บทที่ 3
วิธีดำเนินการวิจัย

วิธีดำเนินการวิจัย

เพื่อให้ได้ระบบงานใหม่ที่สอดคล้องกับความต้องการ ได้กำหนดกรอบของระบบโดยแสดงในรูปของเครื่องมือที่ใช้ในการออกแบบ ดังนี้

1. Data Flow Diagram

ระบบการตรวจสอบการแสดงตนจะอยู่ที่บริษัทผู้ออกบัตร และมีผู้เกี่ยวข้องอีก 2 กลุ่ม คือผู้ถือบัตรและร้านค้ารับบัตร (รูปที่ 3.1)

1.1 ผู้ถือบัตร

1.1.1 ผู้ถือบัตรจะต้องขอลงทะเบียนกับบริษัทผู้ออกบัตร ข้อมูลของผู้ถือบัตรที่ใช้เป็นข้อมูลนำเข้าได้แก่ เลขที่บัตรเครดิต , เดือน / ปีที่บัตรหมดอายุ , ชื่อที่ปรากฏบนหน้าบัตร , รหัสผู้ใช้ที่ผู้ถือบัตรเป็นผู้เลือก

1.1.2 บริษัทผู้ออกบัตรตรวจสอบความถูกต้องของข้อมูลนำเข้า สร้างรหัสอีกตัวหนึ่งสำหรับผู้ถือบัตรบันทึกข้อมูลลงฐานข้อมูลของบริษัทผู้ออกบัตร แล้วส่งผลการลงทะเบียนให้ผู้ถือบัตร

1.1.3 เมื่อผู้ถือบัตรทำรายการสั่งซื้อสินค้าจากที่ใด และต้องการชำระเงินจะต้องส่งข้อมูลทางการเงิน คือเลขที่บัตรเครดิต แนบมาพร้อมกับรหัสที่ผู้ถือบัตรเก็บไว้แต่เพียงผู้เดียวนั้นมายังบริษัทผู้ออกบัตรเพื่อใช้ในการตรวจสอบตัวตน

1.1.4 หลังการตรวจสอบบริษัทผู้ออกบัตรจะส่งผลการยืนยันหรือปฏิเสธการตรวจสอบตัวตนกลับไปให้ผู้ถือบัตร

1.2 ร้านค้ารับบัตร

1.2.1 ร้านค้ารับบัตรจะต้องขอลงทะเบียนกับบริษัทผู้ออกบัตร ข้อมูลของผู้ถือบัตรที่ใช้เป็นข้อมูลนำเข้าได้แก่ ชื่อจดทะเบียนของร้าน

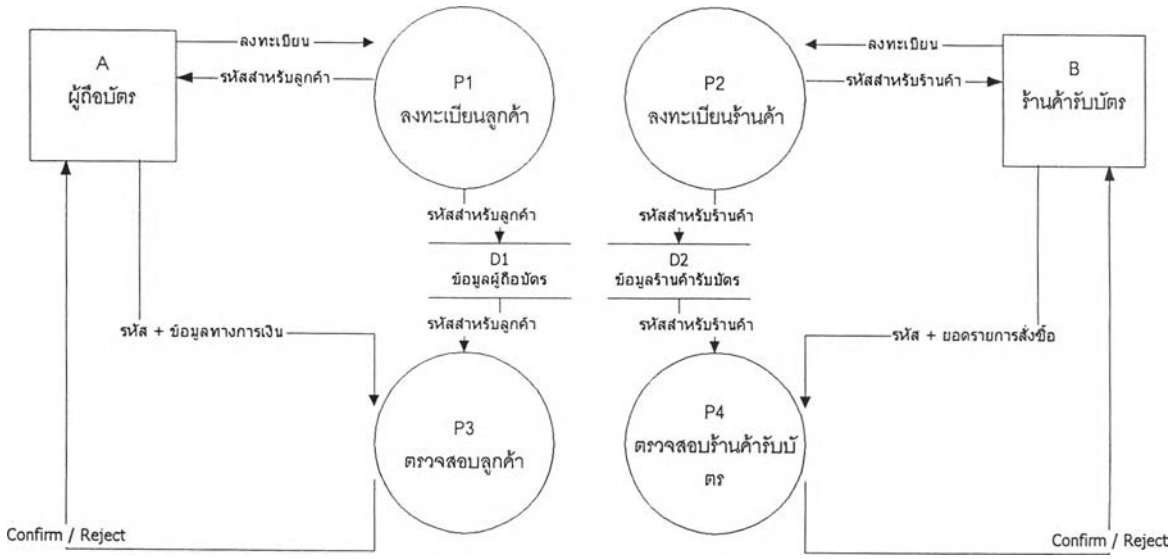
1.2.2 บริษัทผู้ออกบัตรตรวจสอบความถูกต้องของข้อมูลนำเข้า สร้างรหัสอีกตัวหนึ่งสำหรับร้านค้ารับบัตร บันทึกข้อมูลลงฐานข้อมูลของบริษัทผู้ออกบัตร แล้วส่งผลการลงทะเบียนให้ร้านค้ารับบัตร

1.2.3 เมื่อร้านค้ารับบัตรทำรายการขายซื้อสินค้า และผู้ถือบัตรต้องการชำระเงินผ่านระบบการตรวจสอบตัวตน ร้านค้ารับบัตรจะต้องส่งข้อมูลรวมการสั่งซื้อของรายการค้านั้น ๆ แนบมาพร้อมกับรหัสที่ร้านค้ารับบัตรเก็บไว้แต่เพียงผู้เดียวนั้นมายังบริษัทผู้ออกบัตรเพื่อใช้ในการตรวจสอบตัวตน

1.2.4 หลังการตรวจสอบบริษัทผู้ออกบัตรจะส่งผลการยืนยันหรือปฏิเสธการตรวจสอบตัวตนกลับไปให้ร้านค้ารับบัตร

