะถูกคำนวณให้สั้นลงโดยใช้แฮชฟังก์ชันซึ่งจะได้ข้อความที่สั้นลงเรียกว่าเมสเชงไคเจสต์ จากนั้นเมสเชงไคเจสต์จะถูกเข้ารหัสโดยคีย์ส่วนตัวของผู้สร้างเอกสารเป็นลายมือชื่อดิจิตอล ข้อความเดิมจะถูกส่งไปพร้อมกับลายมือชื่อดิจิตอล โดยผู้รับสามารถตรวจสอบได้โดยนำลายมือชื่อดิจิตอลของผู้ส่งมาถอดรหัสโดยใช้คีย์สาธารณะของผู้ส่ง ซึ่งจะได้ เมสเชงไคเจสต์ จากนั้นจึงคำนวณข้อความเริ่มต้นเพื่อหาเมสเชงไคเจสต์ที่ได้จากข้อความ นำมาเปรียบเทียบกับเมสเชงไคเจสต์ที่ได้จากการถอดรหัสจากลายมือชื่อดิจิตอล หากเหมือนกันแสดงว่าข้อความที่ส่งมานั้นมาจากผู้ส่งจริง และข้อความไม่มีการ

เปลี่ยนแปลงระหว่างการส่ง แต่หากข้อความที่ส่งมานั้น ไม่ได้มาจากผู้ส่ง หรือข้อความถูกดัดแปลงจากบุคคลอื่น จะได้เมสเซจไคเจสต์ที่ต่างกัน

## Digital Signature



รูปที่ 2.4 แสดงการลงลายมือชื่อดิจิตอล

### 2.1.2.6 ใบรับรองดิจิทัล (Digital Certificate)

การเข้ารหัส และ ลายมือชื่อดิจิตอล ในการทำธุรกรรม เราสามารถรักษาความลับของข้อมูล สามารถรักษาความถูกต้องของข้อมูล และสามารถระบุตัวบุคคลได้ระดับหนึ่ง เพื่อเพิ่มระดับความปลอดภัยในการระบุตัวบุคคล โดยสร้างความเชื่อถือมากขึ้นด้วย ใบรับรองดิจิทัล (Digital Certificate) ซึ่งออกโดยองค์กรกลางที่เป็นที่เชื่อถือ เรียกว่า องค์กรรับรองความถูกต้อง หรือองค์กรพิสูจน์สิทธิ์ (CA : Certification Authority) จะถูกนำมาใช้สำหรับยืนยันในการทำ ธุรกรรมว่า เป็นบุคคลนั้นๆจริงตามที่ได้อ้างไว้ ใบรับรองดิจิทัลที่ออกตามมาตรฐาน X.509 Version 3 ซึ่งเป็นมาตรฐานที่ได้รับความนิยมอย่างแพร่หลายที่สุด จะประกอบด้วยข้อมูลดังต่อไปนี้

- หมายเลขของใบรับรอง (serial number)
- วิธีการที่ใช้ในการเข้ารหัสข้อมูล (algorithm)
- หน่วยงานที่ออกใบรับรอง (issuer)
- เวลาเริ่มใช้ใบรับรอง (starting time)
- เวลาที่ใบรับรองหมดอายุ (expiring time)
- ผู้ได้รับการรับรอง (subject)
- กุญแจสาธารณะของผู้ได้รับการรับรอง (subject 's public key)
- ลายมือชื่อดิจิตอลของหน่วยงานที่ออกใบรับรอง (CA signature)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

### 2.1.2.7 องค์กรรับรองความถูกต้อง (CA : Certification Authority)

เป็นองค์กรที่น่าเชื่อถือที่ทำหน้าที่บุคคลที่สามดำเนินการออกใบรับรองดิจิทัล ให้กับผู้ทำธุรกรรมอิเล็กทรอนิกส์ ที่ขอใช้บริการ โดยบริการต่างๆขององค์กรออกใบรับรอง ได้แก่ บริการเทคโนโลยีเข้ารหัส ซึ่งประกอบด้วยการผลิตกุญแจส่วนตัว (generation of private key) การส่งมอบกุญแจส่วนตัว (distribution of private key) การผลิตกุญแจสาธารณะและกุญแจส่วนตัว (generation of public/private key) การผลิตลายมือชื่อดิจิทัล (generation of digital signature) และการรับรองลายมือชื่อดิจิทัล (validation of digital signature)

นอกจากนี้ยังมีบริการที่เกี่ยวข้องกับการออกใบรับรอง ประกอบไปด้วย การออกใบรับรอง (certificate Issuance) การตีพิมพ์ใบรับรองเพื่อเผยแพร่แก่บุคคลทั่วไป (certificate publishing) การเก็บต้นฉบับใบรับรอง (Certificate archiving) และการกำหนดนโยบายการออกและอนุมัติใบรับรอง (Policy creation / approval) ส่วนบริการเสริมต่างๆ ได้แก่ การลงทะเบียน (registration) การตรวจสอบสัญญาต่างๆ และการกู้กุญแจ (key recovery) เป็นต้น

## 2.2 อัลกอริทึมในการเข้ารหัส

### 2.2.1 ตัวอย่างอัลกอริทึมในการเข้ารหัส

#### 2.2.1.1 ตัวอย่างอัลกอริทึมการเข้ารหัสแบบสมมาตร

##### 2.2.1.1.1 อัลกอริทึม DES (Data Encryption Standard)

เป็นอัลกอริทึมที่ได้รับการรับรองจากรัฐบาลสหรัฐอเมริกา เพื่อเป็นมาตรฐานในการเข้ารหัสข้อมูลสำหรับหน่วยงานของรัฐบาล และเป็นมาตรฐานในการเข้ารหัสข้อมูลระดับนานาชาติตามมาตรฐาน ANSI ด้วย อัลกอริทึมนี้เป็นแบบบล็อกซึ่งใช้กุญแจขนาดความยาว 56 บิต ซึ่งถือว่าไม่เพียงพอเนื่องจากผู้บุกรุกสามารถใช้การลองผิดลองถูกหากุญแจในการถอดรหัสได้

##### 2.2.1.1.2 อัลกอริทึม Triple-DES

พัฒนามาจากอัลกอริทึม DES เพื่อเพิ่มความปลอดภัยมากยิ่งขึ้น โดยทำการเข้ารหัสแบบ DES จำนวนสามครั้งแต่ละครั้งใช้กุญแจที่ต่างกัน ซึ่งเปรียบได้กับการเข้ารหัสด้วยกุญแจขนาด 168 บิต

##### 2.2.1.1.3 อัลกอริทึม IDEA (International Data Encryption Algorithm)

เป็นอัลกอริทึมที่ใช้กุญแจขนาด 128 บิต ซึ่งถูกพัฒนาขึ้นที่ประเทศสวิสเซอร์แลนด์ ใช้งานกับการเข้ารหัสและลงลายมือชื่อดิจิทัลในระบบอีเมลล์ PGP การนำไปใช้งานต่างๆไม่เป็นที่แพร่หลายมากนักเนื่องจากติดปัญหาด้านลิขสิทธิ์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

#### 2.2.1.1.4 อัลกอริทึม AES

เป็นมาตรฐานการเข้ารหัสชั้นสูงของประเทศสหรัฐอเมริกา ใช้กุญแจขนาด 128, 192 และ 256 บิต

#### 2.2.1.2 ตัวอย่างอัลกอริทึมการเข้ารหัสแบบไม่สมมาตร

##### 2.2.1.2.1 อัลกอริทึม RSA

พัฒนาโดยนักวิจัยจากสถาบันเทคโนโลยีแห่งแมสซาชูเซตส์ (MIT : Massachusetts Institute of Technology) คือ Ronald Rivest, Adi Shamir และ Leonard Adleman ซึ่งชื่ออัลกอริทึมมาจากชื่อตัวแรกของนักวิจัยทั้งสาม

##### 2.2.1.3 ตัวอย่างอัลกอริทึมการสร้างเมสเซจไคเจสต์

###### 2.2.1.3.1 อัลกอริทึม MD2

ผู้พัฒนาคือ Ronald Rivest ซึ่งเป็นอัลกอริทึมที่ปลอดภัยที่สุดในอัลกอริทึมต่างๆที่เขาคิดขึ้นมา แต่ก็มีข้อเสียอยู่ที่ว่าใช้เวลาในการทำเมสเซจไคเจสต์ 128 บิต เป็นเวลานานจึงไม่ได้รับการนิยม

###### 2.2.1.3.2 อัลกอริทึม MD4

ผู้พัฒนาคือ Ronald Rivest ซึ่งแก้ปัญหาด้านความช้าแต่ก็ยังมีข้อบกพร่องตรงที่ว่าอาจคำนวณได้ เมสเซจไคเจสต์ที่เหมือนกันทั้งคู่ที่ข้อความต่างกัน MD4 ทำเมสเซจไคเจสต์ขนาด 128 บิต

###### 2.2.1.3.3 อัลกอริทึม MD5

ผู้พัฒนาคือ Ronald Rivest ซึ่งได้ปรับปรุงให้มีความปลอดภัยสูงขึ้น ได้ถูกใช้อย่างแพร่หลายแต่ในปี 1996 มีผู้พบจุดบกพร่องของ MD5 คือการได้ข้อความเมสเซจไคเจสต์ที่ซ้ำกัน MD5 ทำเมสเซจไคเจสต์ขนาด 128 บิต

###### 2.2.1.3.4 อัลกอริทึม SHA(Secure Hash Algorithm)

ได้นำแนวคิดมาจาก MD4 และพัฒนามาเพื่อใช้ในการลงลายมือชื่ออิเล็กทรอนิกส์ แต่องค์กร NIST ก็ประกาศตามมาว่าอัลกอริทึมนี้จำเป็นต้องได้รับการปรับปรุงเพื่อเติมอีกเล็กน้อย เพื่อให้ดียิ่งขึ้น ซึ่ง SHA สร้างเมสเซจไคเจสต์ที่มีขนาด 160 บิต

### 2.2.1.3.5 อัลกอริทึม SHA-1

SHA-1 ได้เพิ่มเติมความปลอดภัยจาก SHA ให้ดียิ่งขึ้น ซึ่ง SHA-1 สร้างเมสเซจไดเจสต์ที่มีขนาด 160 บิต

### 2.2.1.3.6 อัลกอริทึม SHA-256, SHA-384 และ SHA-512

NIST เป็นผู้นำเสนอทั้ง 3 อัลกอริทึมนี้ในปี 2001 เพื่อใช้งานอัลกอริทึม AES ซึ่งเป็นอัลกอริทึมในการเข้ารหัสแบบสมมาตร ซึ่งเมสเซจไดเจสต์ที่มีขนาด 256,384,512 บิตตามลำดับ

## 2.2.2 อัลกอริทึมในการเข้ารหัสโดยละเอียด

### 2.2.2.1 อัลกอริทึมการเข้ารหัสแบบสมมาตร

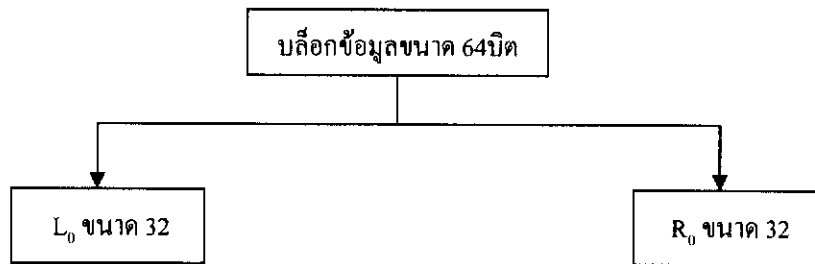
#### 2.2.2.1.1 อัลกอริทึม DES (Data Encryption Standard)

อัลกอริทึม DES(Data Encryption Standard) เป็นอัลกอริทึมในการเข้ารหัสที่แพร่หลายในโลก DES จะทำงานโดยการเข้ารหัสกลุ่มของข้อความ 64 บิต ซึ่งเหมือนกับเลขฐาน 16 และเป็นการเข้ารหัสแบบเป็นบล็อกขนาด 64 บิต ซึ่งมันจะใช้ คีย์ ขนาด 56 บิต (โดยจะไม่ใช้บิตตัวที่ 8,16,24,32,40,48,56,64 เพราะจะถูกกำหนดให้เป็น Parity bit) และในการถอดรหัสก็จะใช้คีย์ตัวเดียวกัน



รูปที่ 2.5 แสดงคีย์ 56 บิต ที่เรียงลำดับแล้วถูกแบ่งเป็น 2 ส่วน

อัลกอริทึมนี้จะมีบล็อกข้อมูลขนาด 64 บิต ซึ่งจะถูกแบ่งออกเป็น 2 บล็อก และประกอบด้วย 0 หรือ 1 แต่ละบล็อกของ 64 บิต จะถูกแบ่งเป็น 2 บล็อก เป็นบล็อกครึ่งซ้าย(L)และบล็อกครึ่งขวา(R) ซึ่งแต่ละครึ่งมีขนาด 32 บิต ดังรูป



รูปที่ 2.6 แสดงบล็อกของข้อมูลขนาด 64 บิต ถูกแบ่งเป็น 2 บล็อก

ในการทำเริ่มใช้อัลกอริทึม DES โดย

- ขั้นตอนที่ 1 : สร้างคีย์ย่อย 16 ตัว แต่ละตัวมีความยาว 48 บิต

คีย์ 64 บิต จะถูกเปลี่ยนแปลงเป็นไปตามตาราง PC-1 เนื่องจากข้อมูลแรกในตารางจะเป็น 57 ดังนั้น บิตที่ 57 ของคีย์เดิม(K)จะกลายเป็นบิตแรกของคีย์ (K+) แล้วบิตที่ 49 ของคีย์เดิม (K)จะกลายเป็นบิตที่ 2 ของคีย์(K+) และบิตที่ 4 ของคีย์เดิม (K) จะกลายเป็นคีย์ตัวสุดท้ายของคีย์ (K+) ซึ่งคีย์ K+ ที่ได้นี้มีขนาด 56 บิต

ตารางที่ 2.2 PC-1

PC-1						
57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

**ตัวอย่าง** จากคีย์ (K) ที่มีขนาด 64 บิต แล้วจะได้คีย์ K+ ขนาด 56 บิต

K= 00010011 00110100 01010111 01111001 10011011 10111100 11011111 11110001

K+= 1111000 0110011 0010101 0101111 0101010 1011001 1001111 0001111

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

แบ่งคีย์ (K+) ออกเป็นซ้ายกับขวา ( $C_0$  และ  $D_0$ ) ซึ่งจะมีขนาด 28บิต

**ตัวอย่าง** ก็แบ่งคีย์(K+)ได้เป็น

$C_0 = 1111000\ 0110011\ 0010101\ 0101111$

$D_0 = 0101010\ 1011001\ 1001111\ 0001111$

ซึ่ง  $C_0$  และ  $D_0$  เราก้จะสร้างเป็น 16 บล็อก จะได้ว่า  $C_n$  และ  $D_n$  ( $1 \leq n \leq 16$ ) แต่ละบล็อกของ  $C_n$  และ  $D_n$  จะได้มาจากคู่ของตัวก่อนหน้าก็คือ  $C_{n-1}$  และ  $D_{n-1}$  สำหรับ  $n = 1, 2, \dots, 16$  โดยจะทำการ Left shift ก็คือจะย้ายบิตตัวแรกของทางซ้ายมือไปอยู่ที่ตัวสุดท้ายของบล็อกนั้น

ตารางที่ 2.3 แสดงจำนวนการเลื่อนทางซ้าย

จำนวนบิตที่ทำซ้ำ	จำนวนที่เลื่อนทางซ้าย
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

**ตัวอย่าง** จากเดิมคู่ของ  $C_n$  และ  $D_n$  แล้วจะหาคู่ถัดไปโดย

$C_0 = 1111000\ 0110011\ 0010101\ 0101111$

$D_0 = 0101010\ 1011001\ 1001111\ 0001111$

หมายเลข 1 ก็จะมาอยู่ที่นี้ เกิดจากการ Left

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

$$C_1 = 1110000 \ 1100110 \ 0101010 \ 1011111$$

$$D_1 = 1010101 \ 0110011 \ 0011110 \ 0011110$$

|  
| ทำไปเรื่อยจนถึง  $C_{16}D_{16}$   
|

$$C_{16} = 1111000 \ 0110011 \ 0010101 \ 0101111$$

$$D_{16} = 0101010 \ 1011001 \ 1001111 \ 0001111$$

โดย  $K_n$  สำหรับ  $1 \leq n \leq 16$  ซึ่งจะทำการต่อคู่  $C_n D_n$  เดิม PC-1 จะใช้ 56 บิต แต่ PC-2 จะใช้เพียง 48 บิต ดังนั้นบิตตัวแรกของ  $K_n$  จะเป็นบิตที่ 14 ของ  $C_n D_n$  แล้วบิตที่ 2 ก็จะเป็นบิตที่ 17 ของ  $C_n D_n$  และตัวสุดท้ายก็จะเป็นบิตที่ 32 ของ  $C_n D_n$

#### ตารางที่ 2.4 PC-2

PC-2					
14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

**ตัวอย่าง** สำหรับคีย์ตัวแรกจะมี  $C_1 D_1 = 1110000 \ 1100110 \ 0101010 \ 1011111 \ 1010101$

$0110011 \ 0011110 \ 0011110$

หลังจากที่เปลี่ยนแปลง PC-2 ก็จะกลายเป็น

$K_1 = 000110 \ 110000 \ 001011 \ 101111 \ 111111 \ 000111 \ 000001 \ 110010$

ดังนั้นคีย์ตัวอื่นๆก็จะเป็นดังนี้

$K_2 = 011110 \ 011010 \ 111011 \ 011001 \ 110110 \ 111100 \ 100111 \ 100101$

$K_3 = 010101 \ 011111 \ 110010 \ 001010 \ 010000 \ 101100 \ 111110 \ 011001$

⋮  
⋮ ทำไปเรื่อยๆจนถึง  $K_{16}$   
⋮

$K_{16} = 110010 \ 110011 \ 110110 \ 001011 \ 000011 \ 100001 \ 011111 \ 110101$

● **ขั้นตอนที่ 2 : เข้ารหัสบล็อกข้อมูลขนาด 64 บิตแต่ละตัว**

จะทำการเข้ค่าเริ่มต้นของการเปลี่ยนลำดับ IP ของ ข้อความ (M) ขนาด 64บิต และจะจัดเตรียมบิตใหม่ตามตารางที่แสดงจากการ initial order ซึ่งบิตที่ 58 ของ M จะกลายเป็นบิตตัวแรกของ IP แล้วบิตตัวที่ 50 ของ M จะกลายเป็นบิตตัวที่ 2 ของ IP และบิตตัวที่ 7 ของ M จะเป็นบิตตัวสุดท้ายของ IP

ตารางที่ 2.5 แสดง IP

IP							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5

**ตัวอย่าง** จะหา IP จาก M ได้ดังนี้

$M = 0000 \ 0001 \ 0010 \ 0011 \ 0100 \ 0101 \ 0110 \ 0111 \ 1000 \ 1001 \ 1010 \ 1011 \ 1100$

$1101 \ 1110 \ 1111$

$IP = 1100 \ 1100 \ 0000 \ 0000 \ 1100 \ 1100 \ 1111 \ 1111 \ 1111 \ 0000 \ 1010 \ 1010 \ 1111$

$0000 \ 1010 \ 1010$

แล้วแบ่ง IP เป็น 32บิตก็จะได้  $L_0$  และ  $R_0$  ดังนี้

$L_0 = 1100 \ 1100 \ 0000 \ 0000 \ 1100 \ 1100 \ 1111 \ 1111$

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

$$R_0 = 1111\ 0000\ 1010\ 1010\ 1111\ 0000\ 1010\ 1010$$

ซึ่งในการหา  $L_n$  และ  $R_n$  จะทำซ้ำ 16 ครั้ง สำหรับ  $1 \leq n \leq 16$  จะใช้ function ( $f$ ) ซึ่งทำงานบนบล็อกข้อมูลขนาด 32 บิต และคีย์ ( $K_n$ ) ที่มีขนาด 48บิต จะแบ่งเป็นบล็อกข้อมูลขนาด 32 บิต(ขวา 32บิต และซ้าย 32บิต) หาได้จาก

$$L_n = R_{n-1}$$

$$R_n = L_{n-1} + f(R_{n-1}, K_n)$$

- ในการคำนวณ  $f$  นั้นแต่ละบล็อก  $R_{n-1}$  จาก 32บิต ไปเป็น 48 บิต จะให้ ฟังก์ชัน  $E$  มาดั่งนั้น จะเป็น  $E(R_{n-1})$  ซึ่งมีบล็อกอินพุต 32 บิต และมีบล็อกเอาพุต 48บิต

ตารางที่ 2.6 แสดง E BIT-SELECTION TABLE

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

**ตัวอย่าง** คำนวณหา  $E(R_0)$  จาก  $R_0$

$$R_0 = 1111\ 0000\ 1010\ 1010\ 1111\ 0000\ 1010\ 1010$$

$$E(R_0) = 011110\ 100001\ 010101\ 010101\ 011110\ 100001\ 010101\ 010101$$

ถัดไปก็จะคำนวณ function ( $f$ ) โดย XOR เอาพุต  $E(R_{n-1})$  ด้วย  $K_n$

$$K_n + E(R_{n-1})$$

ซึ่ง  $K_n$  จะมีขนาด 48 บิต หรือ 8 กลุ่มของ 6บิต แต่ในแต่ละกลุ่มของ 6บิตจะให้ address ในตารางที่เรียกว่า "S boxes" และให้ address ใน S box ที่แตกต่างกัน

$$K_n + E(R_{n-1}) = B_1 B_2 B_3 B_4 B_5 B_6 B_7 B_8$$

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ในแต่ละ  $B_i$  จะเป็นกลุ่มของ 6 บิตดังนั้นจะคำนวณ

$$S_1(B_1) S_2(B_2) S_3(B_3) S_4(B_4) S_5(B_5) S_6(B_6) S_7(B_7) S_8(B_8)$$

ซึ่ง  $S_i(B_i)$  โดยเป็นเอาพุตของตัวที่  $i$  ใน S box

ตารางที่ 2.7 แสดงของ  $S_1$

S1																
Column Numbers																
Row																
No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

**ตัวอย่าง** บล็อกอินพุต  $B = 011011$  โดยจะมีบิตแรกเป็น "0" และบิตสุดท้ายเป็น "1" แล้วบิต 4 ตัวตรงกลางจะเป็น "1101" ซึ่งเลขฐานสองนี้มีค่าเลขฐานสิบคือ "13" ดังนั้นจะเป็น column ที่ 13 ใน row ที่ 1 ซึ่งจะมีเลข 5 ปรากฏอยู่ เอาพุตที่ได้ก็คือ 5 จะมีเลขฐานสองเป็น 0101 ดังนั้นจะได้ว่า  $S_1(011011) = 0101$

สุดท้ายในการคำนวณ function (f) จะเป็นการเปลี่ยนแปลง P ของ S box

$$f = P(S_1(B_1) S_2(B_2) \dots S_8(B_8))$$

การเปลี่ยนแปลงของ P จะถูกกำหนดตามตาราง ซึ่ง P จะให้เอาพุต 32บิต จากอินพุต 32บิต โดยการเปลี่ยนแปลงบิตของบล็อกอินพุต

ตารางที่ 2.8 แสดง P

P			
16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

**ตัวอย่าง** จากเอาพุตของ 8 S boxes ที่ได้จากข้างต้น

$S_1(B_1) S_2(B_2) S_3(B_3) S_4(B_4) S_5(B_5) S_6(B_6) S_7(B_7) S_8(B_8) = 0101 \ 1100 \ 1000 \ 0010 \ 1011 \ 0101$   
 $1001 \ 0111$  เราก็จะรับ

$f = 0010 \ 0011 \ 0100 \ 1010 \ 1010 \ 1001 \ 1011 \ 1011$

$R_1 = L_0 + f(R_0, K_1)$

$= 1100 \ 1100 \ 0000 \ 0000 \ 1100 \ 1100 \ 1111 \ 1111$

$+ 0010 \ 0011 \ 0100 \ 1010 \ 1010 \ 1001 \ 1011 \ 1011$

$= 1110 \ 1111 \ 0100 \ 1010 \ 0110 \ 0101 \ 0100 \ 0100$

ดังนั้นเราก็จะได้  $R_2 = L_1 + f(R_1, K_2)$  จาก  $L_2 = R_1$  แล้วก็ทำต่อไป 16 รอบ

แล้วจากนั้นทำการ Reverse ของ 2 บล็อกนั้นได้  $R_{16}L_{16}$

และไปประยุกต์กับ  $IP^{-1}$  กำหนดได้ตามตารางดังนี้

ตารางที่ 2.9 แสดง  $IP^{-1}$

$IP^{-1}$							
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

**ตัวอย่าง** ถ้ากระบวนการทั้งหมด 16 บล็อก

$$L_{16} = 0100\ 0011\ 0100\ 0010\ 0011\ 0010\ 0011\ 0100$$

$$R_{16} = 0000\ 1010\ 0100\ 1100\ 1101\ 1001\ 1001\ 0101$$

ส่วนกลับของ 2 บล็อกนี้จะได้

$$R_{16} L_{16} = 00001010\ 01001100\ 11011001\ 10010101\ 01000011\ 01000010\ 00110010\ 00110100$$

$$IP^{-1} = 10000101\ 11101000\ 00010011\ 01010100\ 00001111\ 00001010\ 10110100\ 00000101$$

ซึ่งจะได้รูปแบบเลขฐานสิบหกคือ 85E813540F0AB405

จากข้างบนเป็นการเข้ารหัสของข้อความ (M) = 0123456789ABCDEF

$$C = 85E813540F0AB405$$

ส่วนการถอดรหัสจะตรงข้ามกับการเข้ารหัส ซึ่งจะเป็นตามขั้นตอนเหมือนเดิม แต่คีย์ย่อยจะสลับย้อนกลับ

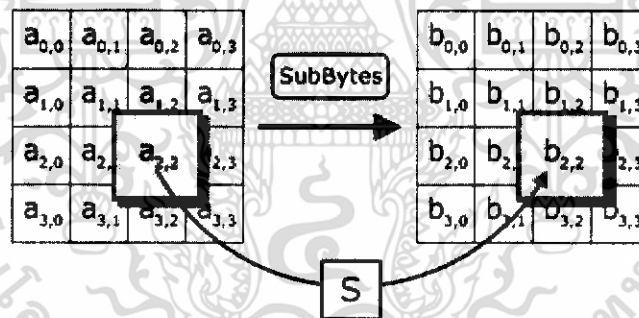
### 2.2.2.1.2 อัลกอริทึม AES (Advanced Encryption Standard)

มีลักษณะเป็น block cipher เป็นอัลกอริทึมของการเข้ารหัสที่มาตรฐานถูกพัฒนาโดยรัฐบาลของประเทศสหรัฐอเมริกาซึ่งก็คือองค์กร NIST ซึ่งเหตุผลที่ทำให้เกิดการเปลี่ยนแปลงก็คือแต่เดิมเรามี DES จริงๆ แล้ว AES ไม่ได้เป็น Rijindael อย่างเหมือนกันซะทีเดียวอย่างเช่น Rijindael สนับสนุนบล็อกที่มีช่วงขนาดใหญ่รวมถึงขนาดของคีย์ด้วย AES มีการกำหนดขนาดบล็อกที่แน่นอนดังนี้ 128 บิตและมีคีย์ขนาดดังต่อไปนี้ 128, 192 หรือ 256 บิต ด้วยเหตุที่ Rijindael สามารถระบุด้วยขนาดคีย์และบล็อกได้โดยคูณ 32 บิตซึ่งขนาดน้อยที่สุดคือ 128 บิตถึงมากที่สุด 256 บิต

เราจะทำการเพิ่มคีย์โดยใช้ key schedule ของ Rijindael โดยการคำนวณ AES นั้นส่วนมากจะถูกทำใน finite field พิเศษ และทำในอาร์เรย์ขนาด  $4 \times 4$  ของไบต์ สำหรับการเข้ารหัสแต่ละรอบของ AES (ยกเว้นรอบสุดท้าย) จะประกอบด้วยขั้นตอนดังนี้

- SubBytes

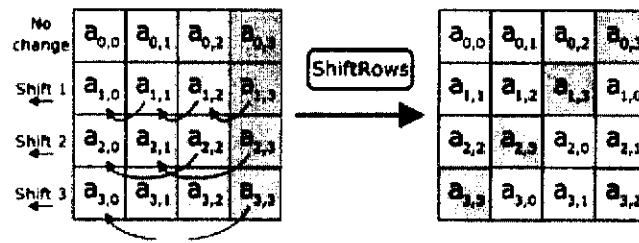
เป็นขั้นตอนการแทนที่ในแบบไม่เชิงเส้น ซึ่งในแต่ละไบต์นั้นจะถูกแทนที่ด้วยส่วนที่เกี่ยวข้องดังในตาราง



