การเพิ่มประสิทธิภาพการเข้ารหัสของกองทัพบกไทย

PERFORMANCE ENHANCEMENT OF THE ENCRYPTION SYSTEM IN THE ROYAL THAI ARMY

พันตรี นรเศรษฐ์ พงษ์เจริญ

MAJ.NORASED PONGJAROEN

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต

สาขาวิชาวิทยาการคอมพิวเตอร์และเทคโนโลยีสารสนเทศ

บัณฑิตวิทยาลัย

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ.2541

ISBN 974-622-183-3

PERFORMANCE ENHANCEMENT OF THE ENCRYPTION SYSTEM IN THE ROYAL THAI ARMY

NORASED PONGJAROEN

A THESIS SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENT FOR THE DEGREE

MASTER OF SCIENCE IN COMPUTER SCIENCE AND INFORMATION TECHNOLOGY

SCHOOL OF GRADUATE STUDIES

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

1998

ISBN 974-622-183-3

หัวข้อวิทยานิพนธ์	การเพิ่มประสิทธิภาพการเข้ารหัสของกองทัพบกไทย
นักศึกษา	พันตรี นรเศรษฐ์ พงษ์เจริญ
อาจารย์ผู้ควบคุมวิทยานิพนธ์	รองศาสตราจารย์ ภัคคินี ชิตสกุล
ระดับการศึกษา	วิทยาศาสตรมหาบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์และเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
พ.ศ.	2541

บทคัดย่อ

ในการปฏิบัติภารกิจทางทหารของกองทัพบกไทย มีองค์ประกอบหลักที่สำคัญ 4 ประการ คือ การบังคับบัญชา (Command) การควบคุม (Control) การติดต่อสื่อสาร (Communication) และการข่าวกรอง (Intelligence) ซึ่งรู้จักกันโดยทั่วไปในวงการข่าวกรองทางทหารว่า C^3I การที่ภารกิจจะสามารถสำเร็จลุล่วงไปได้ในแต่ละสถานการณ์ จำเป็นที่จะต้องมีความพร้อมด้าน C^3I ทั้งนี้ การสื่อสารเป็นองค์ประกอบที่สำคัญยิ่ง ใน C^3I

การส่งข่าวทางยุทธวิธีของกองทัพบกไทย โดยเฉพาะอย่างยิ่งข่าวที่มีชั้นความลับสูงจำเป็นต้องทำการเข้ารหัสเสียก่อน ปัจจุบันการเข้ารหัสกระทำด้วยมือโดยใช้วิธีการเข้ารหัสที่ไม่ซับซ้อน ทำให้ง่ายต่อการถูกลอบถอดรหัส ด้วยเหตุผลข้างต้นการวิจัยนี้จึงได้พยายามคิดค้นวิธีที่จะปรับปรุงพัฒนาการเข้า-ถอดรหัส รวมทั้งการรับ-ส่งข่าวเข้ารหัสให้มีประสิทธิภาพ ทำงานได้อย่างรวดเร็ว ถูกต้อง และมีความซับซ้อนมากขึ้น ด้วยการนำระบบคอมพิวเตอร์ทันสมัยในปัจจุบันมาประยุกต์ ดัดแปลง เพื่อเพิ่มประสิทธิภาพและสมรรถนะการเข้า-ถอดรหัส ตลอดจนการรับ-ส่งข่าวเข้ารหัสของกองทัพบกไทย อันจะเป็นประโยชน์อย่างยิ่งในในการป้องกันประเทศ และการรักษาความมั่นคง

Thesis Title	Performance Enhancement of the Encryption System in the Royal Thai Army
Student	Major Norased Pongjaroen
Thesis Advisor	Associate Professor Pakkinee Chitsakul
Level of Study	Master of Science in Computer Science and Information Technology King Mongkut's Institute of Technology Ladkrabang
Year	1998

ABSTRACT

In carrying out military duties and missions of the Royal Thai Army, four principal factors are involved. They are Command, Control, Communication and Intelligence or commonly known in the military circle as "C^3I". In any given situation, the readiness in "C^3I" will determine the success of military mission. Among the three "C"s and the one "I", it is generally agreed that Communication is, indeed, a single very important factor.

For the Royal Thai Army, the communications of strategically important messages, especially the ones with higher classification, have the need to undergo encryption process. Currently, the encryption procedure used by the Royal Thai Army is done manually, using encryption system that is not complicate. This makes communication vulnerable to attacks.

Due to the above reasons, this research attempts to find the means by which the encryption capability of the Royal Thai Army, as well as the way encrypted messages are send and received, can be improved and enhanced. The improvement and enhancement attempted by this research will adapt and apply existing modern computer technology. As a result, the improved encryption model will not only allow a higher performance and a greater degree of accuracy, but also a more complicate encryption system. This is done with a view to increasing the capability of the Royal Thai Army in message encryption and decryption as well as in sending and receiving the encrypted messages, which will be of great use for the security and defense of Thailand.

กิตติกรรมประกาศ

ผู้เขียนขอขอบคุณรองศาสตราจารย์ภัคคินี ชิตสกุล ที่กรุณาสละเวลาให้คำปรึกษาและคำแนะนำในการวิจัย จนสำเร็จลุล่วงได้ด้วยดี

นอกจากนี้ ผู้เขียนยังใคร่ขอขอบคุณ พันเอก ขราวุธ เขมะโยธิน ผู้อำนวยการกองวิทยาการ กรมการทหารสื่อสาร ที่เอื้อเฟื้อเอกสารและข้อมูลประกอบการวิจัย รวมทั้งข้าราชการในกรมการทหารสื่อสารทุกนาย โดยเฉพาะอย่างยิ่งเพื่อนร่วมงานของผู้เขียนในกองวิทยาการที่ได้ให้ความร่วมมือเป็นอย่างดี และขอขอบคุณเจ้าหน้าที่ฝึกร่วมของหน่วยทหารสื่อสารทั่วประเทศ ที่ได้ช่วยให้การทดสอบโปรแกรมสามารถดำเนินไปได้อย่างราบรื่น

ในการทำวิจัยนี้ ผู้เขียนขอขอบคุณนาวาตรี ชัชวาล ชาติไทย ซึ่งเป็นเพื่อนผู้ให้กำลังใจและการสนับสนุนเป็นอย่างดียิ่ง

ท้ายที่สุด ผู้เขียนขอขอบคุณสมาชิกในครอบครัวทุกคนที่ช่วยเหลือและให้กำลังใจจนการวิจัยนี้สำเร็จลุล่วงลงได้

นรเศรษฐ์ พงษ์เจริญ

สารบัญ

สารบัญ (ต่อ)

บทที่ หน้า

สารบัญ (ต่อ)

บทที่ หน้า

สารบัญตาราง

ตารางที่ หน้า

สารบัญภาพ

หน้า

สารบัญภาพ (ต่อ)

หน้า

สารบัญภาพ (ต่อ)

หน้า

คำศัพท์เฉพาะ

ศูนย์การสื่อสาร	:	หน่วยงานที่ทำหน้าที่ในการรับส่งข่าวของทางทหารในสภาวะการทางยุทธวิธี
ลำดับความเร่งด่วน	:	ความรวดเร็วที่ข่าวนั้นจะต้องถึงผู้รับ ปลายทาง แบ่งออกเป็นปกติ ด่วน ด่วนมาก และ ด่วนที่สุด
ลำดับความลับ	:	การกำหนดบุคคลที่สามารถเข้าถึงข่าวได้ โดยใช้พื้นฐานความจำเป็นต้องรู้ (needs to know) เป็นเกณฑ์ แบ่งเป็นลำดับ ดังนี้ เปิดเผย ปกปิด ลับ ลับมาก และ ลับที่สุด
ตอนอักษรลับ	:	หน่วยงานซึ่งทำหน้าที่เข้า-ถอดรหัสข่าว ประจำอยู่ในศูนย์การสื่อสาร
ตอนเครื่องมือ	:	หน่วยงานซึ่งทำหน้าที่รับส่ง-ข่าวด้วยเครื่องมือสื่อสารที่มีอยู่
มัชฌิมการสื่อสาร	:	ช่องทาง หรือ ตัวกลางที่ใช้ในการติดต่อสื่อสาร อาทิ พลนำสารสัตว์นำสาร เสียง โทรศัพท์ วิทยุ ทัศนะสัญญาณ เป็นต้น
กระดาษเขียนข่าว	:	แบบฟอร์มที่กำหนดให้ใช้ในการเขียนเนื้อข่าว เพื่อส่งไปผ่านกระบวนการรับ-ส่ง กระดาษเขียนข่าวประกอบด้วยส่วนต่าง ๆ เช่น ชื่อผู้ส่ง ชื่อผู้รับ วันเวลาที่ส่งข่าว ฯลฯ
ชุดวิทยุถ่านทอดสนาม	:	วิทยุ FM ซึ่งใช้เชื่อมการติดต่อสื่อสารทางโทรศัพท์
Cipher	:	รหัส
Encryption	:	การเข้ารหัส
Decryption	:	การถอดรหัส
Plain Text	:	ข่าวกระจ่าง
Cipher Text	:	ข่าวเข้ารหัส
Authentication	:	การพิสูจน์ทราบ
Digital Signature	:	ลายเซ็นดิจิตอล
Digital Finger Print	:	ลายนิ้วมือดิจิตอล
Digital Envelope	:	ซองจดหมายดิจิตอล
Electronic Mail (E-mail	:	ไปรษณีย์อีเล็คโทรนิคส์

สารบัญภาพ (ต่อ)

หน้า

บทที่ 1
บทนำ

1.1 ความเป็นมา

ในการรบ การติดต่อสื่อสารถือเป็นเรื่องจำเป็น และสำคัญมาก ถึงแม้ว่ากำลังพลจะมีประสิทธิภาพเพียงใด ผ่านการฝึกซ้อมมาอย่างไร อาวุธยุทโธปกรณ์จะดีแค่ไหน ผู้บังคับบัญชาก็ไม่สามารถนำมาใช้ประโยชน์ให้เกิดประสิทธิภาพในการรบได้ ถ้าขาดการควบคุมบังคับบัญชาและการติดต่อสื่อสาร

ปัจจุบันกองทัพบก มีหน่วยงานที่ทำหน้าที่สนับสนุนทางด้านการติดต่อสื่อสารคือ กรมการทหารสื่อสารในระดับกองทัพบก และกองพันทหารสื่อสารในระดับ กองทัพภาค และกองพล

ในการติดต่อสื่อสารระหว่างกันนั้น การรักษาความปลอดภัยทางการสื่อสารถือเป็นเรื่องสำคัญ เพราะถ้าข้าศึกทราบถึงข่าวที่ส่งถึงกัน ข้าศึกจะนำข่าวนั้นไปใช้ประโยชน์ทางยุทธวิธี เช่น กำหนดวันเวลาและสถานที่ซึ่งจะมีการเข้าโจมตี ถึงแม้จะเป็นข่าวทางธุรการ เช่น ข่าวของการส่งเสื้อผ้าหรืออาหาร ข้าศึกจะสามารถนำไปประเมินได้ว่าฝ่ายเรามีกำลังพลเท่าใด

ปัจจุบันกองทัพบกใช้วิธีการเข้ารหัสด้วยมือ โดยเจ้าหน้าที่ ซึ่งทำให้เกิดปัญหาความล่าช้าและความผิดพลาดในการปฏิบัติงานของเจ้าหน้าที่ ส่วนเครื่องมือเข้ารหัสที่มีขายอยู่โดยทั่วไปก็มีราคาแพง ไม่มีการเปิดเผยเทคโนโลยี และมีกฎหมายของประเทศผู้ผลิตควบคุมอยู่ การจัดซื้อจัดหาจึงกระทำได้ยาก นอกจากนี้ ยังมีปัญหาเรื่องความเข้ากันไม่ได้ของเครื่องมือแต่ละรุ่น หรือแต่ละชนิด และฝ่ายตรงข้ามก็สามารถหาซื้อเครื่องมือชนิดเดียวกันได้ อันจะทำให้เกิดจุดอ่อนด้านความปลอดภัยและความมั่นคง

ฉะนั้นจากเหตุผลข้างต้น ผู้บังคับบัญชาระดับสูงจึงมีแนวความคิดว่ากองทัพบกควรวิจัยพัฒนาการเข้ารหัสข่าวของตนเอง เพื่อเป็นการรักษาความลับในการสื่อสาร ทั้งยังช่วยประหยัดงบประมาณของชาติ

1.2 วัตถุประสงค์

การวิจัยนี้มีวัตถุประสงค์ที่จะเพิ่มประสิทธิภาพของการรับ-ส่งข่าวด้วยวิธีการเข้ารหัส โดยนำคอมพิวเตอร์ที่มีอยู่ทั่วไปในกองทัพบกมาใช้ทดแทนเครื่องเข้า-ถอดรหัสที่มีราคาสูงและปรับปรุงให้มีความทันสมัยยิ่งขึ้นด้วยการพัฒนาโปรแกรมและการทำงานของระบบ เพื่อลดเวลาที่ใช้ในการ

เข้า-ถอดรหัสลง เพิ่มความถูกต้องแม่นยำในการทำงาน เพิ่มประสิทธิภาพและความซับซ้อนของการเข้ารหัสเพื่อการรักษาความปลอดภัยที่สูงขึ้น ลดกำลังพลที่ปฏิบัติงาน และประหยัดงบประมาณของชาติโดยไม่ต้องซื้ออุปกรณ์เข้า-ถอดรหัสที่มีราคาสูงจากต่างประเทศ ซึ่งสอดคล้องกับนโยบายการพัฒนากองทัพบกและการพัฒนาประเทศ

1.3 ขอบเขตการวิจัย

เริ่มตั้งแต่รับข้อมูลข่าวที่ต้องการจะส่งซึ่งอยู่ในรูปของแฟ้มข้อมูล นำมาผ่านกรรมวิธีเข้ารหัสได้เป็นแฟ้มข้อมูลเข้ารหัส และนำแฟ้มข้อมูลที่เข้ารหัสแล้วมาผ่านกรรมวิธีถอดรหัสได้เป็นแฟ้มข้อมูลข่าวต้นฉบับ

1.4 วิธีการวิจัย

การวิจัยเป็นแบบพรรณาและการโปรแกรมเพื่อปรับปรุงให้ประสิทธิภาพให้ดีขึ้น ในการออกแบบระบบเข้า-ถอดรหัสที่นำเสนอใหม่อาศัยพื้นฐานจากทฤษฎีและวิธีการเข้า-ถอดรหัสที่ได้รับการยอมรับเป็นมาตราฐานสากลว่ามีความปลอดภัยสูง เชื่อถือได้ ผ่านการพิสูจน์มาเป็นระยะเวลานานพอสมควร และสามารถนำมาใช้ได้โดยไม่ผิดกฎหมาย

ระบบเข้า-ถอดรหัสที่นำเสนอใหม่นี้ ได้นำการเข้ารหัสหลายวิธีมาประยุกต์ใช้ร่วมกันเพื่อเสริมข้อดีและลบข้อบกพร่องซึ่งกันและกัน อันจะทำให้การทำงานมีประสิทธิภาพและมีการรักษาความปลอดภัยมากขึ้น

1.5 ประโยชน์ที่ได้รับจากการวิจัย

ประโยชน์ที่ได้รับจากการวิจัยมีดังนี้

1.5.1 ช่วยลดเวลาในการเข้าและถอดรหัส

1.5.2 เพิ่มความปลอดภัยให้แก่ข่าวเข้ารหัสทำให้ข้าศึกไม่สามารถลักลอบถอดรหัสได้

1.5.3 เป็นแนวทางในการที่จะปรับปรุงและพัฒนาระบบการเข้าถอดรหัสที่ใช้อยู่ในกองทัพบกไทย ให้มีความทันสมัยอย่างต่อเนื่องต่อไป

บทที่ 2
วรรณกรรมและทฤษฎีที่เกี่ยวข้อง

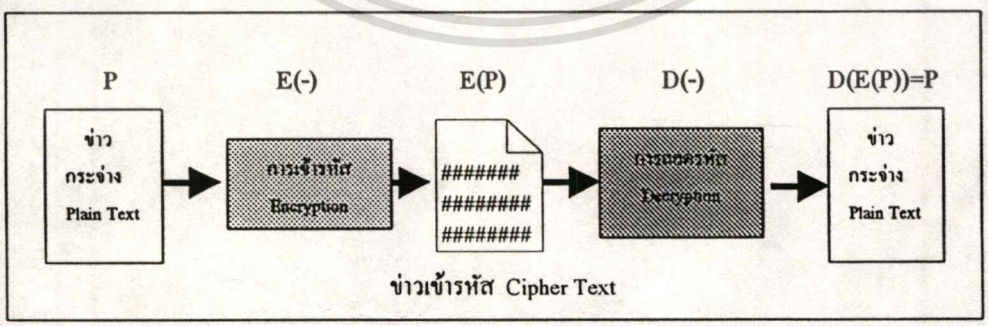
2.1 การเข้า และ ถอดรหัส

ในบทนี้ จะกล่าวถึงความรู้เบื้องต้นเกี่ยวกับการเข้า-ถอดรหัส โดยจะอธิบายว่าการเข้า-ถอดรหัสคืออะไร มีความมุ่งหมายอย่างไร และมีความสำคัญอย่างไรโดยเฉพาะอย่างยิ่งต่อการปฏิบัติการทางทหาร นอกจากนี้ ยังจะอธิบายถึงการเข้า-ถอดรหัสแบบต่างๆ ที่ใช้เป็นพื้นฐานของการวิจัย และแนวคิดเกี่ยวกับลายเซ็นดิจิตอล (Digital Signature)

2.1.1 การเข้า-ถอดรหัสคืออะไร

โดยทั่วไปการเข้า-ถอดรหัสหมายถึงการแปลงข่าวสารข้อมูลจากรูปแบบหนึ่งไปเป็นอีกรูปแบบหนึ่ง โดยมีวิธีที่สามารถทำให้กลับเป็นรูปแบบเดิมได้ ในภาษาอังกฤษการเข้ารหัสสามารถใช้ได้ 2 คำ คือคำว่า Encode หรือ Encrypt แต่คำว่า Encode หมายถึงการเข้ารหัสโดยทั่วๆ ไป ส่วนคำว่า Encrypt หมายถึงการเข้ารหัสที่มีวัตถุประสงค์เพื่อรักษาความลับ สำหรับการถอดรหัสใช้คำว่า Decode หรือ Decrypt

ในการวิจัยนี้จะกล่าวถึงการเข้ารหัสสำหรับการส่งข่าวทางการทหาร ซึ่งภาษาอังกฤษใช้คำว่า Encryption[1] การเข้า-ถอดรหัสทำงานด้วยการแปลงข้อมูลจากเอกสารธรรมดา หรือข่าวกระจ่าง (Plain Text) ด้วยการเข้ารหัส (Encryption) เพื่อเปลี่ยนไปเป็นข้อมูลอีกชนิดหนึ่งที่เรียกว่าเอกสารเข้ารหัส (Cipher Text) โดยใช้การทำงานทางคณิตศาสตร์และใช้ กุญแจ (Key) ในการเข้ารหัส ส่วนการถอดรหัส (Decryption) จะกระทำด้วยวิธีกลับกัน (ภาพที่ 1)



ภาพที่ 1 การเข้ารหัส และ การถอดรหัส

---

[1] James Arlin Cooper, Computer and Communications Security : Strategies for the 1990's (McGraw-Hill Book Company, 1989), P. 355.