แสดงในรูปของ Data Flow Diagram ได้ดังนี้

รูปที่ 3.1 Data Flow Diagram Level 0 – Context Diagram



รูปที่ 3.2 Data Flow Diagram Level 1

จากรูปที่ 3.1 Data Flow Diagram Level 0 - Context Diagram

A แทน Entity ผู้ถือบัตร

B แทน Entity ร้านค้ารับบัตร

P0 แทน Process การตรวจสอบการแสดงตน

จากรูปที่ 3.2 Data Flow Diagram Level 1

P0 จาก Context Diagram แบ่งเป็น 4 ส่วนย่อย ได้แก่

P1 แทน Process การลงทะเบียนผู้ถือบัตร

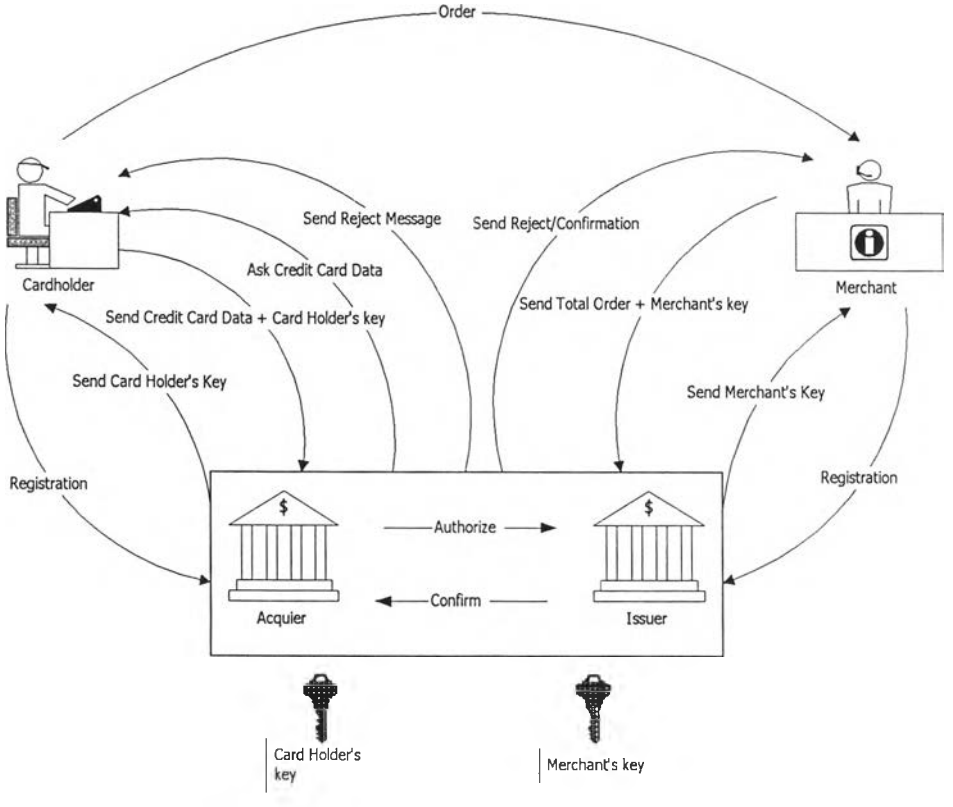
P2 แทน Process การลงทะเบียนร้านค้ารับบัตร

P3 แทน Process การตรวจสอบลูกค้า

P4 แทน Process การตรวจสอบร้านค้ารับบัตร

D1 แทน ข้อมูลผู้ถือบัตร ข้อมูลนำเข้าได้จาก P1 และข้อมูลจะถูกดึงไปใช้ที่ P3

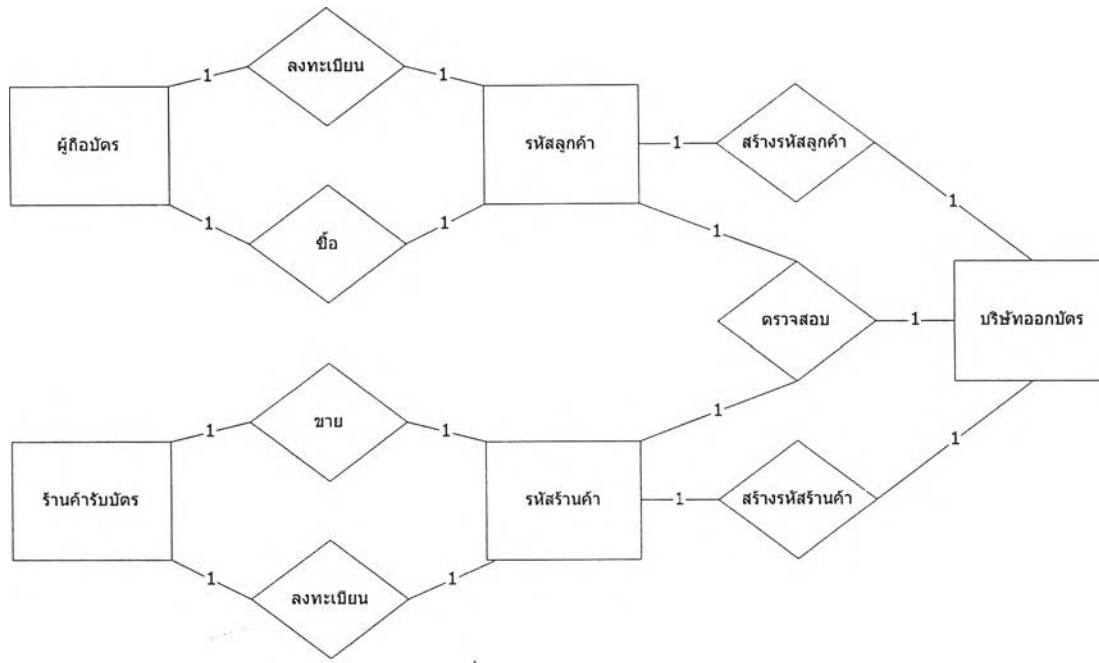
D2 แทน ข้อมูลร้านค้ารับบัตร ข้อมูลนำเข้าได้จาก P2 และข้อมูลจะถูกดึงไปใช้ที่ P4



รูปที่ 3.3 ภาพรวมของระบบที่ทำการทดลอง (System Overview)

2. Data Model

จากกรอบของระบบ ออกแบบ Data model ได้ดังรูปที่ 3.4



รูปที่ 3.4 Data Model

2.1 ผู้ถือบัตร 1 คน จะลงทะเบียนเพียง 1 ครั้งเท่านั้นเพื่อมีเพียง 1 รหัสสำหรับการทำรายการในระบบทดลอง

2.2 บริษัทผู้ออกบัตรตรวจสอบการลงทะเบียนของผู้ถือบัตรทุกรายว่าทำเพียง 1 ครั้งเท่านั้นและรหัสที่สร้างให้ต่อ 1 ผู้ถือบัตรจะมีเพียงรหัสเดียวที่ใช้งานได้

2.3 ผู้ถือบัตรแต่ละคนที่ทำรายการซื้อสินค้าและ/หรือบริการต่อ 1 รายการ จะใช้รหัสที่มีอยู่รหัสเดียวนั้นในการทำรายการ

2.4 บริษัทผู้ออกบัตรจะตรวจสอบตัวตนของผู้ถือบัตรด้วยรหัสที่คู่กันอีก 1 รหัสของผู้ถือบัตร

2.5 ร้านค้ารับบัตร 1 ราย จะลงทะเบียนเพียง 1 ครั้งเท่านั้นเพื่อมีเพียง 1 รหัสสำหรับการทำรายการในระบบทดลอง

2.6 บริษัทผู้ออกบัตรตรวจสอบการลงทะเบียนของร้านค้ารับบัตรทุกรายว่าทำเพียง 1 ครั้งเท่านั้นและรหัสที่สร้างให้ต่อ 1 ร้านค้ารับบัตรให้มีเพียงรหัสเดียวที่ใช้งานได้

2.7 ร้านค้ารับบัตรแต่ละรายที่ทำรายการซื้อสินค้าและ/หรือบริการต่อ 1 รายการ จะใช้รหัสที่มีอยู่รหัสเดียวนั้นในการทำรายการ