รูปที่ 2.7 แสดงการทำ SubBytes

- ShiftRows

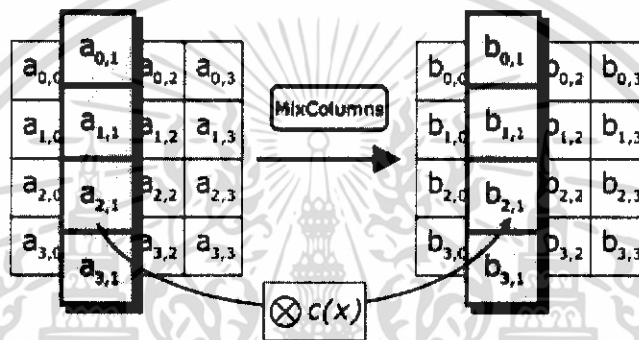
เป็นขั้นตอนการทำการเปลี่ยนตำแหน่ง ที่แต่ละแถวของ state จะถูกเลื่อนไป ซึ่งเป็นตัวเลขที่แน่นอนเรื่อยๆจนครบรอบ ซึ่งแถวที่ 0 ไม่ต้องเลื่อน ส่วนแถวที่ 1 จะเลื่อนไปที่ละ 1 แถว แถวที่สองเลื่อนไปที่ละ 2 และแถวที่สามเลื่อนไปที่ละสองตำแหน่งไปเรื่อยๆ



รูปที่ 2.8 แสดงการทำ ShiftRows

• MixColumns

นำคอลัมน์ของแต่ละสถานะมาคูณกับ  $c(x)$

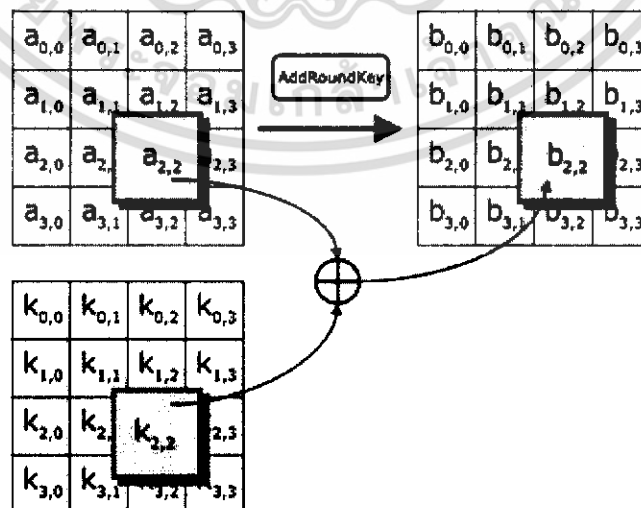


รูปที่ 2.9 แสดงการทำ MixColumns

• AddRoundKey

แต่ละไบต์ของสถานะจะถูกรวม (ใช้ XOR) กับ round key ซึ่งมาจาก cipher key

โดยใช้ key schedule



รูปที่ 2.10 แสดงการทำ AddRoundKey

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

### • Optimization of the cipher

ตอนนี้ระบบกับ 32 บิต มันเป็นไปได้ที่จะเพิ่มความเร็วของการทำ cipher นี้ โดยจะเปลี่ยนรูปเข้าที่ ไปในตาราง ซึ่งจะใช้ SubBytes, ShiftRows และ MixColumns ในการเปลี่ยนรูปเข้าไปในตาราง แล้วใน 1 ตารางขณะนั้นมี 256 รายการ ที่เข้าไป ตารางขนาด 32 บิตมีอยู่ 4 ตัว ซึ่งใช้ประโยชน์ของทั้งหมด 4 กิโลไบต์ (4096 ไบต์) ของหน่วยความจำซึ่งจะเป็น 1 กิโลไบต์สำหรับแต่ละตาราง A รอบสามารถถูกทำกับ 16 ตาราง และบล็อกของ 32 บิตมีอยู่ 12 ตัว จะทำการแยกออกหรือทำการดำเนินการ โดยตามด้วยบล็อกของ 32 บิตมีอยู่ 4 ตัว ไม่รวมอยู่ด้วยหรือการคำนวณใน ขั้นตอน AddRoundKey

ถ้าผลขนาดตาราง 4 กิโลไบต์ ก็คือจะขนาดใหญ่ เพื่อสำหรับให้ target platform ตารางนั้นก็จะสามารถถูกกระทำด้วยตัวเดียว 256 บิต เข้ามายังตาราง 32 บิต โดยใช้การหมุน

## 2.2.2.2 อัลกอริทึมในการเข้ารหัสแบบไม่สมมาตร

### 2.2.2.2.1 อัลกอริทึม RSA

อัลกอริทึม RSA เป็นการเข้ารหัสแบบไม่สมมาตรด้วยและเป็นฟังก์ชันทางเดียว โดยมีขั้นตอนการทำงานดังนี้

การสร้างคีย์ (Key Generator) หาจำนวนเฉพาะ 2 ตัวคือ  $p$  และ  $q$  สำหรับใช้ในการคำนวณค่าดังนี้

- เลือกจำนวนเฉพาะ 2 จำนวนคือ  $p, q$  ซึ่ง  $p, q$  ต้องเป็นความลับ
- $n = p * q$  ซึ่ง  $n$  คือ modulus
- $\phi(n) = (p-1)(q-1)$  ( totient  $\phi(n)$  คือหาค่าจำนวนเต็มบวกที่น้อยกว่าหรือเท่ากับ  $n$  และไม่มีตัวหารร่วมกับ  $n$  ว่ามีกี่จำนวน)
- เลือกตัวเลขสุ่ม  $e$  ซึ่งอยู่ระหว่าง  $1 < e < \phi(n)$  และ  $e$  กับ  $\phi(n)$  ไม่มีตัวหารร่วมกัน (coprime)
- คีย์สาธารณะคือ  $(e, n)$  เป็นคีย์ที่เปิดเผยได้ ผู้คัดลอกข้อมูลสามารถรู้ค่านี้ได้โดยไม่เกิดผลอะไร
- $d = e^{-1} \pmod{\phi(n)}$  หรือ  $(d * e \pmod{\phi(n)} = 1)$  ซึ่ง  $d$  เป็นคีย์ส่วนตัว
- คีย์สาธารณะคือ  $e$  และ ใช้ในการเข้ารหัสข้อความ  $m$  ดังนี้  $c = m^e \pmod{n}$  โดย  $c$  เป็น ciphertext ที่ถูกส่ง
- สามารถถอดรหัสข้อความ  $c$  ที่ได้รับ ดังสมการ  $m = c^d \pmod{n}$  ได้ผลลัพธ์เป็น plaintext  $m$  ที่ต้องการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

\*\*\*\*\* สมการที่ใช้ในการทำ plaintext คือ  $c^d = (m^e)^d = m^{1(\text{mod } \phi(n))} = m$  \*\*\*\*\*

ตัวอย่างเช่น ถ้าจำนวนเฉพาะ p และ q เท่ากับ 19 และ 7 ตามลำดับ จะได้

p=61

q=53

n=p\*q=3233

e=17

d=2753

### 2.2.2.3 อัลกอริทึมสำหรับสร้างเมสเซจไคเจสต์

#### 2.2.2.3.1 MD5 Algorithm

เป็นอัลกอริทึมสำหรับสร้างเมสเซจไคเจสต์ที่พัฒนาโดย Rivest โดยพัฒนาต่อจาก MD4 เพื่อให้มีความปลอดภัยสูงขึ้น โดย MD5 จะสร้างเมสเซจไคเจสต์ขนาด 128 บิต ไม่ว่าข้อความเริ่มต้นจะมีความยาวเท่าไรก็ตาม มีขั้นตอนการทำงานดังนี้

- ทำการเพิ่มบิต(padding bit)เพื่อให้ความยาวของข้อความเป็นขนาด 448 เมื่อทำการด้วย mod512 โดยการเพิ่มนั้นจะทำการเพิ่มบิต 1 จำนวน 1บิตจากนั้นจึงเพิ่ม 0 ให้ความยาวของข้อความเป็นขนาด448 เมื่อทำการ ด้วย mod512

- ทำการเพิ่ม64บิต ที่แทนความยาวของข้อความก่อนที่จะทำการเพิ่ม padding bitลงในผลลัพธ์ที่ได้จากขั้นตอนที่ 1 แต่หากความยาวของข้อความเริ่มต้นนั้นมากกว่า 2ยกกำลัง 64 จะใช้เพียง 64 บิตค่าเท่านั้น เมื่อทำการเพิ่ม 64 บิตนี้ลงไปแล้ว ผลลัพธ์จะได้ข้อความที่มีความยาวเป็นจำนวนเท่าของ 512 บิตซึ่งจะได้เป็นจำนวนเท่าของ 16 word (1 word = 32 bit)

- ให้  $M[0..N-1]$ แทน word ของผลลัพธ์ที่ได้ โดย N จะเป็นจำนวนเท่าของ 16 ทำการตั้งค่าเริ่มต้นของเมสเซจไคเจสต์ โดยแบ่งเป็น 4 ส่วนคือ A, B, C และ D

word A: 01 23 45 67

word B: 89 ab cd ef

word C: fe dc ba 98

word D: 76 54 32 10

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- ทำการคำนวณข้อความที่แบ่งเป็นบล็อกละ 512 บิต โดยแต่ละบล็อกจะทำการเปลี่ยนฟังก์ชัน การทำงานไปด้วย โดยมีทั้งหมด 4 ฟังก์ชันการทำงานคือแต่ละฟังก์ชันประกอบด้วยการทำงานที่คล้ายกัน 16 แบบ โดยขึ้นอยู่กับ ฟังก์ชัน F การ mod และการหมุนทางซ้าย (Left Rotation)

โดยฟังก์ชันการทำงานทั้ง 4 ฟังก์ชันจะประกอบด้วยข้อมูลเข้าขนาด 32 บิต จำนวน 3 ตัว และได้ผลลัพธ์เป็นข้อมูลขนาด 32 บิต ดังนี้

$$F(X,Y,Z) = (X \text{ and } Y) \text{ or } ((\text{not } X) \text{ and } Z)$$

$$G(X,Y,Z) = (X \text{ and } Z) \text{ or } (Y \text{ and } (\text{not } Z))$$

$$H(X,Y,Z) = X \text{ xor } Y \text{ xor } Z$$

$$I(X,Y,Z) = Y \text{ xor } (X \text{ or } (\text{not } Z))$$

การทำงานจำเป็นต้องมีการใช้ตารางข้อมูลขนาด 64 ค่า ( $T[1..64]$ ) ซึ่งสร้างจากฟังก์ชันไซน์ (sine function) โดย  $T[i] = 2^{32} * \text{abs}(\sin(i))$  (i เป็น radian)

- การทำงานจะมีขั้นตอนที่ทำเป็นบล็อกกับข้อมูลดังนี้  
เมื่อแบ่งข้อมูลออกเป็นบล็อกละ 512 บิต โดยการรวม word ขนาด 32 บิตเข้าด้วยกันแล้วทำการคำนวณแต่ละรอบดังนี้

```
/* Save A as AA, B as BB, C as CC, and D as DD. */
```

```
AA = A
```

```
BB = B
```

```
CC = C
```

```
DD = D
```

```
/* Round 1. */
```

```
/* Let [abcd k s i] denote the operation
```

```
a = b + ((a + F(b,c,d) + X[k] + T[i]) <<< s). */
```

```
/* Do the following 16 operations. */
```

```
[ABCD 0 7 1] [DABC 1 12 2] [CDAB 2 17 3] [BCDA 3 22 4]
```

```
[ABCD 4 7 5] [DABC 5 12 6] [CDAB 6 17 7] [BCDA 7 22 8]
```

```
[ABCD 8 7 9] [DABC 9 12 10] [CDAB 10 17 11] [BCDA 11 22 12]
```

```
[ABCD 12 7 13] [DABC 13 12 14] [CDAB 14 17 15] [BCDA 15 22 16]
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```

/* Round 2. */
/* Let [a b c d k s i] denote the operation
   a = b + ((a + G(b,c,d) + X[k] + T[i]) <<< s). */
/* Do the following 16 operations. */
[ABCD 1 5 17] [DABC 6 9 18] [CDAB 11 14 19] [BCDA 0 20 20]
[ABCD 5 5 21] [DABC 10 9 22] [CDAB 15 14 23] [BCDA 4 20 24]
[ABCD 9 5 25] [DABC 14 9 26] [CDAB 3 14 27] [BCDA 8 20 28]
[ABCD 13 5 29] [DABC 2 9 30] [CDAB 7 14 31] [BCDA 12 20 32]

/* Round 3. */
/* Let [abcd k s t] denote the operation
   a = b + ((a + H(b,c,d) + X[k] + T[i]) <<< s). */
/* Do the following 16 operations. */
[ABCD 5 4 33] [DABC 8 11 34] [CDAB 11 16 35] [BCDA 14 23 36]
[ABCD 1 4 37] [DABC 4 11 38] [CDAB 7 16 39] [BCDA 10 23 40]
[ABCD 13 4 41] [DABC 0 11 42] [CDAB 3 16 43] [BCDA 6 23 44]
[ABCD 9 4 45] [DABC 12 11 46] [CDAB 15 16 47] [BCDA 2 23 48]

/* Round 4. */
/* Let [abcd k s t] denote the operation
   a = b + ((a + I(b,c,d) + X[k] + T[i]) <<< s). */
/* Do the following 16 operations. */
[ABCD 0 6 49] [DABC 7 10 50] [CDAB 14 15 51] [BCDA 5 21 52]
[ABCD 12 6 53] [DABC 3 10 54] [CDAB 10 15 55] [BCDA 1 21 56]
[ABCD 8 6 57] [DABC 15 10 58] [CDAB 6 15 59] [BCDA 13 21 60]
[ABCD 4 6 61] [DABC 11 10 62] [CDAB 2 15 63] [BCDA 9 21 64]

/* Then perform the following additions. (That is increment each
   of the four registers by the value it had before this block
   was started.) */