ระบบการเข้า-ถอดรหัสที่มีการใช้อยู่ในปัจจุบันสามารถจำแนกอย่างกว้างๆ ได้เป็น 2 ระบบ[2] คือ

2.1.1.1 ระบบเข้า-ถอดรหัสที่ใช้กุญแจเพียงกุญแจเดียวสำหรับทั้งการเข้าและการถอดรหัส ระบบนี้เรียกว่าการเข้ารหัสแบบกุญแจเดียว หรือการเข้ารหัสแบบกุญแจลับ (Synchronous or Secret Key) ได้แก่ รหัสเดส (Data Encryption Standard-DES)

2.1.1.2 ระบบการเข้า-ถอดรหัสที่ใช้กุญแจมากกว่าหนึ่ง คือ กุญแจที่ใช้ในการเข้ารหัสและกุญแจที่ใช้ในการถอดรหัสเป็นกุญแจที่ต่างกัน ระบบนี้เรียกว่าการเข้ารหัสแบบหลายกุญแจ หรือการเข้ารหัสแบบกุญแจสาธารณะ (Asynchronous or Public Key) ได้แก่ รหัสอาร์เอสเอ (RSA)

วิชาที่ว่าด้วยการคำนวณเกี่ยวกับการเข้ารหัสและการวิเคราะห์รหัสเรียกว่าวิชารหัสวิทยา หรือ Cryptology ผู้ที่เชี่ยวชาญในแขนงวิชานี้เรียกว่านักรหัสวิทยา หรือ Cryptologist วิชาที่ว่าด้วยศาสตร์และศิลป์ในการเข้ารหัสเรียกว่าวิชาการเข้ารหัส หรือ Cryptography ส่วนวิชาที่ว่าด้วยศาสตร์และศิลป์ในการถอดรหัสของผู้อื่นเรียกว่าวิชาวิเคราะห์รหัส หรือ Cryptanalysis และผู้ชำนาญการถอดรหัสของผู้อื่นเรียกว่านักวิเคราะห์รหัส หรือ Cryptanalist

2.1.2 วัตถุประสงค์ของการเข้ารหัส

การเข้า-ถอดรหัสมิได้มีความมุ่งหมายเพื่อรักษาความลับอย่างเดียว[3] แต่สามารถใช้เพื่อวัตถุประสงค์อื่นๆ อีกได้ อาทิ

2.1.2.1 เพื่อให้สามารถส่งข่าวไปกับช่องทางการสื่อสารได้

2.1.2.2 เพื่อให้การส่งข่าวมีข้อผิดพลาดน้อยที่สุด

2.1.2.3 เพื่อให้พิสูจน์ทราบได้ว่าข่าวที่รับได้ผิดไปจากข่าวที่ส่งหรือไม่ รหัสชนิดนี้เรียกว่า Error Detecting Code

2.1.2.4 เพื่อให้สามารถแก้ไขข้อความของข่าวที่ได้รับในส่วนที่ผิดให้ถูกต้องได้ รหัสชนิดนี้เรียกว่า Error Correcting Code

2.1.2.5 เพื่อย่อข่าวสารข้อมูลให้สั้นลง เพื่อประหยัดเนื้อที่ในการเก็บหรือเวลาในการส่งข่าว

---

[2]Bruce Schneier, Applied Cryptography (John Wiley & Sons, Inc., 1994), P. 3.

[3]James Arlin Cooper, Computer and Communications Security : Strategies for the 1990's , P. 18.

2.1.3 การเข้ารหัสกับปฏิบัติการทางทหาร

องค์ประกอบที่สำคัญของปฏิบัติการทางทหาร คือ การบังคับบัญชา(Command) การควบคุม (Control) การติดต่อสื่อสาร (Communication) และ การข่าว (Intelligence) หรือ C^3I ซึ่งหากมีความบกพร่องที่องค์ประกอบส่วนใดส่วนหนึ่ง ก็ยากที่ปฏิบัติการทางทหารครั้งนั้นจะประสบความสำเร็จหรือได้รับชัยชนะ[4]

ในปฏิบัติการทางทหารนั้น การสื่อสารเป็นการประสานเชื่อมโยงทุกองค์ประกอบของระบบที่กล่าวถึงข้างต้นเข้าด้วยกันเพื่อให้สามารถปฏิบัติงานได้ การสื่อสารใช้ในการส่งคำสั่งจากหน่วยเหนือไปยังหน่วยรอง ส่งรายงานจากหน่วยรองกลับไปยังหน่วยเหนือ รวมทั้ง ประสานการปฏิบัติระหว่างหน่วยต่างๆ นอกจากนี้ การสื่อสารยังช่วยในการส่งข่าวและข่าวกรอง จากหน่วยที่ทำหน้าที่รวบรวมข่าวไปยังหน่วยเหนือ และกระจายข่าวและข่าวกรองที่ได้รับไปยังหน่วยต่างๆ ที่สามารถจะนำข่าวหรือข่าวกรองนั้นๆ ไปใช้ประโยชน์ได้

ด้วยเหตุนี้ นอกจากที่การติดต่อสื่อสารจะต้องสะดวกและรวดเร็วแล้ว ยังจะต้องมีการรักษาความปลอดภัยด้วยเพื่อป้องกันจากการดักรับของข้าศึก และหากข้าศึกสามารถดักรับการสื่อสารได้ก็ต้องมีมาตรการป้องกันมิให้ข้าศึกล่วงรู้ถึงเนื้อความของข่าวหรือข่าวกรองนั้นๆ ในทางกลับกันการติดต่อสื่อสารก็ต้องมีมาตรการที่จะป้องกันมิให้ข้าศึกส่งคำสั่งหรือข่าวสารปลอมมาได้ ทั้งนี้ การติดต่อสื่อสารไม่ว่าจะเป็นทางวิทยุ ทางสาย หรือการนำสาร ก็มีความเป็นไปได้เสมอว่าข้าศึกอาจจะดักรับการสื่อสาร และอาจสร้างข่าวสารหรือคำสั่งปลอมส่งมาลวงได้

การป้องกันมิให้ข้าศึกทราบข้อความในข่าวที่สื่อสาร สามารถกระทำได้ด้วยการนำข่าวมาเข้ารหัสก่อนที่จะส่งไปโดยการสื่อสาร และเมื่อถึงปลายทางจึงนำไปถอดรหัสออกมาเป็นข่าวกระจ่างต้นฉบับดังเดิม ในกรณีที่ข้าศึกสามารถดักรับการสื่อสารได้ ถ้าไม่รู้วิธีถอดรหัสก็ไม่สามารถแปลการสื่อสารที่รับออกมาเป็นข่าวที่เป็นประโยชน์ได้ ด้วยเหตุนี้ ปฏิบัติการทางทหารตั้งแต่อดีตจนถึงปัจจุบันจึงถือว่าเทคโนโลยีในการเข้า-ถอดรหัสมีความสำคัญอย่างยิ่ง และได้ปรากฏแล้วหลายครั้งในประวัติศาสตร์ว่าฝ่ายที่มีความเหนือกว่าในการเข้า-ถอดรหัส สามารถนำความเหนือกว่านี้ มาสร้างความได้เปรียบจนทำให้ได้รับชัยชนะในการรบได้ ทั้งที่มีความเสียเปรียบในด้านอื่นๆ หลายประการก็ตาม

ในระหว่างสงครามโลกครั้งที่สอง ฝ่ายสัมพันธมิตรมีอุปกรณ์และเทคโนโลยีในการเข้า-ถอดรหัส ที่มีสมรรถนะสูงมาก ทำให้สามารถรักษาความปลอดภัยในการติดต่อสื่อสารทาง

---

[4]U.S. Commander in Chief Pacific (USCINCPAC), "Military Intelligence", Report of Thailand/ U.S. Command and Control Interoperability Board Phuket, Thailand, 3-7 September 1997.

วิทยุระหว่างอังกฤษกับสหรัฐฯ ได้ แม้ว่าฝ่ายเยอรมันจะสามารถดักรับการสื่อสารได้แต่ก็ไม่สามารถถอดรหัสได้ ส่วนเยอรมันนั้นใช้อุปกรณ์เข้า-ถอดรหัสที่เรียกว่าเครื่องเอ็นนิกม่า (Enigma)[5] ฝ่ายเยอรมันมั่นใจว่าการเข้ารหัสด้วยเครื่องดังกล่าวมีความสลับซับซ้อนมากจนฝ่ายสัมพันธมิตรไม่สามารถถอดรหัสได้ แต่สิ่งที่เยอรมันไม่ทราบก็คือ การที่อังกฤษจัดตั้งกลุ่มผู้เชี่ยวชาญในการถอดรหัสขึ้น นำโดย อลัน ทูริ่ง (Alan Turing) เพื่อสร้างอุปกรณ์ถอดรหัสซึ่งมีหลักการทำงานคล้ายกับเครื่องคอมพิวเตอร์ และอุปกรณ์ดังกล่าวสามารถถอดรหัสเอ็นนิกม่าได้สำเร็จ ช่วยให้อังกฤษรู้แผนปฏิบัติการของเยอรมันได้ล่วงหน้า เป็นเหตุให้เยอรมันประสบความสูญเสียอย่างใหญ่หลวงหลายครั้ง ข้อเท็จจริงเกี่ยวกับการที่อังกฤษสามารถถอดรหัสเอ็นนิกม่าได้นี้ถูกเปิดเผยต่อสาธารณชนหลังจากที่สงครามโลกครั้งที่สองยุติลงไปแล้วกว่า 10 ปี

สำหรับญี่ปุ่นนั้นใช้การเข้ารหัสที่คล้ายกับรหัสเอ็นนิกม่าของเยอรมัน และมีความมั่นใจสูงว่าไม่มีผู้สามารถถอดรหัสของตนได้ ทั้งที่ความจริงแล้วสหรัฐฯ สามารถถอดรหัสของญี่ปุ่นได้ แม้เมื่อญี่ปุ่นส่งข่าวเข้ารหัสไปให้เอกอัครราชทูตของตนประกาศสงคราม ฝ่ายสหรัฐฯ ก็สามารถถอดรหัสข่าวดังกล่าวได้เสร็จก่อนสถานทูตญี่ปุ่นเสียอีก สหรัฐ ฯ ได้ใช้ประโยชน์จากการที่สามารถดักรับและถอดรหัสข่าวได้ โดยก่อให้เกิดความเสียหายแก่ญี่ปุ่นอย่างใหญ่หลวงในหลายๆ ครั้ง เช่น การโจมตีเรือประจัญบานยามาโต้ ที่ใหญ่ที่สุดของกองทัพเรือญี่ปุ่นจนจม การลอบสังหารพลเรือเอกยามาโมโต้แม่ทัพเรือญี่ปุ่น โดยสหรัฐ ฯ ดักรับและถอดรหัสข่าวการเดินทางทางเครื่องบินและส่งเครื่องบินขับไล่เข้าโจมตีขณะที่เครื่องบินร่อนลงซึ่งเป็นช่วงเวลาที่อันตรายที่สุด

เหตุการณ์ที่พลิกผันโฉมหน้าของสงครามโลกครั้งที่สอง ก็เป็นผลจากสมรรถนะในการถอดรหัสของสหรัฐฯ เช่นกัน ก่อนที่ญี่ปุ่นจะเข้าโจมตีฐานทัพบนเกาะมิดเวย์ สหรัฐฯ สามารถดักรับและถอดรหัสข่าวได้ทำให้รู้แผนปฏิบัติการของฝ่ายญี่ปุ่นล่วงหน้า และส่งเรือบรรทุกเครื่องบินที่มีอยู่เพียง 2 ลำ ไปรอได้ทันการณ์โดยที่ฝ่ายญี่ปุ่นไม่ทราบ สหรัฐฯ ยังค้นพบกองเรือของญี่ปุ่นได้ก่อนและส่งเครื่องบินทั้งหมดเข้าโจมตี ผลการรบครั้งนั้นทำให้สหรัฐฯ ได้รับชัยชนะในการรบทางทะเลอย่างเด็ดขาด แม้ว่าสหรัฐฯ จะเสียเปรียบทั้งด้านจำนวนเรือรบ เครื่องบิน และความชำนาญของนักบินก็ตาม ส่วนญี่ปุ่นต้องสูญเสียเรือบรรทุกเครื่องบินขนาดใหญ่ไป 4 ลำ ทำให้เสียความเป็นผู้นำในการรบทางทะเล และนำไปสู่การพ่ายแพ้สงครามในที่สุด

---

[5]Simson Garfinkel and Gene Spafford, Practical Unix Security (O'Rielly &Associates, Inc., 1993), P.54.

ปัจจุบันสมรรถนะในการเข้า-ถอดรหัสยิ่งทวีความสำคัญขึ้น เพราะปฏิบัติการทางทหารมิได้จำกัดอยู่แต่การสู้รบเต็มรูปแบบเท่านั้น แต่ยังรวมถึงปฏิบัติการอื่นๆ เช่น การหาข่าวกรอง และการต่อต้านการก่อการร้าย

ในการส่งเสริมการก่อการร้าย ทางการลิเบียใช้เครื่องเข้ารหัสที่ผลิตจากประเทศสวีเดนในการส่งคำสั่งไปให้ผู้ก่อการร้ายในยุโรปปฏิบัติการ การสื่อสารดังกล่าวถูกกองเรือของสหรัฐฯ ที่ปฏิบัติการในทะเลใกล้ประเทศลิเบียดักรับได้ ส่งผ่านดาวเทียมไปถอดรหัสที่กองบัญชาการและใช้เป็นหลักฐานในการพิสูจน์ว่าลิเบียพัวพันกับการก่อการร้ายระหว่างประเทศ

สำหรับประเทศไทยในการปราบปรามผู้ก่อการร้าย ในระยะแรกของปฏิบัติการหน่วยทหารของกองทัพบกส่งข่าวทางวิทยุโดยเข้ารหัสชั้นเดียวอย่างง่ายๆ ทำให้ถูกฝ่ายตรงข้ามดักรับและถอดรหัสได้ เป็นเหตุให้ได้รับความสูญเสียหลายครั้ง

จะเห็นได้ว่า การเข้าและถอดรหัสมีความสำคัญอย่างยิ่งต่อปฏิบัติการทางทหาร เทคโนโลยีในการเข้า-ถอดรหัสเป็นแสนยานุภาพทางการรบที่มองไม่เห็นตัวตน แต่ในหลายกรณีก็เป็นปัจจัยที่นำไปสู่ชัยชนะหรือความพ่ายแพ้ ด้วยเหตุนี้ประเทศที่มีบทบาทสำคัญทางทหาร อาทิ สหรัฐฯ รัสเซีย อังกฤษ ฝรั่งเศส อิสราเอล จึงถือว่าอุปกรณ์และเทคโนโลยีในการเข้า-ถอดรหัสเป็นยุทโธปกรณ์ประเภทหนึ่ง และมีกฎหมายควบคุมอย่างเข้มงวด

นอกจากนี้ หลายประเทศยังทุ่มเทงบประมาณจำนวนมหาศาลในการวิจัยและพัฒนาเครื่องเข้า-ถอดรหัสเพื่อรักษาความปลอดภัยด้านการข่าว และพยายามที่จะถอดรหัสของฝ่ายอื่นๆ ให้จงได้ โดยแต่ละประเทศต่างก็พยายามพัฒนาอุปกรณ์และเทคโนโลยีของตนเอง

เป็นที่ทราบในวงการข่าวกรองว่าแต่ละประเทศจะไม่ขายอุปกรณ์เข้า-ถอดรหัสที่มีความปลอดภัยสูง และจะขายแต่อุปกรณ์ซึ่งมีจุดอ่อน เพื่อให้ประเทศผู้ผลิตสามารถถอดรหัสได้โดยง่าย เช่น หลังสงครามโลกครั้งที่สองสหรัฐฯ ได้ขายเครื่องเข้าถอดรหัสที่คล้ายเครื่องเอ็นนิกม่าของเยอรมันให้กับหลายประเทศ โดยปิดเป็นความลับว่าสหรัฐฯ และอังกฤษ สามารถถอดรหัสได้ และปัจจุบันสหรัฐฯ มีกฎหมายควบคุมการส่งออกอุปกรณ์และโปรแกรมคอมพิวเตอร์สำหรับการเข้า-ถอดรหัสที่เข้มงวดมาก เครื่องเข้ารหัสที่สหรัฐฯ อนุญาตให้ขายไปยังต่างประเทศได้จะมีการเข้ารหัสที่มีจุดอ่อน ซึ่งหน่วยรักษาความปลอดภัยของสหรัฐฯ สามารถถอดรหัสได้

2.1.4 จำเป็นต้องเก็บกรรมวิธีเข้า-ถอดรหัสเป็นความลับหรือไม่

ในอดีตเทคโนโลยีการเข้า-ถอดรหัสเป็นที่รู้กันเฉพาะภายในหน่วยงานด้านการ

รักษาความปลอดภัยระดับชาติซึ่งมีหน้าที่ในการเข้ารหัสและถอดรหัสโดยตรง มีบุคคลภายนอกน้อยมากที่มีความรู้ด้านนี้ ดังนั้น หนังสือและตำราเกี่ยวกับวิชานี้จึงหาได้ยาก หรือหากมี หน่วยงานของรัฐบาลก็มักกำหนดให้เป็นเอกสารลับ

อย่างไรก็ดี ในช่วง 2 ทศวรรษที่ผ่านมามีการเปลี่ยนแปลงในโลกอย่างมากมาย เทคโนโลยีและโลกาภิวัติได้นำโลกไปสู่ยุคเทคโนโลยีสารสนเทศ ทำให้สามารถนำการเข้า-ถอดรหัสมาใช้ประโยชน์ในเชิงพาณิชย์ได้ คอมพิวเตอร์ที่ใช้เพื่อการนำข้อมูลข่าวสารมาดำเนินกรรมวิธีหาได้ง่าย ราคาถูก และมีสมรรถนะสูงขึ้น การเข้า-ถอดรหัสจึงเริ่มมีผู้ศึกษาค้นคว้ากันโดยเปิดเผยและกว้างขวางขึ้นมีหนังสือตำราเกี่ยวกับเรื่องนี้มากขึ้น