2.8 บริษัทผู้ออกบัตรจะตรวจสอบตัวตนของร้านค้ารับบัตรด้วยรหัสที่คู่กันอีก 1 รหัสของร้านค้ารับบัตร

3. โครงสร้างแฟ้มข้อมูล (File Structure)

3.1 โครงสร้างแฟ้มข้อมูล (File Structure) ส่วนของบริษัทผู้ให้บริการบัตรเครดิต

File ID.					
File Name	Member_Account				
File Description	เก็บข้อมูลผู้ถือบัตรที่ลงทะเบียน				
Key Field					
Seq.	Field Name	Field Type	Length	Description	Null
1	card_no	VarChar	16	เลขที่บัตรเครดิต	N
2	card_name	VarChar	20	ชื่อผู้ถือบัตร	N
3	expire_month	VarChar	2	เดือนที่บัตรหมดอายุ	N
4	expire_year	VarChar	4	ปีที่บัตรหมดอายุ	N

ตารางที่ 3.1 แฟ้มข้อมูลสำหรับเก็บข้อมูลผู้ถือบัตรที่ลงทะเบียน

File ID.					
File Name	decrypt_key				
File Description	เก็บข้อมูลรหัสของผู้ถือบัตรที่ลงทะเบียน				
Key Field					
Seq.	Field Name	Field Type	Length	Description	Null
1	card_no	VarChar	16	เลขที่บัตรเครดิต	N
2	User	VarChar	8	รหัสผู้ใช้	N
3	decrypt_key	Number	Long Integer	รหัสใช้สำหรับการถอดรหัส	N

ตารางที่ 3.2 แฟ้มข้อมูลสำหรับเก็บข้อมูลรหัสของผู้ถือบัตรที่ลงทะเบียน

File ID.					
File Name	Merchant_Account				
File Description	เก็บข้อมูลร้านค้ารับบัตรที่ลงทะเบียน				
Key Field					
Seq.	Field Name	Field Type	Length	Description	Null
1	Merchant_no	VarChar	16	เลขที่ร้านค้า (ระบบสร้างเมื่อลงทะเบียน)	N
2	Marchant_name	VarChar	20	ชื่อจดทะเบียนของร้านค้ารับบัตร	N
3	Expire_month	VarChar	2	เดือนสิ้นสุดการลงทะเบียนใช้งานของร้านค้ารับบัตร	N
4	expire_year	VarChar	4	ปีสิ้นสุดการลงทะเบียนใช้งานของร้านค้ารับบัตร	N

ตารางที่ 3.3 แฟ้มข้อมูลสำหรับเก็บข้อมูลร้านค้ารับบัตรที่ลงทะเบียน

File ID.					
File Name	Merchant_decrypt_key				
File Description	เก็บข้อมูลรหัสของร้านค้ารับบัตรที่ลงทะเบียน				
Key Field					
Seq.	Field Name	Field Type	Length	Description	Null
1	Merchant_no	VarChar	16	เลขที่ร้านค้า	N
2	User	VarChar	8	รหัสผู้ใช้	N
3	decrypt_key	Number	Long Integer	รหัสใช้สำหรับการถอดรหัส	N

ตารางที่ 3.4 แฟ้มข้อมูลสำหรับเก็บข้อมูลรหัสของร้านค้ารับบัตรที่ลงทะเบียน

File ID.					
File Name	Transaction				
File Description	เก็บข้อมูลรายการค้า (รายการซื้อ / ขายสินค้า)				
Key Field					
Seq.	Field Name	Field Type	Length	Description	Null
1	card_no	Char	16	เลขที่บัตรเครดิต	N
2	shop_id	Char	3	เลขที่ร้านค้า	N
3	order_num	Char	5	เลขที่รายการสั่งซื้อสินค้า	N
4	Amount	Number	Long Integer	จำนวนเงินรวมสำหรับการสั่งซื้อสินค้า	N
5	Tdate	Date		วันที่ที่เกิดรายการสั่งซื้อ	N
6	Ttime	Time		เวลาที่เกิดรายการสั่งซื้อ	N

ตารางที่ 3.5 แฟ้มข้อมูลสำหรับเก็บข้อมูลรายการค้า (รายการซื้อ / ขายสินค้า)

4. รายละเอียดโปรแกรม (Program Specification)

4.1 รายชื่อโปรแกรม หน้าจอ และส่วนจำเพาะ (module) ของระบบทดลองส่วนของบริษัทผู้ให้บริการบัตรเครดิต

Program Name	Program Description	Screen Name / Module Name
1. ApsBankGenKey 2. SvrBankGenKey	สร้างรหัสเมื่อผู้ถือบัตรลงทะเบียน	• UBankGenKey
		• ModBankGenKey
1. ApsBankGenKeyMerchant 2. SvrBankGenKeyMerchant	สร้างรหัสเมื่อร้านค้ารับบัตรลงทะเบียน	• UBankGenKeyMerchant
		• ModBankGenKey
1. ApsBankDecrypt 2. SvrBankDecrypt	ถอดรหัสรายการที่รับจากร้านค้ารับบัตร	• UBankDecrypt
		• modBankDecrypt
1. ApsBankCardReceive 2. SvrBankCardReceive	รับข้อมูลการเงินของผู้ถือบัตร เพื่อทำรายการชำระเงิน	• UbankCardReceive
		• modBankEncryptDataForPayment

ตารางที่ 3.6 รูปแสดงรายชื่อโปรแกรม หน้าจอ และส่วนจำเพาะ (module) ของระบบทดลองส่วนของบริษัทผู้ให้บริการบัตรเครดิต

4.2 รายชื่อโปรแกรม หน้าจอ และส่วนจำเพาะ (module) ของระบบทดลองส่วนของร้านค้ารับบัตร

Program Name	Program Description	Screen Name Module Name
1. ApsMSendOrder 2. SvrMSendOrder	สำหรับส่งเลขที่รายการสั่งซื้อสินค้าและจำนวนเงินรวมจากร้านค้ารับบัตรไปยังบริษัทผู้ออกบัตร	• UMSendOrder

ตารางที่ 3.7 รูปแสดงรายชื่อโปรแกรม หน้าจอ และส่วนจำเพาะ (module) ของระบบทดลองส่วนของร้านค้ารับบัตร