```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```

A = A + AA
B = B + BB
C = C + CC
D = D + DD
end /* of loop on i */

```

- นำผลลัพธ์ A,B,C และ D ที่ได้มาต่อกัน โดยเริ่มจากบิตต่ำของ A และจบด้วยบิตสูงของ D

### 2.2.2.3.2 อัลกอริทึม SHA-1

พัฒนามาจาก MD4 โดยหลักการต่างๆมีส่วนที่คล้าย MD5 แต่ได้เมสแซจไคเจสต์ที่มีความยาวกว่าคือ 160 บิต และมีจำนวนรอบการทำงานที่สูงกว่า มีขั้นตอนการทำงานดังนี้

- ทำการเพิ่มบิต(padding bit) เพื่อให้ความยาวของข้อความเป็นจำนวนเท่าของ 512 (เพื่อให้ได้บล็อกข้อมูลขนาด 512 บิต) โดย 64 บิตท้ายจะสงวนไว้สำหรับใส่ความยาวของข้อความเริ่มต้น โดยการเพิ่มนั้นจะทำการเพิ่มบิต 1 จำนวน 1 บิตจากนั้นจึงเพิ่ม 0 ให้ความยาวของข้อความเป็นขนาด 448 เมื่อทำการ ด้วย mod 512
- เพิ่มความยาวของข้อความเริ่มต้น โดยทำเป็นข้อมูลขนาด 64 บิตความยาวของข้อความเริ่มต้นที่เป็นข้อมูลขนาด 64 บิต จะได้บล็อกข้อความ  $M_1, M_2, \dots, M_n$  โดยที่แต่ละ  $M_i$  ประกอบไปด้วยข้อมูลขนาด 16 คำ(ข้อมูล 32 บิตจำนวน 16 ชุด)
- ฟังก์ชันที่ใช้ในอัลกอริทึม SHA -1 จะคล้ายกับ MD5 คือการประมวลผล ข้อมูลเข้าขนาด 32 บิตจำนวน 3 ตัว และให้ผลลัพธ์เป็นข้อมูลออก 32 บิต 1 ตัว โดยแตกต่างกันที่ฟังก์ชันที่ใช้ ซึ่งแสดงดังนี้

$$f_i(B,C,D) = (B \text{ and } C) \text{ or } ((\text{not } B) \text{ and } D) \quad (0 \leq i \leq 19)$$

$$f_i(B,C,D) = B \text{ xor } C \text{ xor } D \quad (20 \leq i \leq 39)$$

$$f_i(B,C,D) = (B \text{ and } C) \text{ or } (B \text{ and } D) \text{ or } (C \text{ and } D) \quad (40 \leq i \leq 59)$$

$$f_i(B,C,D) = B \text{ xor } C \text{ xor } D \quad (60 \leq i \leq 79)$$

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- กำหนดค่าเริ่มต้นให้การคำนวณดังนี้

$$K(t) = 5A827999 \quad (0 \leq t \leq 19)$$

$$K(t) = 6ED9EBA1 \quad (20 \leq t \leq 39)$$

$$K(t) = 8F1BBCDC \quad (40 \leq t \leq 59)$$

$$K(t) = CA62C1D6 \quad (60 \leq t \leq 79)$$

- เริ่มต้นการคำนวณ โดยกำหนดค่าเริ่มต้นของเมสเซจไคเจสต์ดังนี้

$$H_0 = 67452301$$

$$H_1 = EFCDAB89$$

$$H_2 = 98BADCFE$$

$$H_3 = 10325476$$

$$H_4 = C3D2E1F0$$

- การทำงานกับบล็อก M จะทำทั้งหมด 80 ขั้นตอนดังนี้

แบ่ง M ออกเป็น 16 คำ (16 ชุดของข้อความ 32 บิต) คือ  $W_0, W_1, \dots, W_{15}$

โดย  $W_0$  คือคำซ้ายสุด

For  $t = 16$  to  $79$  ให้  $W_t = S^1(W_{t-3} \text{ XOR } W_{t-8} \text{ XOR } W_{t-14} \text{ XOR } W_{t-16})$ .

ให้  $A = H_0, B = H_1, C = H_2, D = H_3, E = H_4$

For  $t = 0$  to  $79$  ให้  $\text{TEMP} = S^5(A) + f_1(B, C, D) + E + W_t + K_t$ ;

$E = D; D = C; C = S^{30}(B); B = A; A = \text{TEMP}$ ;

ให้  $H_0 = H_0 + A, H_1 = H_1 + B, H_2 = H_2 + C, H_3 = H_3 + D, H_4 = H_4 + E$

- จะได้เมสเซจไคเจสต์ขนาด 160 บิต ดังนี้

$$H_0 H_1 H_2 H_3 H_4$$

## บทที่ 3

### การทำงานของระบบ

#### 3.1 ขอบเขตการทำงาน

ระบบนี้พัฒนาขึ้นโดยใช้ Visual C++ .NET บนระบบปฏิบัติการวินโดวส์ โดยระบบประกอบด้วยการทำงาน 3 ส่วนหลักคือ ส่วนการซื้อขายสินค้าออนไลน์ ส่วนการชำระเงินออนไลน์ ส่วนการบริการออกใบรับรองอิเล็กทรอนิกส์และการพิสูจน์สิทธิ์

##### 3.1.1 ส่วนการซื้อขายสินค้าออนไลน์

เป็นการติดต่อกันระหว่างร้านค้าและลูกค้าเพื่อทำการสั่งซื้อสินค้าตามแคตตาล็อกสินค้า ซึ่งจะมีการตรวจสอบจำนวนสินค้าคงเหลือในคลังสินค้าก่อน หากมีพอจำนวนที่ลูกค้าต้องการจึงจะสามารถสั่งซื้อได้

##### 3.1.2 ส่วนการชำระเงินออนไลน์

แบ่งการชำระเงินเป็น 3 รูปแบบคือ ชำระเงินผ่านบัตรเครดิตกรณีลูกค้าไม่มีใบรับรองอิเล็กทรอนิกส์ จะใช้การพิสูจน์ตัวตนจากบริษัทบัตรเครดิต ชำระเงินผ่านบัตรเครดิตกรณีมีใบรับรองอิเล็กทรอนิกส์ จะใช้การพิสูจน์ตัวตนโดยการลงลายมือชื่อดิจิทัล และชำระเงินโดยการตัดบัญชีที่ลูกค้าชำระเงินกับทางร้านค้าไว้ล่วงหน้า

##### 3.1.3 ส่วนการบริการออกใบรับรองอิเล็กทรอนิกส์และการพิสูจน์สิทธิ์

เป็นการออกใบรับรองอิเล็กทรอนิกส์จากองค์กรพิสูจน์สิทธิ์ เพื่อใช้ในการพิสูจน์สิทธิ์ในการเข้ารหัส และการใช้ลายมือชื่อดิจิทัล

ทุกส่วนจะมีการเข้ารหัสข้อมูลที่สำคัญ และมีการยืนยันตัวตนโดยการลงลายมือชื่อดิจิทัล ซึ่งการเข้ารหัสนั้นใช้การผสมข้อดีของการเข้ารหัสแบบสมมาตร และอสมมาตรเข้าด้วยกัน โดยมี การยืนยันสิทธิ์จากใบรับรองอิเล็กทรอนิกส์ซึ่งออกโดยองค์กรพิสูจน์สิทธิ์

#### 3.2 การแบ่งส่วนโปรแกรม

##### 3.2.1 ส่วนของลูกค้า

เป็นโปรแกรมที่ใช้ในการติดต่อเพื่อลงทะเบียนและซื้อสินค้าจากร้านค้า ชำระเงินผ่านธนาคาร โดยพิสูจน์ตัวตนจากบัตรเครดิต หรือ โดยการลงลายมือชื่อดิจิทัล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

### 3.2.2 ส่วนของร้านค้า

เป็นโปรแกรมในการรับคำสั่งซื้อจากลูกค้า และดูแลยอดคงเหลือของสินค้าในคลังสินค้า

### 3.2.3 ส่วนของธนาคาร

เป็นโปรแกรมในการตรวจสอบเครดิตของลูกค้า และโอนเงินระหว่างบัญชีเครดิตลูกค้า และบัญชีของร้านค้า

### 3.2.4 ส่วนของบริษัทบัตรเครดิต

เป็นโปรแกรมในการพิสูจน์ตัวตนของเจ้าของบัตรเครดิต

### 3.2.5 ส่วนขององค์กรพิสูจน์สิทธิ์

เป็นโปรแกรมในออกใบรับรองอิเล็กทรอนิกส์ และพิสูจน์สิทธิ์

## 3.3 การสื่อสารกันภายในระบบ

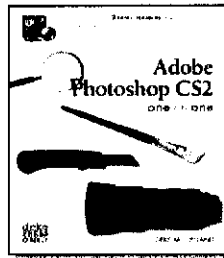
หากลูกค้าต้องการซื้อสินค้าจะทำการติดต่อไปยังร้านค้าโดยผ่านทางโปรแกรมซึ่งดาวน์โหลดผ่านทางเว็บไซต์หรือจากแผ่นติดตั้ง และติดต่อกับบริษัทบัตรเครดิตและธนาคารในการชำระเงิน นอกจากนี้ระบบจะมีการติดต่อกับองค์กรพิสูจน์สิทธิ์ในการยืนยันตัวตนบุคคล



รูปที่ 3.1 การสื่อสารกันระหว่างลูกค้า ร้านค้า ธนาคาร บริษัทบัตรเครดิต และองค์กรพิสูจน์สิทธิ์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

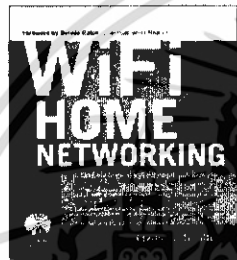
### 3.3.1 การสื่อสารระหว่างลูกค้ากับร้านค้า



รหัส : 0001  
ชื่อ : Adobe Photoshop CS2  
ราคา : 1,290 บาท



รหัส : 0002  
ชื่อ : XML HANDBOOK 5th  
ราคา : 1,359 บาท



รหัส : 0003  
ชื่อ : WiFi Home Networking  
ราคา : 1,950 บาท



รหัส : 0004  
ชื่อ : Training Kit  
ราคา : 2,170 บาท

### รูปที่ 3.2 ตัวอย่างแคตตาล็อกสินค้า

- ชั้นแรกลูกค้าจะต้องทำการติดตั้งโปรแกรมซึ่งสามารถดาวน์โหลดได้จากเว็บไซต์ของร้านค้าหรือจากแผ่นติดตั้งโปรแกรม
- ลูกค้าจะต้องทำการลงทะเบียนกับทางร้านค้าก่อนที่จะซื้อสินค้าได้
- หากเลือกการชำระเงินแบบหักบัญชีที่ลูกค้าชำระไว้กับทางร้านล่วงหน้านั้นเราจะต้องโอนเงินไปเข้าบัญชีของทางร้านก่อนถึงจะทำการซื้อสินค้าได้
- การซื้อสินค้านั้นลูกค้าจะต้องทำการล็อกอินเข้าสู่ระบบโดยใช้ username และ password ที่ได้จากการลงทะเบียน
- ลูกค้าสามารถเลือกรายการสินค้าได้จากแคตตาล็อกสินค้า , เว็บไซต์ หรือผ่านทางโปรแกรมได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

### 3.3.2 การสื่อสารระหว่างลูกค้ากับธนาคาร

กรณีเลือกการชำระเงินผ่านบัตรเครดิต ลูกค้าจะต้องสมัครบัตรเครดิตกับทางธนาคารที่ เป็นผู้ออกบัตรก่อน โดยการชำระเงินผ่านบัตรเครดิตนั้น เลือกได้ว่าลูกค้าจะพิสูจน์ตัวตนโดยผ่านทางบริษัทบัตรเครดิต หรือโดยการลงลายมือชื่อดิจิทัล หากพิสูจน์ตัวตนโดยการลงลายมือชื่อดิจิทัล จะส่งผ่านข้อมูลบัตรเครดิตไปยังธนาคารได้เลยโดยไม่ต้องผ่านการพิสูจน์ตัวตนโดยบริษัทบัตรเครดิตก่อน

### 3.3.3 การสื่อสารระหว่างลูกค้ากับบริษัทบัตรเครดิต

ในการซื้อสินค้าออนไลน์โดยชำระเงินผ่านบัตรเครดิตแบบไม่ใช้การลงลายมือชื่อดิจิทัล ลูกค้าจะต้องพิสูจน์ตัวตนผ่านบริษัทบัตรเครดิต ซึ่งจะต้องทำการลงทะเบียนก่อน โดยการยืนยันตัวตนลูกค้าจะต้องใส่รหัสบัตรเครดิต และรหัสผ่านเพื่อเป็นการยืนยันตัวตน และทำการชำระเงินกับทางธนาคารต่อไป

### 3.3.4 การสื่อสารระหว่างลูกค้ากับองค์กรพิสูจน์สิทธิ์

ลูกค้าต้องมีใบรับรองอิเล็กทรอนิกส์ซึ่งขอได้จากองค์กรพิสูจน์สิทธิ์ หากต้องการชำระเงินผ่านบัตรเครดิตโดยพิสูจน์ตัวตนจากการลงลายมือชื่อดิจิทัล

### 3.3.5 การสื่อสารระหว่างร้านค้ากับองค์กรพิสูจน์สิทธิ์

ร้านค้าต้องมีการขอใบรับรองอิเล็กทรอนิกส์ซึ่งออกจากร้านค้ากับองค์กรพิสูจน์สิทธิ์

### 3.3.6 การสื่อสารระหว่างร้านค้ากับธนาคาร

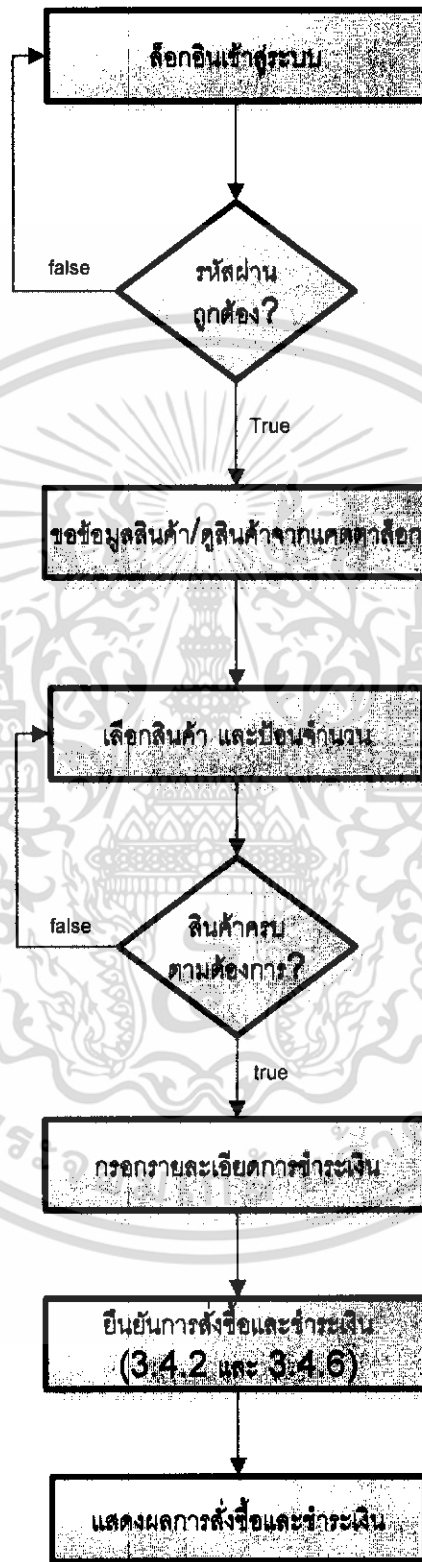
ร้านค้าจะต้องมีบัญชีธนาคารสำหรับให้ธนาคาร โอนเงินเข้าเมื่อมีการซื้อขายผ่านบัตรเครดิต และสำหรับลูกค้าที่ใช้บริการตัดบัญชีชำระล่วงหน้า โอนเงินเข้าในบัญชีนี้

### 3.3.7 การสื่อสารระหว่างบริษัทบัตรเครดิตกับธนาคาร

กรณีที่ลูกค้าซื้อสินค้าออนไลน์โดยชำระเงินผ่านบัตรเครดิตแบบไม่ใช้การลงลายมือชื่อดิจิทัลหลังจากที่ลูกค้ายืนยันตัวตนผ่านบริษัทบัตรเครดิตแล้ว บริษัทบัตรเครดิตจะส่งผลการยืนยันตัวตนมาให้ธนาคารเพื่อทำการ โอนเงินค่าสินค้า

### 3.4 ขั้นตอนการทำงานในระบบ

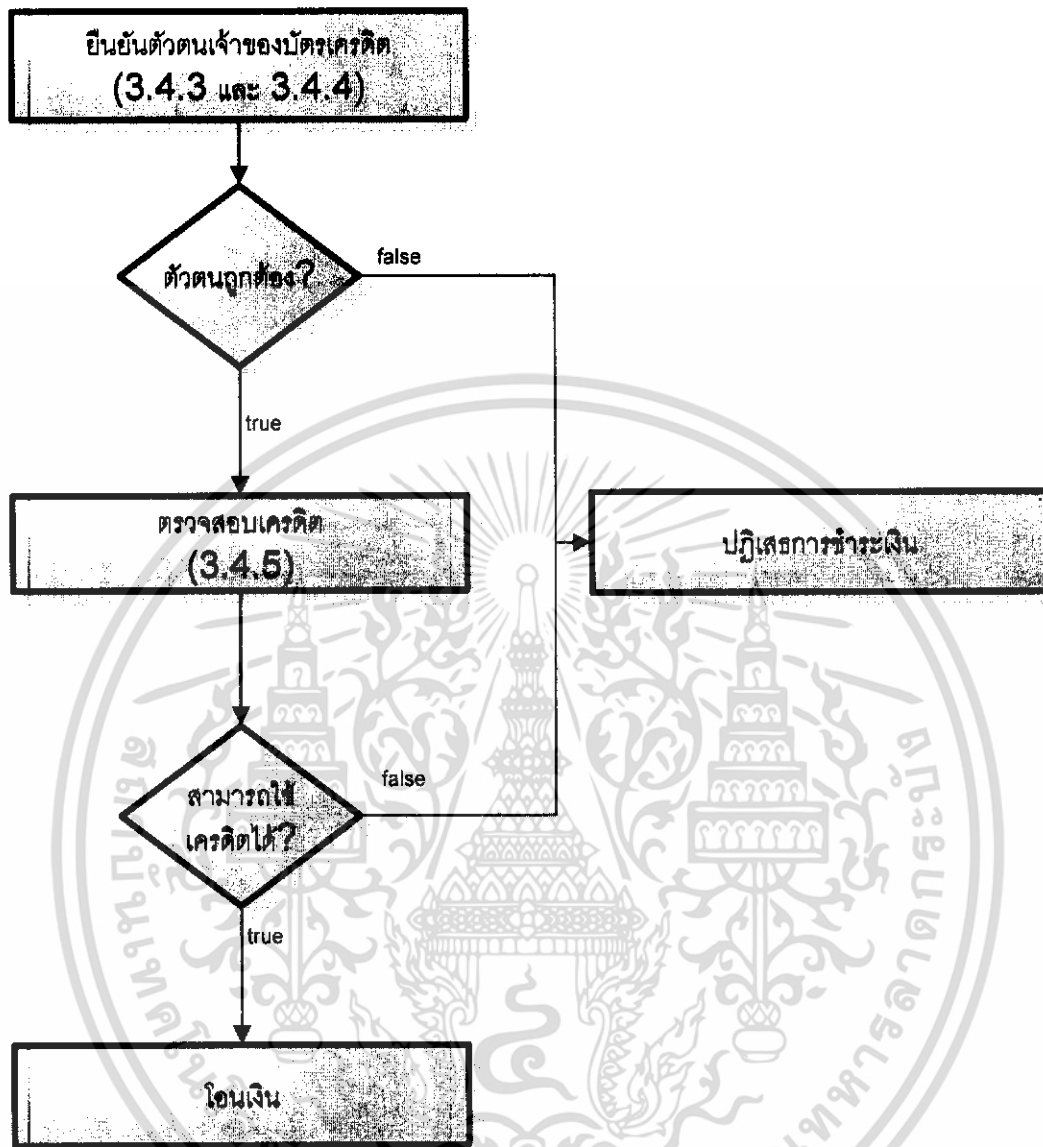
#### 3.4.1 ขั้นตอนการสั่งซื้อสินค้า



รูปที่ 3.3 ขั้นตอนการสั่งซื้อสินค้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## 3.4.2 ขั้นตอนการชำระเงินโดยบัตรเครดิต

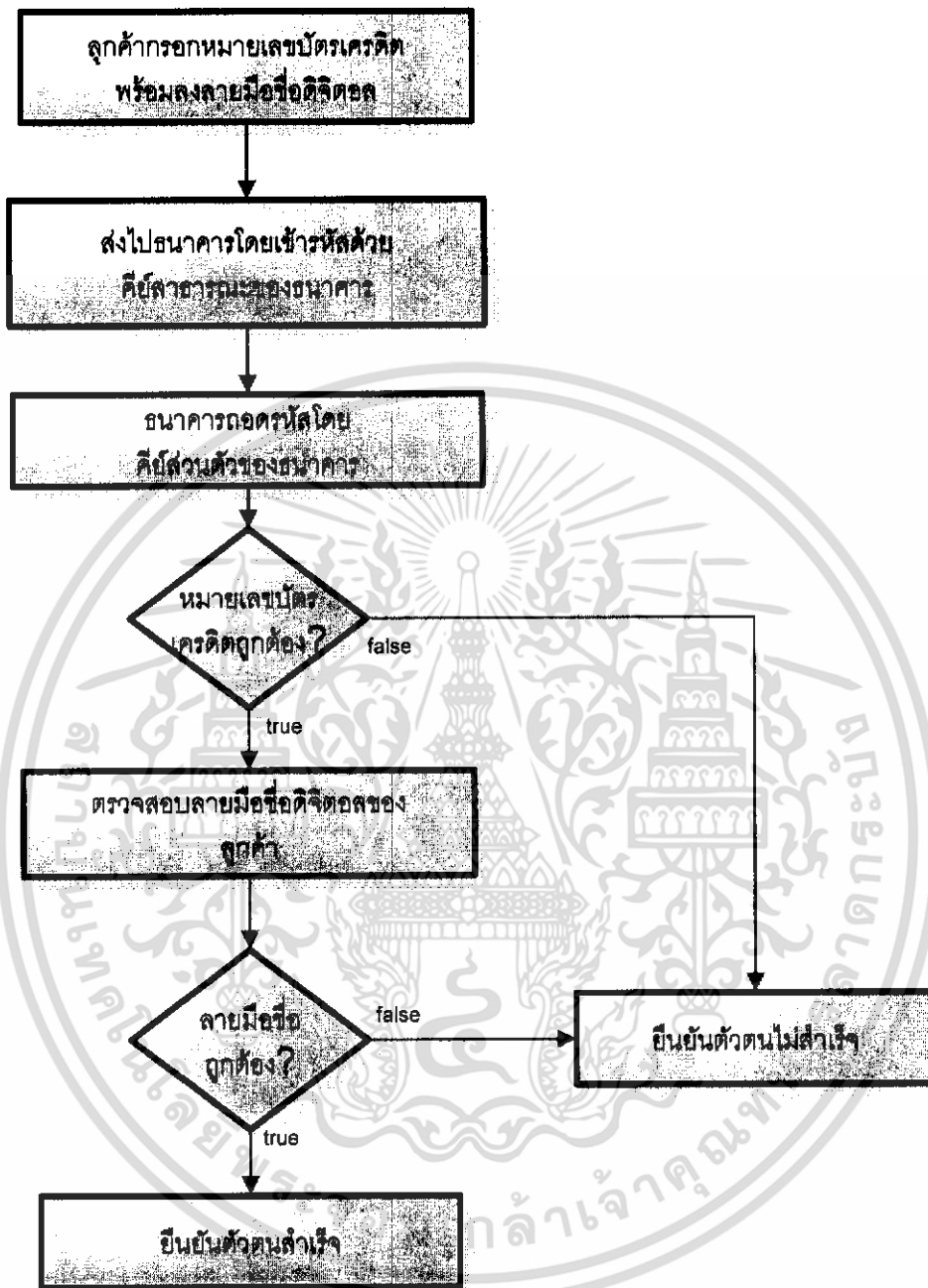


รูปที่ 3.4 ขั้นตอนการชำระเงินโดยบัตรเครดิต

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



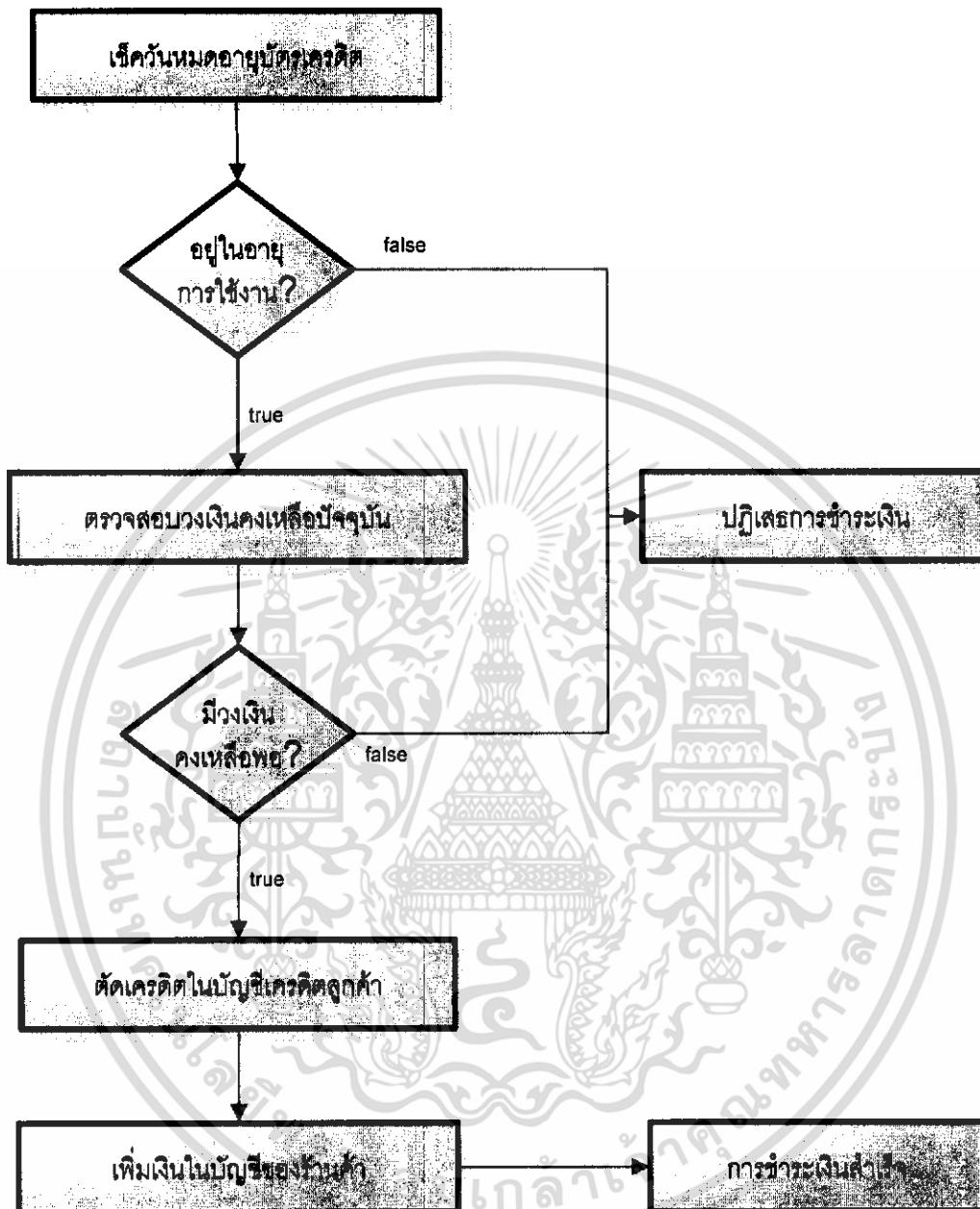
### 3.4.4 ขั้นตอนการยืนยันตัวตนสำหรับบัตรเครดิตกรณีลงลายมือชื่อดิจิทัล



รูปที่ 3.6 ขั้นตอนการยืนยันตัวตนสำหรับบัตรเครดิตกรณีลงลายมือชื่อดิจิทัล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

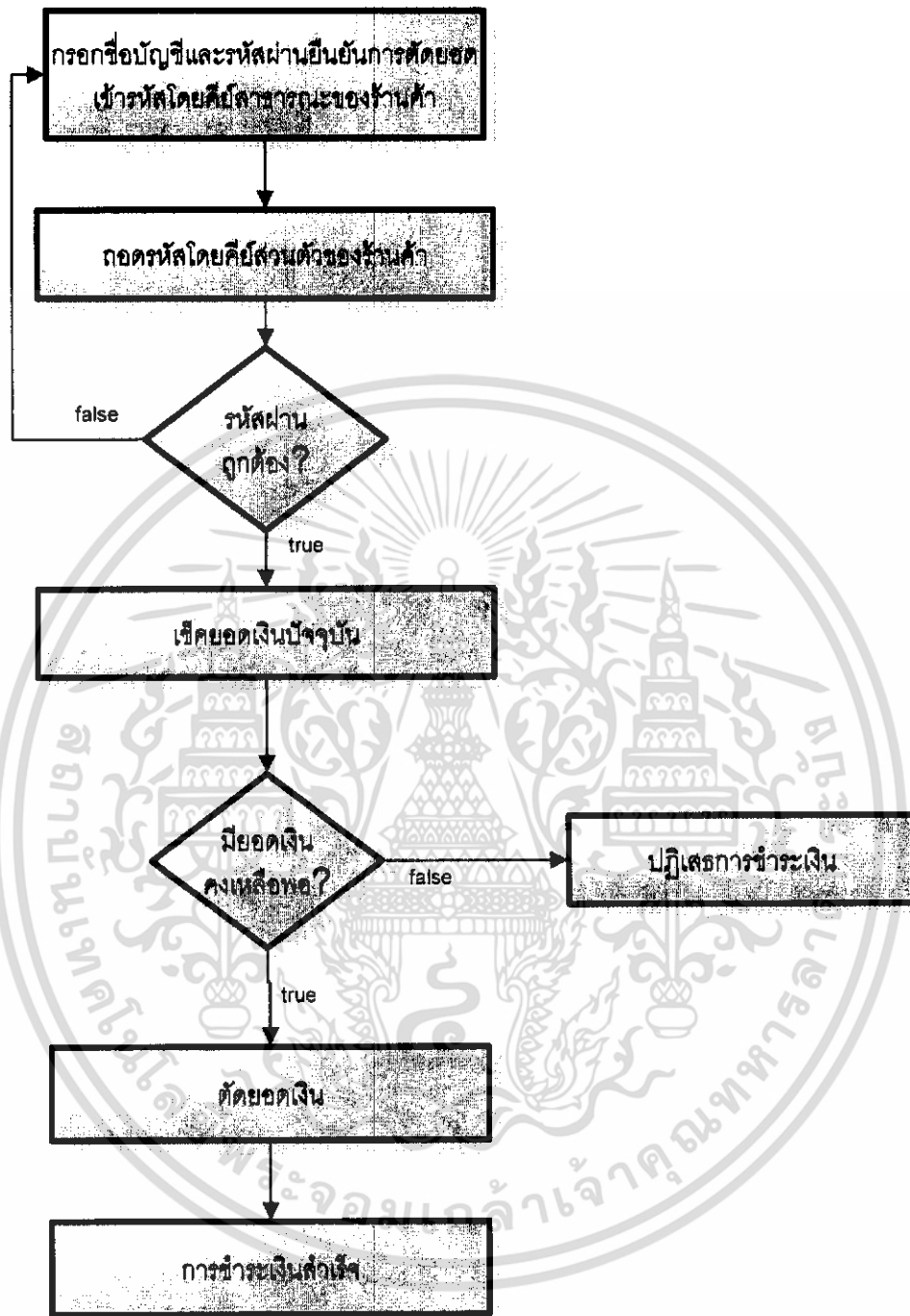
## 3.4.5 ขั้นตอนการตรวจสอบเครดิตและโอนเงิน



รูปที่ 3.7 ขั้นตอนการตรวจสอบเครดิตและโอนเงิน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

### 3.4.6 ขั้นตอนการชำระเงินโดยการตัดบัญชีชำระล่วงหน้า



รูปที่ 3.8 ขั้นตอนการชำระเงินโดยการตัดบัญชีชำระล่วงหน้า

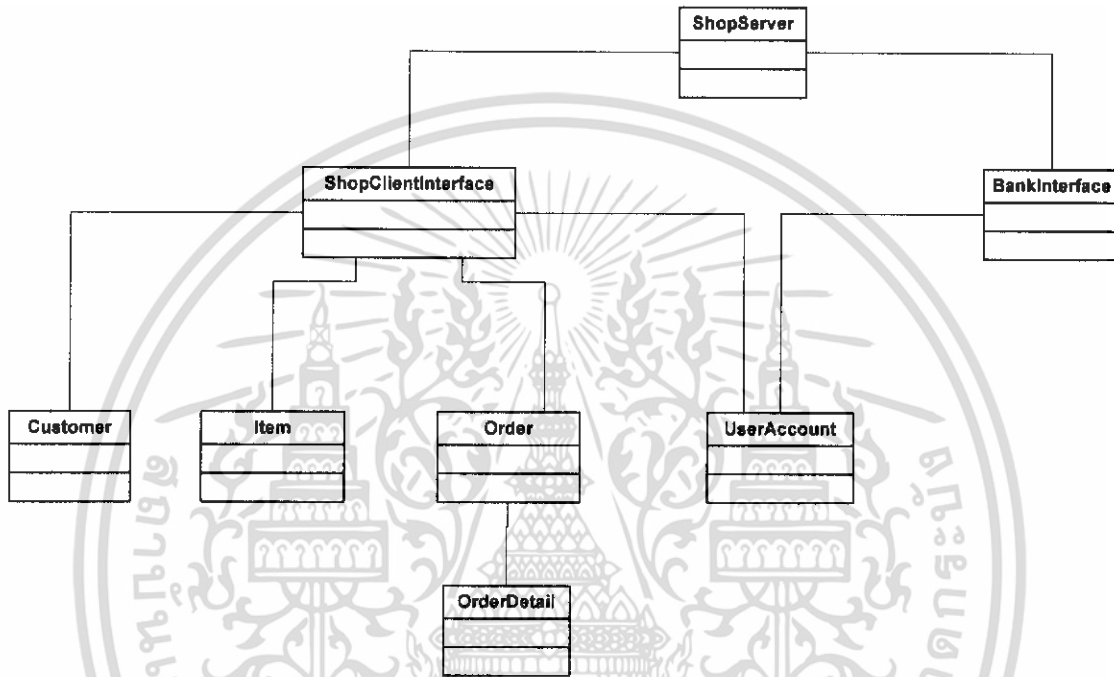
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## บทที่ 4

### การออกแบบระบบและพัฒนาระบบ

#### 4.1 โครงสร้างของโปรแกรม

##### 4.1.1 โครงสร้างของโปรแกรมส่วนร้านค้า



รูปที่ 4.1 โครงสร้างของโปรแกรมส่วนร้านค้า

#### คลาส ShopServer

เป็นคลาสที่จัดการด้านเครือข่ายได้แก่ การเริ่มติดต่อด้านเครือข่าย, การสิ้นสุดการติดต่อด้านเครือข่าย, เมื่อมีการรับข้อมูลจะทำการถอดรหัสข้อความรวมถึงตรวจสอบลายมือชื่อดิจิทัล ซึ่งจะได้เป็นข้อมูลที่ระบบสามารถนำไปทำงานต่อได้ และเป็นคลาสที่นำข้อมูลที่ได้จากขั้นตอนข้างต้นมาทำการตรวจสอบว่าจะส่งข้อมูลไปยังคลาสใด ต่อไปเมื่อคลาสนั้นๆทำการเสร็จก็จะส่งข้อมูลกลับมายัง คลาส ShopServer เพื่อตอบกลับไปยังผู้ส่งต่อไป โดยจะทำการส่งข้อมูลตอบกลับโดยทำการเข้ารหัสข้อมูลก่อนส่งและการทำจัดเก็บข้อมูลในรูป bitstream เพื่อที่จะจัดส่งทางด้านเครือข่ายได้

### คลาส ShopClientInterface

เป็นคลาสที่ได้รับการจัดสรรให้ดูแลเมื่อมีคำร้องขอจากโปรแกรมของลูกค้าที่ส่งมา มีความต้องการติดต่อกับทางร้านค้า ได้แก่ การสมัครสมาชิก, การลงชื่อเข้าใช้ระบบ, บริการส่งข้อมูลรายการสินค้าต่างๆ, การซื้อสินค้า, การสมัครการชำระเงินแบบชำระล่วงหน้ากับทางร้าน, การชำระเงิน และสุดท้ายส่งผลกลับไปยังคลาส ShopServer