นอกจากที่เทคโนโลยีในปัจจุบันจะทำให้อุปกรณ์เข้า-ถอดรหัสแบบที่มีการรักษาความปลอดภัยสูงมีใช้อย่างแพร่หลายขึ้นแล้ว เทคโนโลยียังช่วยให้สร้างโปรแกรมเข้า-ถอดรหัสซึ่งจะทำให้คอมพิวเตอร์ที่ราคาแพงกลายเป็นอุปกรณ์เข้า-ถอดที่มีสมรรถนะสูงได้ ดังนั้น การรักษากรรมวิธีการเข้ารหัสเป็นความลับจึงทำได้ยาก

สำหรับกองทัพบก การเข้า-ถอดรหัสจำเป็นต้องมีผู้ที่รู้กรรมวิธีมากกว่า 1 คน และคนใดคนหนึ่งในจำนวนนี้อาจนำความลับไปเปิดเผยได้ นอกจากนี้ จำนวนของเครื่องเข้า-ถอดรหัสก็ต้องมีเป็นจำนวนมาก และบ่อยครั้งที่ต้องนำไปใช้ในพื้นที่ของฝ่ายตรงข้ามทำให้เกิดความเสี่ยงสูงว่าอาจจะถูกยึดแล้วนำไปวิเคราะห์การเข้า-ถอดรหัสได้

ด้วยเหตุผลต่างๆ ข้างต้นในปัจจุบันจึงไม่นิยมใช้เครื่องเข้า-ถอดรหัสแบบที่ต้องเก็บกรรมวิธีเป็นความลับ และนักรหัสวิทยาก็นิยมเปิดเผยกรรมวิธีการเข้ารหัสแบบใหม่ๆ ที่คิดค้นได้ให้สาธารณชนทราบ เพื่อเปิดโอกาสให้นักวิเคราะห์รหัสช่วยวิเคราะห์หาจุดอ่อน หากไม่มีผู้ค้นพบจุดอ่อนได้ก็ยิ่งเพิ่มความมั่นใจในการรักษาความปลอดภัยของกรรมวิธีเข้า-ถอดรหัสนั้นๆ แต่หากพบว่ามีจุดอ่อนก็สามารถแก้ไข ปรับปรุง หรือยกเลิกได้

2.2 ระบบและกรรมวิธีเข้า-ถอดรหัส ซึ่งเป็นพื้นฐานของการวิจัย

การวิจัยนี้ได้นำกรรมวิธีการเข้ารหัสที่เป็นที่นิยมและมีความน่าเชื่อถือมาศึกษาถึงข้อดีและข้อบกพร่อง ก่อนจะนำมาประยุกต์เข้าด้วยกัน และใช้เป็นพื้นฐานในการพัฒนาการเข้า-ถอดรหัสที่นำเสนอใหม่ ดังนี้

2.2.1 การเข้ารหัสแบบกุญแจลับ (Secret-key Cryptography)

เมื่อมีการเปิดเผยกรรมวิธีเข้า-ถอดรหัสแล้ว การรักษาความปลอดภัยของข้อมูลข่าวสารสามารถกระทำได้ด้วยการใช้กุญแจลับ (Secret Key)[6] ในการนี้ กุญแจรหัสมักเป็นตัวเลขจำนวนมากทำให้ยากต่อการคาดเดาค่าที่เป็นไปได้ของกุญแจรหัสได้ เช่น กุญแจรหัสที่เป็นตัวเลข 56 บิทจะมีค่าของกุญแจที่เป็นไปได้ เท่ากับ 2^{56} คือมีค่าได้ตั้งแต่เลข 0 ถึงเลข 72,057,594,037,227,936 หากฝ่ายตรงข้ามรู้ค่าของกุญแจรหัสจะถอดรหัสได้เฉพาะข่าวที่ใช้กุญแจนั้นๆ เข้ารหัส แต่ไม่สามารถถอดรหัสข่าวที่ใช้กุญแจอื่นเข้ารหัสได้ (ภาพที่ 2)

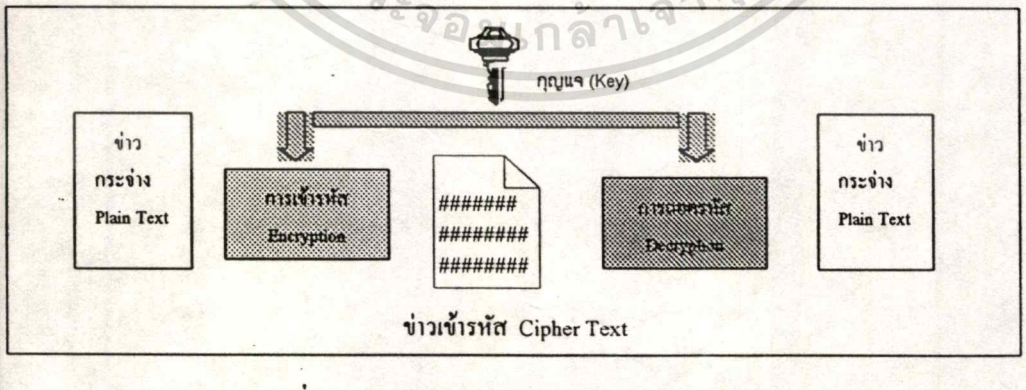
การเข้ารหัสแบบนี้เรียกว่า การเข้ารหัสแบบสมมาตร (Symmetric Cryptography) เพราะใช้กุญแจเดียวกันในการเข้าและการถอดรหัส หรือเรียกอีกอย่างหนึ่งว่า การเข้ารหัสแบบกุญแจลับ (Secret-key Cryptography) เพราะต้องเก็บค่าของกุญแจรหัสเป็นความลับ

การเข้ารหัสแบบกุญแจลับก็มีข้อบกพร่อง คือ

2.2.1.1 มีความยุ่งยาก ในการจัดการกุญแจ (Key Management) เนื่องจากในระบบกุญแจลับผู้ส่งกับผู้รับใช้กุญแจเดียวกันในการเข้าและถอดรหัส ทำให้ต้องมีการเปลี่ยนกุญแจรหัสบ่อยครั้ง ซึ่งต้องมีการนัดหมายล่วงหน้าว่าจะเปลี่ยนกุญแจเมื่อใด และเปลี่ยนเป็นกุญแจใด การนัดหมายนี้จะต้องใช้ช่องทางติดต่อทางอื่นหรือบางครั้งอาจต้องนำส่งกุญแจโดยผู้นำสาร

2.2.1.2 ต้องใช้กุญแจในการสื่อสารเป็นจำนวนมาก การใช้กุญแจเดียวกันหมดจะทำให้ผู้ส่งข่าวแต่ละคนใดคนหนึ่งสามารถถอดรหัสได้ทุกข่าว ทำให้การรักษาความปลอดภัยลดลง

2.2.1.3 การที่ผู้ส่งและผู้รับใช้กุญแจรหัสเดียวกัน ทำให้มีผู้ทราบค่าของกุญแจมากกว่า 1 คน เป็นการเพิ่มโอกาสที่ความลับจะรั่วไหล



ภาพที่ 2 การเข้ารหัสและถอดรหัสแบบกุญแจลับ

---

[6] Bruce Schneier, E-mail Security : How to Keep Your Electronic Messages Private (John Wiley & Sons, Inc.,1995), P. 75-77.

2.2.2 การเข้ารหัสแบบกุญแจสาธารณะ (Public- key Cryptography)

การเข้ารหัสระบบกุญแจสาธารณะใช้กรรมวิธีแบบเดียวกับการเข้ารหัสแบบกุญแจลับ แต่กุญแจที่ใช้ในการเข้ารหัสต่างจากกุญแจรหัสที่ใช้ในการถอดรหัส ผู้ที่คิดค้นการเข้ารหัสแบบนี้มี 2 กลุ่ม คือ ราล์ฟ เมอร์เคิล (Ralph Merkel) และอีกกลุ่มหนึ่งคือ วิทฟิลด์ ดิฟฟี่ (Whitfield Diffie) ซึ่งร่วมมือกับ มาร์ติน เฮลแมน (Martin Hellman) ทั้งสองกลุ่มแยกกันทำการวิจัยแต่ประสบผลสำเร็จในปีเดียวกันคือ ค.ศ. 1976อย่างไรก็ดี องค์การรักษาความปลอดภัยแห่งชาติของสหรัฐฯ (National Security Agency – NSA) อ้างว่าคิดค้นการเข้ารหัสแบบนี้ได้สิบปีก่อนหน้าทั้งสองกลุ่ม แต่ NSA ไม่แสดงหลักฐานเพื่อพิสูจน์[7]

การเข้ารหัสแบบนี้ในทางปฏิบัติจะมีกุญแจรหัส 2 กุญแจ กุญแจหนึ่งเรียกว่ากุญแจสาธารณะ (Public Key) เพราะเป็นกุญแจที่เปิดเผยไม่จำเป็นต้องเก็บเป็นความลับ ผู้ที่รู้กุญแจรหัสสามารถเข้า-ถอดรหัสข่าวได้ทุกคน ส่วนอีกกุญแจหนึ่งเรียกว่ากุญแจส่วนตัว (Private Key) เก็บเป็นความลับรู้เฉพาะเจ้าของกุญแจเท่านั้น ทำให้มีเพียงเจ้าของกุญแจผู้เดียวเท่านั้นที่สามารถถอดรหัสได้ การเข้ารหัสแบบนี้ จึงเรียกว่า การเข้ารหัสแบบกุญแจสาธารณะ (Public Key Cryptography) หรือ การเข้ารหัสแบบอสมมาตร (Asymmetric Cryptography) (ภาพที่ 3)

คุณสมบัติเด่นของการเข้ารหัสแบบนี้ คือผู้ที่รู้กุญแจสำหรับเข้ารหัสสามารถเข้ารหัสได้แต่ถอดรหัสไม่ได้ ส่วนผู้ที่รู้กุญแจสำหรับถอดรหัสก็สามารถถอดรหัสได้แต่เข้ารหัสไม่ได้ และกุญแจสำหรับเข้ารหัสกับกุญแจสำหรับการถอดรหัสยังสามารถใช้สลับหน้าที่กันได้ ซึ่งเป็นการเพิ่มประโยชน์ในการใช้งาน นอกจากนี้ เจ้าของกุญแจยังใช้กุญแจส่วนตัวเข้ารหัสข่าวส่งไปให้ผู้รู้กุญแจสาธารณะได้ทุกคน และเมื่อถอดรหัสข่าวได้ผู้รับยังทราบได้ด้วยว่าผู้ส่งข่าวคือใครเพราะกุญแจส่วนตัวแต่ละกุญแจมีเจ้าของกุญแจเพียงผู้เดียวเท่านั้นที่รู้

การเข้ารหัสแบบกุญแจสาธารณะมีจุดเด่นที่แก้ข้อเสียของระบบกุญแจลับได้ คือ

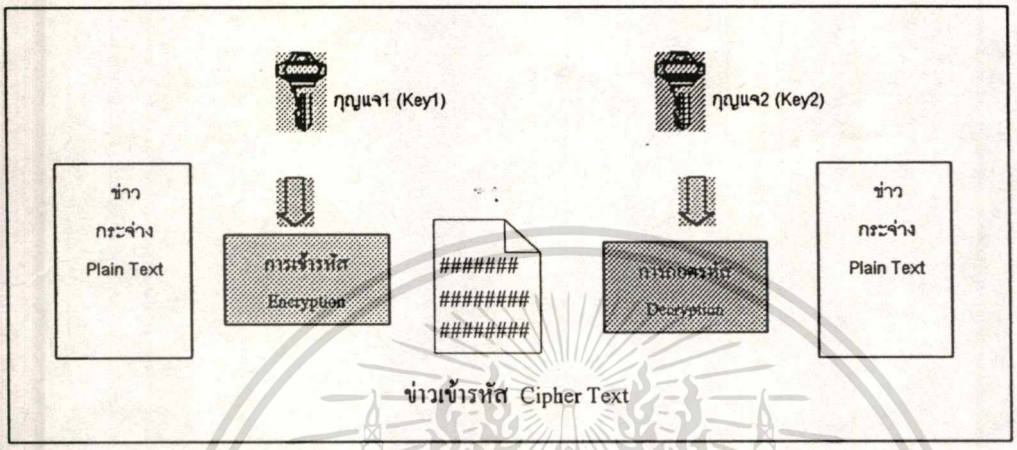
2.2.2.1 กุญแจรหัสส่วนตัวซึ่งจะต้องเก็บเป็นความลับ มีผู้รู้เพียงคนเดียวโอกาสที่ความลับจะรั่วไหลมีอยู่น้อย ดังนั้น จึงไม่จำเป็นจะต้องเปลี่ยนรหัสบ่อย

2.2.2.2 จำนวนกุญแจรหัสที่จำเป็นต้องใช้มีจำนวนน้อยลง แต่ละบุคคลมีกุญแจคนละ 1 คู่ โดยกุญแจหนึ่งประกาศให้สาธารณชนทราบ อีกกุญแจหนึ่งเก็บเป็นความลับ ดังนั้น แต่ละคนจึงต้องจำกุญแจรหัสลับเพียงชุดเดียวเท่านั้น

---

[7] Bruce Schneier, E-mail Security : How to Keep Your Electronic Messages Private, P. 172-174.

2.2.2.3 สามารถใช้ช่องทางที่ใช้ในการสื่อสารส่งกุญแจลับของผู้รับได้ โดยนำไปเข้ารหัสด้วยกุญแจสาธารณะของผู้รับ ทำให้สามารถติดต่อสื่อสารกันได้อย่างปลอดภัย โดยไม่จำเป็นต้องมีช่องการสื่อสารลับอีกช่องหนึ่งสำหรับส่งกุญแจรหัส



ภาพที่ 3 การเข้ารหัสและการถอดรหัสแบบกุญแจสาธารณะ

2.2.3 ซองจดหมาย ลายเซ็น และลายนิ้วมือดิจิตอล

กระบวนการของการเข้ารหัสแบบกุญแจลับเปรียบเทียบได้กับการเขียนข่าวใส่ซองจดหมายดิจิตอล (Digital Envelope) บุคคลอื่นไม่ว่าจะเป็นผู้เขียนจดหมายเองหรือบุรุษไปรษณีย์ก็ไม่สามารถเปิดซองจดหมายอ่านได้ เพราะหากเปิดก็จะมีรอยทำให้ผู้ที่รับข่าวทราบว่ามีผู้แอบเปิดซองจดหมาย

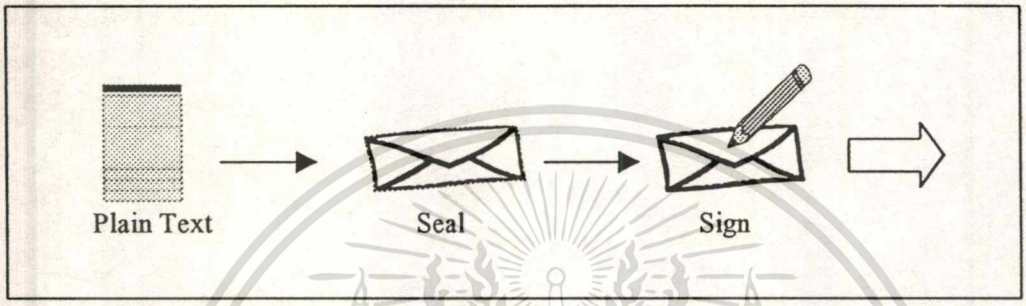
กระบวนการของการใช้ลายเซ็นดิจิตอล มีดังนี้ หากผู้ส่งข่าวคือ A และ ผู้รับข่าวคือ B A จะต้องส่งข่าวไปถึง B 2 ขั้นตอน โดยขั้นตอนแรกเข้ารหัสด้วยกุญแจสาธารณะของ B ซึ่งเรียกว่าการปิดซองเอกสาร หรือ Seal ในขั้นที่สอง A ต้องส่งข่าวที่ได้จากขั้นที่หนึ่งโดยเข้ารหัสด้วยกุญแจส่วนตัวของตนเอง เรียกว่า การเซ็นชื่อ หรือ Sign (ภาพที่ 4)

การนำกรรมวิธีเข้า-ถอดรหัสมาใช้ประโยชน์ในกรณีนี้จึงเรียกกันว่า ลายเซ็นดิจิตอล (Digital Signature) เนื่องจากเทียบเท่ากับการลงลายมือชื่ออันเป็นเอกลักษณ์เฉพาะตัว ทั้งนี้กฎหมายของสหรัฐฯ ให้การยอมรับลายเซ็นดิจิตอลเทียบเท่ากับการที่บุคคลได้ลงลายมือชื่อในเอกสารด้วยตนเองทุกประการ ด้วยเหตุผลที่ว่า

- ลายเซ็นดิจิตอลนั้นปลอมแปลงไม่ได้ (Unforgetable)
- เป็นการพิสูจน์ทราบว่าเป็นบุคคลที่แท้จริง (Authentic)
- นำไปใช้กับเอกสารอื่นไม่ได้ (Non-reusable)

- แก้ไขเปลี่ยนแปลงหลังลงนามไม่ได้ (Un-alterable)
- จะปฏิเสธว่ามิได้ลงนามไม่ได้ (Can Not Be Repudiated)

แท้ที่จริงแล้วลายเซ็นดิจิตอลนั้นปลอมแปลงยากยิ่งกว่าลายมือชื่อจริงๆ เสียอีก แต่มีจุดอ่อนที่เจ้าของจะต้องเก็บกุญแจรหัสส่วนตัวของตนเองไว้เป็นความลับ



ภาพที่ 4 แนวความคิดลายเซ็นดิจิตอล

อย่างไรก็ดี ในทางปฏิบัติมักไม่เข้ารหัสข่าวด้วยกุญแจส่วนตัวของผู้ส่ง (Seal) แต่เพียงอย่างเดียว เนื่องจากการเข้ารหัส อาร์เอสเอ ด้วยกุญแจส่วนตัวใช้เวลานานมาก โดยทั่วไปมักจะเลือกกุญแจสาธารณะค่า c ให้เท่ากับ 65,537 เพื่อความรวดเร็วในการเข้ารหัสส่วนกุญแจส่วนตัว ส่วนค่า d จะเป็นตัวเลขที่สูงกว่านี้มาก

แม้ว่า การเข้ารหัส อาร์เอสเอ ด้วยกุญแจส่วนตัวของผู้ส่งข่าวมีประโยชน์ในการพิสูจน์ทราบ (Authentication)[8] ว่าเอกสารนั้นมาจากผู้ส่งอย่างแท้จริงโดยไม่มีการปลอมแปลง แต่ก็ทำให้เกิดจุดอ่อนในด้านการรักษาความปลอดภัยเพราะมีการประกาศให้ทุกคนที่เกี่ยวข้องทราบกุญแจสาธารณะแล้ว ดังนั้น ทุกคนที่ทราบจึงสามารถถอดรหัสได้ จึงมักใช้วิธีพิเศษประกอบกัน คือ แทนที่จะเข้ารหัสข้อความทั้งหมดซึ่งอาจมีความยาวหลายพันตัวอักษร ก็เลี่ยงไปใช้วิธีเข้ารหัสแบบลายนิ้วมือดิจิตอล (Digital Finger Print) เพื่อให้มีความยาวเพียง 128 บิท หรือ 160 บิทแล้วจึงส่งไปแทน อีกนัยหนึ่ง ลายนิ้วมือดิจิตอลก็คือกระบวนการที่จะทำให้ข้อมูลมีเอกลักษณ์เฉพาะตัว ด้วยการนำข้อมูลนั้นมาผ่านกระบวนการเข้ารหัสแบบทางเดียว (One-way Hash Function) ซึ่งกระบวนการดังกล่าวมีความสำคัญต่อการวิจัยพัฒนาระบบที่จะนำเสนอใหม่และจะกล่าวถึงในรายละเอียดต่อไป

---

[8] Bruce Schneier, E-mail Security : How to Keep Your Electronic Messages Private, P. 334.