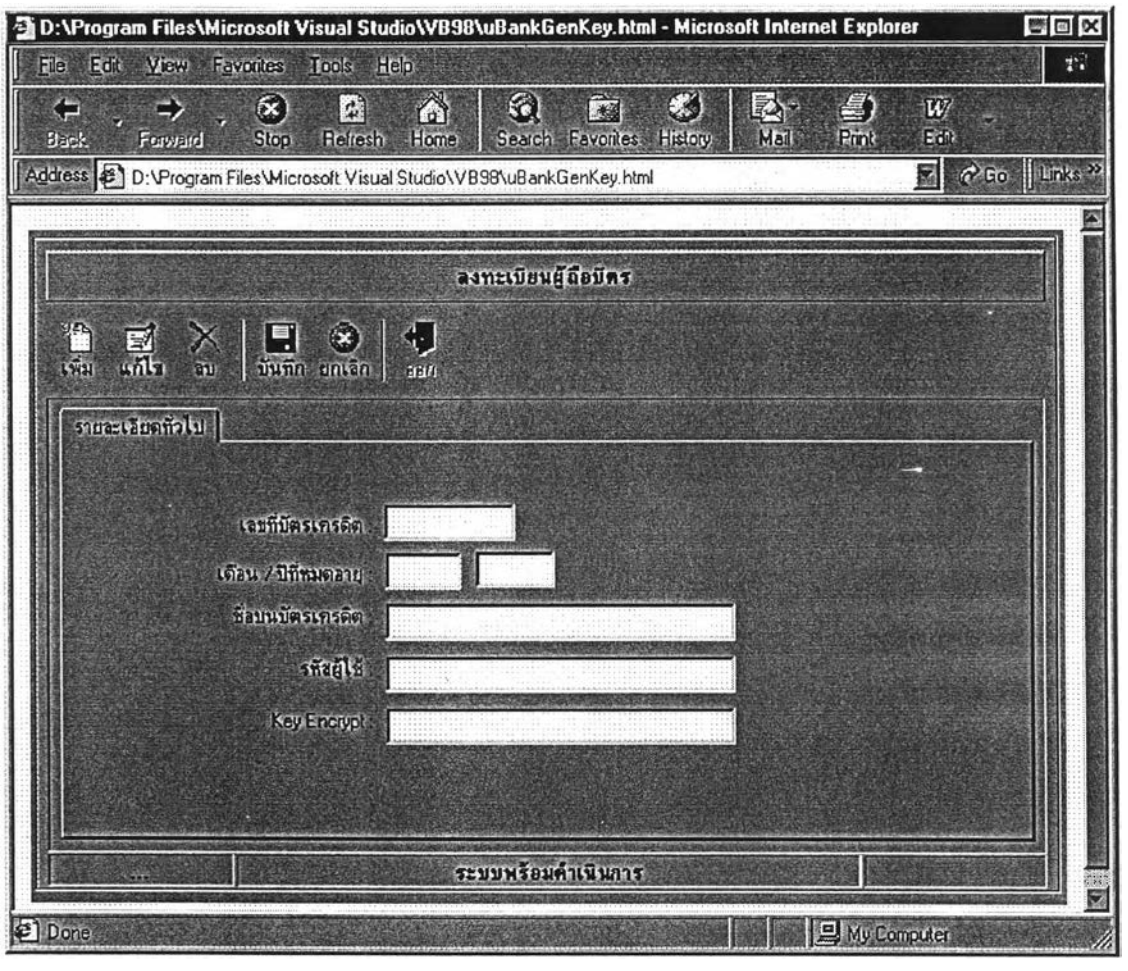
จากตารางที่ 3.6 และ 3.7 ซึ่งแสดงรายชื่อของหน้าจอในระบบนี้ หน้าจอต่าง ๆ จะถูกเรียกใช้งานตามตารางที่ 3.8 ดังนี้

ผู้ใช้	การทำงาน	ชื่อหน้าจอ
ร้านค้ารับบัตร	ลงทะเบียน	UBankGenKeyMerchant
	ส่งยอดรวมรายการสั่งซื้อ	UMSendOrder
ผู้ถือบัตร	ลงทะเบียน	UBankGenKey
	บันทึกข้อมูลทางการเงินของผู้ถือบัตร	UbankCardReceive
บริษัทผู้ออกบัตร	ถอดรหัสรายการที่รับจากร้านค้ารับบัตร	UBankDecrypt

ตารางที่ 3.8 ตารางแสดงการเรียกใช้งานหน้าจอ

5. ตัวอย่างหน้าจอ

5.1 การลงทะเบียนสำหรับผู้ถือบัตร



รูปที่ 3.5 หน้าจอสำหรับการลงทะเบียนของผู้ถือบัตร

ผู้ถือบัตรสามารถเข้ามาลงทะเบียนเพื่อขอใช้บริการการชำระเงินด้วยบัตรเครดิตผ่านระบบการค้าอิเล็กทรอนิคส์ โดยระบุเลขที่บัตรเครดิต , เดือน / ปีที่บัตรหมดอายุ , ชื่อที่ปรากฏบนหน้าบัตร แล้วเลือกรหัสผู้ใช้ เมื่อทำการบันทึกข้อมูล จะมีการสร้างรหัสเก็บไว้ในฐานข้อมูลของบริษัทผู้ออกบัตร เพื่อใช้ในการตรวจสอบตัวตนผู้ถือบัตรต่อไป การลงทะเบียนนี้จะมีอายุการลงทะเบียนตามเดือน / ปีที่บัตรหมดอายุ ก่อนวันหมดอายุของบัตร ผู้ถือบัตรสามารถเข้ามาทำรายการเปลี่ยนแปลงรหัสได้ และหากบัตรหมดอายุหรือผู้ถือบัตรผิดเงื่อนไขใด ๆ กับบริษัทผู้ออกบัตร บริษัทผู้ออกบัตรอาจทำรายการลบรหัสของผู้ถือบัตรรายนั้น ๆ ได้

หน้าที่หลักของหน้าจอนี้

1. การตรวจสอบว่าผู้ลงทะเบียนเป็นผู้ถือบัตรเครดิตตัวจริง (Authentication)

การตรวจสอบนั้นสามารถตรวจสอบได้จาก ข้อมูล 3 อย่างคือ

- เลขที่บัตรเครดิต (Credit Card Number)
- วันที่บัตรหมดอายุ (Expire Date)
- ชื่อผู้ถือบัตรที่ปรากฏอยู่บนบัตร (Name on Card)

ซึ่งข้อมูลทั้ง 3 อย่าง จะปรากฏอยู่บนบัตรเครดิต ถ้าผู้ลงทะเบียน กรอกข้อมูลทั้ง 3 ส่วน ได้ถูกต้องก็แสดงว่าเป็นผู้ถือบัตรตัวจริง

วิธีการตรวจสอบคือ

- นำข้อมูลทั้ง 3 อย่าง ไปค้นหาในฐานข้อมูลของธนาคารหรือบริษัทบัตรเครดิต ถ้าพบแสดงว่าเป็นผู้ถือบัตรตัวจริง แต่ถ้าไม่พบแสดงว่าไม่ใช่ผู้ถือบัตร

2. การตรวจสอบ User ที่ผู้ลงทะเบียนกำหนดว่ามีผู้ใช้แล้วหรือไม่

ถ้ามีการกำหนดซ้ำ จะบอกไม่ได้ว่า จะใช้ Key ใดในการ Decrypt

วิธีการตรวจสอบ คือ

- นำข้อมูลผู้ลงทะเบียนไปค้นหาในฐานข้อมูลของธนาคารหรือบริษัทบัตรเครดิต ถ้าพบแสดงว่ามีการใช้ข้อมูลบัตรเครดิตชุดนี้เข้ามาลงทะเบียนไว้แล้ว ต้องแก้ไขหรือยกเลิกการลงทะเบียนครั้งก่อนหน้า

