

สารบัญ

	หน้าที่
กิตติกรรมประกาศ	ค
บทคัดย่อภาษาไทย	ง
บทคัดย่อภาษาอังกฤษ	ฉ
สารบัญ	ช
สารบัญตาราง	ฉ
สารบัญภาพ	ฉ
บทที่ 1 บทนำ	
1.1 หลักการและเหตุผล	1
1.2 วัตถุประสงค์ของการศึกษา	2
1.3 ประโยชน์ที่คาดว่าจะได้รับ	2
1.4 ระยะเวลาการศึกษา	2
1.5 ขอบเขตและวิธีการศึกษา	2
1.6 แนวคิดที่ใช้ในการศึกษา	3
1.7 นิยามคำศัพท์	4
บทที่ 2 ความสำคัญของพาณิชย์อิเล็กทรอนิกส์ (E-Commerce)	
2.1 ความหมายและรูปแบบของพาณิชย์อิเล็กทรอนิกส์	5
2.2 ข้อมูลทางสถิติของพาณิชย์อิเล็กทรอนิกส์	6
2.3 ความสำคัญของพาณิชย์อิเล็กทรอนิกส์	8
2.4 ตัวอย่างของพาณิชย์อิเล็กทรอนิกส์	9
2.5 ประโยชน์ของพาณิชย์อิเล็กทรอนิกส์ต่อผู้ขายและผู้ซื้อ	9
2.6 ขั้นตอนการทำพาณิชย์อิเล็กทรอนิกส์	10
2.7 ระบบการชำระเงินผ่านอินเทอร์เน็ต	12
2.8 ภัยคุกคามและมาตรการรักษาความปลอดภัยของข้อมูล	13
2.9 เทคโนโลยีในการรักษาความปลอดภัย	14
2.10 กฎหมายในระบบพาณิชย์อิเล็กทรอนิกส์	18

	หน้าที่
บทที่ 3 การรักษาความปลอดภัยของการทำธุรกรรม(Transaction Security)	
3.1 การเข้ารหัสและถอดรหัสข้อมูล (Encryption and Decryption)	20
3.1.1 พื้นฐานของการเข้ารหัสข้อมูล	21
3.1.2 การเข้ารหัสแบบ Secret Key Encryption	26
3.1.3 การเข้ารหัสแบบ Public Key Encryption	27
3.1.4 การเข้ารหัสข้อมูลแบบ DES (Data Encryption Standard)	28
3.1.5 การเข้ารหัสข้อมูลแบบ RSA(Rivest-Shamir-Adelman Encryption)	29
3.1.6 หลักการเข้ารหัสข้อมูลที่ดี	33
3.2 นโยบายการเข้ารหัส	34
3.2.1 ตัวอย่างนโยบายเทคโนโลยีเข้ารหัส	36
3.2.2 แนวคิดในการกำหนดนโยบายควบคุมเทคโนโลยีเข้ารหัส	37
3.3 ความปลอดภัยในการพาณิชย์อิเล็กทรอนิกส์และเทคโนโลยีที่เกี่ยวข้อง	39
3.3.1 ลายมือชื่อและใบรับรองอิเล็กทรอนิกส์	40
3.3.2 สภาพแวดล้อมแบบเปิดและสภาพแวดล้อมแบบปิด	43
3.3.3 ข้อจำกัดในการระบุตัวตนบุคคลด้วยใบรับรองดิจิทัล	44
3.4 ระบบ SET (Secure Electronic Transaction)	45
3.4.1 การทำงานของระบบ SET	46
3.4.2 ระบบรักษาความปลอดภัยของ SET	48
3.4.3 การนำระบบ SET มาใช้งานอย่างมีประสิทธิภาพ	50
3.5 ระบบ SSL (Secure Socket Layer)	51
บทที่ 4 การรักษาความปลอดภัยของเครือข่าย(Network Security)	
4.1 พื้นฐานของระบบเครือข่ายคอมพิวเตอร์	52
4.2 ภัยคุกคามที่มีต่อระบบเครือข่าย(Threats in Network)	53
4.3 การวิเคราะห์ความเสี่ยงด้านความปลอดภัยในระบบเครือข่าย (Security Threats Analysis)	55
4.4 การรักษาความปลอดภัยของข้อมูลในระบบเครือข่าย(Network Security)	60