### คลาส BankInterface

เป็นคลาสที่จัดการด้านการเงินของการซื้อขายสินค้า คือเมื่อได้รับผลการชำระเงินจากธนาคารในกรณีที่ลูกค้าชำระเงินด้วยบัตรเครดิต หรือ ข้อมูลจากลูกค้าโดยตรง กรณีที่ลูกค้าชำระเงินโดยหักบัญชีที่ชำระไว้ก่อนกับร้านค้า ก็จะทำการบันทึกข้อมูลการชำระเงิน จากนั้นจึงส่งไปยังคลาส ShopServer เพื่อส่งผลการทำงานกลับไปยังลูกค้าต่อไป

### คลาส Customer

เป็นคลาสที่ทำงานเกี่ยวกับข้อมูลลูกค้า ได้แก่ การนำข้อมูลลูกค้าลงฐานข้อมูล , การติดต่อฐานข้อมูลลูกค้ากับ Oracle และส่งผลตอบกลับไปยังคลาส ShopClientInterface

### คลาส Item

เป็นคลาสที่ทำงานเกี่ยวกับข้อมูลสินค้า ได้แก่ การนำข้อมูลสินค้าลงฐานข้อมูลและปรับปรุงข้อมูล, การติดต่อฐานข้อมูลสินค้ากับ Oracle และส่งผลตอบกลับไปยังคลาส ShopClientInterface

### คลาส Order

เป็นคลาสที่ทำงานเกี่ยวกับข้อมูลคำสั่งซื้อ ได้แก่ การนำข้อมูลคำสั่งซื้อลงฐานข้อมูล, การติดต่อฐานข้อมูล คำสั่งซื้อกับ Oracle และส่งผลตอบกลับไปยังคลาส ShopClientInterface

### คลาส OrderDetail

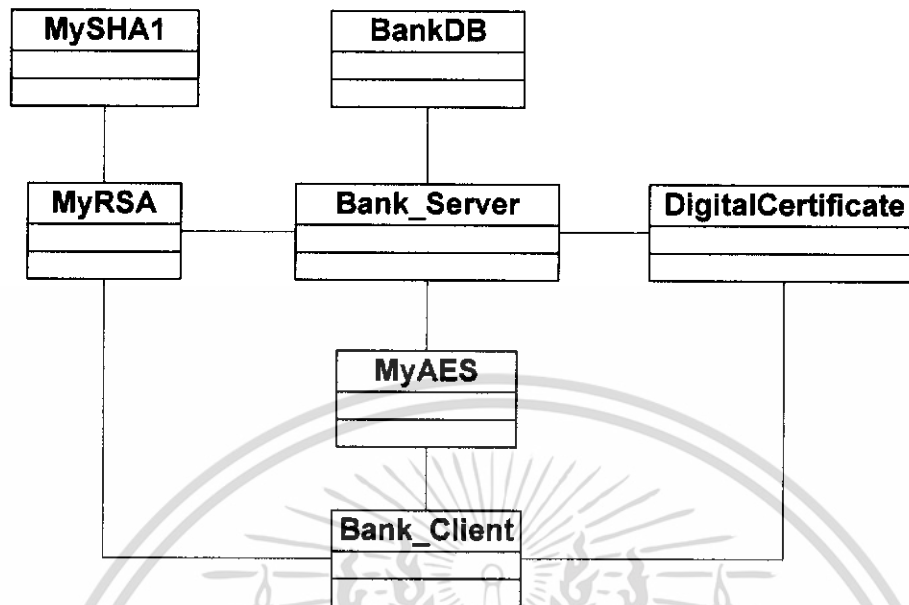
เป็นคลาสที่ทำงานเกี่ยวกับข้อมูลรายละเอียดคำสั่งซื้อและทำการปรับปรุงข้อมูลให้กับคงคลังของสินค้าเมื่อการชำระเงินไม่สำเร็จผล ได้แก่ การนำข้อมูลรายละเอียดคำสั่งซื้อลงฐานข้อมูล , การติดต่อฐานข้อมูลคำสั่งซื้อกับ Oracle และส่งผลตอบกลับไปยังคลาส ShopClientInterface

### คลาส UserAccount

เป็นคลาสที่ทำงานเกี่ยวกับข้อมูลบัญชีที่ลูกค้าชำระล่วงหน้าไว้กับทางร้าน ได้แก่ การนำข้อมูลลงฐานข้อมูล, การติดต่อฐานข้อมูล กับ Oracle และส่งผลตอบกลับไปยังคลาส ShopClientInterface

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

#### 4.1.2 โครงสร้างของโปรแกรมส่วนธนาคาร



รูปที่ 4.2 โครงสร้างของโปรแกรมส่วนธนาคาร

##### คลาส Bank\_Server

เป็นเครื่องแม่ข่ายที่ทำหน้าที่ในส่วนการติดต่อกับร้านค้า, บริษัทบัตรเครดิต และบริษัทองค์กรพิศุจน์สิทธิ์ โดยเริ่มต้นจะทำการรับแพคเกจที่ส่งมาจากร้านค้า หรือบริษัทบัตรเครดิต แล้วทำการจัดการกับแพคเกจนั้นตามฟังก์ชันที่กำหนด ซึ่งได้แก่ ถ้าเป็นร้านค้าส่งแพคเกจมาจะทำการตรวจสอบหมายเลขบัตรเครดิต, ตรวจสอบลายมือชื่อดิจิทัลของบุคคล, ส่งใบรับรองดิจิทัลไปตรวจสอบที่บริษัทองค์กรพิศุจน์สิทธิ์เพื่อยืนยันบัญชี, ทำการตัดยอดเงิน และเพิ่มเงินในบัญชีของร้านค้า ส่วนถ้าเป็นบริษัทบัตรเครดิตส่งแพคเกจมาจะทำการตรวจสอบหมายเลขบัตรเครดิต, ตรวจสอบลายมือชื่อของบุคคล, ทำการตัดยอดเงิน และเพิ่มเงินในบัญชีของร้านค้า และทั้ง 2 ส่วนนี้จะส่งผลตอบรับไปเครื่องลูกข่ายที่เรียกมา เป็นต้น

##### คลาส Bank\_Client

ทำหน้าที่ในการรวมแพคเกจที่สำคัญส่งข้อมูลไปที่ร้านค้าและองค์กรพิศุจน์สิทธิ์

##### คลาส BankDB

ทำหน้าที่ในการติดต่อกับฐานข้อมูล เช่น ทำการดึงข้อมูล เปลี่ยนแปลงข้อมูล เพิ่มข้อมูล และทำการลบข้อมูล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

### คลาส MyRSA

ทำหน้าที่ในการสร้างคีย์แบบไม่สมมาตร คือคีย์ส่วนตัว และคีย์สาธารณะ เข้ารหัสและถอดรหัสแบบไม่สมมาตร รวมทั้งสร้างและตรวจสอบลายมือชื่อดิจิตอล

### คลาส MyAES

ทำหน้าที่ในการสร้างคีย์แบบสมมาตร และเข้ารหัสและถอดรหัสข้อมูลแบบสมมาตร

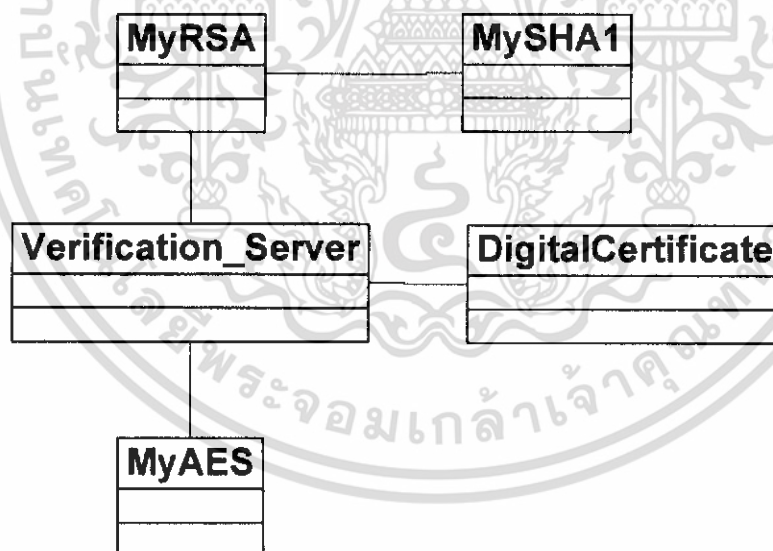
### คลาส DigitalCertificate

ทำหน้าที่ในการจัดการใบรับรองดิจิตอล คือการร้องขอใบรับรองดิจิตอลจากองค์กรพิสูจน์สิทธิ์ (CA : Certification Authority) และอ่านข้อมูลจากใบรับรองดิจิตอล

### คลาส MySHA1

ทำหน้าที่ในการสร้างเมสเซจไดเจสต์จากข้อมูลที่รับเข้ามา

#### 4.1.3 โครงสร้างของโปรแกรมส่วนบริษัทบัตรเครดิต



รูปที่ 4.3 โครงสร้างของโปรแกรมส่วนบริษัทบัตรเครดิต

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

### คลาส Verificaton\_Server

เป็นเครื่องแม่ข่ายที่ทำหน้าที่ในการรับบริการจากเครื่องลูกข่าย(ลูกค้าและร้านค้า) ที่เรียกเข้ามา โดยเริ่มต้นจะทำการรับแพคเกจที่ส่งมา และทำการติดต่อกับคลาส MyRSA คลาส MyAES และ คลาส DigitalCertificate เพื่อทำการเข้ารหัสข้อมูล แล้วทำการจัดการกับแพคเกจนั้นตามฟังก์ชันที่กำหนด ซึ่งได้แก่ การลงทะเบียนบัตรเครดิตของลูกค้า การตรวจสอบการยืนยันตัวตนของผู้ใช้บัตรเครดิต และส่งผลการทำงาน เช่นส่งผลตอบรับการลงทะเบียนบัตรเครดิตของลูกค้า และ ส่งผลการยืนยันตัวตนไปยังธนาคารเพื่อทำการโอนเงิน เป็นต้น โดยการส่งข้อมูลกลับจะมีการติดต่อกับคลาส MyRSA คลาส MyAES และคลาส DigitalCertificate เพื่อทำการเข้ารหัสข้อมูลพร้อมกับลงลายมือชื่อดิจิทัล

### คลาส MySHA1

ทำหน้าที่ในการสร้างเมสเซจไคเจสต์จากข้อมูลที่ได้รับเข้ามา

### คลาส MyRSA

ทำหน้าที่ในการสร้างคีย์แบบไม่สมมาตร คือคีย์ส่วนตัว และคีย์สาธารณะ เข้ารหัสและถอดรหัสแบบไม่สมมาตร รวมทั้งสร้างและตรวจสอบลายมือชื่อดิจิทัล

### คลาส MyAES

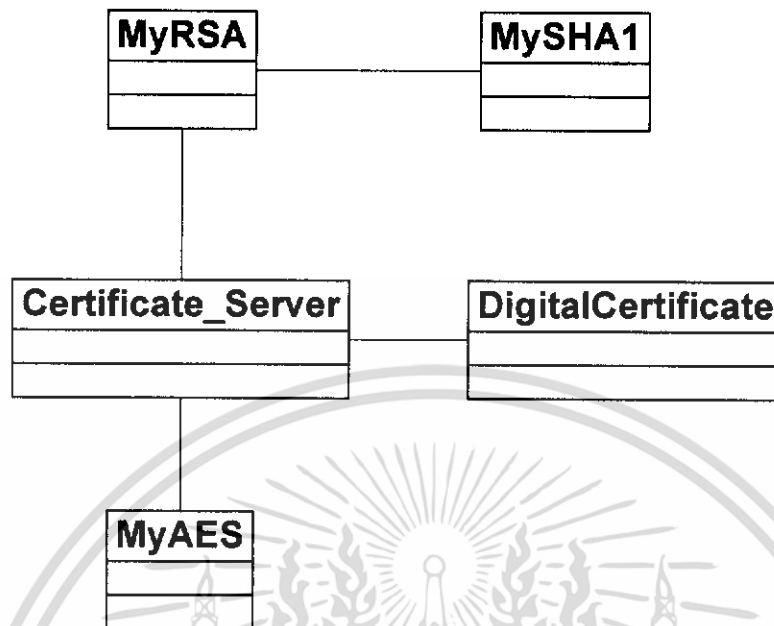
ทำหน้าที่ในการสร้างคีย์แบบสมมาตร และเข้ารหัสและถอดรหัสข้อมูลแบบสมมาตร

### คลาส DigitalCertificate

ทำหน้าที่ในการจัดการใบรับรองดิจิทัล คือการร้องขอใบรับรองดิจิทัลจากองค์กรพิสูจน์สิทธิ์ (CA : Certification Authority) และอ่านข้อมูลจากใบรับรองดิจิทัล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

#### 4.1.4 โครงสร้างของโปรแกรมส่วนองค์กรพิสูจน์สิทธิ์



รูปที่ 4.4 โครงสร้างของโปรแกรมส่วนองค์กรพิสูจน์สิทธิ์

##### คลาส Certificate\_Server

เป็นเครื่องแม่ข่ายที่ทำหน้าที่ในการรับบริการจากเครื่องลูกข่ายที่เรียกเข้ามา โดยเริ่มต้นจะทำการรับแพคเกจที่ส่งมา ติดต่อกับคลาส คลาส MyRSA คลาส MyAES และคลาส DigitalCertificate เพื่อทำการถอดรหัสข้อมูล แล้วทำการจัดการกับแพคเกจนั้นตาม โดยไปเรียกการทำงานจากคลาส DigitalCertificate ตามฟังก์ชันที่กำหนด แล้วส่งผลการทำงานหรือใบรับรองดิจิทัลกลับไปยังเครื่องลูกข่ายที่เรียกเข้ามา

##### คลาส MySHA1

ทำหน้าที่ในการสร้างเมสเฮจไคเจสต์จากข้อมูลที่ได้รับเข้ามา

##### คลาส MyRSA

ทำหน้าที่ในการสร้างคีย์แบบไม่สมมาตร คือคีย์ส่วนตัว และคีย์สาธารณะ เข้ารหัสและถอดรหัสแบบไม่สมมาตร รวมทั้งสร้างและตรวจสอบลายมือชื่อดิจิตอล

##### คลาส MyAES

ทำหน้าที่ในการสร้างคีย์แบบสมมาตร และเข้ารหัสและถอดรหัสข้อมูลแบบสมมาตร

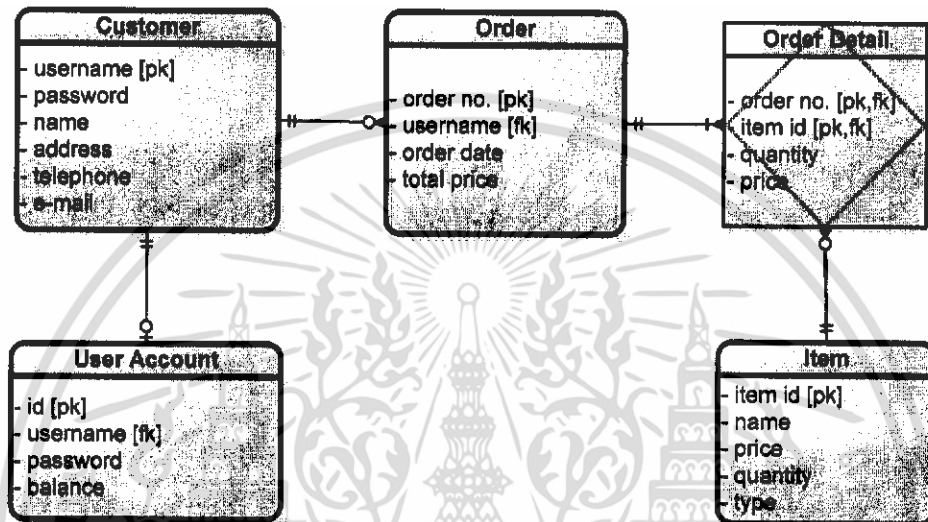
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## คลาส DigitalCertificate

ทำหน้าที่ในการจัดการใบรับรองดิจิทัล คือสร้างและเก็บข้อมูลใบรับรองดิจิทัลให้กับผู้ที่มาร้องขอ และบริการใบรับรองดิจิทัลให้กับผู้ที่มาร้องขอ

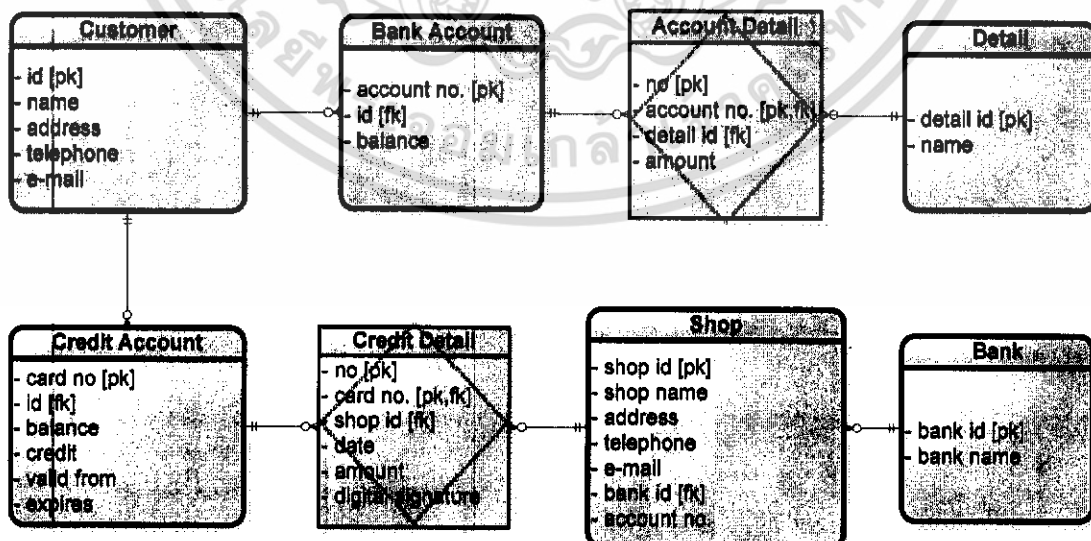
## 4.2 การเก็บข้อมูล

### 4.2.1 ฐานข้อมูลของร้านค้า



รูปที่ 4.5 แผนผังแสดงความสัมพันธ์ในฐานข้อมูลร้านค้า

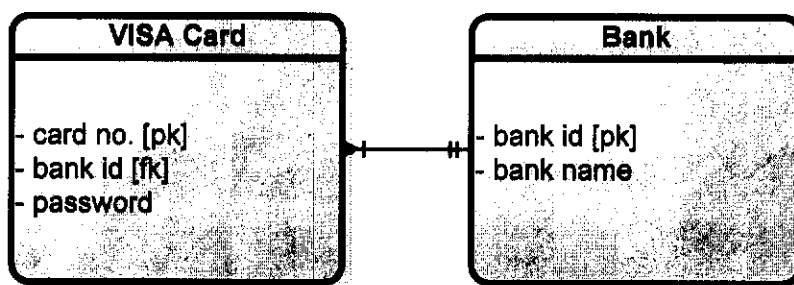
### 4.2.2 ฐานข้อมูลของธนาคาร



รูปที่ 4.6 แผนผังแสดงความสัมพันธ์ในฐานข้อมูลธนาคาร

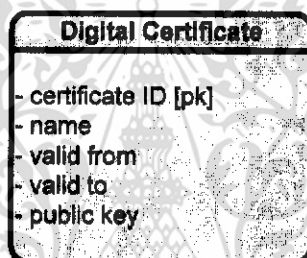
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

### 4.2.3 ฐานข้อมูลของบริษัทบัตรเครดิต



รูปที่ 4.7 แผนผังแสดงความสัมพันธ์ในฐานข้อมูลบริษัทบัตรเครดิต

### 4.2.4 ฐานข้อมูลขององค์กรพิสูจน์สิทธิ์



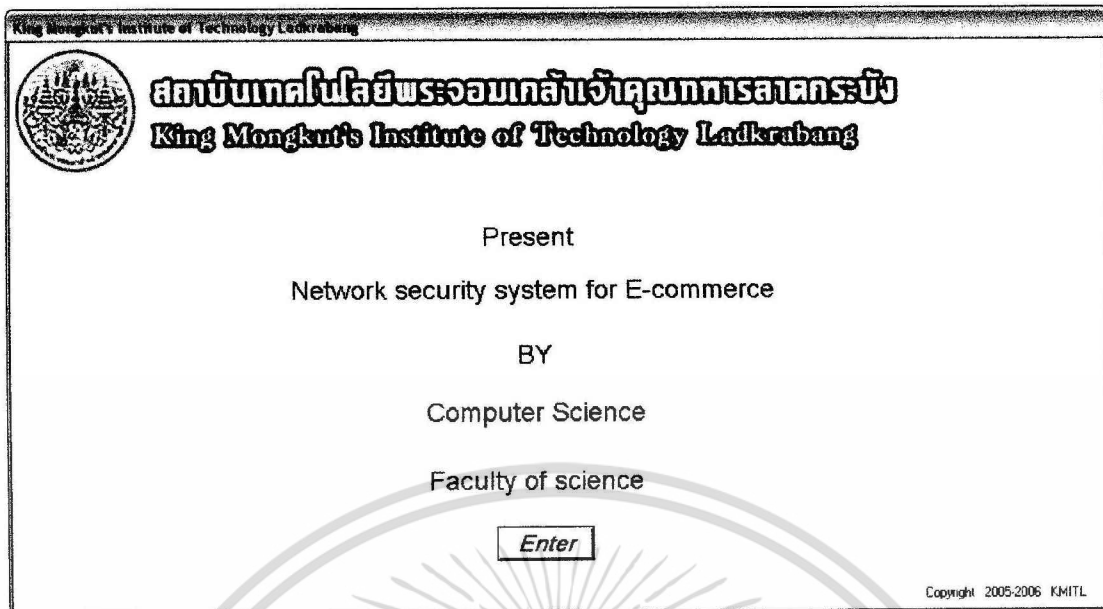
รูปที่ 4.8 แผนผังแสดงฐานข้อมูลองค์กรพิสูจน์สิทธิ์

## 4.3 หน้าจอของระบบ

ระบบนี้แบ่งโปรแกรมออกเป็น 5 ส่วน ได้แก่ ส่วนของลูกค้า ส่วนของร้านค้า ส่วนของธนาคาร ส่วนของบริษัทบัตรเครดิต และส่วนขององค์กรพิสูจน์สิทธิ์ ดังนี้

### 4.3.1 หน้าจอส่วนของลูกค้า

เมื่อเปิด โปรแกรมจะปรากฏหน้าจอต้อนรับดังภาพ กดปุ่ม Enter เพื่อเข้าสู่หน้าจอหลัก



รูปที่ 4.9 หน้าจอต้อนรับเมื่อเข้าสู่โปรแกรม

ส่วนของลูกค้ามีหน้าจการทำงานหลักดังนี้



รูปที่ 4.10 หน้าจอหลักของส่วนลูกค้า

และแบ่งหน้าจการทำงานของส่วนต่างๆดังนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## หน้าจอกการสมัครสมาชิกร้านค้า

รูปที่ 4.11 หน้าจอกการสมัครสมาชิก

ผู้ใช้จะต้องกรอกข้อมูลของตัวเอง จากนั้นกดปุ่ม OK เพื่อทำการส่งข้อมูลไปยังร้านค้า หากการสมัครสมาชิกสำเร็จ จะมีข้อความตอบรับแสดงแต่หากไม่สำเร็จจะแสดงข้อความปฏิเสธ

## หน้าจอกการลงทะเบียนบัตรเครดิตกับบริษัทบัตรเครดิต

รูปที่ 4.12 หน้าจอกการลงทะเบียนบัตรเครดิต

ลูกค้าจะต้องลงทะเบียนโดยกรอกหมายเลขบัตรเครดิต และรหัสผ่าน หากข้อมูลถูกต้องจะมีข้อความตอบรับแสดงแต่หากไม่สำเร็จจะแสดงข้อความปฏิเสธ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## หน้าจอการลงทะเบียนขอใบรับรองดิจิทัล

รูปที่ 4.13 หน้าจอการลงทะเบียนขอใบรับรองดิจิทัล

ผู้ใช้งานจะต้องกรอกข้อมูลคือชื่อของตัวเอง จากนั้นกดปุ่ม OK เพื่อทำการส่งข้อมูลไปยังองค์กรพิสูจน์สิทธิ์ และจะแสดงผลการทำงาน และแสดงคีย์ที่ได้ดังภาพ

รูปที่ 4.14 หน้าจอแสดงผลการแสดงผลคีย์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## หน้าจอการลงทะเบียนบัญชีชำระเงินล่วงหน้ากับทางร้านค้า

รูปที่ 4.15 หน้าจอการลงทะเบียนบัญชีชำระเงินล่วงหน้ากับทางร้านค้า

ลูกค้าจะต้องลงทะเบียนโดยชื่อผู้ใช้ ชื่อบัญชี และรหัสผ่าน หากข้อมูลถูกต้อง จะมีข้อความ  
ตอบรับแสดงแต่หากไม่สำเร็จจะแสดงข้อความปฏิเสธ

## หน้าจอการเข้าสู่ระบบ

รูปที่ 4.16 หน้าจอการเข้าสู่ระบบ

เมื่อลูกค้าคลิกปุ่ม Order Product จะปรากฏหน้าจอให้กรอกชื่อผู้ใช้ และรหัสผ่าน เพื่อทำการ  
ล็อกอินเข้าสู่ระบบ หากข้อมูลถูกต้อง จะปรากฏหน้าจอการสั่งซื้อสินค้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## หน้าจอการสั่งซื้อสินค้า

**Order Product**

Choose Type:

ID	Name	Price
00000002	AI In Game Programming	2700

Add to cart    Close

**Add to cart**

Name	QTY	SubTotal
Total Price: 0		

Remove    Buy

รูปที่ 4.17 หน้าจอการสั่งซื้อสินค้า

ลูกค้าสามารถเลือกประเภทของสินค้า จากนั้นจึงเลือกสินค้าที่ต้องการ แล้วกดปุ่ม Add to cart จะปรากฏหน้าจอให้ใส่จำนวนสินค้าที่ต้องการ

**Order Product**

Choose Type:

ID	Name	Price
00000002	AI In Game Programming	2700

Add to cart    Close

**Quantity**

Enter Quantity:

OK

รูปที่ 4.18 หน้าจอรอกจำนวนสินค้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Order\_Product

Choose Type: Book

ID	Name	Price
00000001	.net Cryptography System	1800
00000002	AI In Game Programming	2700

Add to cart

Name	QTY	SubTotal
00000001	2	3600
00000002	1	2700

Total Price: 6300

Buttons: Add to cart, Close, Remove, Buy

รูปที่ 4.19 หน้าจอแสดงการสั่งซื้อสินค้า

เมื่อลูกค้าเลือกซื้อสินค้าครบตามต้องการแล้ว กดปุ่ม Buy จะเป็นการเช็คสต็อกสินค้ากับทางร้าน หากไม่สามารถซื้อสินค้าได้จะปรากฏข้อความเตือน แต่หากสามารถซื้อสินค้าได้ จะปรากฏหน้าจอการชำระเงิน

### หน้าจอการชำระเงิน

Payment

Order ID: 00010

Total: 6300 Baht

Payment Method:

- Withdraw from Shop Account
- VISA Card with Digital Certificate
- VISA Card without Digital Certificate

Payment Detail:

Buttons: OK, Close

รูปที่ 4.20 หน้าจอการชำระเงิน

ลูกค้าสามารถเลือกวิธีการชำระเงินได้ จากนั้นจึงกรอกรายละเอียดการชำระเงิน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

รูปที่ 4.21 หน้าจอการชำระเงินแสดงรายละเอียดการชำระเงิน

แล้วจึงกดปุ่ม OK หากผลการชำระเงินถูกต้อง จะปรากฏหน้าจอ จะมีข้อความตอบรับ แสดงแต่หากไม่สำเร็จจะแสดงข้อความปฏิเสธการชำระเงิน ถูกค้าจะต้องกรอกรายละเอียดการชำระเงินใหม่

#### 4.3.2 หน้าจอส่วนของร้านค้า

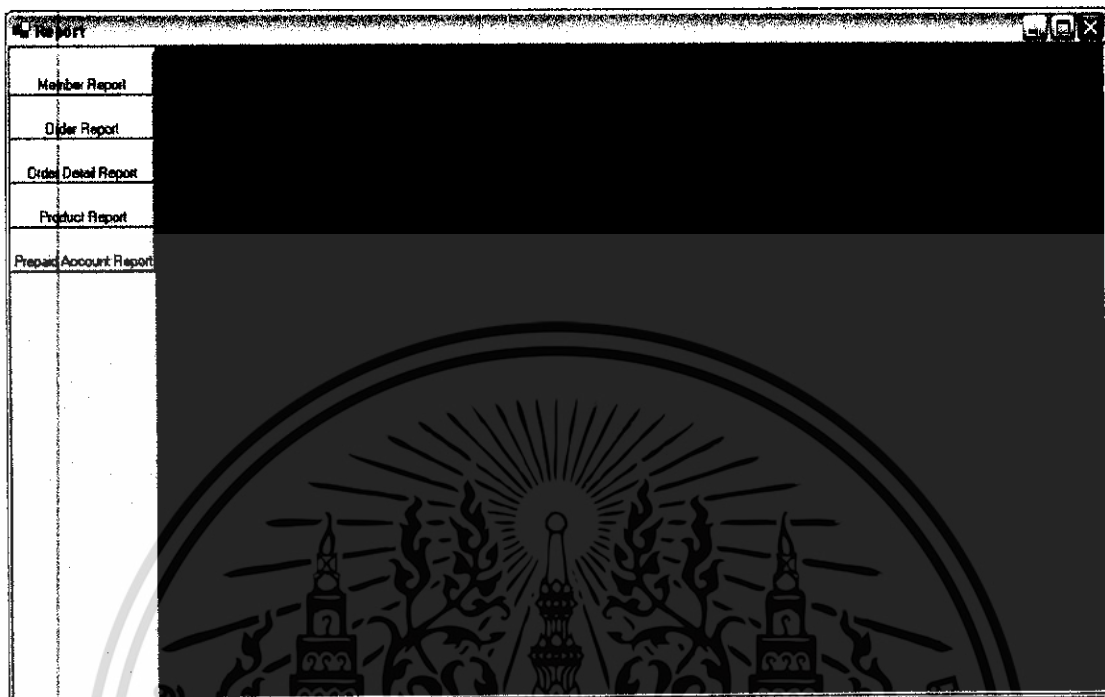