3. การตรวจสอบกุญแจสำหรับการเข้ารหัส (Key Encryption) ว่าใช้ได้หรือไม่

ในการเข้ารหัส แบบ RSA Security นั้น การกำหนด Key สำหรับการ Encrypt จะต้องเป็นตัวเลขที่ Relative Prime กับ (P-1)(Q-1) ซึ่งถ้า Key ที่ผู้ลงทะเบียนกำหนด ไม่เป็น Relative Prime แล้ว Key นั้นจะไม่สามารถนำมาใช้ได้

วิธีการตรวจสอบคือ

Relative Prime คือ GCD(X,Y) = 1

ดังนั้นการตรวจสอบว่าตัวเลขที่กำหนดเป็น Relative Prime กันหรือไม่ สามารถเช็คได้จากการคำนวณ GCD ระหว่าง Key Encryption ที่ผู้ลงทะเบียนกำหนดกับ (P-1)*(Q-1) ซึ่งถ้าเท่ากับ 1 แสดงว่า เป็น Relative Prime กัน Key ที่กำหนดสามารถทำมาใช้ในการ Encrypt ได้ ซึ่งมี Algorithm ที่ใช้ในการหา GCD คือ Euclidean Algorithm ดังนี้

C_0 := (P-1)*(Q-1)

C_1 : = Key Encryption

i := 1

Repeat

$C_{i+1} := C_{i-1}$ Mod C_i

$t := C_{i-1}$ DIV C_i

Until $C_i := 0$

If ($B_i = 1$) then 'Key is Valid'

Else 'Key is Invalid'

4. การสร้างรหัส (Generate Key Pair) สำหรับการถอดรหัส (Decrypt) เพื่อใช้ยืนยันตัวตนของผู้ถือบัตร

การเข้ารหัสแบบ RSA Security นั้น ถ้าทราบกุญแจสำหรับเข้ารหัส (Key Encrypt) และ P,Q ซึ่งเป็นจำนวนเฉพาะ (Prime Number) ขนาดใหญ่ ซึ่ง ทั้ง P,Q นี้จะต้องเก็บเป็นความลับไม่สามารถเปิดเผยได้ แล้วก็สามารถที่จะคำนวณหากุญแจสำหรับการถอดรหัส (Key Decrypt)ได้

วิธีการหากุญแจสำหรับการถอดรหัส (Key Decrypt) คือ

การหาค่า Inverse ของ (Key Encrypt) Mod (P-1)*(Q-1) ซึ่งการคำนวณ Key Decrypt นั้นต้องผ่านขั้นตอนการตรวจสอบ Key Encrypt ก่อนว่าสามารถใช้ได้ จึงนำ Key Encrypt ที่ได้ มาคำนวณ หา Key Decrypt

ซึ่งมี Algorithm ที่ใช้ในการหา Key Decrypt คือ Euclidean Algorithm with Backward ดังนี้