2.2.4 มาตรฐานการเข้ารหัสข้อมูล (Data Encryption Standard-DES)

การเข้ารหัสตามมาตรฐานการเข้ารหัสข้อมูล (Data Encryption Standard-DES) หรือรหัสเดสเป็นกรรมวิธีเข้ารหัสที่ทั่วโลกยอมรับเป็นมาตรฐานมานาน และนักวิเคราะห์รหัสได้พยายามหาจุดอ่อนของรหัสเดสมาตั้งแต่เพิ่งเริ่มมีการนำมาใช้ แต่จนกระทั่งปัจจุบันก็ไม่มีผู้ค้นพบจุดอ่อนที่ร้ายแรง จึงเป็นยอมรับว่ารหัสเดสมีการรักษาความปลอดภัยสูง

เนื่องจากความต้องการใช้อุปกรณ์เข้า-ถอดรหัสเพื่อวัตถุประสงค์ในเชิงพาณิชย์มีมากขึ้นเป็นลำดับ ในปี ค.ศ. 1973 สำนักงานมาตรฐานแห่งชาติของสหรัฐ (National Bureau of Standard-NBS) ได้เปิดโอกาสให้มีการเสนอกรรมวิธีการเข้า-ถอดรหัส เพื่อให้ NBS คัดเลือกใช้เป็นมาตรฐาน โดยต้องมีคุณสมบัติ ดังนี้

- สามารถรักษาความปลอดภัยได้ในระดับสูง
- รักษาความปลอดภัยโดยเก็บกุญแจรหัสเป็นความลับเพียงประการเดียว
- ระบุรายละเอียดของกรรมวิธีดำเนินการอย่างครบสมบูรณ์
- สามารถตรวจสอบความถูกต้องของกรรมวิธีดำเนินการได้
- ต้องเปิดเผยกรรมวิธีดำเนินการให้สาธารณชนทราบ
- สามารถใช้งานได้เอนกประสงค์ และมีประสิทธิภาพ
- สามารถผลิตเป็นอุปกรณ์อิเล็กทรอนิกส์ได้ในราคาที่ไม่สูงนัก
- สามารถผลิตเป็นสินค้าออกได้

ปรากฏว่าในปี ค.ศ. 1974 NBS ได้ยอมรับกรรมวิธีที่เสนอโดยบริษัท IBM เป็นมาตรฐาน[10] รหัสเดสพัฒนามาจากรหัสลูซิเฟอร์ (Lucifer)[11] โดยใช้การปฏิบัติการทางลอจิกง่ายๆ มาประกอบกับตัวเลขไบนารี่ที่มีจำนวนบิทไม่มากนัก

2.2.4.1 กรรมวิธีเข้ารหัสเดส

รหัสเดสเป็นรหัสแบบ Block Cipher คือการเข้ารหัสจะกระทำทีละบลอก แต่ละบลอกมีขนาด 64 บิท ข้อมูลที่ได้ออกมามีขนาด 64 บิทเช่นกัน แม้ทั่วไปจะถือว่ากุญแจรหัสเดส มีความยาว 64 บิท แต่แท้จริงแล้วบิทที่ 8 ของแต่ละไบท์จะใช้สำหรับการ Parity Check เพื่อตรวจสอบว่าเป็นเลขคู่หรือเลขคี่ โดยมิได้ใช้เป็นกุญแจรหัส

---

[10]Bruce Schneier, E-mail Security : How to Keep Your Electronic Messages Private, P. 26-28.

[11]Karen A. Forcht, Computer Security Management (Thompson Information/Publishing Group, 1993), P.25.

การรักษาความปลอดภัยของรหัสเดสขึ้นอยู่กับกุญแจรหัสเพียงประการเดียว ผู้ใช้จึงต้องรักษากุญแจรหัสเป็นความลับ กุญแจรหัสเดสซึ่งมีความยาว 56 บิทจะเป็นตัวเลข 56 บิทใดๆ ก็ได้ และมีตัวเลขเพียงบางจำนวนที่ไม่ควรนำมาใช้เป็นกุญแจรหัส

การเข้ารหัสและการถอดรหัสเดสต่างกันก็แค่การเรียงลำดับบิทของกุญแจรหัสเท่านั้น นอกเหนือจากนั้นแล้วจะใช้กรรมวิธีเหมือนกัน โดยใช้หลักการ 2 ประการคือ

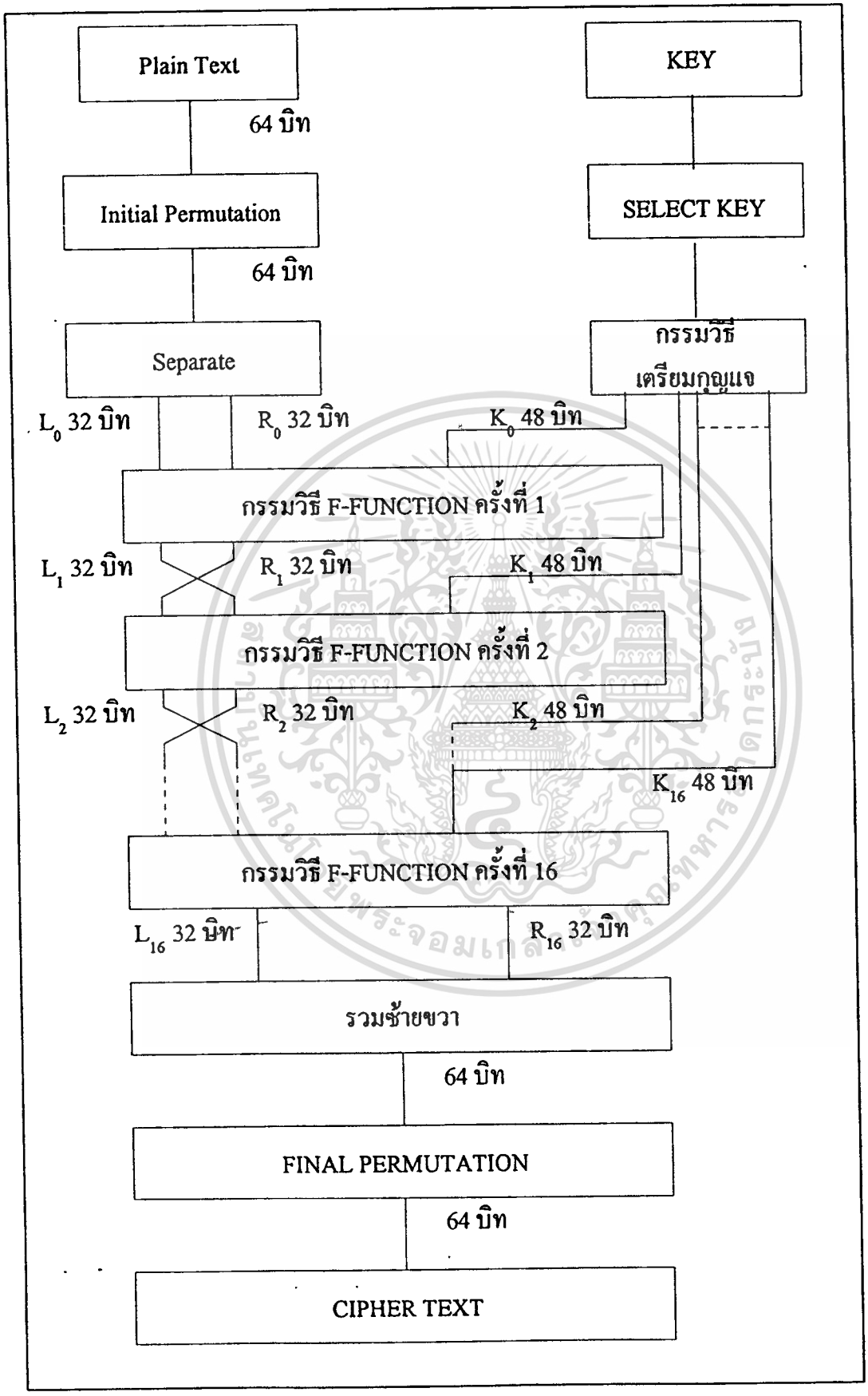
- การทำให้สับสน (Confusion)

- การทำให้ฟุ้งกระจาย (Diffusion) การดำเนินกรรมวิธีแบ่งเป็น กรรมวิธีย่อยที่เหมือนกัน 16 กรรมวิธี แต่ละกรรมวิธีย่อยเริ่มด้วย กระบวนการแทนค่า (Substitution) และตามด้วยกระบวนการสลับตำแหน่ง (Permutation) และเป็นไปตามค่าของกุญแจที่ใช้ กรรมวิธีการเข้ารหัสเดส (ภาพที่ 5) มีดังนี้

- นำข้อมูลที่ป้อนเข้าซึ่งเป็นข่าวกระจ่างขนาด 64 บิท ไปดำเนินกรรมวิธีเปลี่ยนตำแหน่งบิท ตามตารางที่ 1 ขั้นตอนนี้เรียกว่า Initial Permutation

ข้อมูลออกบิทที่	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
มาจากข้อมูลเข้าบิทที่	58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
ข้อมูลออกบิทที่	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
มาจากข้อมูลเข้าบิทที่	62	54	46	38	30	22	14	06	64	56	48	40	32	24	16	8
ข้อมูลออกบิทที่	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
มาจากข้อมูลเข้าบิทที่	57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
ข้อมูลออกบิทที่	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
มาจากข้อมูลเข้าบิทที่	61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7

ตารางที่ 1 การสลับที่ครั้งแรก (Initial Permutation)



ภาพที่ 5 กรรมวิธีการเข้ารหัส DES

- แบ่งข้อมูลเป็น 2 ส่วนเท่าๆ กัน ส่วนละ 32 บิท ส่วนแรกคือบิททางซ้ายเรียกว่า L_0 ส่วนที่สองคือบิททางขวา เรียกว่า R_0

- ดำเนินกรรมวิธี F-Function 16 ครั้ง โดยแต่ละครั้งข้อมูลที่ป้อนเข้า คือ L_{i-1} R_{i-1} และ K_{i-1} ส่วนข้อมูลที่ได้ออกมา คือ L_i และ R_i

- จากนั้นสลับที่ L_i กับ R_i ให้ซ้ายเป็นขวา ขวาเป็นซ้าย เพื่อใช้เป็นข้อมูลที่จะป้อนเข้าในครั้งต่อๆ ไป จนครบ 15 ครั้ง

- ใน F-Function ครั้งที่ 16 ซึ่งเป็นครั้งสุดท้ายจะไม่สลับ L_{16}กับ R_{16}

- สำหรับ K_i เป็น ข้อมูล 48 บิท ที่ได้มาจากข้อมูลกุญแจ 56 บิท ซึ่งได้ผ่านกระบวนการเตรียมกุญแจสำหรับกรรมวิธีแต่ละรอบ F-Function ดังจะกล่าวถึงต่อไป

- รวม L_{16} กับ R_{16} เข้าด้วยกันเป็นตัวเลข 64 บิท

- เปลี่ยนตำแหน่งบิทอีกครั้งหนึ่ง ขั้นตอนนี้เรียกว่า Final Permutation ซึ่งเป็นกรรมวิธีย้อนกลับของ Initial Permutation ในขั้นตอนแรก จะได้ข่าวเข้ารหัสขนาด 64 บิท

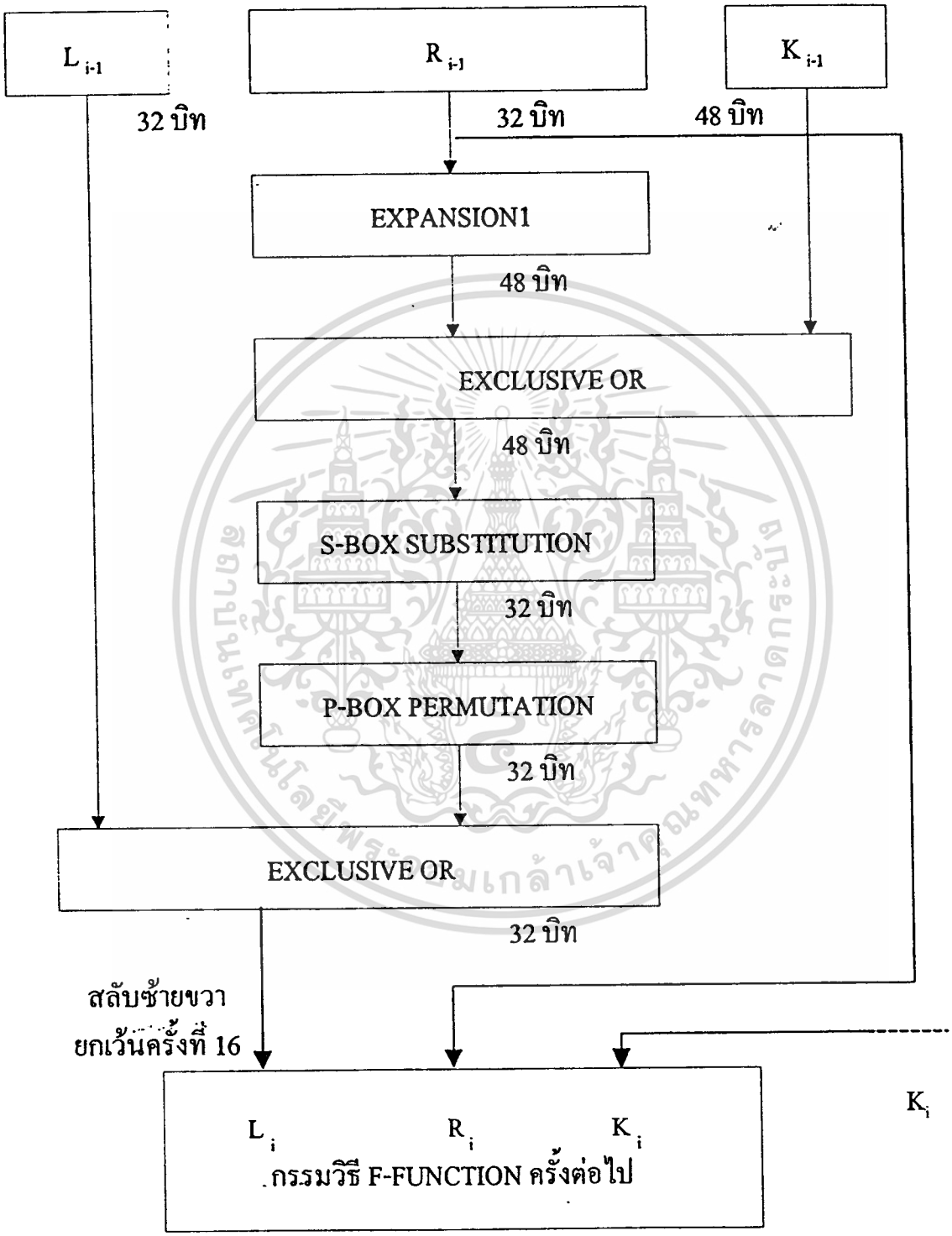
2.2.4.2 กรรมวิธี F-Function

กรรมวิธี F-Function เป็นกรรมวิธีหลักประการหนึ่งที่ทำให้รหัสเดสรักษาความลับได้ดี การดำเนินการของ F-Function มีขั้นตอนดังปรากฏในภาพที่ 6 ข้อมูลเข้าประกอบด้วยข้อมูล 32 บิท ซ้าย L_{i-1} ข้อมูล 32 บิทขวา R_{i-1} และข้อมูลกุญแจ 48 บิท ซึ่งผ่านกรรมวิธีเตรียมกุญแจมาแล้ว K_{i-1}

ข้อมูล 32 บิทขวา R_{i-1} ถูกขยายเป็น 48 บิท รายละเอียดดังตารางที่ 2 ขั้นตอนนี้เรียกว่า Expansion Permutation[12] ผลที่ได้ 48 บิท นำไป Exclusive or กับข้อมูลกุญแจ 48 บิท K_{i-1} ผลที่ได้ 48 บิท จะนำไปผ่านกรรมวิธี S-Box Substitution ข้อมูลที่ออกมามี 32 บิท นำไปดำเนินกรรมวิธีสลับตำแหน่ง ขั้นตอนนี้เรียกว่า P-Box Permutation (ตารางที่ 3) ผลที่ได้ มี 32 บิท นำไป Exclusive or กับข้อมูล 32 บิทซ้าย ผลที่ได้คือข้อมูลออก 32 บิทซ้าย L_i ส่วนข้อมูล ออก 32 บิทขวา R_i ก็คือ ข้อมูลเข้า 32 บิทขวา R_{i-1} ก่อนที่จะเข้าสู่กรรมวิธี F-Function ครั้งต่อไป ข้อมูลซ้ายขวาจะถูกสลับ ซ้ายเป็นขวา ขวาเป็นซ้าย ยกเว้นครั้งสุดท้ายไม่ทำการสลับ

---

[12] Bruce Schneier, Applied Cryptography, P. 227.