หน้าจอในส่วนเครื่องแม่ข่ายของร้านค้าเป็นแบบคอล โลกที่แสดงสถานะการทำงาน ปัจจุบัน ดังภาพ



รูปที่ 4.22 หน้าจอส่วนของร้านค้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

หน้าจอหลักในการแสดงรายงานต่างๆของร้านค้า แสดงดังภาพ สำหรับตัวอย่างรายงาน  
ของร้านค้า แสดงในภาคผนวก ง หัวข้อรายงานของร้านค้า



รูปที่ 4.23 หน้าจอหลักส่วนการแสดงผลรายงานของร้านค้า

### 4.3.3 หน้าจอส่วนของธนาคาร

หน้าจอในส่วนเครื่องแม่ข่ายธนาคารเป็นแบบคอลโซลที่แสดงสถานะการทำงาน  
ปัจจุบัน ดังภาพ



รูปที่ 4.24 หน้าจอส่วนของธนาคาร

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

หน้าจอหลักในการแสดงรายงานต่างๆของธนาคาร แสดงดังภาพ สำหรับตัวอย่างรายงาน  
ของธนาคาร แสดงในภาคผนวก ง หัวข้อรายงานของธนาคาร



รูปที่ 4.25 หน้าจอหลักส่วนการแสดงผลรายงานของธนาคาร

#### 4.3.4 หน้าจอส่วนของบริษัทบัตรเครดิต

หน้าจอในส่วนของเครื่องแม่ข่ายบริษัทบัตรเครดิตเป็นแบบคอล โคลที่แสดงสถานะการ  
ทำงานปัจจุบัน ดังภาพ



รูปที่ 4.26 หน้าจอส่วนของบริษัทบัตรเครดิต

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

#### 4.3.5 หน้าจอส่วนขององค์กรพิสูจน์สิทธิ์

หน้าจอในส่วนของเครื่องแม่ข่ายขององค์กรพิสูจน์สิทธิ์เป็นแบบคอลโซลที่แสดงสถานะการทำงานปัจจุบัน ดังภาพ



รูปที่ 4.27 หน้าจอส่วนขององค์กรพิสูจน์สิทธิ์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## บทที่ 5

### สรุปผลและข้อเสนอแนะ

#### 5.1 สรุปผลปัญหาพิเศษ

จากการศึกษาวิจัยและพัฒนาระบบความปลอดภัยในเครือข่ายสำหรับการซื้อขายสินค้าออนไลน์ โดยใช้ Visual C++.NET บนระบบปฏิบัติการวินโดวส์ แบ่งการทำงานออกเป็น 3 ระบบ คือ ส่วนการซื้อขายสินค้าออนไลน์ ส่วนการชำระเงินออนไลน์ ส่วนการบริการออกใบรับรองอิเล็กทรอนิกส์และการพิสูจน์สิทธิ์ สรุปผลการทำงานได้ดังนี้

1. สามารถจำลองระบบซื้อขายสินค้าผ่านเครือข่ายคอมพิวเตอร์ได้โดยมีความปลอดภัยในระดับหนึ่ง
2. สามารถจำลองระบบการชำระเงินผ่านอินเทอร์เน็ตอย่างง่าย ที่ทำงานได้อย่างถูกต้อง
3. สามารถจำลองการให้บริการออกใบรับรองอิเล็กทรอนิกส์ที่ทำงานได้อย่างถูกต้อง
4. ในการรับส่งข้อมูล สามารถเข้ารหัสข้อมูลและถอดรหัสข้อมูลได้อย่างถูกต้อง
5. สามารถใช้ลายมือชื่อดิจิทัลในการระบุตัวตนของผู้ส่งข้อมูลผ่านเครือข่ายได้อย่างถูกต้อง
6. ในการเก็บรหัสผ่านในฐานข้อมูล มีการเข้ารหัสเพื่อความปลอดภัยมากยิ่งขึ้น
7. มีการใช้งานที่ง่ายและสะดวกต่อผู้ใช้งานที่ไม่มีความรู้ด้านเครือข่ายคอมพิวเตอร์และการเข้ารหัสข้อมูล

#### 5.2 ข้อจำกัดของปัญหาพิเศษ

ในการทำปัญหาพิเศษนี้ เกิดข้อจำกัดบางประการ ทำให้ไม่สามารถพัฒนาโปรแกรมได้เป็นไปอย่างดี ซึ่งข้อจำกัดที่เกิดขึ้น มีดังนี้

1. เพื่อความรวดเร็วในการทำงานของโปรแกรม ซึ่งทำงานบนทรัพยากรที่จำกัด ระบบนี้จึงใช้การศึกษาจากคีย์สำหรับการเข้ารหัสและถอดรหัสที่มีความยาวน้อย ซึ่งมีข้อเสียคือผู้ไม่ประสงค์ดีสามารถทำการแทรกแซงระบบได้ง่าย ซึ่งในการใช้งานจริงจะต้องใช้คีย์ที่มีความยาวมากกว่านี้เพื่อให้ระบบมีความปลอดภัยมากขึ้น
2. ระบบนี้เป็นระบบที่ใช้รูปแบบการส่งแพ็คเกจข้อมูลที่ผู้พัฒนาระบบ พัฒนาขึ้นเองเพื่อการศึกษา จึงไม่สามารถนำไปใช้กับระบบอื่นๆที่มีอยู่ในปัจจุบันได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

### 5.3 ข้อเสนอแนะและแนวทางการศึกษาต่อ

1. ควรเพิ่มความยาวคีย์ที่ใช้ในการเข้ารหัสและถอดรหัส เพื่อความปลอดภัยที่มากขึ้น
2. โปรแกรมนี้สามารถนำเอาไปพัฒนาต่อโดยใช้รูปแบบที่เป็นมาตรฐานเพื่อให้สามารถนำไปใช้กับระบบการซื้อขายสินค้าออนไลน์ต่างๆที่มีอยู่ในปัจจุบันได้



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## บรรณานุกรม

- Julian Templeman and Andy Olsen. 2002. **Microsoft Visual C++.NET Step by Step**.  
Washington : Microsoft Press.
- ยุทธนา ทิลาศวัฒนกุล. 2546. **คู่มือการเขียนโปรแกรมและใช้งาน Visual C++.NET ฉบับสมบูรณ์**.  
นนทบุรี : อินโฟเพรส.
- จตุชัย แพงจันทร์. 2546. **เจาะระบบ Network ฉบับสมบูรณ์**. นนทบุรี : ไอทีซี
- Charlie Kaufman, Radia Perlman and Mike Speciner. 2002. **NETWORK SECURITY  
PRIVATE Communication in a PUBLIC World**. New Jersey : Prentice Hall, Inc.
- Behrouz A.Forouzan. 2003. **Data Communications and Networking**. 3<sup>th</sup> ed. New York :  
McGraw-Hill.
- ศุภชัย จิระรังสีณี และขจรศักดิ์ สังข์เจริญ. 2547. **เรียนรู้ ORACLE Database 10g และภาษา SQL**.  
กรุงเทพฯ : คณะบุคคล เอส เค ซีรีย.
- Ian Abramson, Michael S. Abbey and Michael Corey. 2004. **Oracle database 10g : a  
beginner's guide**. New York : McGraw-Hill/Osborne.
- Kevin Loney and Bob Bryla. 2005. **Oracle Database 10g DBA Handbook**. New York :  
McGraw-Hill/Osborne.
- Federal Information Processing Standards (FIPS). **Secure Hash Standard (SHS), U.S.  
DoC/NIST**. 2002.
- Microsoft. **MSDN Library**. [Online]. Available : <http://msdn.microsoft.com/library/default.asp>.  
2005.
- Rakkarsoft L.L.C.. **Raknet-Network Library**. [Online]. Available : <http://www.rakkarsoft.com>.  
2003.
- Wikimedia Foundation, Inc. **Wikipedia, the free encyclopedia**. [Online]. Available :  
<http://en.wikipedia.org>.
- Chris Maunder. **The Code Project**. [Online]. Available : <http://www.codeproject.com>.  
<http://www.codeguru.com>

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## ภาคผนวก ก

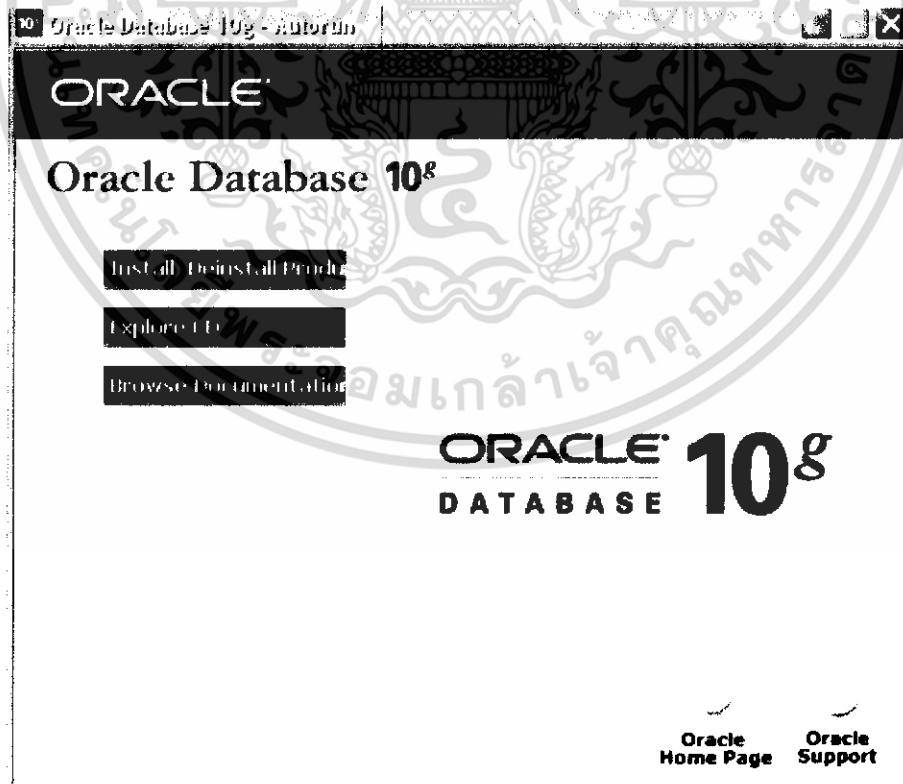
# การติดตั้งโปรแกรม Oracle Database 10g

### ความต้องการของระบบในการติดตั้งโปรแกรม

1. ระบบปฏิบัติการที่ใช้ได้ก็คือ Unix , Linux และ Window เช่น Windows 2000 Service Pack1 เป็นอย่างน้อย, Windows XP Professional และ Windows 2003
2. หน่วยความจำหลักของเครื่องควรมีอย่างน้อย 256 MB แต่ควรจะใช้ 512 MB
3. ฮาร์ดดิสก์ที่ใช้สำหรับการลง Oracle Database ใช้พื้นที่ประมาณ 1.5 GBและมียังอย่างน้อย 200 MB สำหรับพื้นที่ว่างในโฟลเดอร์ Temp ของ Windows
4. Virtual Memory ควรมีอย่างน้อยเป็น 2 เท่าของหน่วยความจำหลักที่มีในเครื่อง
5. ซอฟต์แวร์อื่นๆที่ต้องมีด้วย ได้แก่ WinZip และ Browser เช่น Microsoft Internet Explorer 5.5 หรือ 6.0 และ Netscape Navigator 4.70, 4.79, 7.0.1 หรือ 7.1.0

### ขั้นตอนการติดตั้งโปรแกรม

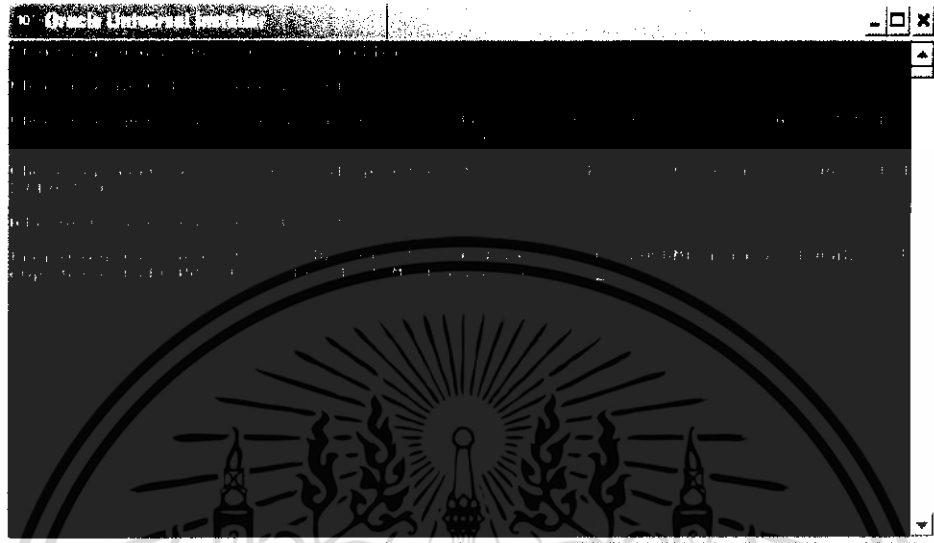
1. เริ่มต้นใส่แผ่นซีดีรอมและแผ่นจะเริ่มทำงานอัตโนมัติเพื่อเริ่มทำการติดตั้ง โปรแกรม



รูปที่ ก-1 หน้าจอเริ่มต้นการติดตั้งโปรแกรม Oracle Database 10g

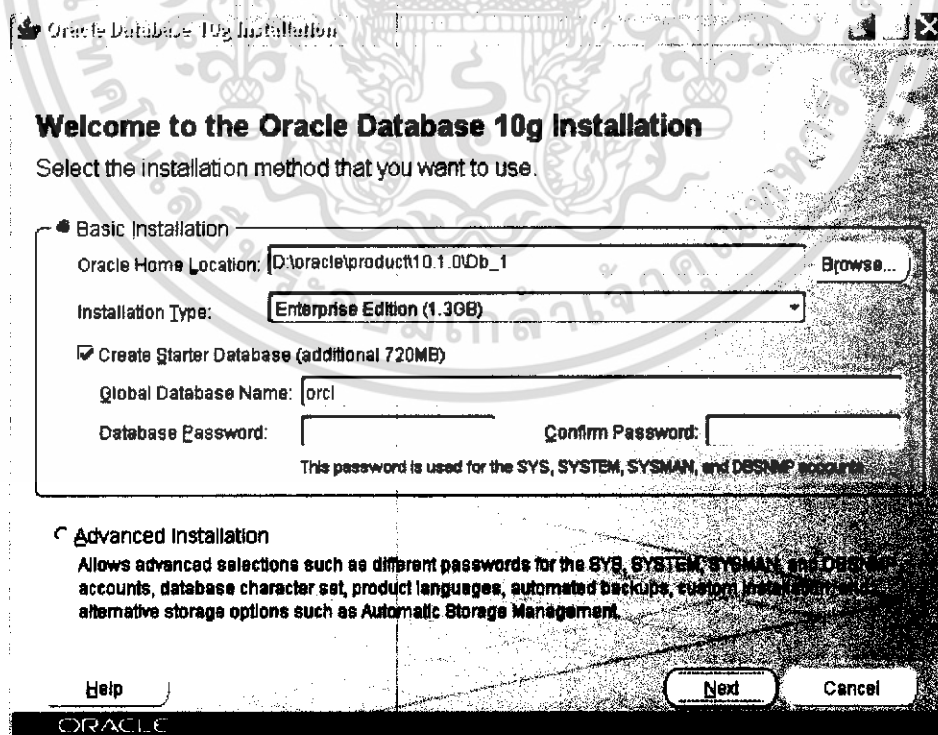
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

หลังจากนั้นกดปุ่ม Install/Deinstall Products แล้วจะมีหน้าจอขอสิทธิ์มาดังรูปที่ ก-2 โดยจะเป็นการตรวจสอบความพร้อมของเครื่อง และถ้าหากเครื่องไม่พร้อมในการติดตั้งก็ควรจะปรับสภาพความพร้อมตามที่แนะนำไว้ก่อนหน้า



รูปที่ ก-2 แสดงการตรวจสอบความพร้อมของเครื่องที่ทำการติดตั้งโปรแกรม

จากนั้นโปรแกรมแสดงหน้าจอ Welcome Screen ดังรูปที่ ก-3 ขึ้นมา



รูปที่ ก-3 แสดงรูปแบบการติดตั้งโปรแกรม Welcome to the Oracle Database 10g

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีกรนำไปใช้

รูปแบบการติดตั้งจะมีอยู่ 2 รูปแบบ

รูปแบบที่ 1 Basic Installation เป็นรูปแบบที่ง่ายและเหมาะสมกับคนที่เริ่มต้นในการเรียนรู้ Oracle Database 10g ซึ่งจะมีส่วนประกอบดังนี้

**1.1 Oracle Home Location** หมายถึงตำแหน่งของไดเรกทอรีบนเครื่องที่ทำติดตั้งโปรแกรม ซึ่งสามารถเปลี่ยนเป็นไดเรกทอรีอื่นได้

**1.2 Installation Type** มี 3 แบบที่ติดตั้งได้คือแบบ Enterprise Edition, Standard Edition และแบบ Personal Edition โดยแบบ Enterprise Edition และ Standard Edition เป็นแบบที่อนุญาตให้มีผู้ใช้งานฐานข้อมูลได้หลายคนพร้อมกัน โดยที่ทั้ง 2 แบบนี้จะมีความสามารถที่ต่างกัน ส่วนแบบ Personal Edition จะให้มีผู้ใช้งานฐานข้อมูลได้เพียงคนเดียว

**1.3 Create Starter Database** ควรจะเลือกเพราะว่าในการติดตั้งจะมีการสร้างฐานข้อมูลขึ้นมาหลังการติดตั้งโปรแกรมเสร็จ

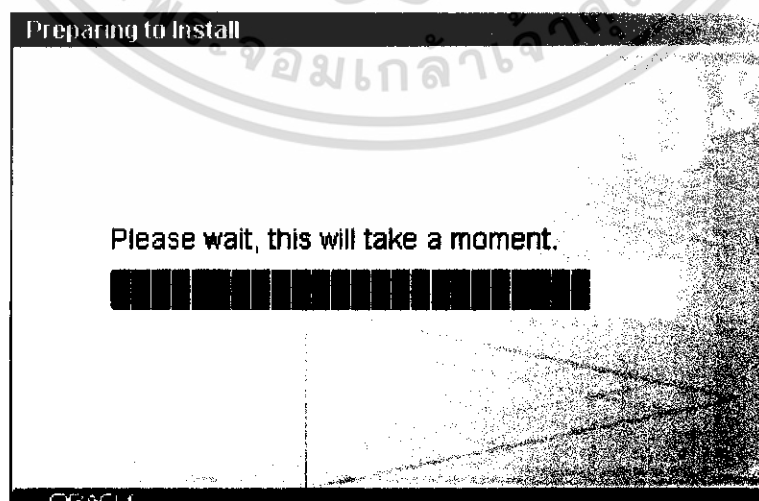
**1.3.1 Global Database Name** คือชื่อเรียกของฐานข้อมูลที่ใช้ในการติดตั้ง

**1.3.2 Database Password/Confirm Password** เป็นพาสเวิร์ดที่ใช้สำหรับผู้ใช้งานต่างๆที่จะถูกสร้างขึ้นจากการติดตั้งฐานข้อมูล สำหรับผู้ใช้ที่ใช้พาสเวิร์ดนี้คือ

SYS, SYSTEM, SYSMAN และ DBSNMP

รูปแบบที่ 2 Advanced Installation เหมาะกับผู้ใช้ Oracle รุ่นเคยแล้ว

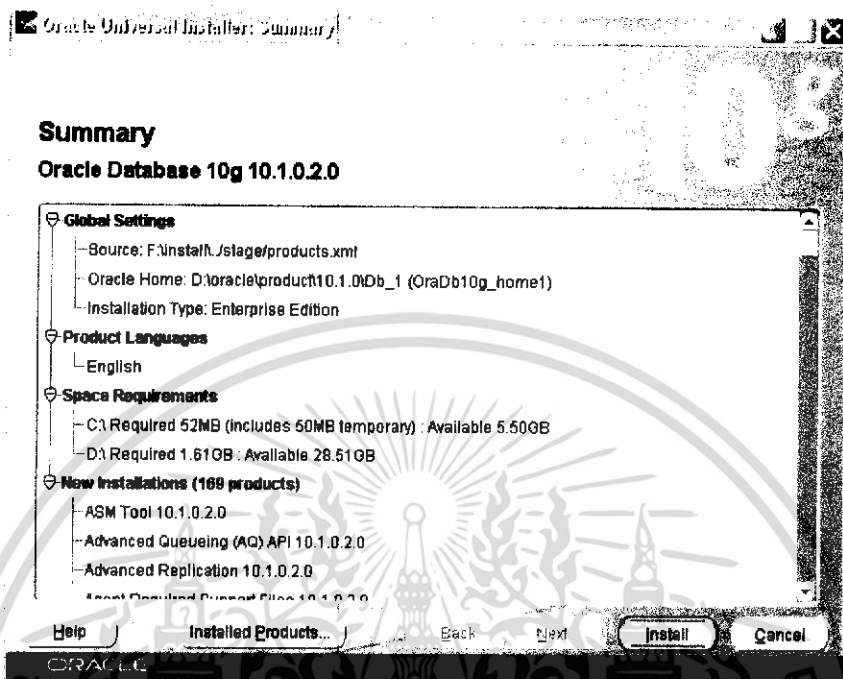
ในที่นี้ขอแนะนำให้เลือกรูปแบบที่ 1 Basic Installation และเลือกการติดตั้งแบบ Enterprise Edition และใส่ Global Database Name ว่า orcl แล้วก็ใส่พาสเวิร์ดด้วย จากนั้นกดปุ่ม Next จะขึ้นดังรูปที่ ก-4



รูปที่ ก-4 Oracle Universal Installer เตรียมการติดตั้ง

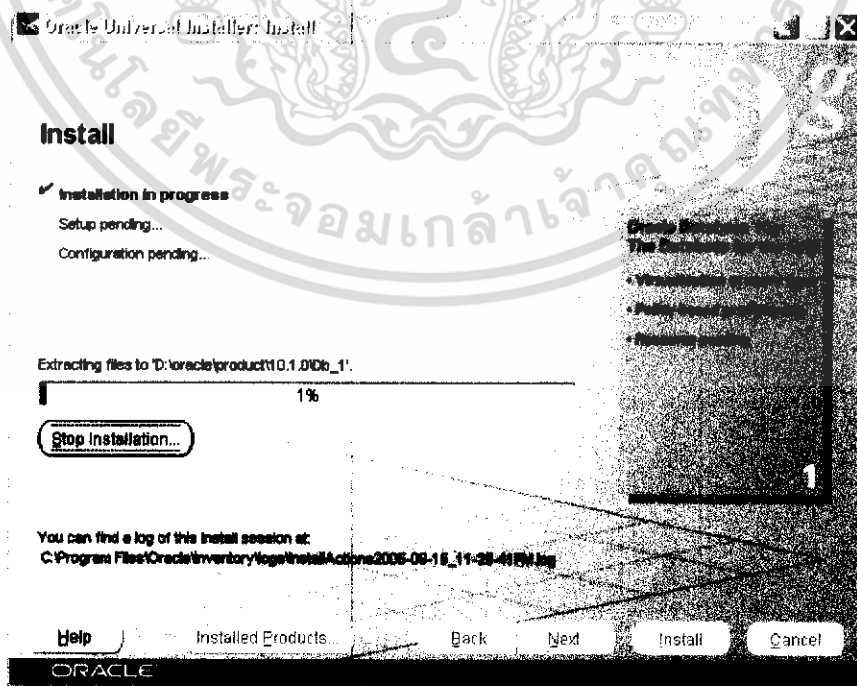
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

โปรแกรมจะปรากฏดังรูปที่ ก-5 เป็นการสรุปว่าในขณะนี้จะมีการติดตั้งอะไรบ้างและรายละเอียดต่างๆที่ติดตั้งบนเครื่อง



รูปที่ ก-5 แสดงผลสรุปรายละเอียดของการติดตั้งโปรแกรม

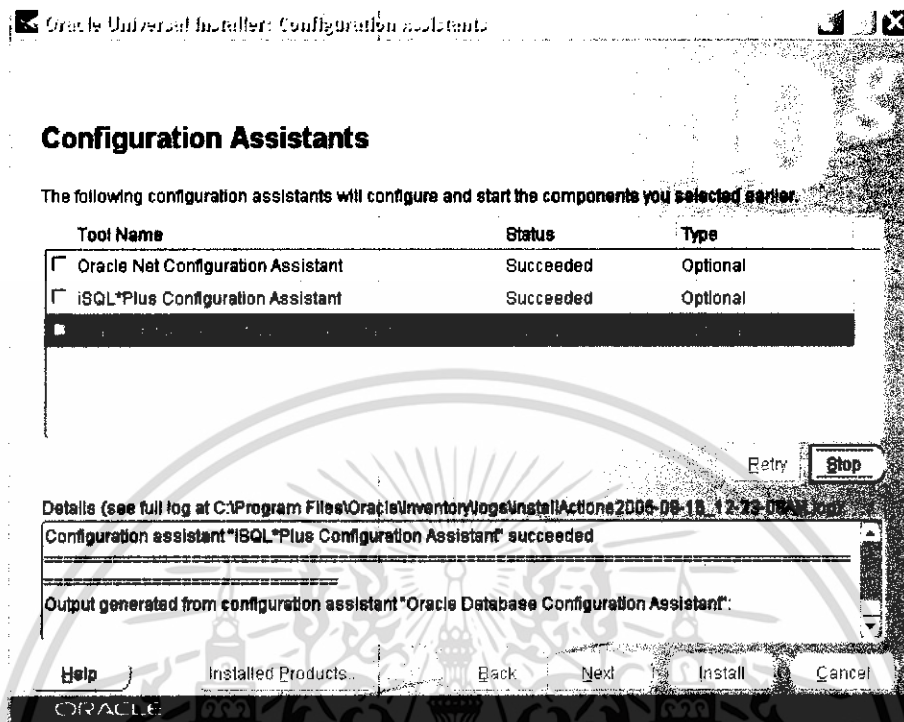
และทำการกดปุ่ม Install จะปรากฏดังรูปที่ ก-6 โดยระหว่างการติดตั้งต้องรอจนเสร็จและกรุณาอย่าทำอะไรกับเครื่อง



รูปที่ ก-6 แสดงการติดตั้งโปรแกรม

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับใช้ภายในเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

หลังจากครบ 100% แล้วทำการปรับแต่งระบบแบบอัตโนมัติ เป็นดังรูปที่ ก-7



รูปที่ ก-7 แสดงการ Configuration Assistants

โดยมีการปรับแต่งระบบ 3 ส่วนคือ

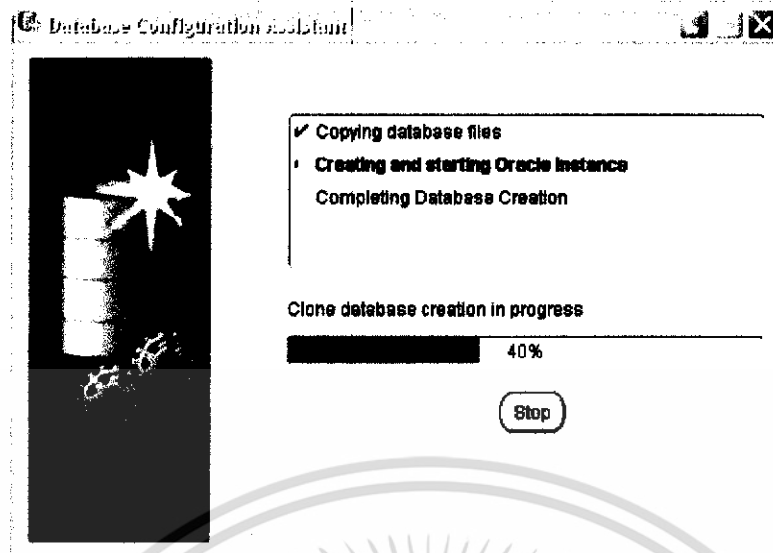
**Oracle Net Configuration Assistant** เป็นการปรับแต่งเกี่ยวกับทางด้าน Network

**iSQL\*PLUS Configuration Assistant** เป็นการปรับแต่งเครื่องมือที่ใช้เขียนคำสั่ง SQL ในแบบเวอร์ชันเว็บ

**Oracle Database Configuration Assistant** เป็นการเริ่มสร้างฐานข้อมูล โดยจะช่วยสร้างฐานข้อมูลไว้เพื่อใช้งานหลังการติดตั้ง

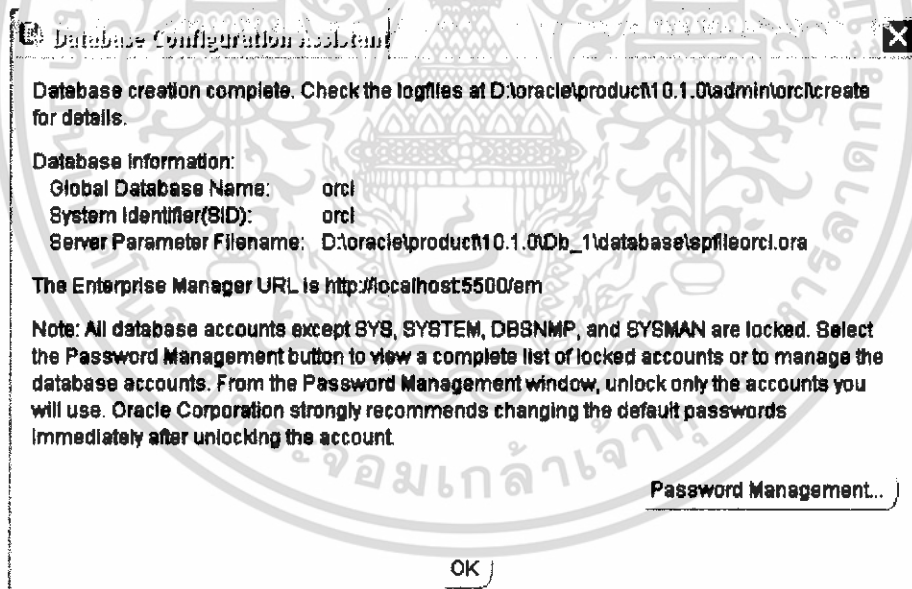
เมื่อโปรแกรม Oracle Database Configuration Assistant เริ่มทำงานจะแสดงการสร้างฐานข้อมูลขึ้นมา ดังรูปที่ ก-8

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ ก-8 แสดงการสร้างฐานข้อมูล

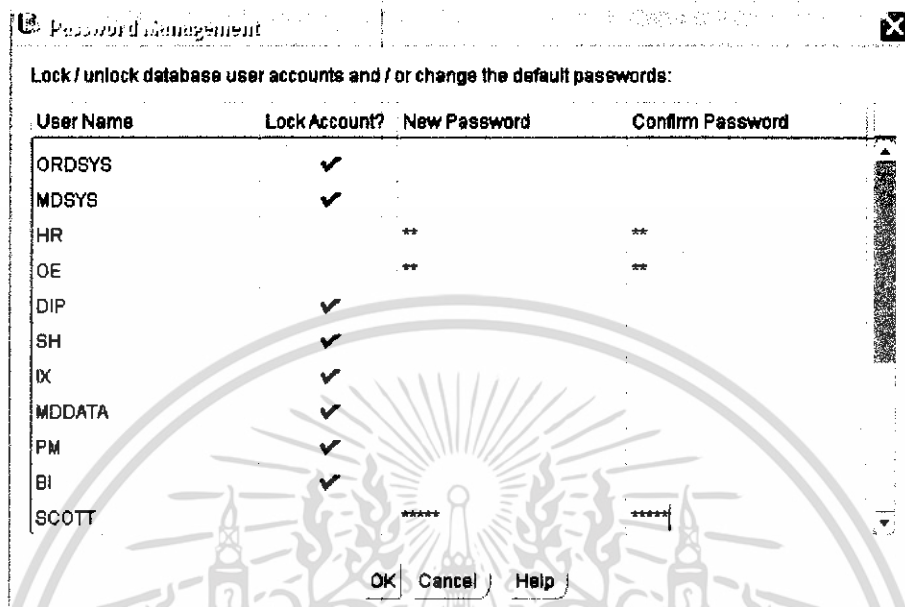
หลังจากสร้างฐานข้อมูลเสร็จแล้ว จะปรากฏจตุรูปที่ ก-9 จะแสดงว่าฐานข้อมูลมีรายละเอียดอย่างไร โดยจะมีผู้ใช้หลายคนถูกสร้างให้แบบอัตโนมัติทั้งผู้ใช้ที่เป็นผู้ดูแลระบบและผู้ใช้ธรรมดา



รูปที่ ก-9 แสดงรายละเอียดของฐานข้อมูล

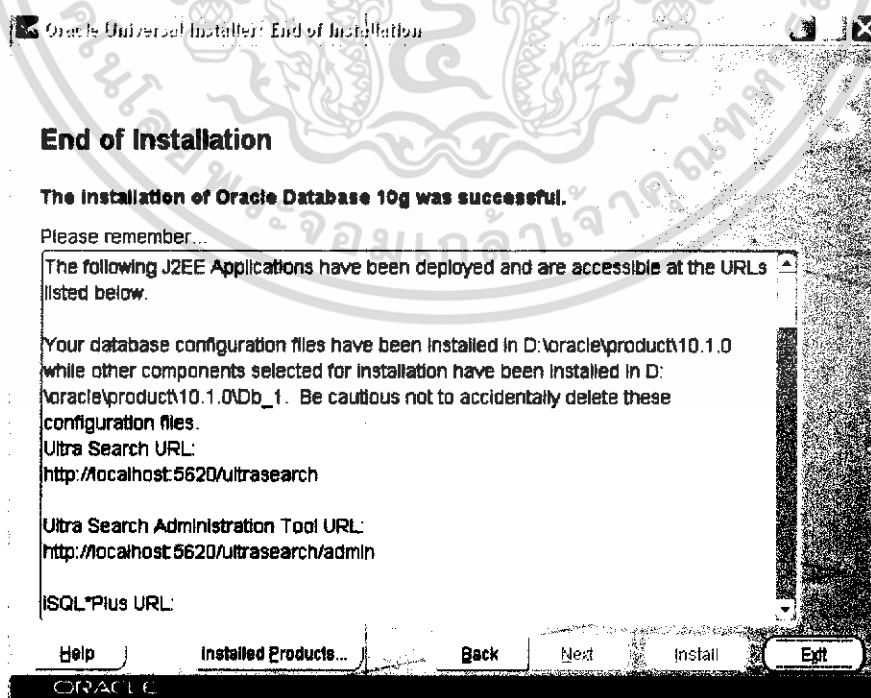
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ทำการกดปุ่ม Password Management เพื่อทำการปลดล็อกผู้ใช้บางคนที่ยังไม่ถูกอนุญาตให้เข้าใช้ฐานข้อมูล และตั้งพาสเวิร์ด จะขึ้นดังรูปที่ ก-10



รูปที่ ก-10 แสดงการจัดการ Password Management

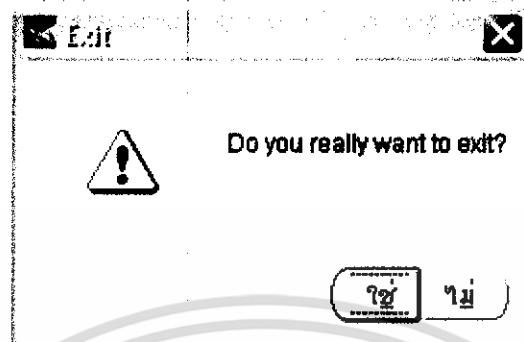