$C_0 := (P-1)*(Q-1)$

$C_1 :=$ Key Encryption

$B_0 := 0$

$B_1 := 1$

$i := 1$

Repeat

$C_{i+1} := C_{i-1}$ Mod C_i

$t := C_{i-1}$ DIV C_i

$B_{i+1} := B_{i-1} - t * B_i$

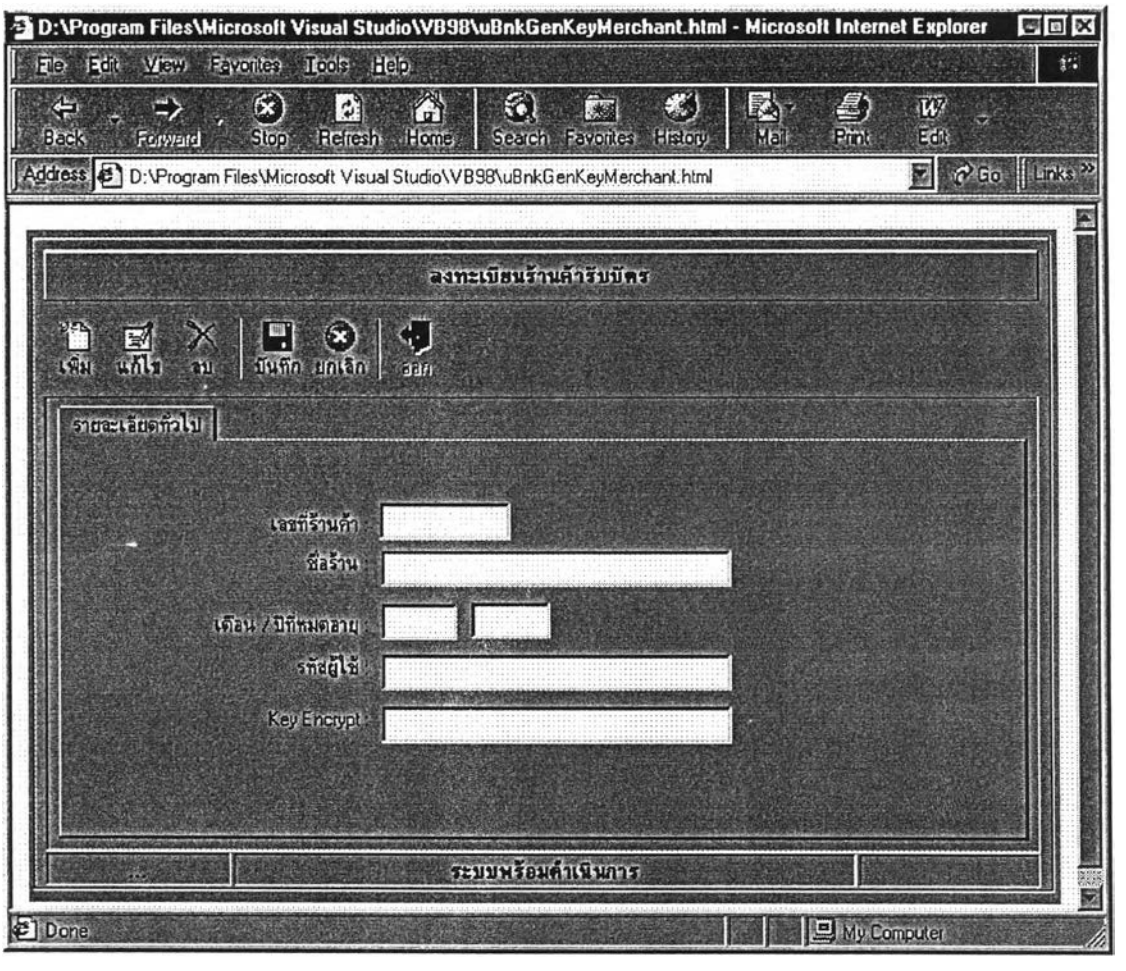
$i : i+1$

Until $C_i := 0$

If ($B_i => 0$) then $a: = B_{i-1}$

Else $A: = (P-1)*(Q-1) + B_{i-1}$

5.2 การลงทะเบียนสำหรับร้านค้ารับบัตร



รูปที่ 3.6 หน้าจอสำหรับการลงทะเบียนของร้านค้ารับบัตร

ร้านค้ารับบัตรสามารถเข้ามาลงทะเบียนเพื่อขอใช้บริการการชำระเงินด้วยบัตรเครดิตผ่านระบบการค้าอิเล็กทรอนิคส์ โดยระบุชื่อร้านค้า เมื่อทำการบันทึกข้อมูล จะมีการสร้างเลขที่ร้านค้า , เดือน / ปีที่หมดอายุ และ รหัสเก็บไว้ในฐานข้อมูลของบริษัทผู้ออกบัตร เพื่อใช้ในการตรวจสอบตัวตนของร้านค้ารับบัตรต่อไป การลงทะเบียนนี้จะมีอายุการลงทะเบียนตามเดือน / ปีที่หมดอายุที่บริษัทผู้ออกบัตรกำหนด ก่อนวันหมดอายุ ร้านค้ารับบัตรสามารถเข้ามาทำรายการเปลี่ยนแปลงรหัสได้ และหากถึงเวลาครบกำหนดหรือร้านค้ารับบัตรผิดเงื่อนไขใด ๆ กับบริษัทผู้ออกบัตร บริษัทผู้ออกบัตรอาจทำรายการลบรหัสของร้านค้ารับบัตรรายนั้น ๆ ได้

หน้าที่หลักของหน้าจอนี้

1. การตรวจสอบว่าผู้ลงทะเบียนเป็นผู้ถือบัตรเครดิตตัวจริง (Authentication) การตรวจสอบนั้นสามารถตรวจสอบได้จาก

- ชื่อร้านค้ารับบัตร

วิธีการตรวจสอบคือ

- นำข้อมูล ไปค้นหาในฐานข้อมูลของร้านค้ารับบัตรของธนาคารหรือบริษัทบัตรเครดิต ถ้าพบแสดงว่าเป็นร้านค้ารับบัตรที่สามารถลงทะเบียนได้ แต่ถ้าไม่พบแสดงว่าไม่ใช่ร้านค้ารับบัตรที่มีสิทธิลงทะเบียน

2. การตรวจสอบ User ที่ผู้ลงทะเบียนกำหนดว่ามีผู้ใช้แล้วหรือไม่
ถ้ามีการกำหนดซ้ำ จะบอกไม่ได้ว่า จะใช้ Key ใดในการ Decrypt
วิธีการตรวจสอบ คือ
   - นำข้อมูลผู้ลงทะเบียนไปค้นหาในฐานข้อมูลของธนาคารหรือบริษัทบัตรเครดิต ถ้าพบแสดงว่ามีการใช้ข้อมูลของร้านค้ารับบัตรชุดนี้เข้ามาลงทะเบียนไว้แล้วต้องแก้ไขหรือยกเลิกการลงทะเบียนครั้งก่อนหน้า
3. การตรวจสอบกุญแจสำหรับการเข้ารหัส (Key Encryption) ว่าใช้ได้หรือไม่
ในการเข้ารหัส แบบ RSA Security นั้น การกำหนด Key สำหรับการ Encrypt จะต้องเป็นตัวเลขที่ Relative Prime กับ (P-1)(Q-1) ซึ่งถ้า Key ที่ผู้ลงทะเบียนกำหนด ไม่เป็น Relative Prime แล้ว Key นั้นจะไม่สามารถนำมาใช้ได้
วิธีการตรวจสอบคือ

Relative Prime คือ GCD(X,Y) = 1

ดังนั้นการตรวจสอบว่าตัวเลขที่กำหนดเป็น Relative Prime กันหรือไม่ สามารถเช็คได้จากการคำนวณ GCD ระหว่าง Key Encryption ที่ผู้ลงทะเบียนกำหนดกับ (P-1)*(Q-1) ซึ่งถ้าเท่ากับ 1 แสดงว่า เป็น Relative Prime กัน Key ที่กำหนดสามารถทำมาใช้ในการ Encrypt ได้ ซึ่งมี Algorithm ที่ใช้ในการหา GCD คือ Euclidean Algorithm ดังนี้

C_0 := (P-1)*(Q-1)

C_1 : = Key Encryption

i := 1

Repeat

$C_{i+1} := C_{i-1}$ Mod C_i

$t := C_{i-1}$ DIV C_i

Until $C_i := 0$

If (B_i = 1) then 'Key is Valid'

Else 'Key is Invalid'

4. การสร้างรหัส (Generate Key Pair) สำหรับการถอดรหัส (Decrypt) เพื่อใช้ยืนยันตัวตนของร้านค้ารับบัตร

การเข้ารหัสแบบ RSA Security นั้น ถ้าทราบกุญแจสำหรับเข้ารหัส (Key Encrypt) และ P,Q ซึ่งเป็นจำนวนเฉพาะ (Prime Number) ขนาดใหญ่ ซึ่ง ทั้ง P,Q นี้จะต้องเก็บเป็นความลับไม่สามารถเปิดเผยได้ แล้วก็สามารถที่จะคำนวณหากุญแจสำหรับการถอดรหัส (Key Decrypt)ได้

วิธีการหากุญแจสำหรับการถอดรหัส (Key Decrypt) คือ

การหาค่า Inverse ของ (Key Encrypt) Mod (P-1)*(Q-1) ซึ่งการคำนวณ Key Decrypt นั้นต้องผ่านขั้นตอนการตรวจสอบ Key Encrypt ก่อนว่าสามารถใช้ได้ จึงนำ Key Encrypt ที่ได้ มาคำนวณ หา Key Decrypt

ซึ่งมี Algorithm ที่ใช้ในการหา Key Decrypt คือ Euclidean Algorithm with Backward ดังนี้

C_0 := (P-1)*(Q-1)