ภาพที่ 6 กรรมวิธี F-FUNCTION

ข้อมูลออกบิทที่	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
มาจากข้อมูลเข้าบิทที่	32	1	2	3	4	5	4	5	6	7	8	9	8	9	10	11
ข้อมูลออกบิทที่	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
มาจากข้อมูลเข้าบิทที่	12	13	12	13	14	15	16	17	16	17	18	19	20	21	20	21
ข้อมูลออกบิทที่	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
มาจากข้อมูลเข้าบิทที่	22	23	24	25	24	25	26	27	28	29	28	29	30	31	32	1

ตารางที่ 2 Expansion Permutation

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

ตารางที่ 3 P-Box Permutation

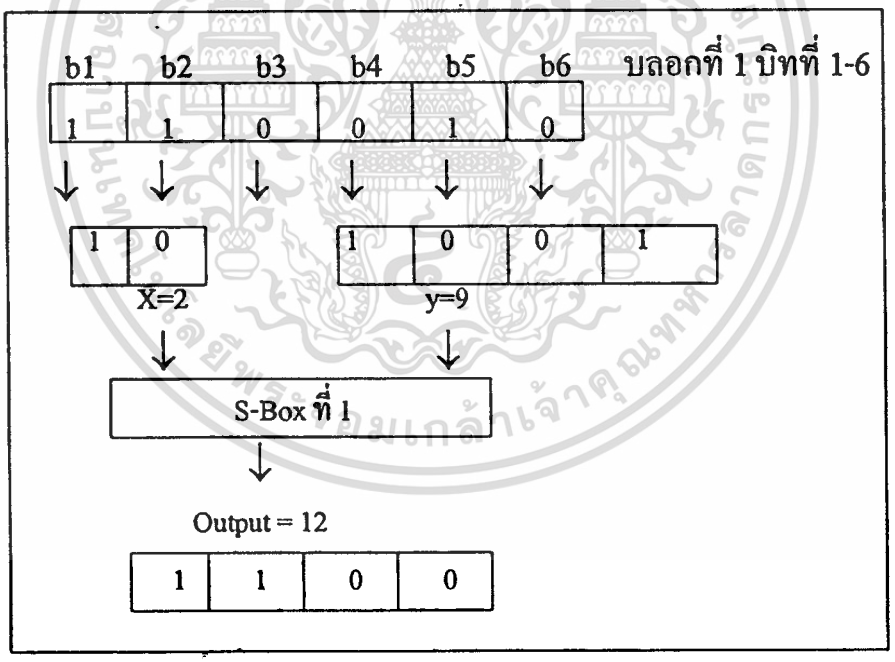
2.2.4.3 กรรมวิธีแทนค่าใน S-Box (S-Box Substitution)

กรรมวิธีแทนค่าใน S-BOX เป็นกรรมวิธีหลักอีกวิธีหนึ่งที่ทำให้รหัสเคสรักษาความลับได้ดี เพราะกรรมวิธีอื่น เช่น การสลับสับเปลี่ยนตำแหน่ง และการ Exclusive or เป็นกรรมวิธีที่มีคุณสมบัติ Linear ทำให้การทำกลับกระทำได้ไม่ยาก แต่กรรมวิธีแทนค่าใน S-Box คุณสมบัติเป็น Non-linear ทำให้ความสัมพันธ์ระหว่างข้อมูลเข้ากับข้อมูลออกมีความซับซ้อนมาก และไม่สามารถหาคำนวณหาสูตรได้ง่ายๆ

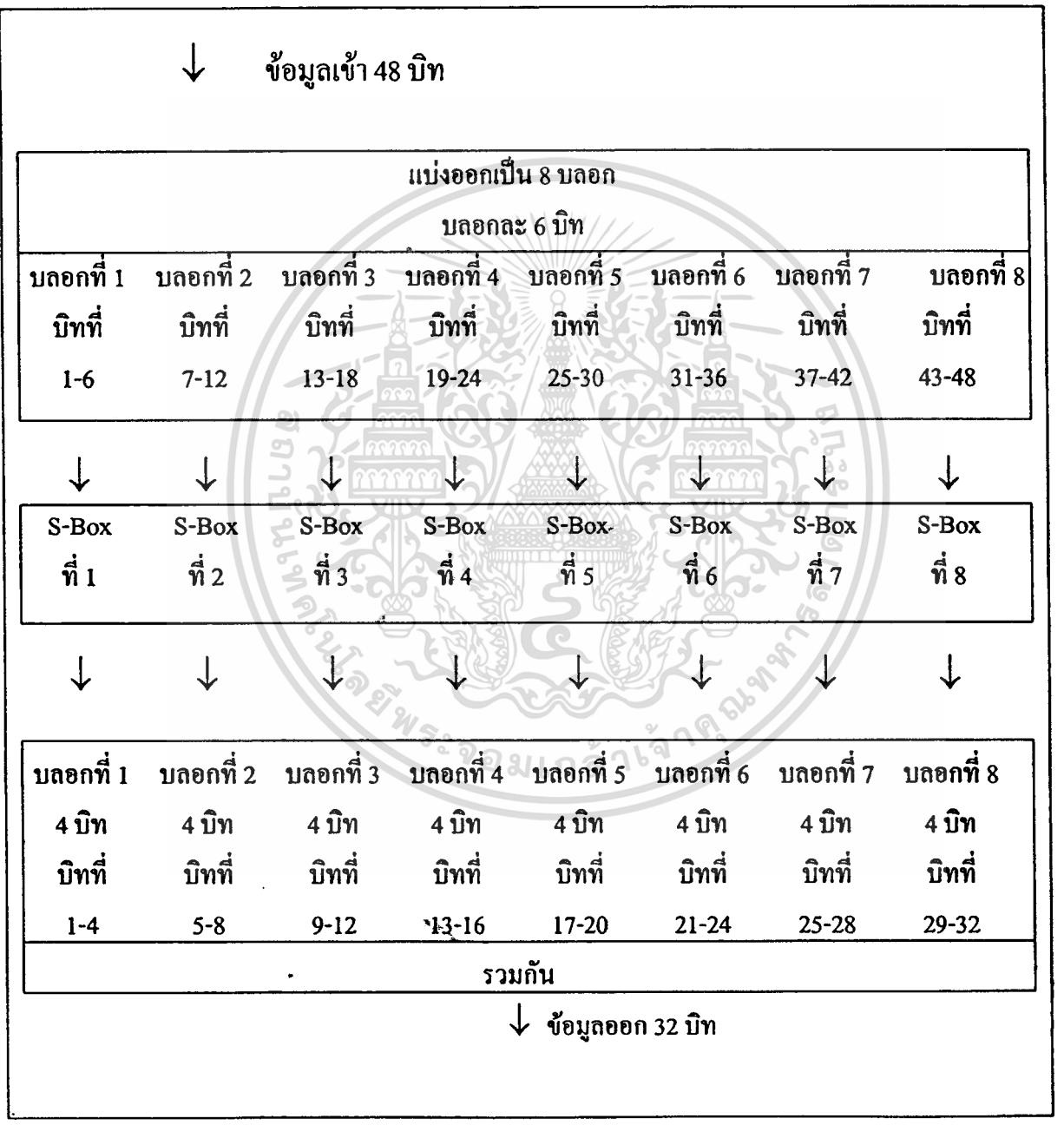
กรรมวิธี แทนค่าใน S-Box (ภาพที่ 7) รับข้อมูลเข้า 48 บิท และส่งข้อมูลออก 32 บิท ข้อมูลที่เข้ามา 48 บิท จะถูกแบ่งออกเป็น 8 ส่วน เท่าๆ กัน ส่วนละ 6 บิท แต่ละส่วนเป็นจะข้อมูลเข้าสำหรับ S-Box แต่ละกล่อง (ภาพที่ 8) โดยมี S-Box ทั้งหมด 8 กล่อง แต่ละกล่องจะใช้ตารางแทนค่าของกล่องนั้นโดยเฉพาะ (ตารางที่ 4)

การแทนค่าใน S-Box ดังภาพนั้น ข้อมูลเข้าของแต่ละ S-Box จะมี 6 บิท (เป็นตัวเลข 0 ถึง 63) และข้อมูลออกมี 4 บิท (เป็นตัวเลข 0-15) ข้อมูลเข้าบิทที่ 1 กับ 6 เป็นค่า X มีค่าระหว่างเลข 0 ถึง 3 ส่วนข้อมูลเข้าบิทที่ 2 ถึง 5 เป็นค่า Y มีค่าระหว่างเลข 0-15

เมื่อนำค่า X และค่า Y ไปเทียบดูจากตารางก็จะได้ค่าของข้อมูลออก ตัวอย่างเช่น ในกรณีของ S-Box ที่ 1 ถ้าข้อมูลเข้าเป็น 110010 จะได้ค่า X = เลขไบนารี่ 10 (คือ 2) และค่า Y = เลขไบนารี่ 1001 (คือ 9) เมื่อเทียบดูจากตาราง S-Box กล่องที่ 1 ข้อมูลออกก็คือ 12 (เลขไบนารี่ 1100)



ภาพที่ 7 กรรมวิธี S-Box



ภาพที่ 8 กรรมวิธีแทนค่าใน S-Box

ตาราง S-Box ที่ 1

Y=	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
X=0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
X=1	0	15	7	4	14	12	13	1	10	6	12	11	9	5	3	8
X=2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
X=3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

ตาราง S-Box ที่ 2

Y=	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
X=0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
X=1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
X=2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
X=3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
Y=	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

ตาราง S-Box ที่ 3

Y=	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
X=0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
X=1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
X=2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
X=3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

ตาราง S-Box ที่ 4

Y=	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
X=0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
X=1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
X=2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
X=3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

ตารางที่ 4 การแทนค่าใน S-Box

ตาราง S-Box ที่ 5

Y=	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
X=0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
X=1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
X=2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
X=3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

ตาราง S-Box ที่ 6

Y=	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
X=0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
X=1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
X=2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
X=3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

ตาราง S-Box ที่ 7

Y=	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
X=0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
X=1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
X=2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
X=3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

ตาราง S-Box ที่ 8

Y=	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
X=0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
X=1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
X=2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
X=3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

ตารางที่ 4 (ต่อ) การแทนค่าใน S-Box

2.2.4.4 กรรมวิธีเตรียมกุญแจ

การเตรียมข้อมูลกุญแจรหัสสำหรับใช้เป็นข้อมูลเข้าของ F-Function แต่ละรอบจากทั้งหมด 16 รอบดังปรากฏตามภาพที่ 9

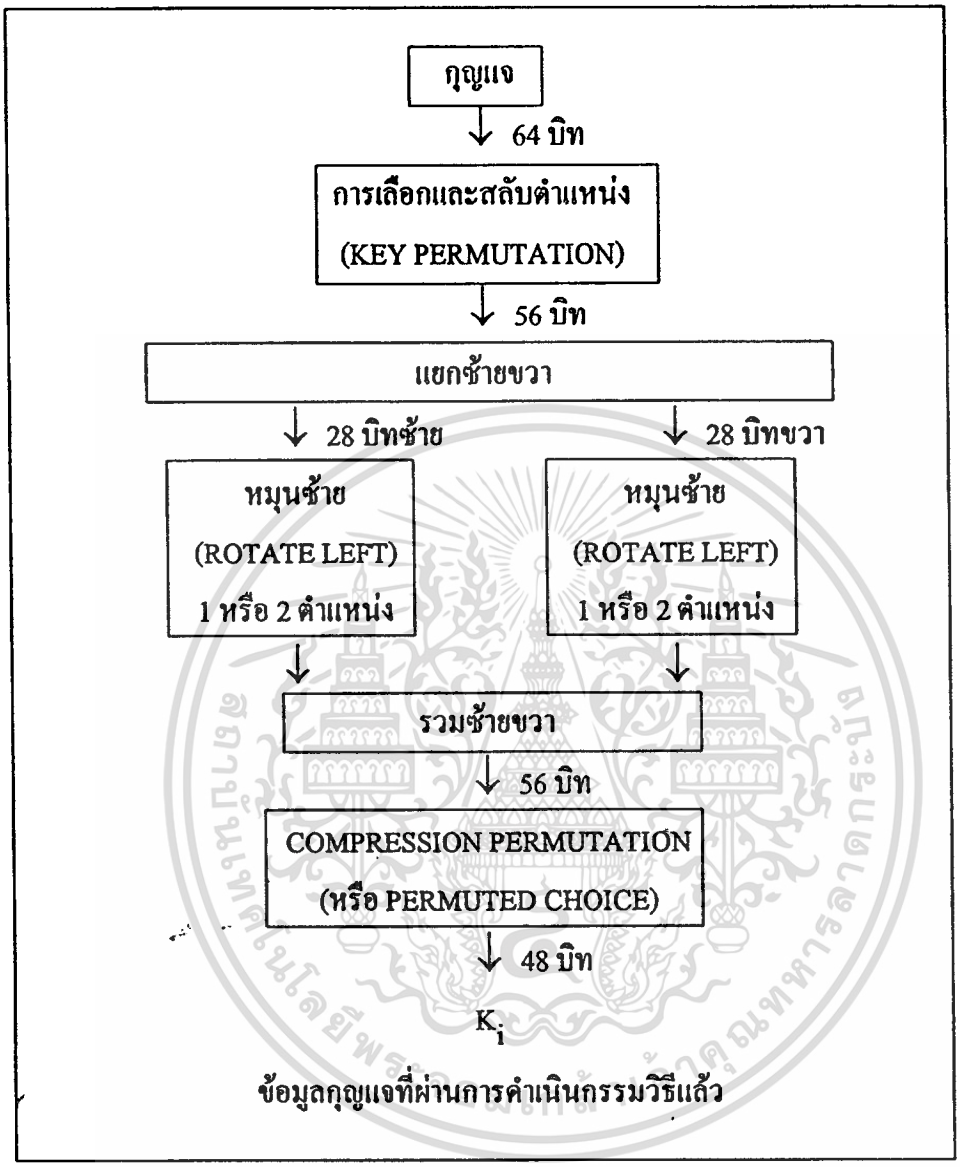
แท้จริงแล้วรหัสเดสใช้กุญแจ 56 บิท แต่นิยมส่งข้อมูลเข้า 64 บิท หรือ 8 ไบท์โดยมีเงื่อนไขว่าไม่ใช้บิทที่หารด้วย 8 ลงตัว คือบิทที่ 8, 16, 24, 32, 40, 48, 56 และ 64

ในขั้นแรกบิทของกุญแจจะถูกคัดเลือกและสลับตำแหน่ง (ตารางที่ 6) ขั้นตอนนี้เรียกว่า Key Permutation การเลือกจะไม่เลือกใช้บิทที่หารด้วย 8 ได้ลงตัว จากนั้น 56 บิท ที่เลือกใช้จะถูกแบ่งเป็น 2 ส่วนเท่าๆ กัน คือ ส่วนทางซ้าย กับ ส่วนทางขวา โดยมีส่วนละ 28 บิท แต่ละส่วนจะถูกหมุนไปทางซ้าย 1 ตำแหน่ง หรือ 2 ตำแหน่ง หลังจากนั้น จึงนำส่วนซ้าย กับ ส่วนขวา มารวมกันอีกครั้งหนึ่ง (ตารางที่ 5)

ในขั้นตอนสุดท้ายซึ่งเรียกว่า Compression Permutation หรือ Permuted Choice เป็นการคัดเลือกและสลับตำแหน่ง โดยจาก 56 บิท ข้างต้น จะเลือกไว้เพียง 48 บิท (ตารางที่ 7) และทำการสลับตำแหน่งไปพร้อมๆ กัน โดยการหมุนบิทจะกระทำต่อเนื่องกัน เช่น หลังจากหมุนซ้าย 2 ตำแหน่งแล้ว จะส่งข้อมูลกุญแจไปดำเนินกรรมวิธีในรอบที่ 1 หลังจากนั้นเมื่อถึงรอบที่ 2 ก็จะทำการหมุนไปอีก 1 ตำแหน่ง ดังนั้น สำหรับรอบที่ 2 จึงเท่ากับเป็นการเริ่มต้นจากสภาพเดิมแล้วจึงหมุนซ้ายไป 2 ตำแหน่ง ในการนี้จะเห็นได้ว่า กุญแจ 56 บิทจะถูกทยอยผลัดเปลี่ยนเข้าไปผสมกับข้อมูลรอบละ 48 บิท จนเมื่อครบ 16 รอบก็จะใช้ทุกบิทของ กุญแจจนครบหมด

รอบที่	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
หมุนซ้ายกี่ตำแหน่ง	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1
นับจากเริ่มต้น	1	2	4	6	8	10	12	14	15	17	19	21	23	25	27	28

ตารางที่ 5 การหมุนกุญแจ



ภาพที่ 9 กรรมวิธีเตรียมกุญแจ

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

ตารางที่ 6 Key Permutation

ข้อมูลออกบิทที่	1	2	3	4	5	6	7	8	9	10	11	12
มาจากข้อมูลเข้าบิทที่	14	17	11	24	1	5	3	28	15	6	21	10
ข้อมูลออกบิทที่	13	14	15	16	17	18	19	20	21	22	23	24
มาจากข้อมูลเข้าบิทที่	23	19	12	4	26	8	16	7	27	20	13	2
ข้อมูลออกบิทที่	25	26	27	28	29	30	31	32	33	34	35	36
มาจากข้อมูลเข้าบิทที่	41	52	31	37	47	55	30	40	51	45	33	48
ข้อมูลออกบิทที่	37	38	39	40	41	42	43	44	45	46	47	48
มาจากข้อมูลเข้าบิทที่	44	49	39	56	34	53	46	42	50	36	29	32

ตารางที่ 7 การคัดเลือกและสลับตำแหน่งกุญแจ

2.2.4.5 กรรมวิธีถอดรหัสเดส

การถอดรหัสเดสใช้กรรมวิธีเช่นเดียวกันกับการเข้ารหัส ต่างกันเพียงว่าจะต้องใช้กุญแจในทิศทางกลับกันเท่านั้น คือในการเข้ารหัสกุญแจของแต่ละรอบ คือ K_1, K_2, K_3, ... K_{16} ดังนั้น ในการถอดรหัสกุญแจแต่ละรอบก็จะเป็น K_{16}, K_{15}, K_{14}, ... K_1 และการหมุนของกุญแจในการเข้ารหัสหมุนไปทางซ้าย ดังนั้น ในการถอดรหัสก็จะหมุนไปทางขวา

2.2.4.6 บทพิสูจน์ความน่าเชื่อถือของรหัสเดส

ความยากง่ายในการถอบถอดรหัสเดสขึ้นอยู่กับ 2 ปัจจัย ปัจจัยแรกคือจุดแข็ง (Strength) ของอัลกอริทึ่มที่ใช้ในกรรมวิธีเข้ารหัส และปัจจัยที่สองคือความยาวของกุญแจ

หากจะสมมุติว่ากรรมวิธีการเข้ารหัสเดสไม่มีจุดอ่อน (Weakness) เลย วิธีเดียวที่จะถอบถอดรหัสได้ก็คือ การถอดรหัสโดยวิธีนำตัวเลขทุกค่าที่มีความเป็นไปได้มาทดลองใช้เป็นกุญแจรหัส วิธีนี้เรียกว่า Brute Force Attack[13] แต่การที่รหัสเดสมีกุญแจยาวถึง 56 บิท ทำให้ค่าของตัวเลขที่มีความเป็นไปได้ของกุญแจมีจำนวนเท่ากับ 2^{56}

ต่อมาในปี ค.ศ. 1990 หรือ 14 ปีหลังจากที่มีการประกาศใช้รหัสเดสเป็นมาตรฐาน นักวิเคราะห์รหัส ชาวอิสราเอล 2 คน คือ อีไล บิแฮม (Eli Biham) กับ อาดี ชาเมียร์ (Adi Shamir) ได้ค้นพบวิธีการวิเคราะห์รหัสแบบใหม่เรียกว่า Differential Cryptanalysis[14] และได้นำวิธีการนี้มาใช้วิเคราะห์รหัสเดส ปรากฏว่าสามารถใช้ในการลอบถอดรหัสเดสอย่างได้ผลกว่าวิธี Brute Force โดย สามารถลอบถอดรหัสได้ด้วยการทดลองใช้กุญแจรหัสเพียง 2^{47} ครั้ง ไม่ต้องใช้ถึง 2^{56} ครั้ง

นักวิเคราะห์รหัสทั้งสองได้ทดลองเปลี่ยนค่า S-Box และพบว่าค่า S-Box ของรหัสเดสตามที่บริษัท IBM ได้ออกแบบไว้เป็นการแทนค่าที่มีประสิทธิภาพสูงสุดในการต่อต้านการลอบถอดรหัสแบบ Differential Cryptanalysis

---

[13]Simpson Garfinkel and Gene Spafford, Practical Unix Security (O'Rielly & Associates, Inc., 1993), P. 67.