หลังจากนั้นทำการเอาเครื่องหมายถูกออก โดยการกดที่เครื่องหมายและทำการใส่รหัส ซึ่งในที่นี้จะทำการใส่ให้กับผู้ใช้ที่ชื่อว่า HR, OE และ SCOTT จากนั้นกดปุ่ม OK จะขึ้นดังรูปที่ ก-11



รูปที่ ก-11 แสดงสรุปวิธีการจัดการและใช้ข้อมูล

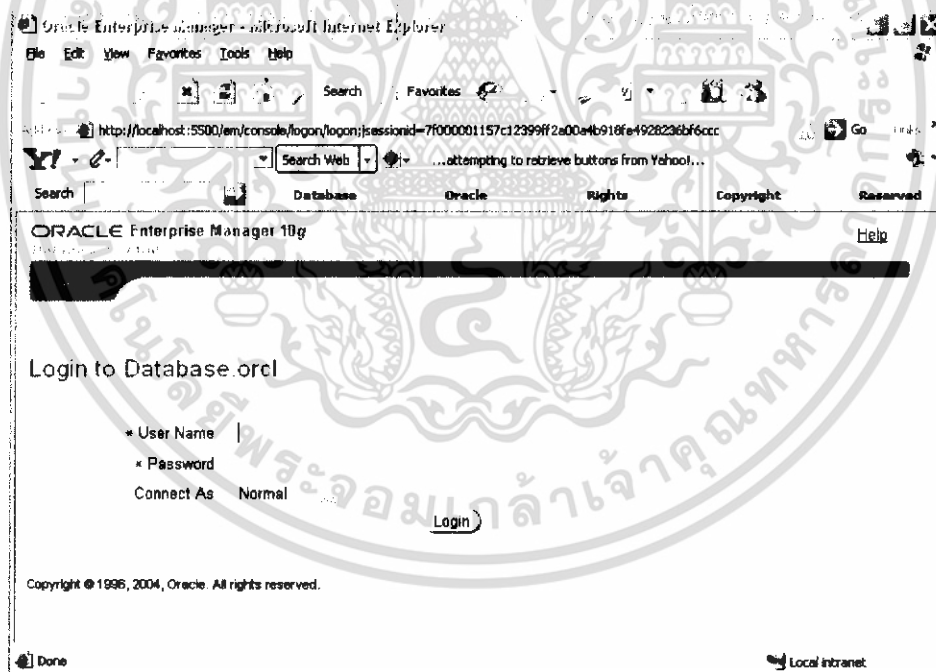
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เป็นการสรุปวิธีการเข้าจัดการและใช้ข้อมูลบนฐานข้อมูล ซึ่งข้อมูลส่วนนี้ควรจะเก็บไว้เพื่อจะได้เอาไว้ใช้ได้จากนั้นกดปุ่ม Exit ก็จะมีปรากฏดังรูปที่ ก-12



รูปที่ ก-12 แสดงการยืนยันการเสร็จสิ้นการติดตั้งโปรแกรม

ถ้าตอบว่า “ใช่” จะแสดงว่าติดตั้งโปรแกรมเรียบร้อยแล้ว แต่ถ้าตอบว่า “ไม่ใช่” ก็จะแสดงว่ายังติดตั้งไม่สำเร็จ ในที่นี้กดปุ่ม “ใช่” จึงแสดงดังรูปที่ ก-13



รูปที่ ก-13 แสดงการติดตั้งโปรแกรมสำเร็จ

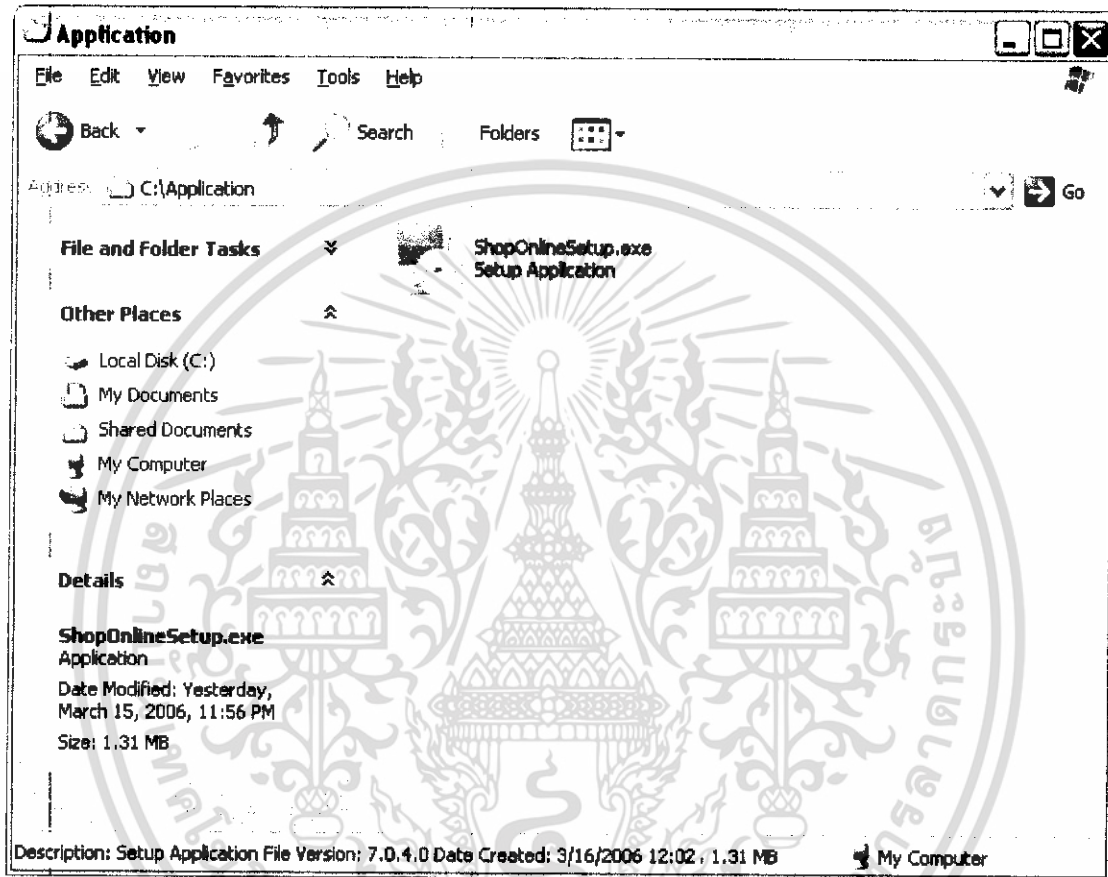
กดปุ่มExit แล้วจะขึ้นดังรูปที่ ก-13 และเป็นอันเสร็จสิ้นขั้นตอนการติดตั้งโปรแกรม Oracle Database 10g

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ภาคผนวก ข  
คู่มือการติดตั้งโปรแกรม

ขั้นตอนการติดตั้งโปรแกรมสำหรับลูกค้า

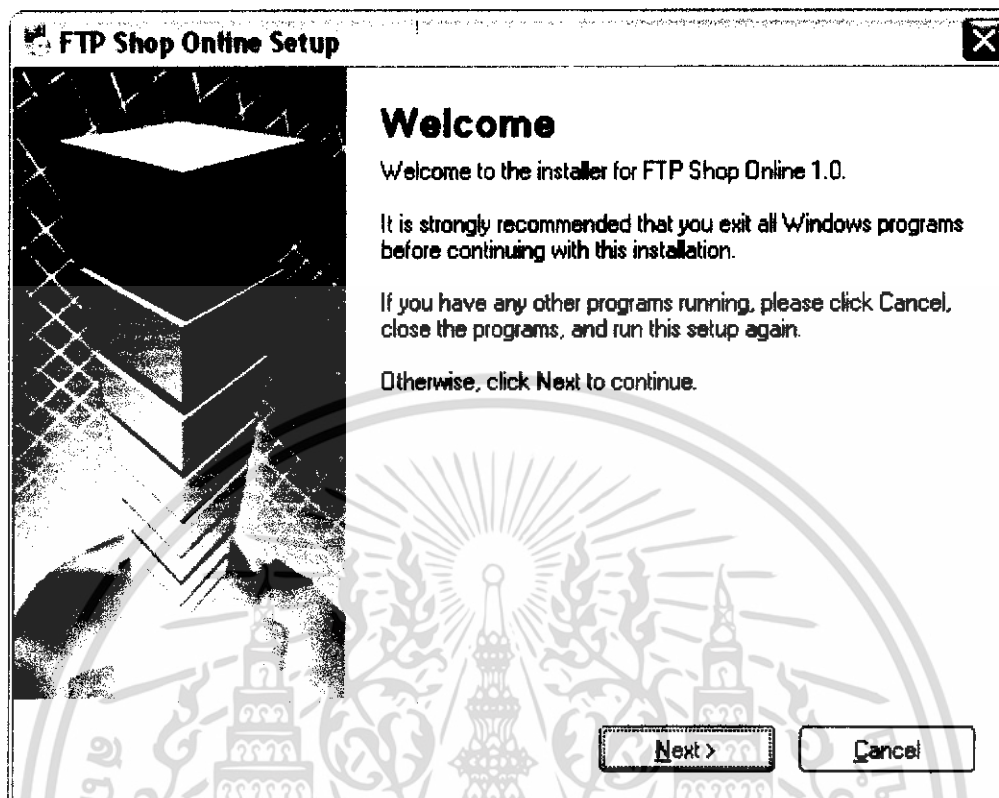
1. เปิดไฟล์ ShopOnlineSetup.exe เพื่อเริ่มทำการติดตั้ง โปรแกรมส่วนซื้อขายสำหรับลูกค้า



รูปที่ ข-1 ไฟล์ที่ใช้ในการติดตั้งโปรแกรมสำหรับลูกค้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

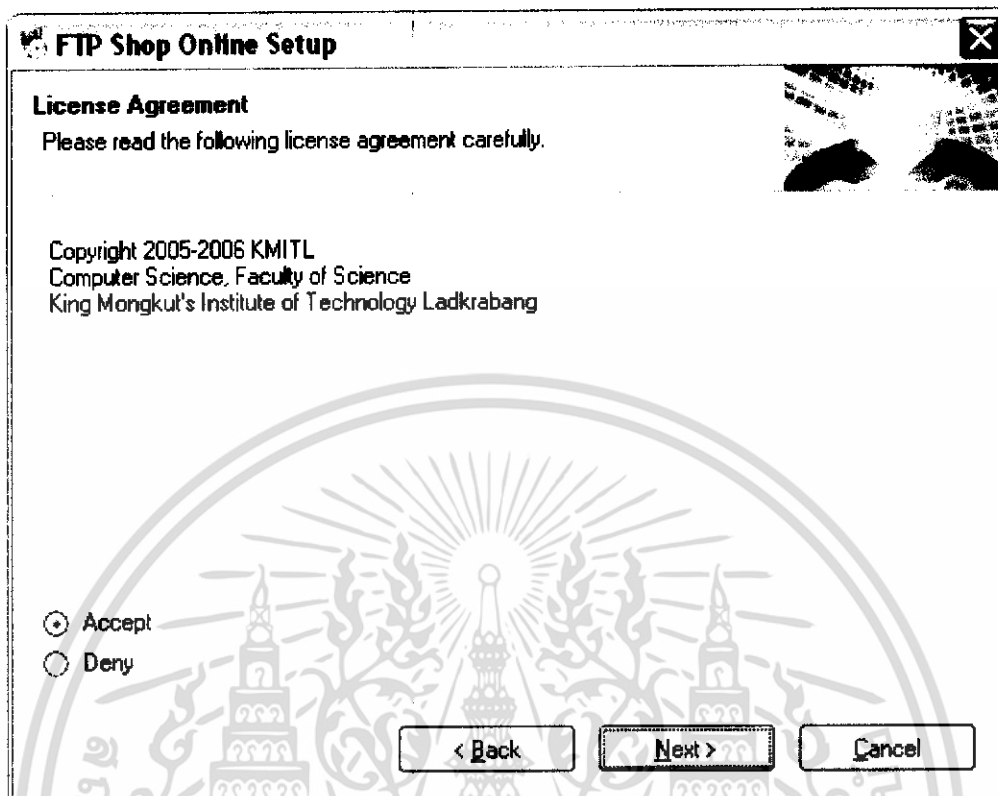
2. จะพบกับหน้าต่างต้อนรับ ให้กด Next เพื่อดำเนินการต่อ



รูปที่ ข-2 หน้าต่างต้อนรับ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3. จะปรากฏหน้าต่างลิขสิทธิ์ เลือกที่ Accept แล้วกด Next เพื่อดำเนินการต่อไป



รูปที่ ข-3 หน้าต่างลิขสิทธิ์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

#### 4. ใส่ชื่อผู้ใช้ และบริษัท จากนั้นกด Next เพื่อดำเนินการต่อไป

**FTP Shop Online Setup**

**User Information**  
Enter your user information and click Next to continue.

Name:  
Nakayoshi

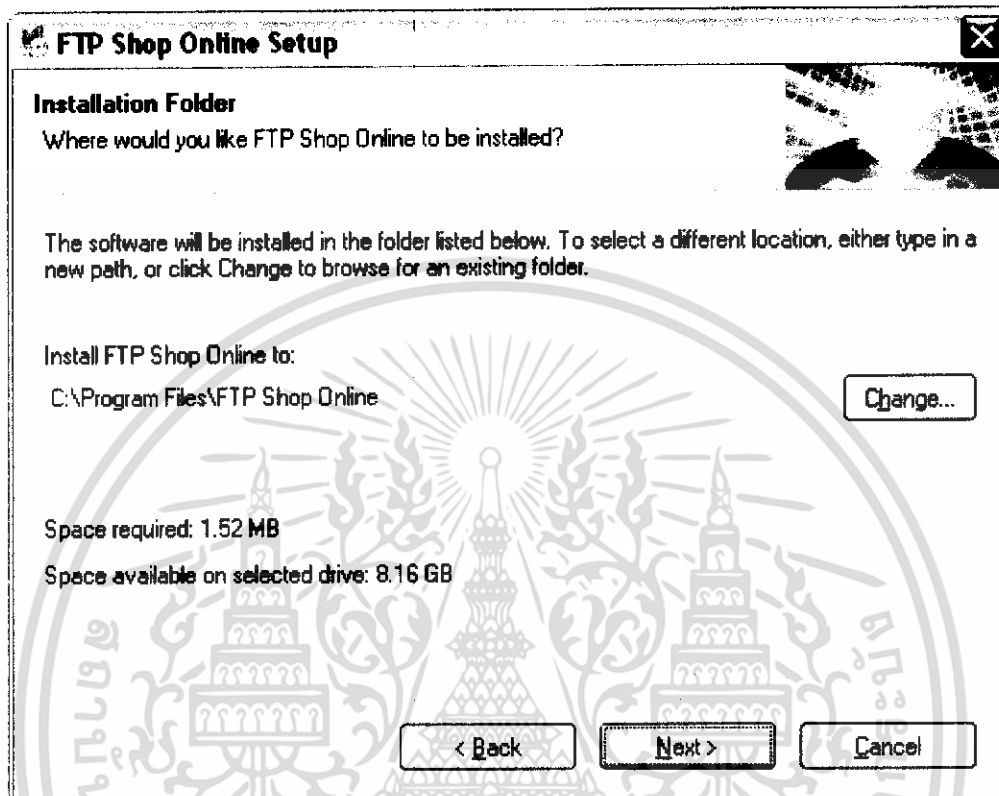
Company:

< Back    Next >    Cancel

รูปที่ ข-4 หน้าต่างระบุผู้ใช้งาน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

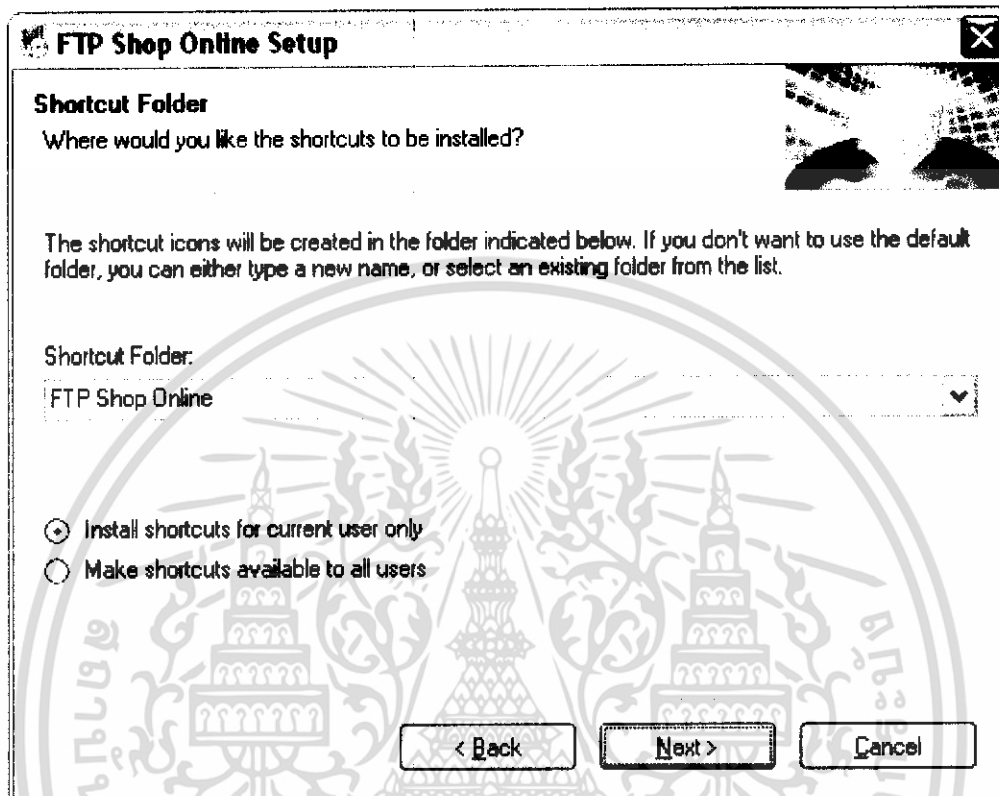
5. จะปรากฏหน้าต่าง แสดงโพลเดอร์มาตรฐานในการติดตั้งโปรแกรม พร้อมทั้ง พื้นที่ที่ต้องการในการลงโปรแกรม และพื้นที่คงเหลือ สามารถเปลี่ยนโพลเดอร์ที่ต้องการลงโปรแกรมได้โดยคลิกปุ่ม Change เพื่อเลือกโพลเดอร์ใหม่ กด Next เพื่อดำเนินการต่อไป



รูปที่ ข-5 หน้าต่างเลือกโพลเดอร์ในการติดตั้งโปรแกรม

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

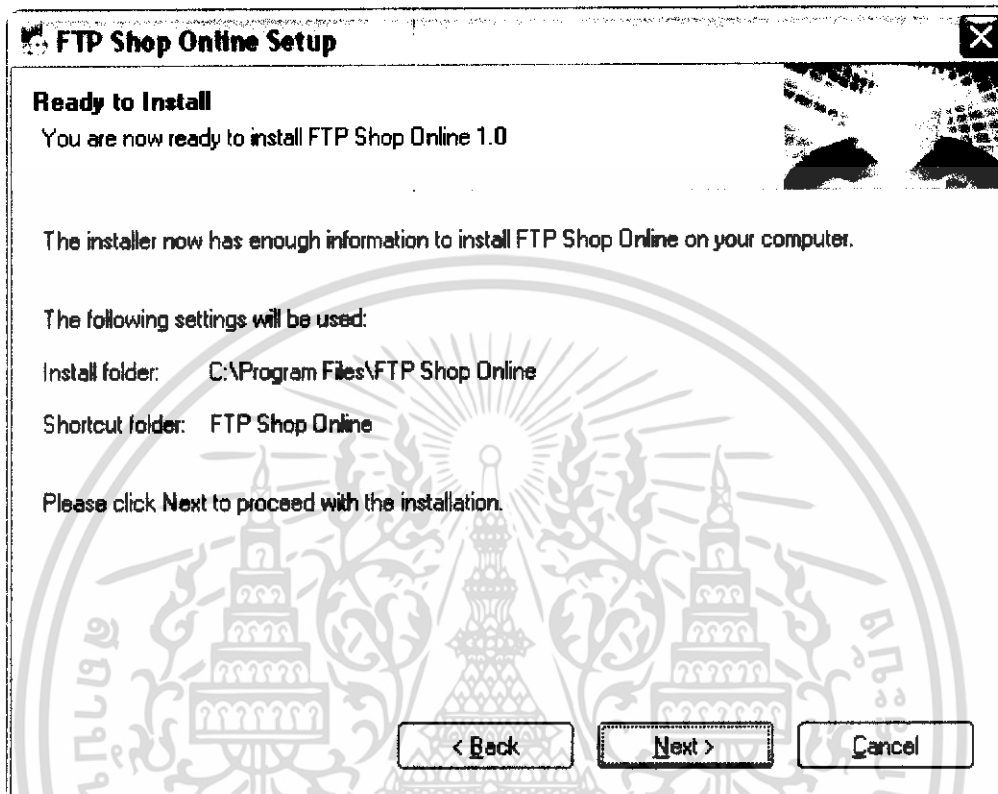
6. หน้าต่างบอกแจ้งโฟลเดอร์ที่ต้องการสร้างช็อตคัท ซึ่งผู้ใช้สามารถเลือกโฟลเดอร์ที่ต้องการได้ แล้วเลือกว่าจะให้โปรแกรมนี้ใช้ได้ทุกคนหรือว่าใช้ได้เพียงแค่มือใช้ที่ใช้อยู่ปัจจุบันเท่านั้น จากนั้นกดปุ่ม Next เพื่อดำเนินการต่อไป



รูปที่ ข-6 หน้าต่างแสดงโฟลเดอร์ที่ต้องการสร้างช็อตคัท

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

7. สุดท้ายจะเป็นการสรุปรายละเอียดต่างๆในการลงโปรแกรม ได้แก่โฟลเดอร์ที่ทำการลงโปรแกรม และ โฟลเดอร์ในการสร้างช็อตคัท เลือก Next เพื่อทำการติดตั้งโปรแกรม หรือ Back เพื่อย้อนกลับไปขั้นตอนก่อนหน้า



รูปที่ ข-7 หน้าต่างแสดงรายละเอียดการลงโปรแกรม

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

8. การติดตั้งเสร็จเรียบร้อยแล้ว กด Finish เพื่อเสร็จสิ้นการติดตั้ง โปรแกรม



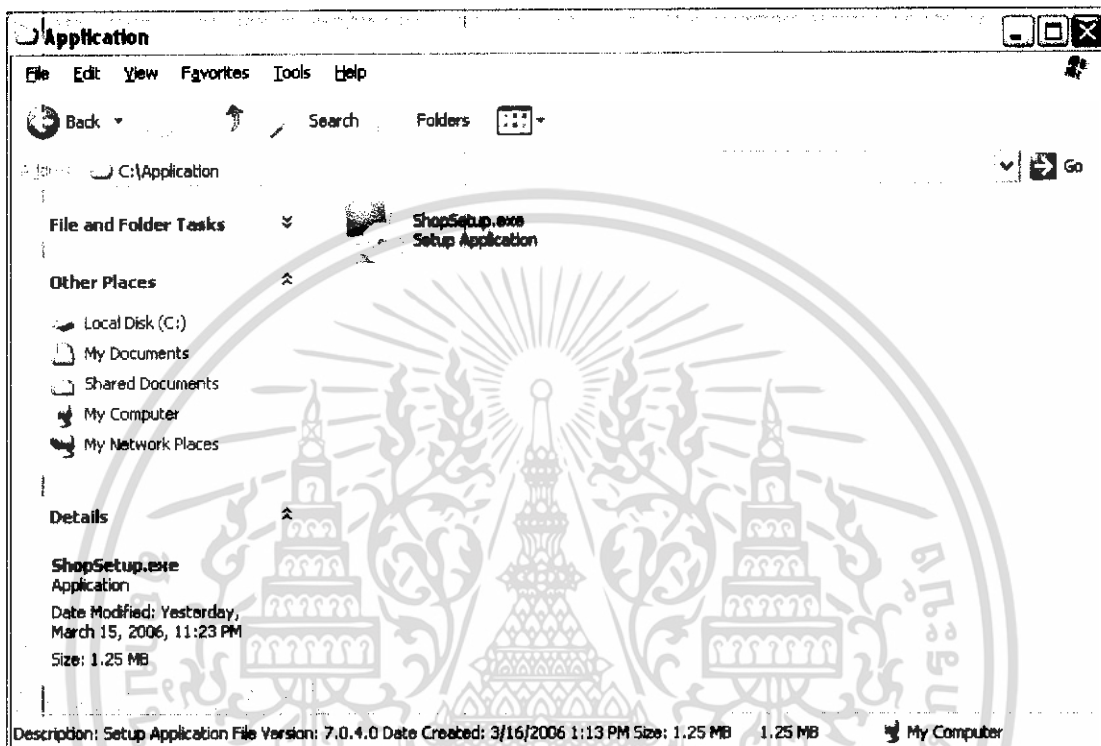
รูปที่ ข-8 หน้าต่างเสร็จสิ้นการลงโปรแกรม

9. ปรับไอพีแอดเดรสในไฟล์ที่อยู่ในโฟลเดอร์ C:\ipFolder

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## ขั้นตอนการติดตั้งโปรแกรมสำหรับร้านค้า

เปิดไฟล์ ShopSetup.exe เพื่อเริ่มทำการติดตั้งโปรแกรมส่วนร้านค้า สำหรับขั้นตอนการติดตั้งเช่นเดียวกับขั้นตอนการติดตั้งโปรแกรมสำหรับลูกค้า หลังจากติดตั้งสำเร็จ จะได้โปรแกรมส่วนแม่ข่ายร้านค้า และส่วนแสดงรายงานของร้านค้า

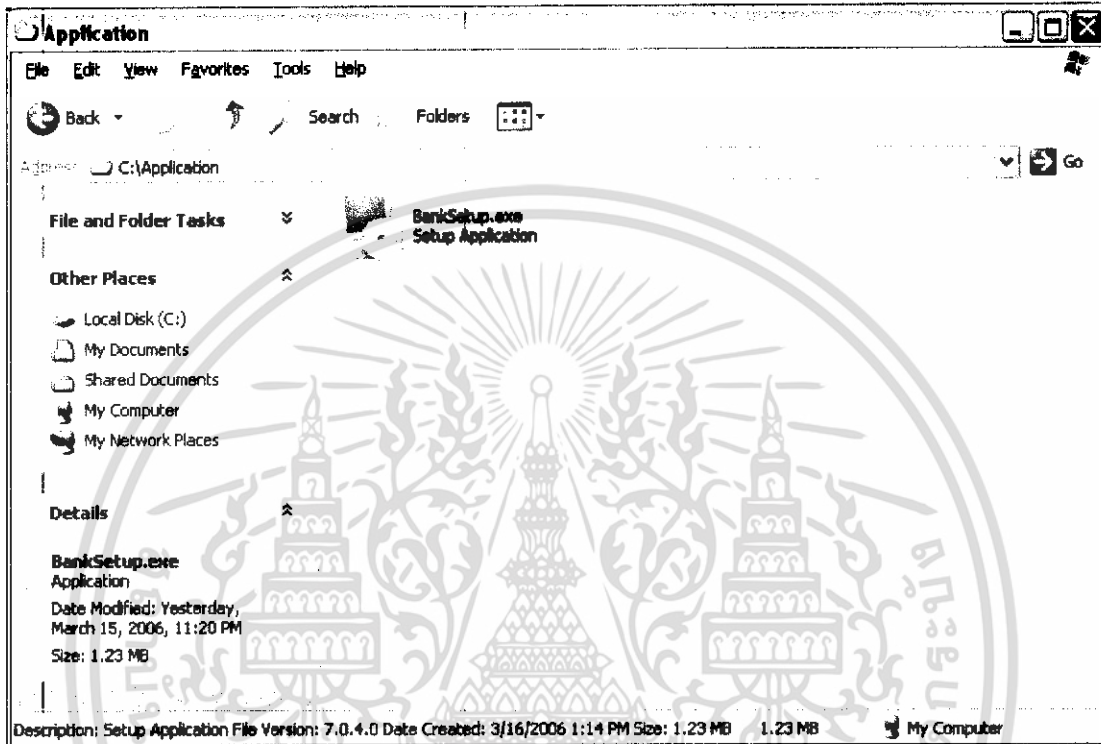


รูปที่ ข-9 ไฟล์ที่ใช้ในการติดตั้งโปรแกรมสำหรับร้านค้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## ขั้นตอนการติดตั้งโปรแกรมสำหรับธนาคาร

เปิดไฟล์ BankSetup.exe เพื่อเริ่มทำการติดตั้งโปรแกรมส่วนธนาคาร สำหรับขั้นตอนการติดตั้งเช่นเดียวกับขั้นตอนการติดตั้งโปรแกรมสำหรับลูกค้า หลังจากติดตั้งสำเร็จ จะได้โปรแกรมส่วนแม่ข่ายธนาคาร และส่วนแสดงรายงานของธนาคาร

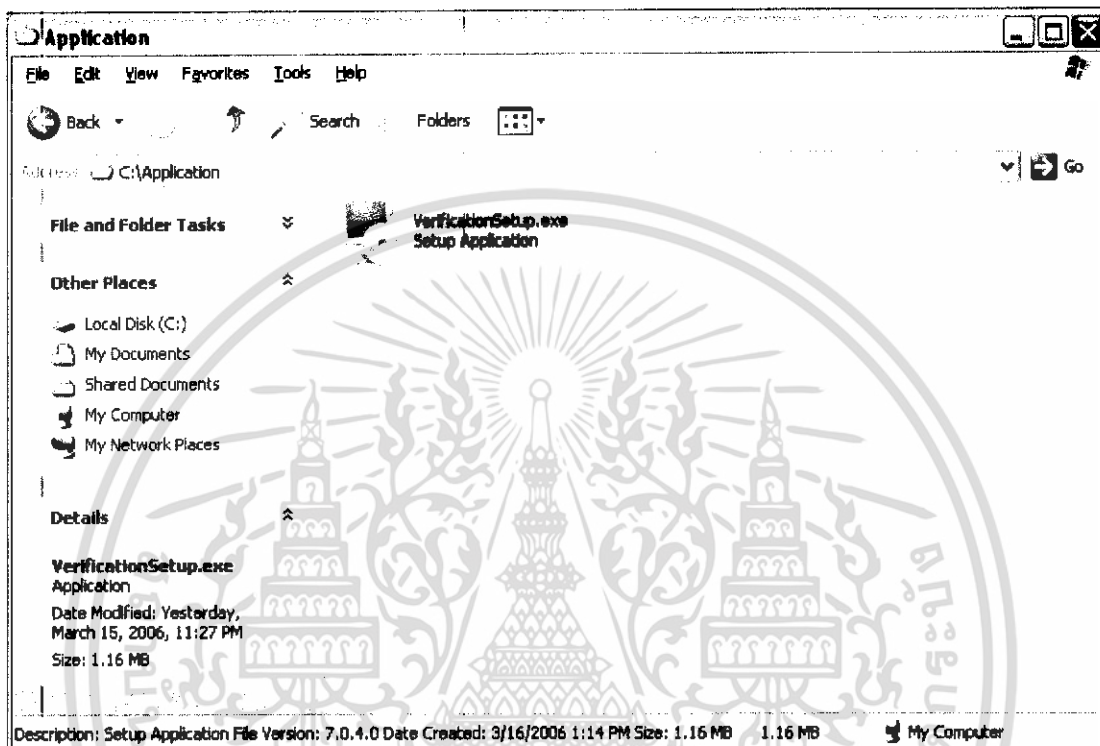


รูปที่ ข-10 ไฟล์ที่ใช้ในการติดตั้งโปรแกรมสำหรับธนาคาร

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## ขั้นตอนการติดตั้งโปรแกรมสำหรับบริษัทบัตรเครดิต

เปิดไฟล์ VerificationSetup.exe เพื่อเริ่มทำการติดตั้งโปรแกรมส่วนบริษัทบัตรเครดิต สำหรับขั้นตอนการติดตั้ง เช่นเดียวกับขั้นตอนการติดตั้งโปรแกรมสำหรับลูกค้า หลังจากติดตั้งสำเร็จ จะได้โปรแกรมส่วนแม่ข่ายของบริษัทบัตรเครดิต

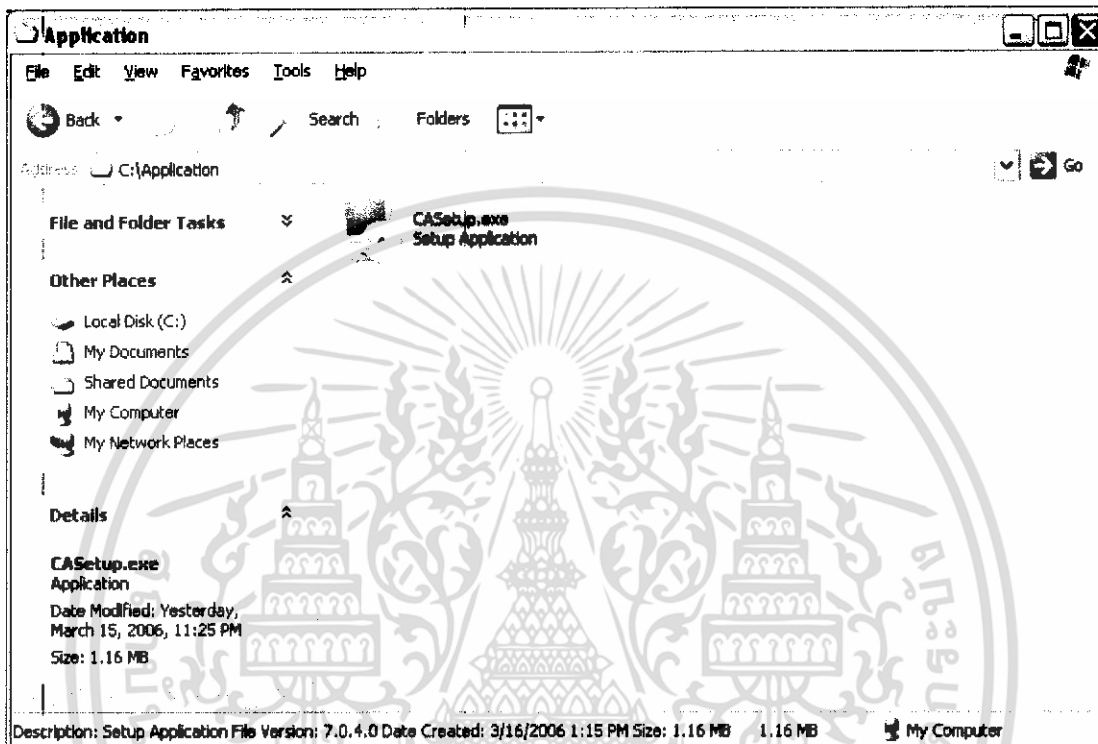


รูปที่ ข-11 ไฟล์ที่ใช้ในการติดตั้งโปรแกรมสำหรับบริษัทบัตรเครดิต

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## ขั้นตอนการติดตั้งโปรแกรมสำหรับองค์กรพิศุจน์สิทธิ์

เปิดไฟล์ CASetup.exe เพื่อเริ่มทำการติดตั้งโปรแกรมส่วนองค์กรพิศุจน์สิทธิ์ สำหรับขั้นตอนการติดตั้ง เช่นเดียวกับขั้นตอนการติดตั้งโปรแกรมสำหรับลูกค้า หลังจากติดตั้งสำเร็จ จะได้โปรแกรมส่วนแม่ข่ายขององค์กรพิศุจน์สิทธิ์



รูปที่ ข-12 ไฟล์ที่ใช้ในการติดตั้งโปรแกรมสำหรับองค์กรพิศุจน์สิทธิ์

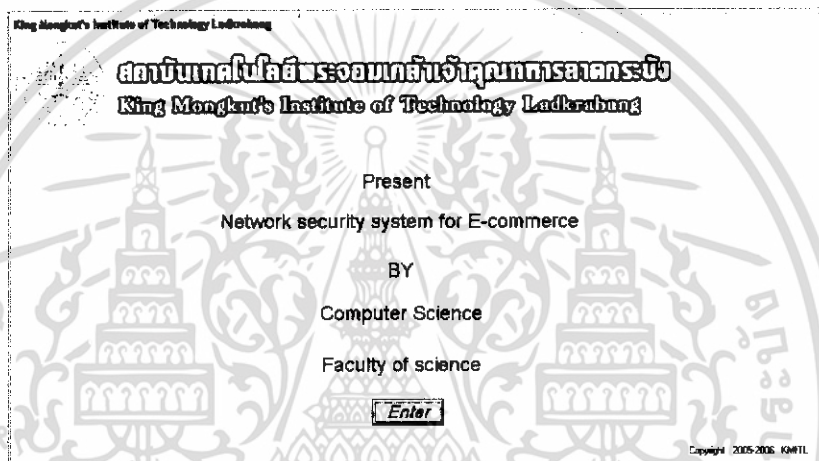
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ภาคผนวก ก  
การใช้งานโปรแกรม

การใช้งานโปรแกรมลูกค้า

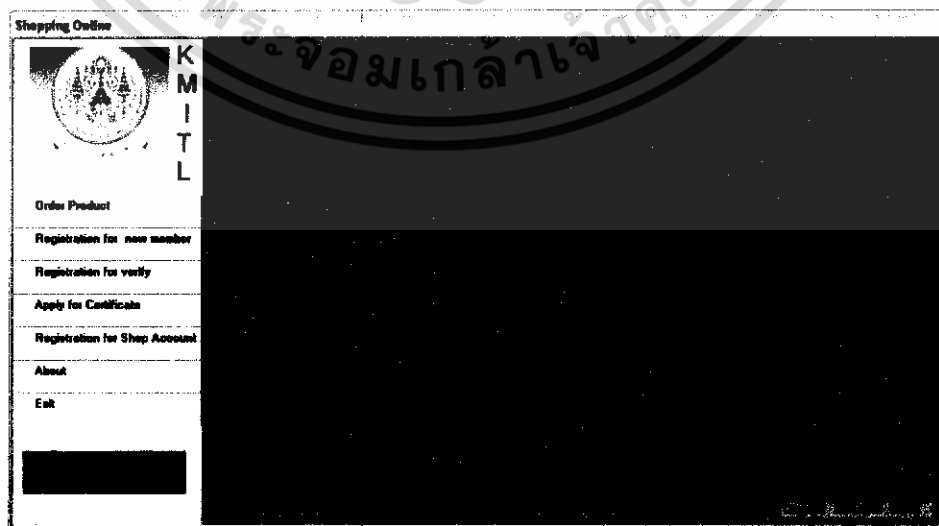
ก่อนใช้งาน โปรแกรมลูกค้า จะต้องทำการเปิดโปรแกรมแม่ข่ายทั้งหมดก่อน โดยจะต้องเปิดโปรแกรมแม่ข่ายธนาคาร,บริษัทบัตรเครดิต และองค์กรพิสูจน์สิทธิ์ก่อน แล้วจึงเปิดโปรแกรมแม่ข่ายร้านค้า จากนั้นจึงจะสามารถใช้งาน โปรแกรมส่วนของลูกค้าได้

1. เปิดโปรแกรมลูกค้า โปรแกรมจะแสดงหน้าจอเริ่มต้นดังนี้



รูปที่ ก-1 แสดงหน้าจอเริ่มต้นของโปรแกรมลูกค้า

2. เมื่อคลิกปุ่ม Enter จะเข้าสู่หน้าจอหลักในการทำงานของโปรแกรมซึ่งทางด้านซ้ายมือจะมีปุ่มต่างๆ ให้ลูกค้าเลือกใช้งานได้ตามต้องการ



รูปที่ ก-2 แสดงหน้าจอหลักในการทำงานของโปรแกรมลูกค้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น เมื่อผู้ผู้ใดเห็นไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3. เมื่อลูกค้ากดปุ่ม Order Product จะปรากฏหน้าจอให้ลูกค้าทำการเข้าสู่ระบบ(ล็อกอิน)ดังรูปที่ ค-3

รูปที่ ค-3 แสดงหน้าจอการล็อกอินทำการสั่งซื้อสินค้า

ถ้าการเข้าสู่ระบบ(ล็อกอิน)ผ่านก็จะปรากฏหน้าจอให้ลูกค้าสั่งซื้อสินค้าดังรูปที่ ค-4 ซึ่งจะแสดงส่วนของรายการสินค้าตามประเภทที่ลูกค้าเลือกด้านซ้ายมือ ส่วนของรายการสินค้าที่ลูกค้าทำการเลือกด้านขวามือ

รูปที่ ค-4 แสดงหน้าจอการสั่งซื้อสินค้า

เมื่อลูกค้าทำการเลือกประเภทสินค้าที่ combo box จะปรากฏรายการสินค้าตามประเภทที่เลือกนั้นๆ ดังรูปที่ ค-5

**Order\_Product**

Choose Type:

ID	Name	Price
0000001	.net Cryptography System	1800
0000002	AI In Game Programming	2700
0000003	Simulation	700
0000004	Principle Of Programming	500
0000005	Computer Networking	750

Add to cart

Name	QTY	SubTotal
<     >		

Total Price:

Buttons: Add to cart, Close, Remove, Buy

รูปที่ ค-5 แสดงหน้าจอการสั่งซื้อสินค้าเมื่อลูกค้าทำการเลือกประเภทของสินค้า

ในการเลือกสินค้าเพื่อที่จะซื้อทำได้โดยกดเลือกซื้อสินค้าที่รายการนั้นๆแล้วทำการกดปุ่ม Add to Cart แล้วจะปรากฏหน้าจอให้ใส่ปริมาณ ดังรูป ค-6

**Order\_Product**

Choose Type:

ID	Name	Price
0000001	.net Cryptography System	1800
0000002	AI In Game Programming	2700
0000003	Simulation	700
0000004	Principle Of Programming	500
0000005	Computer Networking	750

Quantity:

Enter Quantity

Buttons: Add to cart, Close, OK

รูปที่ ค-6 แสดงหน้าจอการสั่งซื้อสินค้าให้ใส่ปริมาณสินค้า

เมื่อกดปุ่ม OK ในหน้าจอการใส่ปริมาณข้อมูลสินค้าก็จะไปปรากฏที่หน้าจอด้านซ้ายดังรูป ค-7 ซึ่งเป็นรายการสินค้าที่เราเลือกทั้งหมด

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

**Order\_Product**

Choose Type:

ID	Name	Price
00000001	.net Cryptography System	1800
00000002	AI In Game Programming	2700
00000003	Simulation	700
00000004	Principle Of Programming	500
00000005	Computer Networking	750

Add to cart

Name	QTY	SubTotal
00000001	2	3600

Total Price: 3600

Buttons: Add to cart, Close, Remove, Buy

รูปที่ ค-7 แสดงหน้าจอการสั่งซื้อสินค้าเมื่อลูกค้าทำการเลือกซื้อรายการสินค้า

ลูกค้าสามารถทำการซื้อสินค้าได้มากกว่า 1 รายการดังรูป ค-8 และลูกค้าสามารถยกเลิกรายการที่เลือกไปแล้วโดยการเลือกรายการสินค้าที่เลือกด้านขวาแล้วทำการกดปุ่ม Remove โปรแกรมก็จะทำการนำรายการนั้นออกไป

**Order\_Product**

Choose Type:

ID	Name	Price
00000001	.net Cryptography System	1800
00000002	AI In Game Programming	2700
00000003	Simulation	700
00000004	Principle Of Programming	500
00000005	Computer Networking	750

Add to cart

Name	QTY	SubTotal
00000001	2	3600
00000002	3	8100

Total Price: 11700

Buttons: Add to cart, Close, Remove, Buy

รูปที่ ค-8 แสดงหน้าจอการสั่งซื้อสินค้าเมื่อลูกค้าทำการเลือกซื้อรายการสินค้า

เมื่อลูกค้าต้องการซื้อสินค้าที่เลือกก็ได้ทำการกดปุ่ม Buy ก็จะปรากฏหน้าจอการชำระเงินดังรูปที่ ค-9 ซึ่งจะมีให้เลือกการชำระเงินสามแบบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

**Payment**

Order ID

Total  Baht

Payment Method                      Payment Detail

Withdraw from Shop Account

VISA Card with Digital Certificate

VISA Card without Digital Certificate

**รูปที่ ค-9 แสดงหน้าจอการชำระเงิน**

แบบที่หนึ่งการชำระเงินแบบหักบัญชีที่ลูกค้าชำระไว้ล่วงหน้า ซึ่งลูกค้าสามารถเลือกชำระวิธีนี้ โดยเลือกที่ Withdraw from Shop Account ดังรูปที่ ค-10 ลูกค้าต้องกรอกรหัสผู้ใช้และรหัสผ่าน ที่ได้สมัครการชำระเงินแบบล่วงหน้าไว้ ซึ่งลูกค้าสามารถตรวจสอบยอดเงินคงเหลือได้โดยการ กดปุ่ม Check Balance จะแสดงยอดเงินคงเหลือปัจจุบัน

**Payment**

Order ID

Total  Baht

Payment Method                      Payment Detail

Withdraw from Shop Account                      User ID

VISA Card with Digital Certificate                      Password

VISA Card without Digital Certificate

**รูปที่ ค-10 แสดงการชำระเงินแบบลูกค้าทำการชำระเงินไว้ล่วงหน้า**

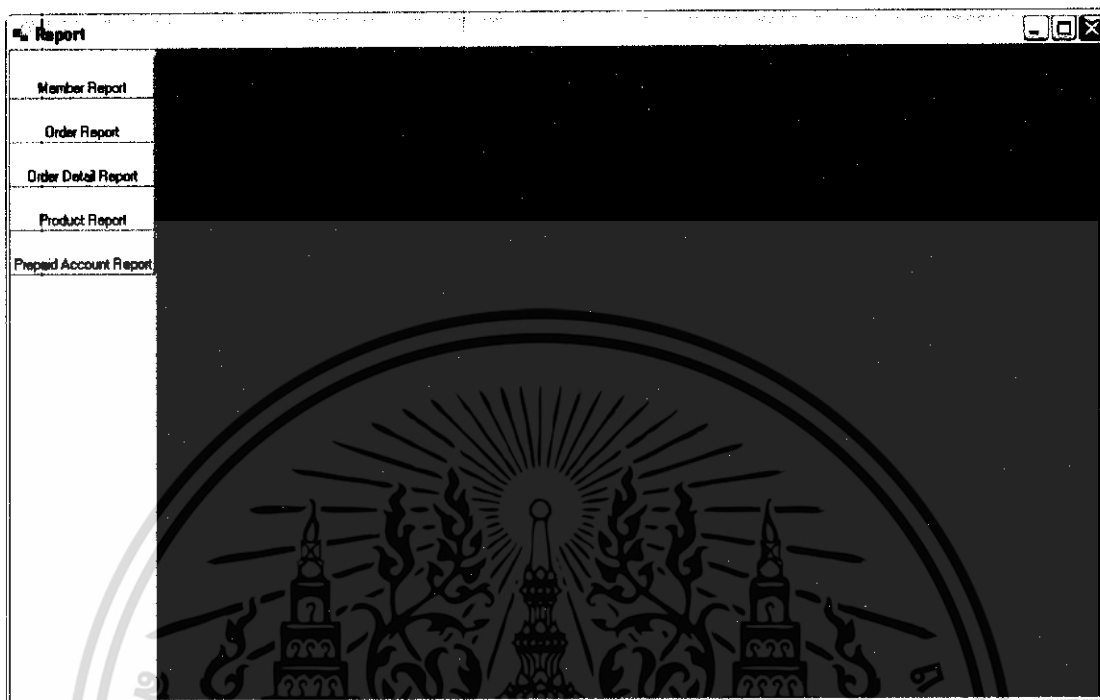
แบบที่สองการชำระเงินแบบที่ลูกค้ามีใบรับรองอิเล็กทรอนิกส์ ซึ่งลูกค้าสามารถเลือกชำระวิธีนี้ โดยเลือกที่ Visa Card with Digital Certificate ดังรูปที่ ค-11 โดยลูกค้ากรอกเพียงแต่รหัสบัตร เครดิต แล้วโปรแกรมจะทำการสร้างลายมือชื่อดิจิทัลเพื่อเป็นการพิสูจน์ตัวตนให้โดยอัตโนมัติ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