C_1 : = Key Encryption

B_0 := 0

B_1 := 1

i := 1

Repeat

C_{i+1} := C_{i-1} Mod C_i

t := C_{I-1} DIV C_I

B_{I+1} := B_{I-1}-t * B_I

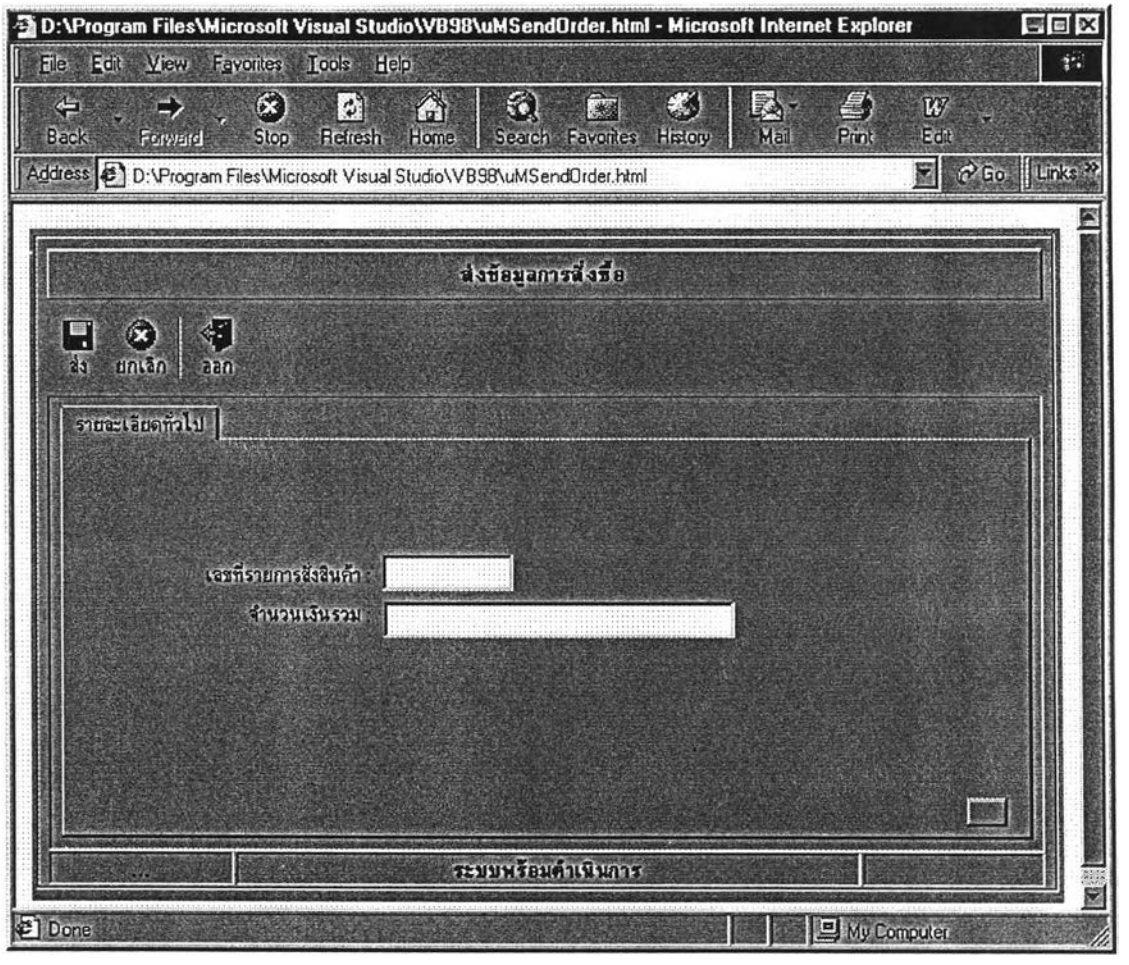
i : i+1

Until C_i := 0

If (B_i => 0) then a: = B_{i-1}

Else A: = (P-1)*(Q-1) + B_{i-1}

5.3 การส่งข้อมูลสั่งซื้อ



รูปที่ 3.7 หน้าจอสำหรับการส่งข้อมูลการสั่งซื้อ

ร้านค้ารับบัตรจะสร้างหน้าจอการรับรายการซื้อสินค้า เมื่อผู้ซื้อเลือกการชำระเงินด้วยบัตรเครดิตแบบขอให้มีการตรวจสอบตัวตน (ร้านค้ารับบัตรและผู้ถือบัตร) ร้านค้ารับบัตรจะต้องส่งรหัสของร้านค้ารับบัตร พร้อมด้วยรหัสร้านค้า , เลขที่ของการสั่งซื้อและจำนวนเงินรวม ไปยังบริษัทผู้ออกบัตร เพื่อทำการตรวจสอบตัวตนร้านค้ารับบัตร หากร้านค้ารับบัตรเป็นร้านที่มีสิทธิทำรายการคือเป็นร้านที่ได้ลงทะเบียนไว้แล้ว บริษัทผู้ออกบัตรจะเปิดหน้าจอให้ผู้ถือบัตรบันทึกข้อมูลการชำระเงินต่อไป

หน้าที่หลักของหน้าจอนี้

1. เมื่อลูกค้าเข้ามาในร้าน หรือ เข้ามาที่ Web Site ของร้านค้า ร้านค้าจะต้องกำหนดเลขที่การสั่งซื้อสำหรับการซื้อขายครั้งนั้น เพื่อนำไปใช้ในการเข้ารหัสข้อมูล