[14]E.Biham and A Shamir, "Differential Cryptanalysis of the Full 16-Round DES," Lecture at Workshop on Cryptanalysis, Washington, D.C., March 1992.

เมื่อทดลองเปลี่ยนจำนวนรอบของการหมุนกุญแจรหัสเดสก็พบว่า จำนวน 16 รอบ ตามที่มีการออกแบบไว้นั้นมีประสิทธิภาพสูงสุดเช่นกัน หากหมุนกุญแจรหัสมากหรือน้อยรอบกว่านั้น ก็จะทำให้ถูกลอบถอดรหัสได้ง่าย

สำหรับตำแหน่งในการหมุนกุญแจรหัสเดส ซึ่งต้องหมุนครั้งละ 2 ตำแหน่ง ยกเว้นรอบที่ 1, 2, 9 และ 16 หมุน เพียง 1 ตำแหน่งเท่านั้น นักวิเคราะห์รหัสทั้งสองได้ทำการทดลองโดยใช้กุญแจ 2^{17} ครั้ง และพบว่าหากหมุนกุญแจรหัส 2 ตำแหน่งในทุกรอบ ก็จะทำให้ข่าวเข้ารหัสถูกลอบถอดรหัสได้ง่ายขึ้นเช่นกัน

การลอบถอดรหัสเดสที่มีสมรรถนะสามารถถอดรหัสได้รวดเร็วที่สุดเท่าที่คิดค้นได้ในปัจจุบันและมีการเปิดเผย คือวิธี Linear Cryptanalysis คิดค้นโดย มิซูรู มัทซุยุ (Mitzuru Matzuyu) ซึ่งสามารถลอบถอดรหัสเดสได้ด้วยการทดลองใช้กุญแจเพียง 2^{43} ครั้งเท่านั้น

จากการวิจัยของนักวิเคราะห์รหัสเป็นจำนวนมาก ต่างก็ได้ข้อสรุปว่ากระบวนการของรหัสเดสที่ได้รับการออกแบบโดยบริษัท IBM นั้นเหมาะสมแล้ว เพราะมีสมรรถนะสูงให้การรักษาความปลอดภัยแก่ข่าวสารที่เข้ารหัส และมีสมรรถนะในการต่อต้านการลอบถอดรหัสได้ดี

แต่อย่างไรดี ก็มิใช่ว่ากรรมวิธีของรหัสเดสนั้นจะปราศจากจุดอ่อนเสียเลยที่เดียว เนื่องจาก ด้วยความบังเอิญหากเกิดมี 2 กุญแจที่มีคุณสมบัติเสริมกันหรือเรียกว่าเป็น One's Compliment ของกันและกัน คือเมื่อกลับ 0 เป็น 1 และ กลับ 1 เป็น 0 ของกุญแจหนึ่งแล้วได้ค่าเท่ากับอีกกุญแจหนึ่ง ก็จะทำให้ข่าวที่เข้ารหัสด้วยกุญแจนี้กลายเป็น One's Compliment ของกันและกันไปด้วย ทำให้ผู้ที่ลอบถอดรหัสไม่ต้องทดลองใช้กุญแจทั้งหมดถึง 2^{56} ครั้ง แต่สามารถนำค่าของกุญแจเพียงค่าเดียวคือ 2^{55} มาทดลองใช้ ก็สามารถถอดรหัสได้ทันที ด้วยเหตุนี้ การสร้างกุญแจรหัสเดสจึงควรต้องมีการทดสอบด้วยการทดลองใช้อย่างถี่ถ้วนก่อนนำออกใช้ในปฏิบัติการจริง

อนึ่ง เกี่ยวกับการที่บริษัท IBM ไม่เปิดเผยหลักการและที่มาของกรรมวิธีที่ใช้ออกแบบรหัสเดส นั้น ต่อมาความจริงจึงปรากฏว่าในระหว่างที่ทำการวิจัยเพื่อออกแบบกรรมวิธีของรหัสเดสนั้น คณะผู้ออกแบบได้ค้นพบวิธีลักลอบถอดรหัสแบบ Differential Cryptanalysis ได้ จึงนำมาเป็นพื้นฐานในการออกแบบให้รหัสเดสสามารถต่อต้านการลอบถอดรหัสแบบนี้ได้อย่างมีประสิทธิภาพสูงสุด แต่สาเหตุที่ไม่มีการเปิดเผยเรื่องนี้ เพราะ NSA สั่งให้ เก็บเป็นความลับ NSA อ้างว่าคิดค้นการวิเคราะห์รหัสแบบ Differential Cryptanalysis ได้นานแล้วแต่ต้องปิดเป็นความลับเพราะเกรงว่าอาจกระตุ้นให้ฝ่ายตรงข้ามพยายามปรับปรุงสมรรถนะของตนในการเข้า-ถอดรหัส และนำไปสู่การเพิ่มขีดความสามารถของข้าศึกในการลอบถอดรหัสของสหรัฐฯ ได้ด้วย

2.2.5 รหัสอาร์เอสเอ (RSA)

รหัสอาร์เอสเอ (RSA) มาจากอักษรย่อของนามสกุลผู้ที่ร่วมกันคิดค้นรหัส 3 คน คือ รอน ริเวสท์ (Ron Rivest) อาดี ชามียร์ (Adi Shamier) และ ลีโอนาร์ด เอเดิลแมน (Leonard Adelman) รหัส อาร์เอสเอ ได้รับการจดทะเบียนลิขสิทธิ์ที่ประเทศสหรัฐฯ และยังมีอายุลิขสิทธิ์ถึงวันที่ 20 กันยายน ค.ศ. 2000[15]

2.2.5.1 คณิตศาสตร์มอดดูโล (Modulo Arithmetics)

การจะเข้าใจถึงระบบของรหัสอาร์เอสเอได้จะต้องมีความเข้าใจเรื่องคณิตศาสตร์มอดดูโล (Modulo Arithmetics) เสียก่อน ในระบบตัวเลขมอดดูโล N จะมีตัวเลขเป็นจำนวน N ตัว คือ 0,1 ,2 , ... N-1 ทั้งนี้ ตัวเลขมอดดูโล N จะสามารถทำการ บวก ลบ คูณ หาร ยกกำลัง และหาค่ารากได้เช่นเดียวกับตัวเลขทั่วๆ ไป หากแต่ผลลัพธ์ที่ได้จะต้องมีค่าอยู่ในระหว่าง 0 กับ N-1 เสมอ

วิธีการคำนวณเลขมอดดูโล N นั้นทำโดย บวก ลบ คูณ ตามปกติ และถ้าผลลัพธ์ที่ได้มีค่ามากกว่า N-1 ก็จะต้องนำผลลัพธ์นั้นมาลบด้วย N เป็นจำนวนกี่ครั้งก็ได้ จนกว่าจะได้ผลลัพธ์ที่มีค่าระหว่าง 0 กับ N-1 แต่ถ้าได้ผลลัพธ์ที่มีค่าน้อยกว่า 0 ก็จะต้องนำผลลัพธ์นั้นมาบวกด้วย N เป็นจำนวนกี่ครั้งก็ได้ จนกระทั่งได้ผลลัพธ์ที่มีค่าระหว่าง 0 กับ N-1 เช่นในระบบตัวเลขมอดดูโล 7 จะมีตัวเลขจำนวน 7 ตัว คือ 0, 1, 2, 3, 4, 5, และ 6

การหารด้วย X ใช้วิธีการคูณด้วย X^{-1} หรือเรียกว่า Multiplicative Inverse ของ X โดย X^{-1} มีค่าเท่ากับตัวเลขที่คูณด้วย X แล้วได้ผลลัพธ์เท่ากับ 1

2.2.5.2 กรรมวิธีเข้ารหัสอาร์เอสเอ

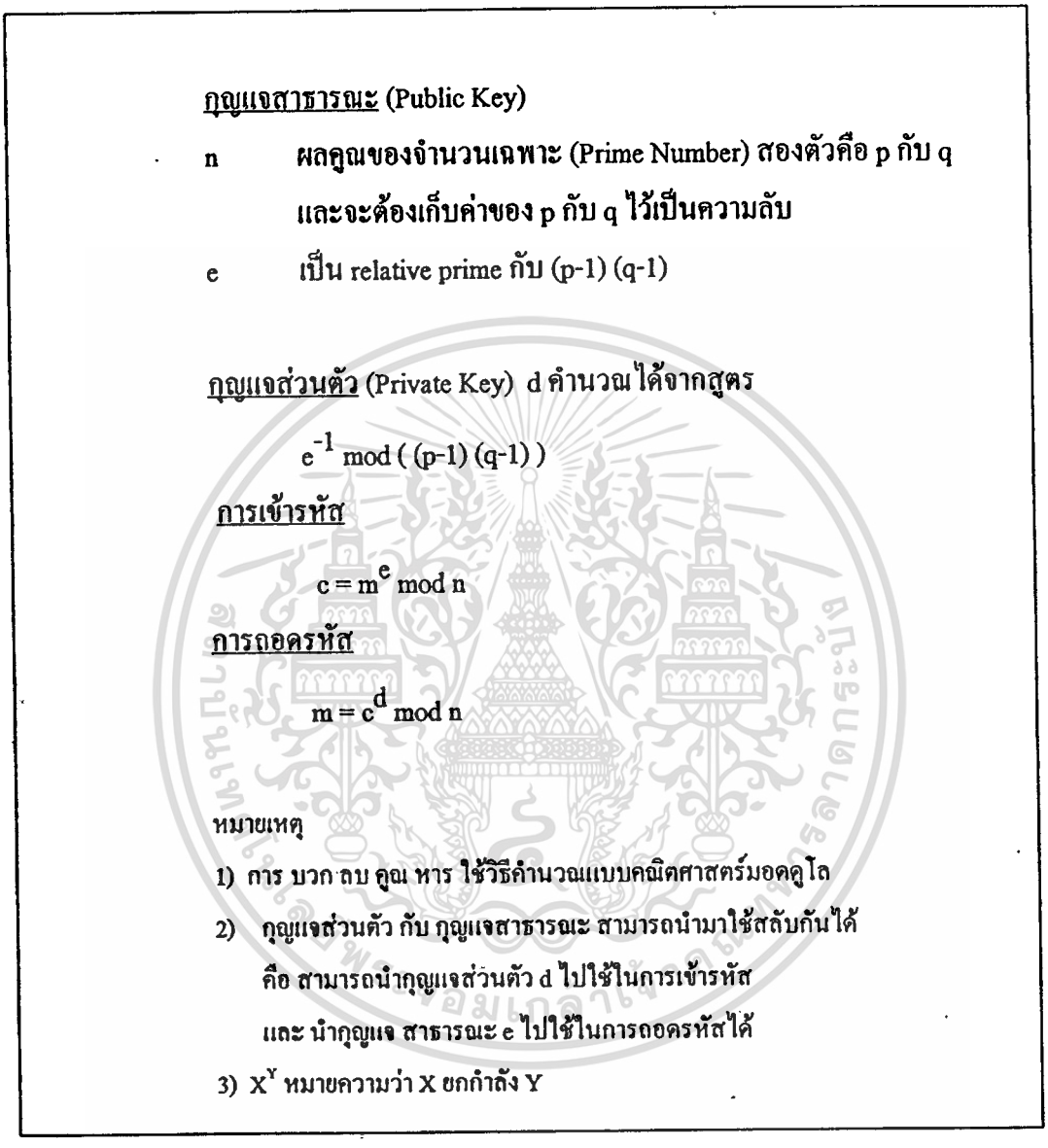
กรรมวิธีเข้ารหัสอาร์เอสเอมีหลักการพื้นฐานมาจาก Number Theoretic ของ Modular Arithmetic และ Integer โดยใช้จำนวนเฉพาะหรือ Prime Number จำนวนเฉพาะคือตัวเลขที่มีค่ามากกว่า 1 และไม่มีตัวเลขใดๆ ที่สามารถมาหารได้ลงตัวเลย นอกจาก 1 และตัวมันเอง

การเข้ารหัสอาร์เอสเอ (ภาพที่ 10) เริ่มต้นด้วยการเลือกจำนวนเฉพาะ 2 จำนวนตัวอย่างเช่น p = 47 และ q = 71 ผลคูณก็คือ n = p x q = 47 x 71 = 3337 และเลือกกุญแจสาธารณะ e ซึ่งเป็นตัวเลขที่ไม่มีแฟคเตอร์ร่วมกับ (p-1) (q-1) = 46 x 70 = 3220 เลือก e = 79 แล้วจึงคำนวณค่ากุญแจส่วนตัว $d = 79^{-1} \bmod 3220 = 1019$ (ทำการตรวจสอบโดยการทดลองคูณ 79 x 1019 = 80501 mod 3220 = (25 x 3220 + 1) mod 3220 = 1) แล้วจึงประกาศค่า n กับ e ซึ่งเป็น

---

[15] Douglas R. Stinson, Cryptography Theory and Practice, P. 128-129.

กุญแจสาธารณะ ให้ผู้ที่ทำหน้าที่ในการส่งข่าวทุกคนได้ทราบ สำหรับค่า d ซึ่งเป็นกุญแจส่วนตัว นั้นจะเก็บไว้เป็นความลับ และส่วนค่า p กับ q จะทำลายไปเพื่อรักษาให้เป็นความลับตลอดไป



กุญแจสาธารณะ (Public Key)

n ผลคูณของจำนวนเฉพาะ (Prime Number) สองตัวคือ p กับ q และจะต้องเก็บค่าของ p กับ q ไว้เป็นความลับ

e เป็น relative prime กับ (p-1) (q-1)

กุญแจส่วนตัว (Private Key) d คำนวณได้จากสูตร

$$e^{-1} \bmod ((p-1)(q-1))$$

การเข้ารหัส

$$c = m^e \bmod n$$

การถอดรหัส

$$m = c^d \bmod n$$

หมายเหตุ

1) การ บวก ลบ คูณ หาร ใช้วิธีคำนวณแบบคณิตศาสตร์มอดคูโล
2) กุญแจส่วนตัว กับ กุญแจสาธารณะ สามารถนำมาใช้สลับกันได้ คือ สามารถนำกุญแจส่วนตัว d ไปใช้ในการเข้ารหัส และ นำกุญแจ สาธารณะ e ไปใช้ในการถอดรหัสได้
3) X^Y หมายความว่า X ยกกำลัง Y

ภาพที่ 10 กรรมวิธีเข้ารหัสอาร์เอสเอ

กำหนดให้ข่าวที่ต้องการส่ง คือ m = 6882326879666683

68 82 32 68 79 66 66 83

เพื่อความสะดวกในการส่งข่าว แบ่งตัวเลขที่จะส่งออกเป็นกลุ่ม กลุ่มละ 3 หลัก ดังนี้

$m_1 = 688$

$m_2 = 232$

$m_3 = 687$

$m_4 = 966$

$m_5 = 668$

$m_6 = 3$

ทำการเข้ารหัสกลุ่มแรก ดังนี้

$$c_1 = 688^{79} \bmod 3337 = 1570$$

ในกรรมวิธีนี้ต้องคำนวณค่า 688 ยกกำลัง 79 แล้วหารด้วย 3337 เศษของการหารคือผลลัพธ์ สำหรับระบบตัวเลขมอดดูโลนั้นสามารถคำนวณโดยกรรมวิธีวิธีลัด ด้วยการนำมาคูณทีละครั้ง ถ้าผลลัพธ์ที่ได้มากกว่า 3336 ก็จะต้องนำมาหารด้วย 3337 แล้วนำมาแทนที่ด้วยเศษของการหาร ทำกระบวนการดังนี้ต่อๆ ไปจนกระทั่งจบ ผลลัพธ์ที่ได้คือข่าวเข้ารหัส

c = 1570 2756 2714 2276 2423 158

การถอดรหัสจะทำโดยการคำนวณค่าของเลขแต่ละจำนวนยกกำลัง 1019 ซึ่งเป็นค่าของกุญแจส่วนตัว ดังนี้

$$m_1 = 1570^{1019} \bmod 3337 = 688$$

ทำกระบวนการดังนี้ต่อๆ ไปจนจบ ก็จะได้ข่าวกระจ่างต้นฉบับ คือ

m = 688 232 687 966 668 3

2.2.5.3 ข้อดีของอาร์เอสเอ

ตัวเลข n และ e หรือ d ถูกเปิดเผยได้โดยไม่ทำให้ความปลอดภัยของรหัสอาร์เอสเอลดลงแต่ประการใด เพราะผู้ลักลอบถอดรหัสจะต้องแยก factor ตัวเลขกุญแจรหัสซึ่งมีค่ามาก การแยก factor จึงมิใช่เรื่องที่กระทำได้ง่าย โดยเฉพาะเมื่อไม่มีวิธีการที่จะแยกแฟคเตอร์ได้อย่างมีประสิทธิภาพ ดังนั้น อาจใช้เวลานานถึงเป็นร้อยๆ ปี ถึงแม้ว่าจะใช้คอมพิวเตอร์ที่มีความเร็วสูงก็ตาม และมีความเป็นไปได้ว่าหาก n มีค่ามากพอก็อาจไม่สามารถแยก factor ได้เลย ด้วยเหตุนี้