## การใช้งานโปรแกรม Shop Report

1. เปิดโปรแกรม Shop Report เมื่อโปรแกรมเริ่มต้นทำงานจะปรากฏหน้าต่างดังรูปที่ ค-13 ดังนี้



รูปที่ ค-13 แสดงหน้าจอหลักของโปรแกรม Shop Report

2. เลือกปุ่มทางซ้ายมือเพื่อดูหน้ารายงานตามที่ต้องการ
3. เมื่อกดปุ่มใดปุ่มหนึ่งแล้วตัวโปรแกรมจะขึ้นหน้าจอให้กรอกรหัสในการเข้าใช้ฐานข้อมูล ดังรูปที่ ค-14

รูปที่ ค-14 แสดงหน้าจอการใส่รหัสฐานข้อมูล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4. เมื่อป้อนข้อมูลรหัสผ่านแล้วรหัสผ่านนั้นถูกต้อง โปรแกรมจะทำการแสดงหน้าจอรายงานปรากฏออกมา ดังรูปที่ ค-15 เกิดจากการกดปุ่ม Member Report เพื่อดูรายงานรายละเอียดสมาชิก

Member Report	Date	20/3/2549	Member Report	FTP Shop Online
Member Report	Username	Name	Address	
Order Report	kei	Kea Siro	99, Sukhavit 11/1, BKK 10250	
Order Detail Report	Telephone	E-Mail		
Product Report	025847189	keai@hotmail.com		
Prepaid Account Report	Member Report	Username	Name	Address
		kuig	Kung Long	79/88, Sukhavit 11/1, BKK 10250
		Telephone	E-Mail	
		025567189	Kungo@hotmail.com	
	Member Report	Username	Name	Address
		paug	Saradol Paug	11/20, Sukhavit 11/1, Prakhong, Klongtoey, BKK 10250
		Telephone	E-Mail	
		023112467	paug@hotmail.com	
	Member Report	Username	Name	Address
		foi	Dangklam Orngpony	21/20, Sukhavit 11/1, Prakhong, Prakhong, BKK10110
		Telephone	E-Mail	
		02325467	foi@hotmail.com	

รูปที่ ค-15 แสดงหน้าจอรายงานรายละเอียดสมาชิก

5. กดปุ่ม Order Report เพื่อดูรายงานการสั่งซื้อ และป้อนข้อมูลรหัสผ่าน หากรหัสผ่านนั้นถูกต้อง จะแสดงหน้าจอ ดังรูปที่ ค-16

Member Report	Date	21/3/2549	Order Report	FTP Shop Online
Member Report	Date	Order No.	Username	Total Price
Order Report	01/15/06	00001	ik	2,500.00
Order Detail Report			Total Price for: 01/15/06	2,500.00
Product Report	01/19/06	00002	pk	5,000.00
Prepaid Account Report		00003	foi	10,000.00
			Total Price for: 01/19/06	15,000.00
	01/21/06	00004	ik	2,000.00
		00005	paug	34,000.00
		00006	foi	1,250.00
			Total Price for: 01/21/06	37,250.00
	01/25/06	00007	pk	3,500.00
		00008	paug	67,600.00
			Total Price for: 01/25/06	71,100.00
	01/27/06	00009	paug	500.00
			Total Price for: 01/27/06	500.00
	01/28/06	00010	paug	100.00
			Total Price for: 01/28/06	100.00
	01/29/06			

รูปที่ ค-16 แสดงหน้าจอรายงานของการสั่งซื้อ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่นิยมนำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้คัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

6. กดปุ่ม Order Detail Report เพื่อดูรายงานรายละเอียดการสั่งซื้อ และป้อนข้อมูลรหัสผ่าน หากกรหัสผ่านนั้นถูกต้อง จะแสดงหน้าจอ ดังรูปที่ ค-17

The screenshot shows the 'Order Detail Report' window. It displays a list of orders with columns for NO, USERNAME, and DATE. Below each order, there is a table of items with columns for Item Name, QTY, and Price. The total price for each order is also shown.

NO	USERNAME	DATE															
00001	nk	01-18-06															
<table border="1"> <thead> <tr> <th>Item Name</th> <th>QTY</th> <th>Price</th> </tr> </thead> <tbody> <tr> <td>net Cryptography System</td> <td>1.00</td> <td>1,800.00</td> </tr> <tr> <td>Penel Pencil</td> <td>1.00</td> <td>200.00</td> </tr> <tr> <td>Drink Pencil</td> <td>1.00</td> <td>200.00</td> </tr> <tr> <td><b>Total:</b></td> <td><b>3.00</b></td> <td><b>2,200.00</b></td> </tr> </tbody> </table>			Item Name	QTY	Price	net Cryptography System	1.00	1,800.00	Penel Pencil	1.00	200.00	Drink Pencil	1.00	200.00	<b>Total:</b>	<b>3.00</b>	<b>2,200.00</b>
Item Name	QTY	Price															
net Cryptography System	1.00	1,800.00															
Penel Pencil	1.00	200.00															
Drink Pencil	1.00	200.00															
<b>Total:</b>	<b>3.00</b>	<b>2,200.00</b>															
00002	pk	01-19-06															
<table border="1"> <thead> <tr> <th>Item Name</th> <th>QTY</th> <th>Price</th> </tr> </thead> <tbody> <tr> <td>AI In Game Programming</td> <td>1.00</td> <td>2,700.00</td> </tr> <tr> <td>Packer Pen</td> <td>1.00</td> <td>5,000.00</td> </tr> <tr> <td><b>Total:</b></td> <td><b>2.00</b></td> <td><b>5,700.00</b></td> </tr> </tbody> </table>			Item Name	QTY	Price	AI In Game Programming	1.00	2,700.00	Packer Pen	1.00	5,000.00	<b>Total:</b>	<b>2.00</b>	<b>5,700.00</b>			
Item Name	QTY	Price															
AI In Game Programming	1.00	2,700.00															
Packer Pen	1.00	5,000.00															
<b>Total:</b>	<b>2.00</b>	<b>5,700.00</b>															
00003	ks	01-19-06															
<table border="1"> <thead> <tr> <th>Item Name</th> <th>QTY</th> <th>Price</th> </tr> </thead> <tbody> <tr> <td>Mont Blanc Pen</td> <td>1.00</td> <td>10,000.00</td> </tr> <tr> <td><b>Total:</b></td> <td><b>1.00</b></td> <td><b>10,000.00</b></td> </tr> </tbody> </table>			Item Name	QTY	Price	Mont Blanc Pen	1.00	10,000.00	<b>Total:</b>	<b>1.00</b>	<b>10,000.00</b>						
Item Name	QTY	Price															
Mont Blanc Pen	1.00	10,000.00															
<b>Total:</b>	<b>1.00</b>	<b>10,000.00</b>															
00005	nan	01-21-06															

รูปที่ ค-17 แสดงหน้าจอรายงานรายละเอียดการสั่งซื้อ

7. กดปุ่ม Product Report เพื่อดูรายงานรายละเอียดสินค้า และป้อนข้อมูลรหัสผ่าน หากกรหัสผ่านนั้นถูกต้อง จะแสดงหน้าจอ ดังรูปที่ ค-18

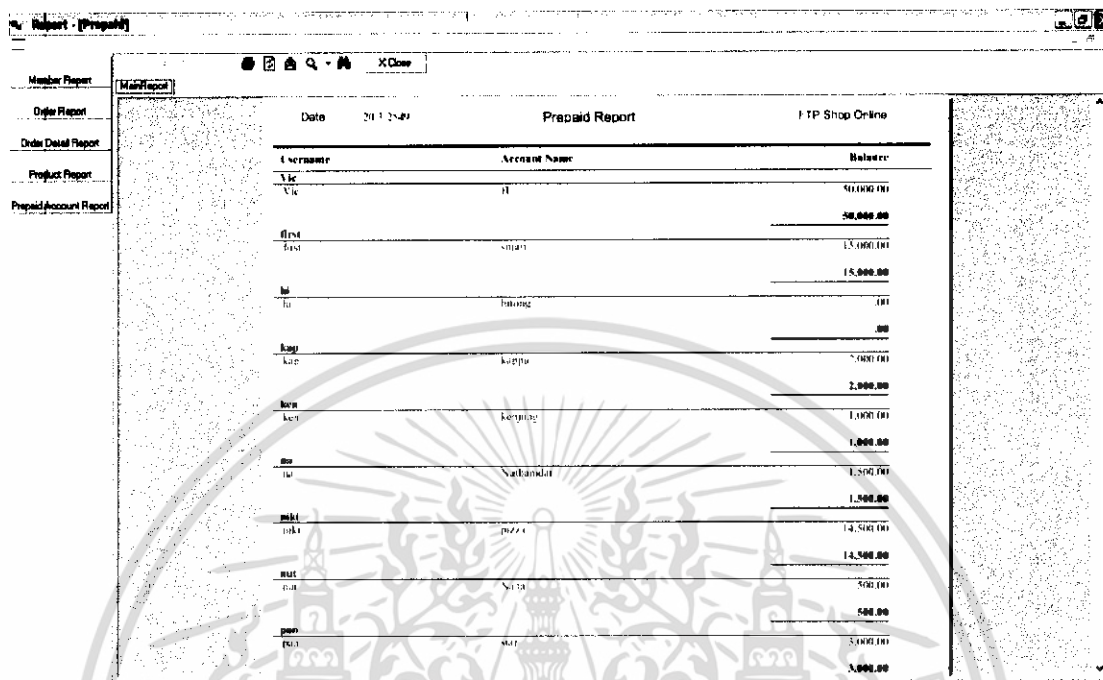
The screenshot shows the 'Product Report' window. It displays a list of products with columns for ID, IP, Name, Price, and QTY. The products are grouped into categories: Book, Electronic Equipment, and Stationery.

ID	IP	Name	Price	QTY
<b>Book</b>				
00000001		net Cryptography System	1,800.00	5.00
00000002		AI In Game Programming	2,700.00	7.00
00000003		Simulation	300.00	30.00
00000004		Principle Of Programming	500.00	20.00
00000005		Computer Networking	750.00	30.00
<b>Electronic Equipment</b>				
00000006		Hammer	1,000.00	5.00
00000007		Use All Condition	30,000.00	10.00
00000008		Washing Air Condition	25,000.00	5.00
00000009		Simon Washing Machine	50,000.00	10.00
<b>Stationery</b>				
00000010		Packer Pen	5,000.00	4.00
00000011		Rolling Pen	300.00	20.00
00000012		Mont Blanc Pen	10,000.00	2.00
00000013		Penel Pencil	500.00	30.00
00000014		Rolling Pencil	100.00	25.00
00000015		Drink Pencil	200.00	17.00

รูปที่ ค-18 แสดงหน้าจอรายงานรายละเอียดสินค้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับใช้ประกอบการเรียนการสอนเท่านั้น เมื่ออนุญาตให้ท่านไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

8. กดปุ่ม Prepaid Account เพื่อดูรายงานบัญชีที่ถูกค้างชำระล่วงหน้า และป้อนข้อมูลรหัสผ่าน หากกรหัสผ่านนั้นถูกต้อง จะแสดงหน้าจอจดังรูปที่ ค-19



The screenshot shows a web application window titled "Report - (Prepaid)". The main content is a "Prepaid Report" for "FTP Shop Online" dated "2012-01-24". The report lists various accounts with their names and current balances. The total balance is 3,000.00.

Account Name	Balance
vic	40,000.00
<b>vic</b>	<b>50,000.00</b>
first	15,000.00
fast	15,000.00
hi	0.00
tu	0.00
kap	2,000.00
kap	2,000.00
ken	1,000.00
ken	1,000.00
ku	1,500.00
ku	1,500.00
mkt	14,500.00
mtk	14,500.00
nut	500.00
nut	500.00
pen	500.00
pen	500.00
<b>Total</b>	<b>3,000.00</b>

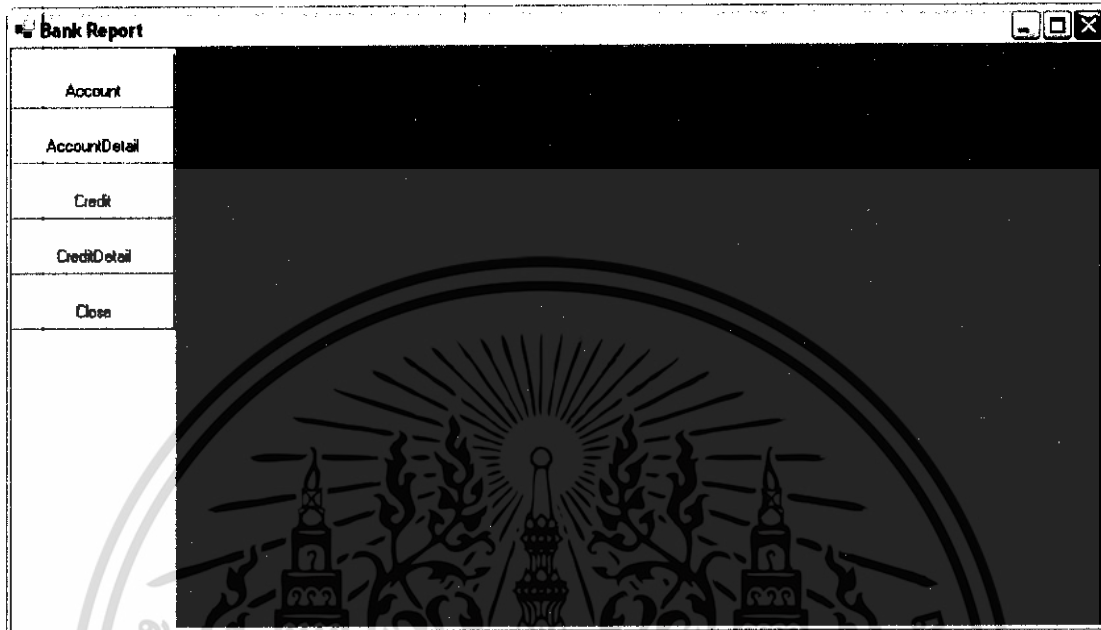
รูปที่ ค-19 แสดงหน้าจอรายงานบัญชีที่ถูกค้างชำระล่วงหน้า

9. เมื่อต้องการปิดหน้าจอรายงานกดปุ่ม X Close

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## การใช้งานโปรแกรม Bank Report

1. เปิดโปรแกรม Bank Report เมื่อโปรแกรมเริ่มต้นทำงานจะปรากฏหน้าจอหลักดังรูปที่ ค-20 ดังนี้



รูปที่ ค-20 แสดงหน้าจอหลักของโปรแกรม Bank Report

2. ปุ่มทางซ้ายมือเพื่อดูหน้ารายงานตามที่ต้องการ
3. เมื่อกดปุ่มใดปุ่มหนึ่งแล้วตัวโปรแกรมจะขึ้นหน้าจอให้กรอกรหัสในการเข้าใช้ฐานข้อมูล ดังรูปที่ ค-21

รูปที่ ค-21 หน้าจอการใส่รหัสฐานข้อมูล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4. เมื่อป้อนข้อมูลรหัสผ่านแล้วรหัสผ่านนั้นถูกต้อง โปรแกรมจะทำการแสดงหน้าจอรายงานปรากฏออกมาดังรูปที่ ค-22 เกิดจากการกดปุ่ม Account เพื่อดูรายงานบัญชีของลูกค้า

Account	MainReport
AccountDetail	Print Date 21/3/2549 <b>Account Report</b> <b>FTP Bank</b>
Credit	
CreditDetail	<u>ACCDUNING</u> <u>NAML</u> <u>BALANCE</u>
Close	1006005365 FTP Shop 1,500,000.00
	1007052418 Narumol 1,150,000.00
	1004568910 Sutthima 1,058,900.00
	1007995641 Beautiful Shop 850,000.00
	1078524478 Mintra 910,000.00
	1005860415 Electronic Shop 500,000.00
	1048485309 Duangkamol 20,000.00
	Current Page No: 1 Total Page No: 1 Zoom Factor: 100%

รูปที่ ค-22 แสดงหน้าจอรายงานบัญชีของลูกค้า

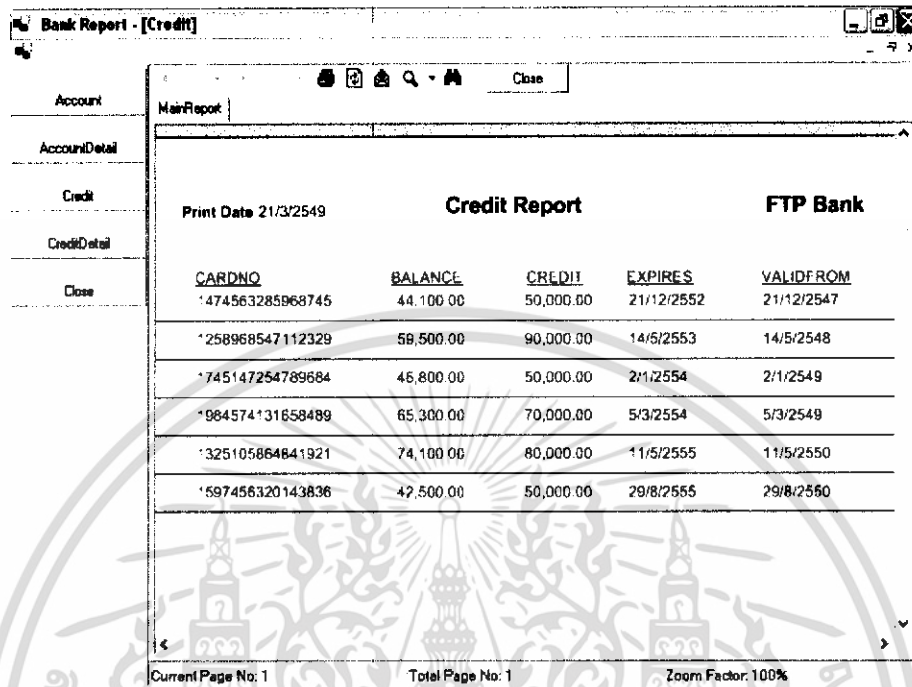
5. กดปุ่ม Account Detail เพื่อดูรายงานรายละเอียดบัญชีของลูกค้า และป้อนข้อมูลรหัสผ่าน หากรหัสผ่านนั้นถูกต้อง จะแสดงหน้าจอดังรูปที่ ค-23

Account	MainReport
AccountDetail	Print Date 21/3/2549 <b>Account Detail Report</b> <b>FTP Bank</b>
Credit	
CreditDetail	<u>NO</u> <u>NAML</u> <u>DETAILNAME</u> <u>AMOUNT</u>
Close	000000009 FTP Shop Deposit 7,500.00
	000000008 FTP Shop Deposit 3,600.00
	000000007 FTP Shop Deposit 2,300.00
	000000005 FTP Shop Deposit 4,700.00
	000000004 FTP Shop Deposit 3,200.00
	000000003 FTP Shop Deposit 30,500.00
	000000001 FTP Shop Deposit 5,800.00
	000000002 FTP Shop Deposit 2,500.00
	Current Page No: 1 Total Page No: 1 Zoom Factor: 100%

รูปที่ ค-23 แสดงหน้าจอรายงานรายละเอียดบัญชีของลูกค้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

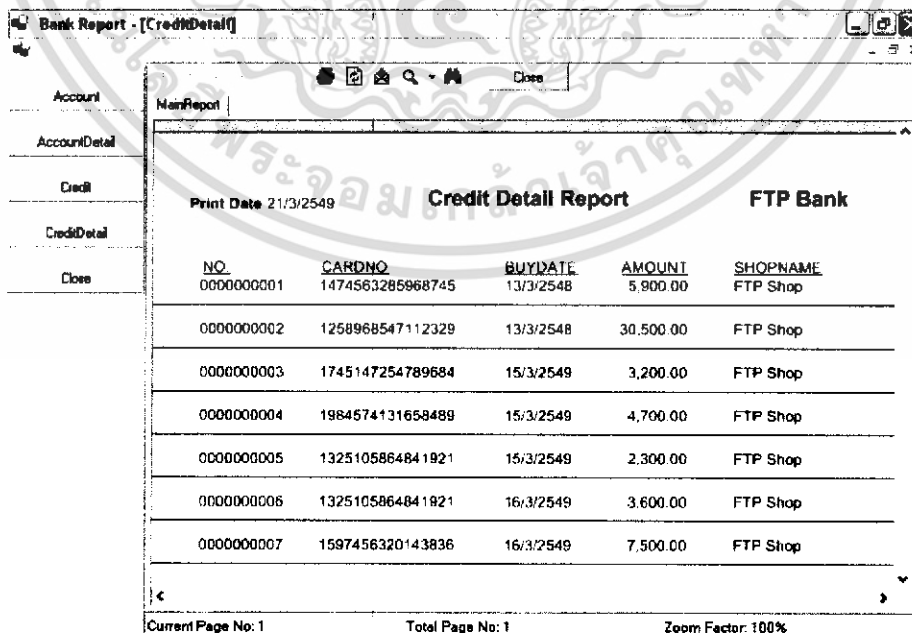
6. กดปุ่ม Credit เพื่อดูรายงานบัตรเครดิต และป้อนข้อมูลรหัสผ่าน หากกรหัสผ่านนั้นถูกต้อง จะแสดงหน้าจอดังรูปที่ ก-24



CARDNO	BALANCE	CREDIT	EXPIRES	VALIDFROM
1474563285968745	44,100.00	50,000.00	21/12/2552	21/12/2547
1258968547112329	59,500.00	90,000.00	14/5/2553	14/5/2548
1745147254789684	46,800.00	50,000.00	21/12/2554	21/12/2549
1984574131658489	65,300.00	70,000.00	5/3/2554	5/3/2549
1325105864841921	74,100.00	80,000.00	11/5/2555	11/5/2550
1597456320143836	42,500.00	50,000.00	29/8/2555	29/8/2550

รูปที่ ก-24 แสดงหน้าจอรายงานบัตรเครดิต

7. กดปุ่ม Credit Detail เพื่อดูรายงานรายละเอียดการใช้บัตรเครดิต และป้อนข้อมูลรหัสผ่าน หากกรหัสผ่านนั้นถูกต้อง จะแสดงหน้าจอดังรูปที่ ก-25