   การกำหนดเลขที่การสั่งซื้อกำหนดโดย

   1.1 รหัสร้านค้า

   1.2 เลขที่การสั่งซื้อ

   1.3 จำนวนเงินรวมทั้งหมด

   รหัสร้านค้า คือ รหัสที่ใช้บอกว่าเป็นการซื้อสินค้าจากร้านไหน เช่น 001 เป็นต้น

   เลขที่การสั่งซื้อ คือ รหัสบอกว่ารายการซื้อสินค้าลำดับใด เช่น 00053 เป็นต้น

   จำนวนเงินรวมที่ลูกค้าซื้อในครั้งนั้น เช่น เงิน 300 บาท จะได้ 00300.00 เป็นต้น

   นำตัวเลขทั้ง 3 มาต่อกัน เป็นข้อมูลการสั่งซื้อครั้งนั้น เช่น

   Order ID : 0010005300300.00

2. การถอดรหัสข้อมูล

   หลังจากที่ธนาคารหรือบริษัทบัตรเครดิตได้ข้อมูลจากร้านค้าซึ่งประกอบด้วย

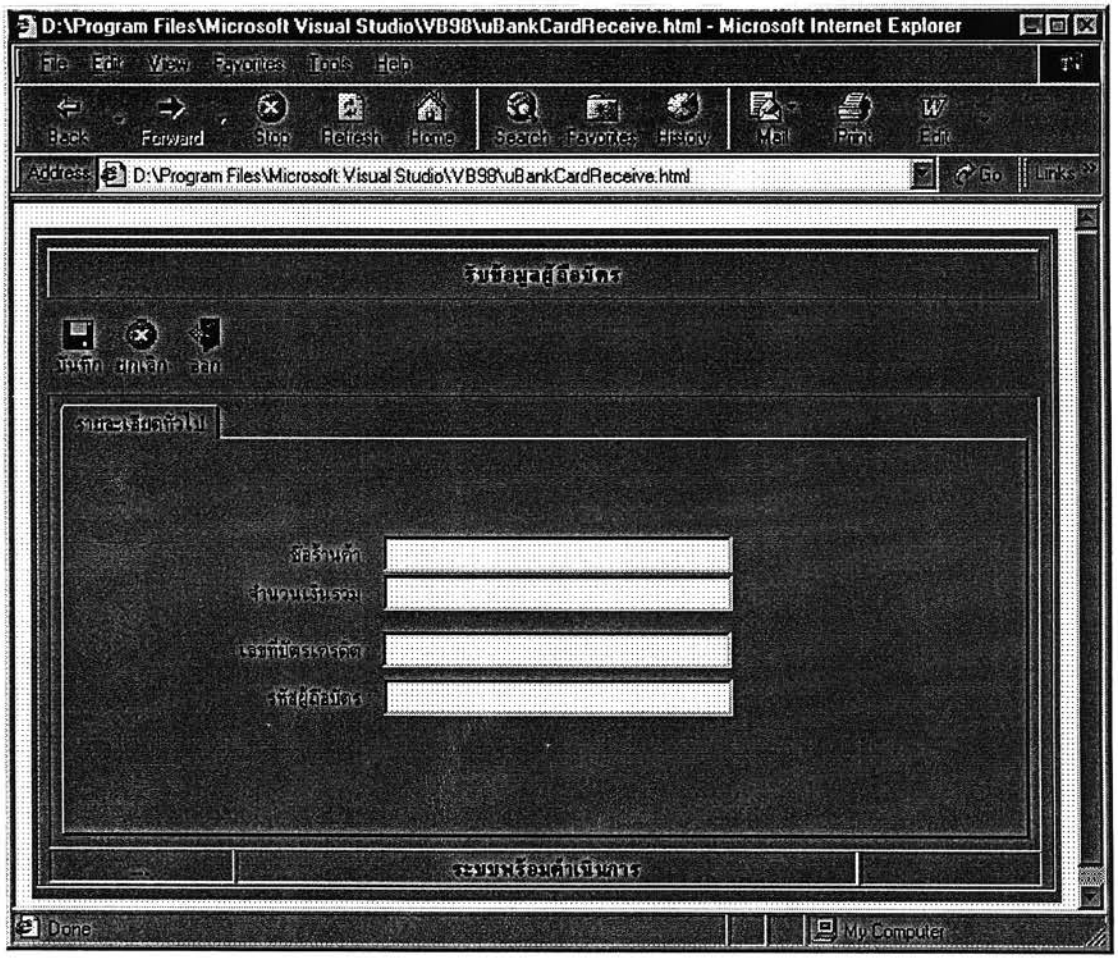
   2.1 รหัสร้านค้า

   2.2 Cipher Text

   ธนาคารหรือบริษัทบัตรเครดิตจะใช้รหัสร้านค้าที่ได้ไปค้นหาในฐานข้อมูลของธนาคารหรือบริษัทบัตรเครดิต เพื่อหากุญแจสำหรับการถอดรหัส (Key Decrypt) เพื่อใช้ถอดรหัส Cipher Text ซึ่งวิธีการจะทำย้อนกลับกับ การเข้ารหัสแต่จะใช้กุญแจสำหรับการถอดรหัส (Key Decrypt) ที่เข้ากับรหัสร้านค้าที่ร้านค้าส่งมา และได้กลับมาเป็น Plain Text ธนาคารหรือบริษัทบัตรเครดิตแยกข้อมูลรหัสร้านค้า เลขที่การสั่งซื้อ และจำนวนเงิน

3. การตรวจสอบความถูกต้องของข้อมูล

5.4 การบันทึกข้อมูลทางการเงินของผู้ถือบัตร



รูปที่ 3.8 หน้าจอสำหรับการบันทึกข้อมูลทางการเงินของผู้ถือบัตร

เมื่อร้านค้ารับบัตรได้รับการตรวจสอบตัวตนแล้ว ผู้ถือบัตรจะได้รับหน้าจอตามภาพ 3.8 จากบริษัทผู้ออกบัตร เพื่อขอให้บันทึกข้อมูลทางการเงิน โดยผู้ถือบัตรจะต้องตรวจสอบชื่อร้านค้าและจำนวนเงินรวมว่าเป็นข้อมูลที่ถูกต้องตามที่ผู้ถือบัตรได้สั่งสินค้า จึงจะบันทึกข้อมูลเลขที่บัตรเครดิตและรหัสของผู้ถือบัตรลงไป

หน้าที่หลักของหน้าจอนี้

1. การเข้ารหัสข้อมูล

ในการเข้ารหัสข้อมูลนั้นจะใช้ข้อมูล 2 ข้อมูลคือ

1.1 Order ID 16 หลัก เช่น 0010005300300.00

1.2 Credit Card Number 16 หลัก เช่น 5081270001025774

แล้วนำข้อมูลทั้งสองมาต่อกันและได้เป็น 32 หลัก เช่น

0010005300300.005081270001025774

แล้วนำมาทำเป็น Plain Text โดยกำหนดให้

0 = 11	6 = 60
1 = 10	7 = 70
2 = 20	8 = 80
3 = 30	9 = 90
4 = 40	. = 99
5 = 50	

จะได้ Plain Text ทั้งหมด 64 หลักคือ

1111101111115030111130111199111150118010207011111110112050707040

จากนั้นกำหนด Box Size ขนาด 4 หลักสำหรับ Encrypt จะได้ 16 Box

นำแต่ละ Box มา Encrypt แบบ RSA Security ดังนี้

สมมุติ Key Encrypt = 31 และ ค่า P*Q = 9577

Cipher1 $= 1111^{31}$ Mod 9577

.....

Cipher16 $= 7040^{31}$ Mod 9577

นำ Cipher มาต่อกันได้ 64 หลัก สมมุติว่าได้

5656565212584569851232541254589577100202541025802578922025102598

แบ่งเป็น Box ละ 2 หลัก

แล้วนำแต่ละ Box มาหักออกจาก 132 เช่น 132 – 56 = 76 แล้วเปลี่ยนเป็นตัวอักษรโดยใช้ Function Chr$ เมื่อทำครบแล้วจะได้ Cipher Text 32 ตัวอักษร เช่น *^uts#&8dlsk%#f)~!Opjirpa=+}?die;

จากนั้นส่ง Cipher Text และ User ไปให้บริษัทผู้ออกบัตรเพื่อทำการถอดรหัส

2. การถอดรหัสข้อมูล

หลังจากที่ธนาคารหรือบริษัทบัตรเครดิตได้ข้อมูลจากร้านค้าซึ่งประกอบด้วย

2.1 รหัสร้านค้า

2.2 Cipher Text

ธนาคารหรือบริษัทบัตรเครดิตจะใช้รหัสร้านค้าที่ได้ไปค้นหาในฐานข้อมูลของธนาคารหรือบริษัทบัตรเครดิต เพื่อหากุญแจสำหรับการถอดรหัส (Key Decrypt) เพื่อใช้ถอดรหัส Cipher Text ซึ่งวิธีการจะทำย้อนกลับกับ การเข้ารหัสแต่จะใช้กุญแจสำหรับการถอดรหัส (Key Decrypt) ที่เข้ากับรหัสร้านค้าที่ร้านค้าส่งมา และได้กลับมาเป็น Plain

Text ธนาคารหรือบริษัทบัตรเครดิตแยกข้อมูลรหัสร้านค้า เลขที่การสั่งซื้อ และจำนวนเงิน

3. การตรวจสอบความถูกต้องของข้อมูล

หลังจาก Decrypt ข้อมูล Cipher Text ออกมาเป็นช่วงข้อมูลต่างได้แล้ว ข้อมูลที่ธนาคารต้องตรวจสอบคือ

3.1 เลขที่บัตรเครดิต (Credit Card Number)

ตรวจสอบในฐานข้อมูลว่าเลขที่บัตรเครดิตมีจริงหรือไม่

3.2 ตรวจสอบการซ้ำของรายการสั่งซื้อ (Transaction)

ธนาคารสามารถตรวจสอบได้จากฐานข้อมูล โดยค้นหารหัสร้านค้าและเลขที่การสั่งซื้อ