	หน้าที่
Controls)	
4.5 การควบคุมการอนุญาตให้เข้ามาในระบบ(Access Control)	62
4.6 การตรวจสอบความถูกต้องระบบคอมพิวเตอร์ในระบบเครือข่าย (Authentication in Distributed System)	63
4.7 การป้องกันการรั่วไหลของข้อมูลจากการส่งข้อมูลผ่านระบบเครือข่าย (Traffic control)	66
4.8 การรักษาความถูกต้องของข้อมูลที่ถูกส่งผ่านระบบเครือข่าย (Data Integrity)	67
4.9 การใช้ Firewall ในการรักษาความปลอดภัยของระบบเครือข่าย	67
4.9.1 ชนิดของ Firewall	68
4.9.2 ตัวอย่างการใช้งานของ Firewall กับระบบ LAN	71
4.9.3 ข้อจำกัดของ Firewall	73
4.10 การรักษาความปลอดภัยกับอุปกรณ์อื่น ๆ ในเครือข่าย	74
4.11 ระบบรักษาความปลอดภัยแบบอื่น ๆ	76
บทที่ 5 สรุปผลและการประยุกต์ใช้	
5.1 สรุปผล	77
5.2 ความปลอดภัยในการซื้อสินค้าผ่านทางอินเทอร์เน็ต	81
5.3 ขั้นตอนการสร้างความปลอดภัยสำหรับพาณิชย์อิเล็กทรอนิกส์	85
บรรณานุกรม	95
ภาคผนวก ก ประมวลคำศัพท์	97
ประวัติผู้เขียน	103

สารบัญตาราง

ตาราง		หน้าที่
1	แสดงมูลค่าการค้าผ่านอินเทอร์เน็ตในอาเซียน	7
2	แสดงความแพร่หลายของการใช้อินเทอร์เน็ตในประเทศไทย (ปี ค.ศ. 2000-2005)	8
3	แสดงข้อดีและข้อเสียของกฎแฉทั้งสองประเภท	17
4	แสดงข้อมูลเพิ่มเติมของกฎแฉทั้งสองประเภท	18
5	แสดงความหมายของรูปแบบของการรักษาความปลอดภัยแบบต่าง ๆ	39
6	แสดงข้อดีข้อเสียของระบบ SET	51
7	แสดงข้อดีข้อเสียของระบบ SSL	51
8	แสดงข้อมูลเปรียบเทียบระหว่าง Screening Router, Proxy Gateway, Guard	71

สารบัญภาพ

รูป		หน้า
1	แสดงรายได้ (อัตราการใช้โทร) ของพาณิชย์อิเล็กทรอนิกส์ผ่านเครือข่ายอินเทอร์เน็ต ปี 1996 – 2002	6
2	ขั้นตอนการชำระเงินผ่านอินเทอร์เน็ต	12
3	แสดงระบบการเข้ารหัส แบบกุญแจสมมาตร	15
4	แสดงระบบการเข้ารหัส แบบกุญแจอสมมาตร	16
5	แสดงพื้นฐานการเข้ารหัสและถอดรหัสข้อมูล	21
6	แสดงการแทนค่าตัวอักษรโดยการใช้สัญลักษณ์อื่น	22
7	แสดงการแทนค่าตัวอักษรโดยการใช้วิธีการเลื่อนค่า	22
8	แสดงการเข้ารหัสข้อมูลแบบทีละตัว	23
9	แสดงการเข้ารหัสแบบ Secret Key Encryption	26
10	แสดงการเข้ารหัสแบบ Public Key Encryption	27
11	แสดงการเข้ารหัสข้อมูลแบบ DES	28
12	แสดงการแจกกุญแจรหัสให้กับเครื่องต่าง ๆ ในระบบเครือข่าย	32
13	แสดงองค์กรออกใบรับรองและการบริการด้านต่าง ๆ	42
14	แสดงระบบการทำงานของ SET	47
15	แสดงรูปแบบของเครือข่ายคอมพิวเตอร์	54
16	แสดงการส่งผ่านข้อมูล โดยวิธี Link Encryption	60
17	แสดงการส่งผ่านข้อมูล โดยวิธี End-To-End Encryption	61
18	แสดงระบบ Kerberos	64
19	แสดงการทำงานของ Screening Router	68
20	แสดงการทำงานของ Proxy Gateway	70
21	แสดงการทำงานของ Firewall กับระบบ LAN	71
22	แสดงการใช้ Proxy Gateway มาทำเป็น Firewall	72
23	แสดงการสร้างกุญแจใน Windows	87
24	แสดง CDR	89

รูป		หน้า
25	แสดงใบรับรองที่จะนำมาติดตั้งในเซิร์ฟเวอร์	90
26	แสดงการติดตั้ง Key Certificate	91
27	แสดงขั้นตอนการชำระเงินตามโปรโตคอล SET	92