NO	CARDNO	BUYDATE	AMOUNT	SHOPNAME
0000000001	1474563285968745	13/3/2548	5,900.00	FTP Shop
0000000002	1258968547112329	13/3/2548	30,500.00	FTP Shop
0000000003	1745147254789684	15/3/2549	3,200.00	FTP Shop
0000000004	1984574131658489	15/3/2549	4,700.00	FTP Shop
0000000005	1325105864841921	15/3/2549	2,300.00	FTP Shop
0000000006	1325105864841921	16/3/2549	3,600.00	FTP Shop
0000000007	1597456320143836	16/3/2549	7,500.00	FTP Shop

รูปที่ ก-25 แสดงหน้าจอรายงานรายละเอียดการใช้บัตรเครดิต

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

8. เมื่อต้องการปิดหน้าจอรายงานกลุ่ม Close
9. เมื่อต้องการจบโปรแกรมกลุ่ม Close ทางด้านซ้ายมือ



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ภาคผนวก ง  
ตัวอย่างรายงาน

**รายงานของร้านค้า**

การแสดงผลงานของร้านค้า ประกอบด้วย 5 ส่วน ดังนี้

1. รายงานสมาชิกของร้านค้า (Member Report)
2. รายงานการสั่งซื้อของลูกค้า (Order Report)
3. รายงานรายละเอียดการสั่งซื้อสินค้า (Order Detail Report)
4. รายงานรายละเอียดสินค้า (Product Report)
5. รายงานบัญชีที่ลูกค้าชำระล่วงหน้า (Prepaid Account Report)

**1. รายงานสมาชิกของร้านค้า (Member Report)**

ประกอบด้วยชื่อที่ใช้ในการเข้าสู่ระบบ ชื่อ ที่อยู่ เบอร์โทรศัพท์ และอีเมลล์

Date	Member Report		FTP Shop Online
<b>Username</b>	<b>Name</b>	<b>Address</b>	
ken	Ken Shin	99 , Sukhumvit Plus,BKK 10250	
<b>Telephone</b>	<b>E-Mail</b>		
025647389	ken@hotmail.com		
<b>Username</b>	<b>Name</b>	<b>Address</b>	
kung	Kung Lung	77/88 , Sukhumvit 22 Rd. ,BKK 10250	
<b>Telephone</b>	<b>E-Mail</b>		
023567389	kung@hotmail.com		
<b>Username</b>	<b>Name</b>	<b>Address</b>	
pung	Narimol Pang	11/56 ,Sukhumvit 50 Rd. ,Prakhanong,Klongtoey,BKK 10250	
<b>Telephone</b>	<b>E-Mail</b>		
023115467	pung@hotmail.com		
<b>Username</b>	<b>Name</b>	<b>Address</b>	
first	Duangkamol Orapinpong	21/76 ,Sukhumvit 71 Rd. ,Prakhanong. Prakhanong,BKK10110	
<b>Telephone</b>	<b>E-Mail</b>		
023225467	first@hotmail.com		
<b>Username</b>	<b>Name</b>	<b>Address</b>	
fon	Saitham Surachawala	21/76 ,Asok-Dindang Rd. , Dindang, Dindang,BKK 10110	
<b>Telephone</b>	<b>E-Mail</b>		
023945678	fon@hotmail.com		
<b>Username</b>	<b>Name</b>	<b>Address</b>	
jib	Warairak Wa	319/51 ,Rama-1 Rd. ,Klongtoey. Klongtoey,BKK 10250	
<b>Telephone</b>	<b>E-Mail</b>		
022345678	jib@hotmail.com		
1			

รูปที่ ง-1 หน้าจอแสดงรายงานสมาชิก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## 2. รายงานการสั่งซื้อของถูกค้า (Order Report)

แสดงวันที่สั่งซื้อ เลขที่ใบสั่งซื้อ ชื่อผู้สั่งซื้อ และราคารวม โดยแบ่งตามวันที่ลูกค้าสั่งซื้อเข้ามา

Date	21/3/2549	Order Report	FTP Shop Online
Date	Order No.	Username	Total Price
01/15/06	00001	tik	2,500.00
Total Price for : 01/15/06			2,500.00
01/19/06	00002	pik	5,700.00
	00003	first	10,000.00
Total Price for : 01/19/06			15,700.00
01/21/06	00004	tik	2,000.00
	00005	pung	30,000.00
	00006	fon	1,250.00
Total Price for : 01/21/06			33,250.00
01/25/06	00007	jib	4,500.00
	00008	pung	67,600.00
Total Price for : 01/25/06			72,100.00
01/27/06	00009	pung	500.00
Total Price for : 01/27/06			500.00
01/28/06	00010	pen	100.00
Total Price for : 01/28/06			100.00
01/29/06	00011	jerry	200.00
Total Price for : 01/29/06			200.00
<b>Grand Total:</b>			<b>124,350.00</b>

รูปที่ ง-2 หน้าจอแสดงรายงานการสั่งซื้อของถูกค้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

### 3. รายงานรายละเอียดการสั่งซื้อสินค้า (Order Detail Report)

แสดงเลขที่ใบสั่งซื้อ ชื่อผู้สั่งซื้อ วันที่สั่งซื้อ และรายการการสั่งซื้อ ซึ่งประกอบด้วย สินค้า จำนวนที่สั่ง และและราคารวม และสรุปเป็นจำนวนและราคารวมสำหรับใบสั่งซื้อแต่ละใบ

Date	21/3/2549	Order Detail Report	FTP Shop Online
<b>NO</b>	<b>USERNAME</b>	<b>DATE</b>	
00001	tik	01/15/06	
	<b>Item Name</b>	<b>QTY</b>	<b>Price</b>
	.net Cryptography System	1.00	1,800.00
	Pentel Pencil	1.00	500.00
	Think Pencil	1.00	200.00
	<b>Total:</b>	<b>3.00</b>	<b>2,500.00</b>
<b>NO</b>	<b>USERNAME</b>	<b>DATE</b>	
00002	pik	01/19/06	
	<b>Item Name</b>	<b>QTY</b>	<b>Price</b>
	AI In Game Programming	1.00	2,700.00
	Parker Pen	1.00	3,000.00
	<b>Total:</b>	<b>2.00</b>	<b>5,700.00</b>
<b>NO</b>	<b>USERNAME</b>	<b>DATE</b>	
00003	first	01/19/06	
	<b>Item Name</b>	<b>QTY</b>	<b>Price</b>
	Mont Blanc Pen	1.00	10,000.00
	<b>Total:</b>	<b>1.00</b>	<b>10,000.00</b>
<b>NO</b>	<b>USERNAME</b>	<b>DATE</b>	
00005	pung	01/21/06	
	<b>Item Name</b>	<b>QTY</b>	<b>Price</b>
	LG Air Condition	1.00	30,000.00
	<b>Total:</b>	<b>1.00</b>	<b>30,000.00</b>
<b>NO</b>	<b>USERNAME</b>	<b>DATE</b>	
00006	fon	01/21/06	
	<b>Item Name</b>	<b>QTY</b>	<b>Price</b>
	Principle Of Programming	1.00	500.00
	Computer Networking	1.00	750.00
	Parker Pen	2.00	2,000.00
	<b>Total:</b>	<b>4.00</b>	<b>3,250.00</b>
<b>NO</b>	<b>USERNAME</b>	<b>DATE</b>	
00007	jjb	01/25/06	

รูปที่ ง-3 หน้าจอแสดงรายงานรายละเอียดการสั่งซื้อสินค้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

#### 4. รายงานรายละเอียดสินค้า (Product Report)

แสดงรายการสินค้า ซึ่งประกอบด้วย เลขที่สินค้า ชื่อสินค้า ราคาสินค้าต่อหนึ่งหน่วย และจำนวนคงเหลือ โดยแบ่งตามประเภทของสินค้า

Date		Item Report		FTP Shop Online	
Type	ID	Name	Price	QTY	
<b>Book</b>					
	00000001	net Cryptography System	1,800.00	5.00	
	00000002	AI In Game Programming	2,700.00	7.00	
	00000003	Simulation	700.00	10.00	
	00000004	Principle Of Programming	500.00	20.00	
	00000005	Computer Networking	750.00	30.00	
<b>Electronic Equipment</b>					
	00000006	Hatari Fan	1,000.00	5.00	
	00000007	LG Air Condition	30,000.00	10.00	
	00000008	Samsung Air Condition	25,000.00	5.00	
	00000009	Simen Washing Machine	39,000.00	3.00	
<b>Stationary</b>					
	00000010	Parker Pen	3,000.00	4.00	
	00000011	Rotring Pett	300.00	20.00	
	00000012	Mont Blanc Pen	10,000.00	2.00	
	00000013	Pentel Pencil	500.00	30.00	
	00000014	Rotring Pencil	100.00	15.00	
	00000015	Think Pencil	200.00	17.00	

รูปที่ ๔-4 หน้าจอแสดงรายงานรายละเอียดสินค้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

### 5. รายงานบัญชีที่ถูกชำระล่วงหน้า (Prepaid Account Report)

ประกอบด้วยชื่อผู้ใช้ ชื่อบัญชี และยอดเงินคงเหลือ โดยแบ่งตามชื่อผู้ใช้ และมีการสรุปยอดเงินคงเหลือรวมสำหรับผู้ใช้แต่ละคน

Date	20/3/2549	Prepaid Report	FTP Shop Online
Username	Account Name	Balance	
Vic	fi	50,000.00	
		<u>50,000.00</u>	
first	smart	15,000.00	
		<u>15,000.00</u>	
hi	hitong	.00	
		<u>.00</u>	
kap	kappu	2,000.00	
		<u>2,000.00</u>	
ken	kenjung	1,000.00	
		<u>1,000.00</u>	
na	Nuthamdai	1,500.00	
		<u>1,500.00</u>	
niki	pizza	14,500.00	
		<u>14,500.00</u>	
nur	Nana	500.00	
		<u>500.00</u>	
pan	star	3,000.00	
		<u>3,000.00</u>	
pik	beautiful	7,000.00	
		<u>7,000.00</u>	
tik	tikky	3,000.00	
		<u>3,000.00</u>	
tim	Nrim	3,000.00	
		<u>3,000.00</u>	
tom	tommy	2,000.00	
		<u>2,000.00</u>	
win	winning	1,000.00	
		<u>1,000.00</u>	
		<u>103,500.00</u>	

รูปที่ ง-5 หน้าจอแสดงรายงานบัญชีที่ถูกชำระล่วงหน้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## รายงานของธนาคาร

การแสดงผลงานของธนาคาร ประกอบด้วย 4 ส่วน ดังนี้

1. รายงานบัญชีของลูกค้า (Account Report)
2. รายงานรายละเอียดบัญชีของลูกค้า (Account Detail Report)
3. รายงานบัตรเครดิต (Credit Report)
4. รายงานรายละเอียดบัตรเครดิต (Credit Detail Report)

### 1. รายงานบัญชีของลูกค้า (Account Report)

ประกอบด้วยหมายเลขบัญชี ชื่อลูกค้า และยอดเงินคงเหลือ

Print Date 21/3/2549		Account Report	FTP Bank
ACCOUNTNO	NAME		BALANCE
1008005365	FTP Shop		1,500,000.00
1007052418	Narumol		1,150,000.00
1004568910	Suthima		1,058,900.00
1087995641	Beautiful Shop		850,000.00
1078524478	Mintra		910,000.00
1005860415	Electronic Shop		500,000.00
1048485309	Duangkamol		20,000.00
1009753612	Computer Shop		480,000.00
1039807136	Sriwapan		139,000.00
1002549738	Suchada		580,000.00

รูปที่ ง-6 หน้าจอแสดงผลงานบัญชีของลูกค้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## 2. แสดงรายงานรายละเอียดบัญชีของลูกค้า (Account Detail Report)

ประกอบด้วยหมายเลขรายการ ชื่อลูกค้า รายละเอียด และจำนวนเงิน

Print Date 21/3/2549		Account Detail Report		FTP Bank
<u>NO.</u>	<u>NAME</u>	<u>DETAILNAME</u>	<u>AMOUNT</u>	
0000000009	FTP Shop	Deposit	7,500.00	
0000000008	FTP Shop	Deposit	3,600.00	
0000000007	FTP Shop	Deposit	2,300.00	
0000000005	FTP Shop	Deposit	4,700.00	
0000000004	FTP Shop	Deposit	3,200.00	
0000000003	FTP Shop	Deposit	30,500.00	
0000000001	FTP Shop	Deposit	5,900.00	
0000000002	Narumol	Withdraw	3,500.00	
0000000006	Srwapan	Withdraw	44,000.00	

รูปที่ ง-7 แสดงรายงานรายละเอียดบัญชีของลูกค้า

## 3. แสดงรายงานบัตรเครดิต (Credit Report)

Print Date 21/3/2549		Credit Report		FTP Bank	
<u>CARDNO</u>	<u>BALANCE</u>	<u>CREDIT</u>	<u>EXPIRES</u>	<u>VALIDFROM</u>	
1474563285968745	44,100.00	50,000.00	21/12/2552	21/12/2547	
1258968547112329	59,500.00	90,000.00	14/5/2553	14/5/2548	
1745147254789684	46,800.00	50,000.00	2/1/2554	2/1/2549	
1984574131658489	65,300.00	70,000.00	5/3/2554	5/3/2549	
1325105864841921	74,100.00	80,000.00	11/5/2555	11/5/2550	
1597456320143836	42,500.00	50,000.00	29/8/2555	29/8/2550	

รูปที่ ง-8 แสดงรายงานบัตรเครดิต

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

#### 4. แสดงรายงานรายละเอียดบัตรเครดิต (Credit Detail Report)

ประกอบด้วยหมายเลขรายการ หมายเลขบัตรเครดิต วันที่ซื้อสินค้า จำนวนเงิน และร้านค้า

Print Date 21/3/2549		Credit Detail Report		FTP Bank	
<u>NO</u>	<u>CARDNO</u>	<u>BUYDATE</u>	<u>AMOUNT</u>	<u>SHOPNAME</u>	
0000000001	1474563285968745	13/3/2548	5,900.00	FTP Shop	
0000000002	1258968547112329	13/3/2548	30,500.00	FTP Shop	
0000000003	1745147254789684	15/3/2549	3,200.00	FTP Shop	
0000000004	1984574131658489	15/3/2549	4,700.00	FTP Shop	
0000000005	1325105864841921	15/3/2549	2,300.00	FTP Shop	
0000000006	1325105864841921	16/3/2549	3,600.00	FTP Shop	
0000000007	1597456320143836	16/3/2549	7,500.00	FTP Shop	

รูปที่ ง-9 แสดงรายงานรายละเอียดบัตรเครดิต

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้