ระบบการเข้ารหัส RSA จึงมีจุดแข็ง ทั้งนี้ ขึ้นอยู่กับการเลือกค่าของ n e และ d ให้ได้ค่าที่เหมาะสมและมีการรักษาไว้เก็บไว้เป็นความลับ

2.2.5.4. บทพิสูจน์ความน่าเชื่อถือของรหัสอาร์เอสเอ

ค่าตัวเลข 200 หลักสามารถแทนที่ได้ด้วย binary 665 บิท การแยก factor ตัวเลข 665 บิทโดยใช้อัลกอริทึมที่ทำงานได้เร็วที่สุดอาจต้องใช้การดำเนินการ (Operation) ถึงประมาณ 1.2×10^{23} ครั้ง และหากสมมุติว่ามีคอมพิวเตอร์ซึ่งสามารถทำคำสั่งได้ 10 พันล้านครั้งต่อวินาที การดำเนินการ 1.2×10^{23} จะต้องใช้เวลา 1.2×10^{23} วินาทีหรือ 380,267 ปี[16]

การทดลองคำนวณเพื่อแยกแฟคเตอร์ตัวเลข 200 หลักหรือ 664 บิท ปรากฏว่าคอมพิวเตอร์จะต้องทำการคำนวณถึง 10^{23} ขั้นตอน ซึ่งหากสมมุติว่าใช้คอมพิวเตอร์ที่มีความเร็วในการคำนวณได้ 1 ล้านครั้งต่อวินาทีมาทำการคำนวณพร้อมๆ กัน 1 ล้านเครื่องก็จะต้องใช้เวลาถึงประมาณ 4,000 ปีจึงจะสามารถแยกแฟคเตอร์ได้ สำหรับตัวเลขขนาด 1024 บิท ก็จะต้องใช้คอมพิวเตอร์ชุดเดียวกันนี้คำนวณเป็นเวลาถึง 10,000 ล้านปี ดังนั้น จึงเป็นที่เชื่อถือได้ว่าการลอบถอดรหัสอาร์เอสเอภายในระยะเวลาที่อาจก่อให้เกิดอันตรายต่อข่าวสารลับที่เข้ารหัสอาร์เอสเอจึงเป็นไปได้ยากมาก

หากต้องการให้การแยกแฟคเตอร์ค่าของกุญแจรหัสทำได้ยากขึ้น ก็สามารถเพิ่มขนาดของจำนวนเฉพาะเป็นสองเท่า ทั้งนี้ ตัวเลข 400 หลัก จะใช้เวลาในการแยกแฟคเตอร์นานถึง 8.6×10^{15} ปีซึ่งก็เป็นเวลาที่นานมากพอในการรักษาความปลอดภัยของข่าวเข้ารหัส ดังนั้น จึงมีหลักฐานที่ทำให้มั่นใจได้ว่าหากปราศจากการค้นพบที่แปลกใหม่ (break through) ในทฤษฎีตัวเลข กระบวนการ RSA ก็จะคงสมรรถนะในการรักษาความปลอดภัยจากการถูกลอบถอดรหัสได้

ในสถานการณ์จริงของปฏิบัติการทางทหาร มีการใช้รหัสอาร์เอสเอที่มีความซับซ้อนมาก ดังนี้

- ข่าวที่มีการรักษาความปลอดภัยต่ำ ใช้ค่า n ประมาณ 116 หลัก หรือ 386 บิท
- ข่าวที่มีรักษาความปลอดภัยปานกลาง ใช้ค่า n ประมาณ 154 หลัก หรือ 512 บิท (ตารางที่ 8)
- ข่าวที่มีการรักษาความปลอดภัยสูงใช้ค่า n ประมาณ 308 หลักหรือ 1024 บิท

---

[16] Bruce Schneier, Applied cryptography, P. 284-285.

จำนวนเฉพาะ : p =	ff 5e 6e e1 c3 ea 31 41 90 e0 8e 24 47 5e b8 16
	f1 21 1e d1 49 ff 95 33 e5 60 de 4c ae ae f8 37
จำนวนเฉพาะ : q =	e1 06 cd d0 08 c9 15 09 14 93 8a 8c a5 d7 84 b8
	56 15 42 38 b7 e7 8e 89 cb d6 56 9f 59 76 20 9f
มอดดูลัส (Modulus) : n =	e0 78 c8 f9 2a c3 d7 b1 6a eb 66 00 15 ed 54 28
	91 81 35 9f 6f 8a b3 6a ac 9d 0a 75 12 df 9e 77
	f0 d3 3c 30 f4 ad 33 6a 9a 65 24 20 89 8b f7 95
	9d be 9a bd 31 77 80 ac 14 0f a4 90 e6 0d 0a 29
กุญแจสาธารณะ : e =	01 00 01
กุญแจส่วนตัว : d =	93 67 3d b2 41 9e f1 59 14 39 18 76 1d f0 07 3f
	cc ac e8 a5 95 fd a2 eb fe 05 f2 04 07 2c c9 46
	06 6b f5 47 6e dc f4 15 f4 27 05 b7 79 15 e2 dc
	b3 9e 29 25 bd aa 33 1c 67 d4 71 1b f6 8c 85 31
(หมายเหตุ : ใช้ระบบตัวเลขฐาน 16)	

ตารางที่ 8 ตัวอย่างกุญแจรหัสอาร์เอสเอ ขนาด 512 บิท

2.2.6 One-way Hash Function

กระบวนการ One-way Hash Function นำมาใช้ตรวจสอบรหัสผ่าน (Password) หรือ พิสูจน์ทราบตัวบุคคล (Authentication) เพื่อเพิ่มการรักษาความปลอดภัยของข่าวสารโดยแทนที่จะเก็บรหัสผ่านของผู้ใช้แต่ละคนไว้ในแฟ้ม คอมพิวเตอร์จะเก็บค่า One-way Hash Function ของรหัสผ่านไว้แทน วิธีนี้ป้องกันมิให้การลอบอ่านแฟ้มรหัสผ่านเพื่อค้นหาว่ารหัสผ่านคืออะไร

ในกระบวนการของการตรวจสอบ คอมพิวเตอร์จะนำรหัสผ่านของจากผู้ใช้ไปคำเนินกรรมวิธี One-way Hash Function จากนั้นจึงนำค่าที่ได้ไปเทียบกับค่า One-way Hash Function ที่เก็บไว้ในแฟ้ม หากตรงกันก็คือรหัสผ่านถูกต้อง ดังนั้น ข้อมูลออก (Output) ที่ได้จาก One-way Hash Function จึงเปรียบเสมือนนิ้วมือของแฟ้มรหัสผ่านอีกทอดหนึ่ง

การคำเนินกรรมวิธี One-way Hash Function คล้ายกับการเข้ารหัสแต่เป็นการเข้ารหัสทางเดียว เมื่อเข้ารหัสแล้วไม่สามารถถอดรหัสได้ สมมุติว่า m เป็นข้อมูลที่ป้อนเข้า (Input)

การดำเนินกรรมวิธี One-way Hash Function คล้ายกับการเข้ารหัสแต่เป็นการเข้ารหัสทางเดียว เมื่อเข้ารหัสแล้วไม่สามารถถอดรหัสได้ สมมุติว่า m เป็นข้อมูลที่ป้อนเข้า (Input)

และ h เป็นข้อมูลที่ได้ออกมา H (.) เป็น One-way Hash Function ดังนั้น

$$h = H(m)$$

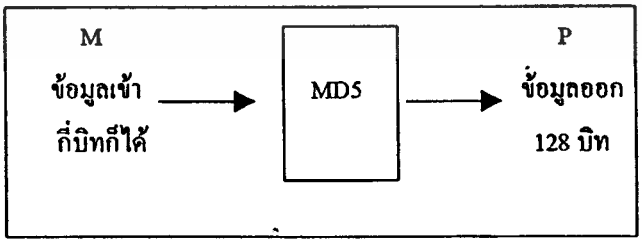
ข้อมูลที่ป้อนเข้า m นั้นมีความยาวเท่าใดก็ได้ แต่ข้อมูลที่ได้ออกมาคือ h มีความยาวคงที่เสมอโดยอาจมีความยาว 128 บิท หรือ 160 บิท

One-way Hash Function ที่ดีจะต้องมีคุณสมบัติดังต่อไปนี้

- ถ้ากำหนดข้อมูลที่ป้อนเข้า m ให้ การหาข้อมูลออก h ทำได้ง่าย
- ถ้ากำหนดว่าข้อมูลออกต้องเป็น h การหาข้อมูลเข้า m ทำได้ยากมาก
- ถ้ากำหนดว่าข้อมูลเข้าต้องเป็น m การหาค่าข้อมูลเข้าอีกแบบหนึ่ง คือ m' ซึ่งเมื่อเป็น One-way Hash Function แล้ว จะได้ข้อมูลออกเท่ากัน คือ $h = H(m) = H(m')$ ทำได้ยากมาก

ดังนั้น การออกแบบกรรมวิธีของ One-way Hash Function ที่ดี จึงเป็นการยากพอกับการออกแบบกรรมวิธีเข้ารหัส

One-way Hash Function ที่ใช้ในการวิจัยนี้ คือ Message Digest 5 หรือ MD5 ซึ่งให้ข้อมูลออกที่มีความยาว 128 บิท มีความยาวเพียงพอแก่การรักษาความปลอดภัยกรรมวิธีของ MD5 ปรากฏในภาพที่ 11 และ ตัวอย่างข้อมูลเข้า-ออกของ MD5 ดังปรากฏในตารางที่ 9



ภาพที่ 11 กรรมวิธี MD5

ในกรรมวิธี MD5 เนื่องจากข้อมูลออกมีความยาวถึง 128 บิท โอกาสที่เอกสาร 2 ฉบับ ซึ่งไม่เหมือนกันจะผ่านกระบวนการของ MD5 แล้ว ได้ผลลัพธ์เท่ากันมีเพียง 1 ใน 2^{128}

เท่านั้น

	ข้อมูลเข้า (ASCII Text)	ข้อมูลออก (Hex)
1	this is a pen<CR><LF>	0454 ca25 11af 9962 1ae1 d309 172e bb0a
2	this is b pen<CR><LF>	811a e9ba 6cb1 ec01 da25 11c7 1444 9521
3	this is a pen.<CR><LF>	c11b 0d3e 833f 44ea 8ae0 ff60 55a0 3d29
4	roses are red <CR><LF>	f028 903c 615f b3bc d63c 3e68 597f ee8d
5	roses are red.<CR><LF>	2ccd e1a1 0c1c ec6f efe8 c127 dad9 7529
6	sugar is sweet<CR><LF>	0140 dcd6 5153 1fcd 2ef3 fe15 90df 2016

ตารางที่ 9 ตัวอย่างข้อมูลเข้าและข้อมูลออกของ MD5

2.2.7 การเข้ารหัสตามมาตรฐาน RFC 822

รหัสตัวอักษร จะต้องเป็นตัวอักษร ตามมาตรฐาน ASCII 7 บิท

2.2.7.1 เข้ารหัสทีละ 6 บิท ดังนั้นรหัสที่ได้จะมีค่าระหว่าง 0 ถึง 63 แทนรหัสแต่ละตัวด้วยรหัสเอสกี้มาตรฐาน 1 ตัว โดยให้ A=0, B=1, C=2, ... ดังแสดงในตาราง ที่ 10

2.2.7.2 เนื่องจากไฟล์คอมพิวเตอร์มาตรฐานจะเข้ารหัสทีละ 8 บิท ดังนั้น ทุก 3 ไบท์ที่เข้า เมื่อแปลง เป็น RFC 822 แล้วจะได้ 4 ไบท์

2.2.7.3 บล๊อกสุดท้ายเป็น ได้ 3 กรณี คือ

- มี 3 ไบท์ กรณีนี้การแปลงรหัสเป็นไปตามปกติไม่มีปัญหา
- มี 2 ไบท์ กรณีนี้ให้เพิ่มไบท์ที่ 3 ไป โดยให้เท่ากับศูนย์ แต่เมื่อแปลงแล้วให้ต่อด้วยเครื่องหมาย เท่ากับ "=" หนึ่งตัว เป็นการบอกว่าเมื่อแปลงกลับให้ลบไบท์สุดท้ายทิ้งไป

- มี 1 ไบท์ กรณีนี้ ให้เพิ่มไบท์ที่ 2 และที่ 3 เข้าไปโดยให้เป็นศูนย์ทั้งคู่ เมื่อแปลงแล้ว ให้ต่อด้วย เครื่องหมายเท่ากับ 2 ตัว "= =" เป็นสัญญาณว่า เมื่อแปลงกลับ ให้ลบ 2 ตัวสุดท้ายทิ้งไป กรรมวิธีดังกล่าว นิยมใช้ในการส่งไฟล์ไปทางจดหมายอีเล็คโทรนิคส์

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

(pad) =

ตารางที่ 10 การเข้ารหัส RFC 822

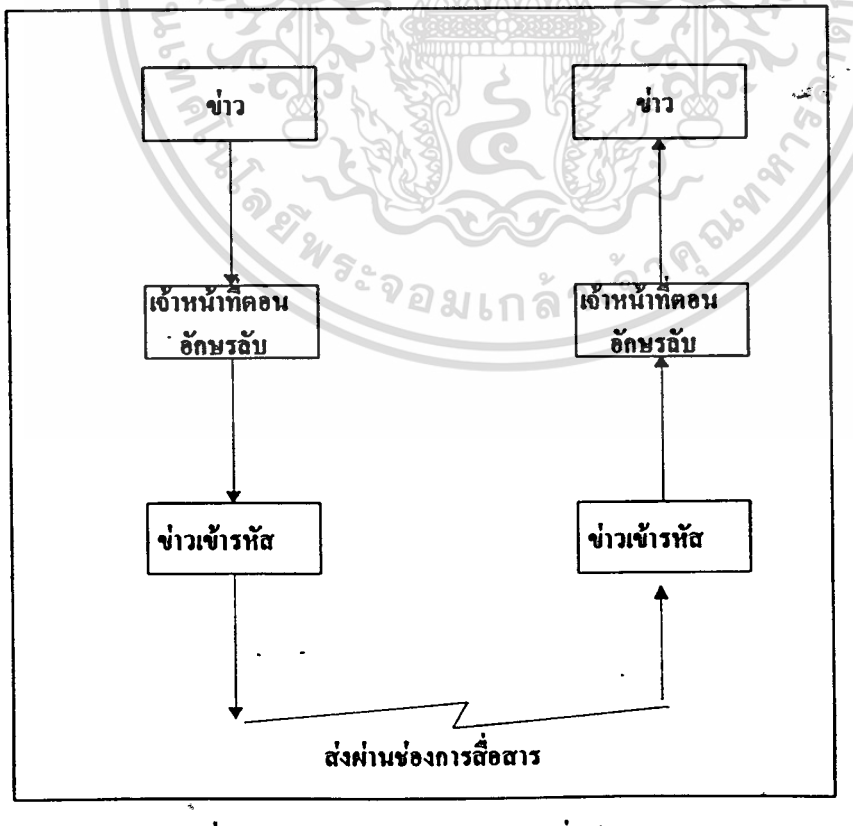
บทที่ 3

วิเคราะห์ และออกแบบระบบ

จากปัญหาข้อขัดข้องในเรื่องการรักษาความลับ และความล่าช้าของการทำงาน ของระบบเดิมที่ใช้อยู่ในกองทัพไทย จึงทำให้เกิดการวิจัย "การเพิ่มประสิทธิภาพ การเข้ารหัสของกองทัพบกไทย" เพื่อช่วยในการเพิ่มประสิทธิภาพ ในการรับส่งข่าวสารที่มีชั้นความลับ ให้มีความปลอดภัยและรวดเร็วยิ่งขึ้น ซึ่งมีขั้นตอนการทำงานดังนี้

3.1 การทำงานของระบบที่ใช้ในปัจจุบัน

ระบบเก่านั้น ผู้ส่งข่าวจะต้องเขียนข่าวที่จะส่งลงในแบบฟอร์มกระดาษเขียนข่าว และส่งข่าวนั้นไปยังเจ้าหน้าที่รับ - ส่ง ซึ่งประจำอยู่ที่ศูนย์การสื่อสารของกองพลหรือกองทัพ เจ้าหน้าที่จะแยกข่าวตามลำดับความเร่งด่วนและชั้นความลับของข่าว ข่าวลับจะนำไปเข้ารหัสที่ตอนอักษรลับ วิธีการเข้ารหัสข่าวจะกระทำด้วยมือโดยเจ้าหน้าที่ตอนอักษรลับ (ภาพที่ 12)

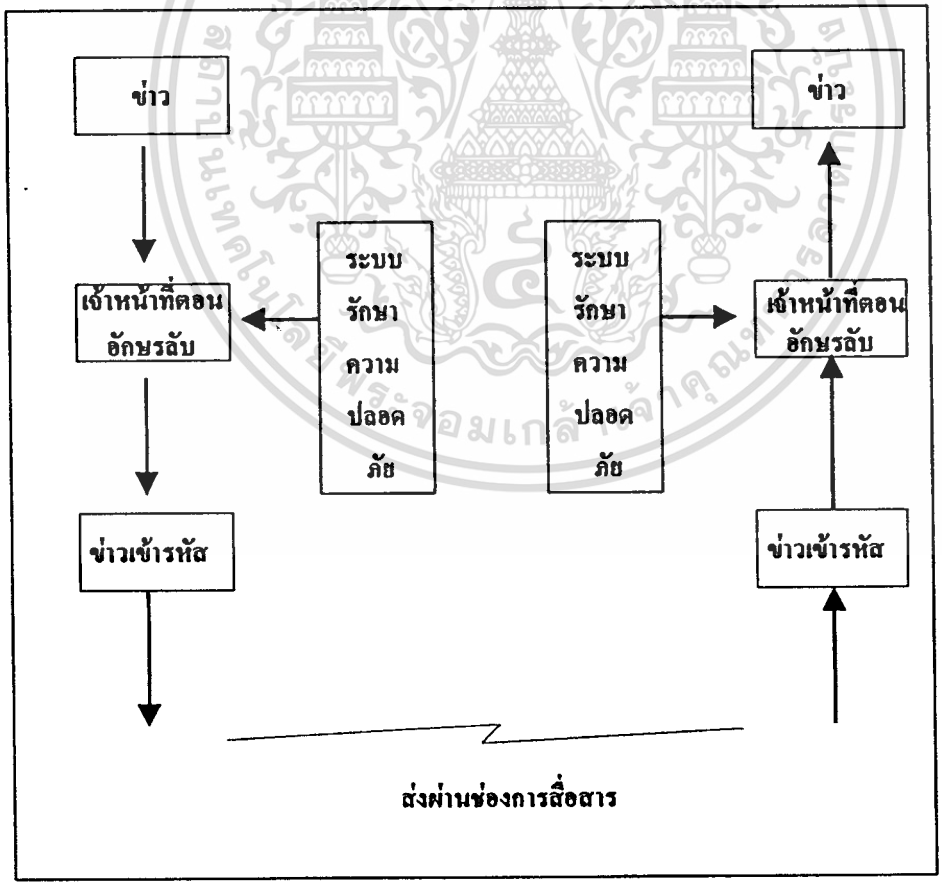


ภาพที่ 12 System Flow Chart ระบบที่ใช้อยู่ในปัจจุบัน

เมื่อได้ข่าวที่เข้ารหัสแล้ว ก็จะนำข่าวไปส่ง ผ่านตอนเครื่องมือ ซึ่งจะทำการส่งข่าวผ่านวิธีรับการสื่อสารต่าง ๆ เช่น พลนำสาร วิทยุโทรศัพท์ ฯลฯ ตามความเหมาะสมเมื่อข่าวผ่านมัชฌิมการสื่อสารไปถึงศูนย์การสื่อสารของผู้รับแล้ว เจ้าหน้าที่ประจำศูนย์ข่าวก็จะทำการแยกตามลำดับความเร่งด่วน และชั้นความลับข่าวที่เข้ารหัส ก็จะนำไปเข้าที่ตอนอักษรลับ เพื่อทำการถอดรหัสข่าวออกมา เมื่อได้ข่าวที่ถูกต้องแล้วจะส่งข่าวจากศูนย์การสื่อสารไปถึงมือผู้รับข่าว

3.2 การทำงานของระบบที่นำเสนอ ใหม่

ในระบบที่นำเสนอใหม่นี้ ผู้ส่งข่าวจะเขียนข่าวลงในกระดาษเขียนข่าวหรือจะเตรียมข่าวให้อยู่ในรูปแบบของแฟ้มข้อมูลส่งให้เจ้าหน้าที่รับส่งข่าว ซึ่งประจำอยู่ที่ศูนย์การสื่อสาร เจ้าหน้าที่ทำการแยกข่าวตามลำดับความเร่งด่วนและชั้นความลับ หากเป็นข่าวลับจะนำไปเข้ารหัสที่ตอนอักษรลับ วิธีการเข้ารหัสข่าวใช้เครื่องคอมพิวเตอร์ และได้ผลออกมาเป็นแฟ้มข้อมูลเข้ารหัส (ภาพที่ 13)



ภาพที่ 13 System Flow Chart ระบบที่นำเสนอใหม่

จากนั้นก็ทำการส่งข่าวผ่านมัชฌิมการสื่อสาร ซึ่งสามารถนำระบบคอมพิวเตอร์มาประยุกต์ใช้ในการส่งข่าวผ่านระบบสายและวิทยุถ่ายทอดสนาม โดยนำอุปกรณ์แปลงสัญญาณ เช่น Modem มาเชื่อมต่อสัญญาณในการส่งแฟ้มข้อมูลเข้ารหัส เมื่อข่าวเดินทางผ่านมัชฌิมการสื่อสารมายังศูนย์การสื่อสารของผู้รับแล้วเจ้าหน้าที่จึงทำการแยกข่าว

หากเป็นข่าวที่เข้ารหัสก็จะส่งไปที่ตอนอักษรลับ เพื่อทำการถอดรหัสข่าวด้วยคอมพิวเตอร์ ตรวจสอบความถูกต้อง และยืนยันความน่าเชื่อถือของข่าว เมื่อเสร็จกระบวนการแล้วก็จะส่งข่าวจากศูนย์การสื่อสารไปถึงมือผู้รับข่าว

3.3 ขั้นตอนการทำงานของระบบ (System Design)

การรับส่งข่าวสารตามระบบใหม่นี้ นำวิธีการเข้ารหัสแบบกุญแจลับ (Secret Key) และวิธีการเข้ารหัสแบบกุญแจสาธารณะ (Public Key) มารวมเข้าด้วยกัน เพื่อเสริมจุดเด่นของระบบ โดยนำข้อดีของทั้งสองระบบมาผสมผสานเข้าด้วยกัน อันเป็นการเพิ่มการรักษาความปลอดภัยให้ระบบใหม่มากยิ่งขึ้น และลดจุดอ่อนของแต่ละระบบลงจากขั้นตอนการทำงานของระบบ และใช้เป็นพื้นฐานในการออกแบบรายละเอียดในกรรมวิธีตามขั้นตอนดังนี้

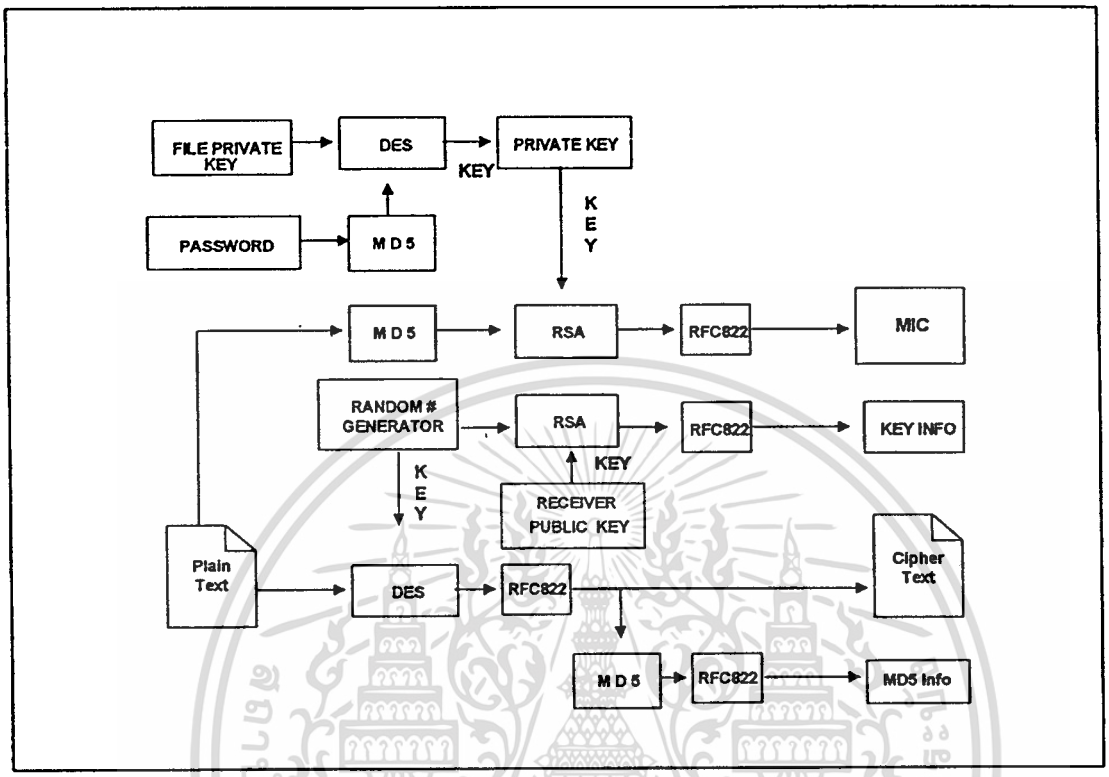
3.3.1 วิธีเข้ารหัส

การเข้ารหัสโดยใช้ระบบใหม่นี้ มีกรรมวิธีดังนี้ (ภาพที่ 14)

3.3.1.1 นำข่าวกระจ่างที่จะส่งมาทำการเข้ารหัสเดส โดยใช้กุญแจที่สร้างขึ้นจากตัวเลขสุ่ม (Random Number) แล้วจึงเข้ารหัส RFC 822 ผลที่ได้คือเอกสารเข้ารหัส (Cipher Text) ขั้นตอนนี้จะต้องสร้างกุญแจรหัสขึ้นมาใหม่ทุกครั้ง ดังนั้น หากนำข่าวเดียวกันไปเข้ารหัส แต่ละครั้งจะได้ผลออกมาไม่เหมือนกัน

3.3.1.2 นำกุญแจรหัสที่สร้างขึ้นมาจากตัวเลขสุ่มตามข้อ 3.3.1.1 ไปเข้ารหัสอาร์เอสเอด้วยกุญแจสาธารณะของผู้รับ แล้วนำไปเข้ารหัส RFC 822 ได้ผลลัพธ์เป็นข้อมูลเข้ารหัสของกุญแจลับ (Key Information) ขั้นตอนนี้ทำให้ผู้รับและผู้ส่งไม่ต้องตกลงกันล่วงหน้าว่าจะใช้กุญแจใดในการเข้า-ถอดรหัส เนื่องจากเฉพาะผู้รับที่ถูกต้องเท่านั้นที่จะสามารถใช้กุญแจส่วนตัวของตนถอดรหัสได้

3.3.1.3 นำรหัสผ่านของผู้ส่ง ไปเข้ากระบวนการสังเคราะห์ข่าว เพื่อนำไปใช้เป็นกุญแจในการถอดรหัสเดส กับแฟ้มข้อมูลกุญแจส่วนตัว (Private Key File) ที่เก็บไว้ในคอมพิวเตอร์ โดยเทียบดูจากชื่อผู้ใช้ วิธีการนี้จะทำให้ได้กุญแจส่วนตัวของผู้ส่ง และเป็นการเพิ่มการรักษาความปลอดภัยแก่กุญแจส่วนตัว เนื่องจากถึงแม้ข้าศึกจะค้นพบแฟ้มข้อมูลที่บันทึกไว้ในเครื่องคอมพิวเตอร์ แต่ก็จำเป็นจะต้องใช้รหัสผ่านของผู้ส่งมาประกอบกันจึงจะสามารถถอดรหัสได้



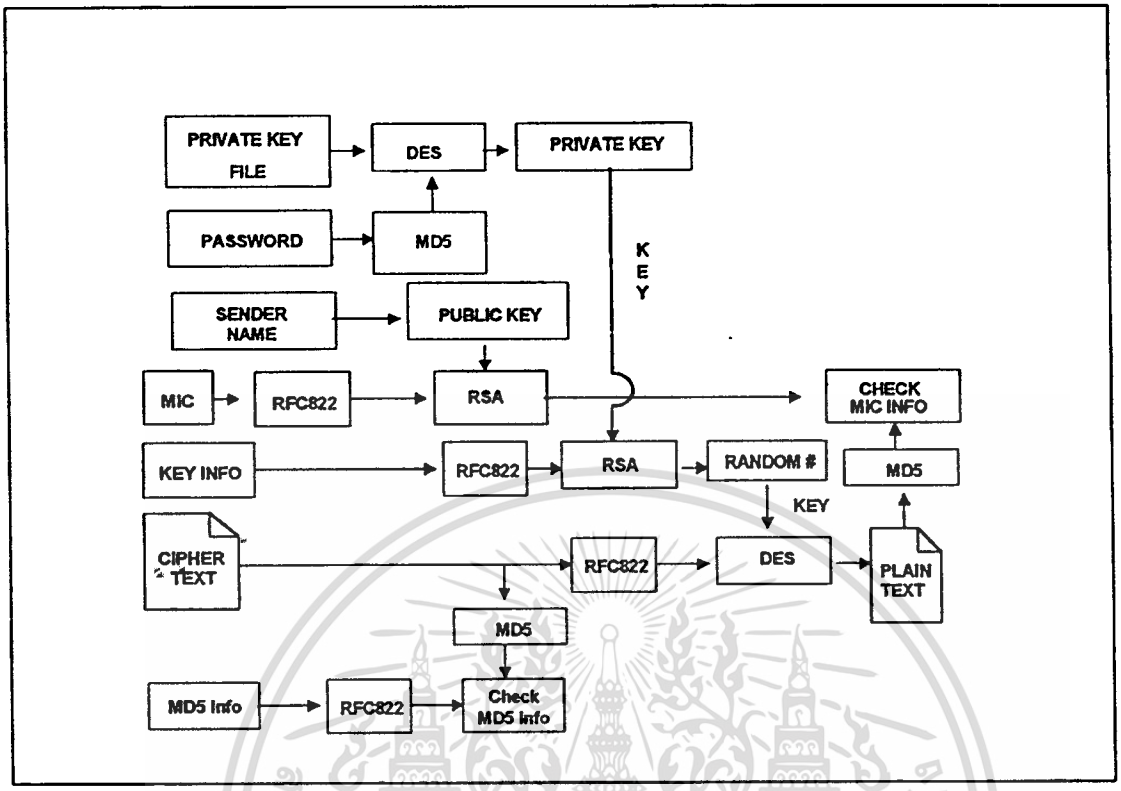
ภาพที่ 14 วิธีเข้ารหัสของระบบใหม่

3.3.1.4 นำข่าวที่ยังไม่ได้เข้ารหัสไปผ่านกระบวนการสังเคราะห์ข่าว เพื่อนำผลลัพธ์ที่ได้ไปเข้ารหัสอาร์เอสเอ โดยใช้กุญแจส่วนตัวของผู้ส่ง ที่ได้จากข้อ 3.3.1.3 แล้วจึงเข้ารหัส RFC 822 จะได้ผลลัพธ์ซึ่งสามารถใช้ตรวจสอบความถูกต้องของข่าวสาร (Message Integrity Check - MIC) ได้ว่าข่าวที่ส่งถูกปลอมแปลงแก้ไขหรือไม่ เพราะต้องใช้กุญแจส่วนตัวของผู้ส่งเท่านั้นในการส่ง

3.3.1.5 นำข่าวที่ผ่านการเข้ารหัสแล้วจากข้อ 3.3.1.1 มาเข้ากระบวนการสังเคราะห์ข่าว แล้วเข้ารหัส RFC 822 ได้ผลลัพธ์เป็น MD5 Info. เพื่อใช้ตรวจสอบความถูกต้องของข่าวเข้ารหัส

3.3.2 วิธีถอดรหัส

ผู้รับข่าวจะทำการถอดรหัสด้วยวิธีการกลับกันกับวิธีเข้ารหัสที่กล่าวมาข้างต้น โดยมีกรรมวิธีดังแสดงในภาพที่ 15 ดังนี้



ภาพที่ 15 วิธีถอดรหัสของระบบใหม่

3.3.2.1 นำข่าวเข้ารหัส (Cipher Text) มาผ่านกระบวนการสังเคราะห์ข่าว ผลลัพธ์ที่ได้นำไปเปรียบเทียบกับ MD5 Info. ที่รับเข้ามาซึ่งผ่านการถอดรหัส RFC 822 แล้ว เพื่อตรวจสอบความถูกต้องของข่าวเข้ารหัส

3.3.2.2 นำรหัสผ่านของผู้รับไปเข้ากระบวนการสังเคราะห์ข่าว เพื่อใช้เป็นกุญแจในการถอดรหัสแบบเดส ด้วยแฟ้มข้อมูลกุญแจส่วนตัวที่เก็บไว้ในเครื่องคอมพิวเตอร์ โดยดูจากชื่อผู้ใช้ ขั้นตอนนี้จะได้กุญแจส่วนตัวของผู้รับ

3.3.2.3 นำข้อมูลของกุญแจลับ ซึ่งผ่านการถอดรหัส RFC 822 แล้ว มาถอดรหัสอาร์เอสเอด้วยกุญแจส่วนตัวของผู้รับที่ได้จากข้อ 3.3.2.2 ขั้นตอนนี้จะได้กุญแจที่เกิดจากตัวเลขสุ่ม

3.3.2.4 นำข้อมูลเข้ารหัส ซึ่งผ่านการถอดรหัส RFC 822 แล้วไปถอดรหัสเดสโดยใช้กุญแจที่ได้จากข้อ 3.3.2.3 ขั้นตอนนี้จะได้ข่าวต้นฉบับที่เป็นข่าวกระจ่างต้นฉบับ

3.3.2.5 นำ MIC ที่ผ่านการถอดรหัส RFC 822 แล้ว มาถอดรหัสอาร์เอสเอ โดยใช้กุญแจสาธารณะของผู้ส่ง ซึ่งมีข้อมูลบันทึกอยู่ในเครื่องคอมพิวเตอร์แล้ว

3.3.2.6 นำข่าวกระจ่างที่ได้จากข้อ 3.3.2.4 มาเข้ากระบวนการสังเคราะห์ข่าว แล้วเปรียบเทียบกับผลลัพธ์ที่ได้จากข้อ 3.3.2.5 เพื่อเป็นการตรวจสอบ หากได้ผลตรงกันแสดงว่าข่าวนั้นมิได้ถูกปลอมแปลงแก้ไข

3.4 รายละเอียดการทำงานของระบบ (Detail Design)

3.4.1 ผลลัพธ์ของระบบ (Output Design)

ผลลัพธ์ที่ต้องการของระบบคือทำการเข้ารหัสข่าวที่จะส่ง และถอดรหัสข่าวที่รับเข้า ให้อยู่ในรูปของแฟ้มข้อมูล(Text File)ได้ถูกต้อง

3.4.2 ข้อมูลนำเข้าระบบ (Input Design)

3.4.2.1 ข้อมูลข่าวในรูปของแฟ้มข้อมูล

3.4.2.2 ข้อมูลประกอบจากผู้ใช้ ได้แก่

- ชื่อผู้ส่งข่าว และ รหัสผ่าน
- ชื่อผู้รับข่าว และ รหัสผ่าน
- ชื่อแฟ้มข่าว ก่อน และหลัง การเข้ารหัส

3.4.3 รูปแบบการจัดเก็บข้อมูลข่าวเข้ารหัส (File Design) ประกอบด้วย

- MD5 Info.
- ชื่อผู้ส่ง
- MIC Info.
- ชื่อผู้รับ
- Key Info.
- เนื้อข่าวเข้ารหัส

3.4.4 การประมวลผลของระบบ (Process Design)

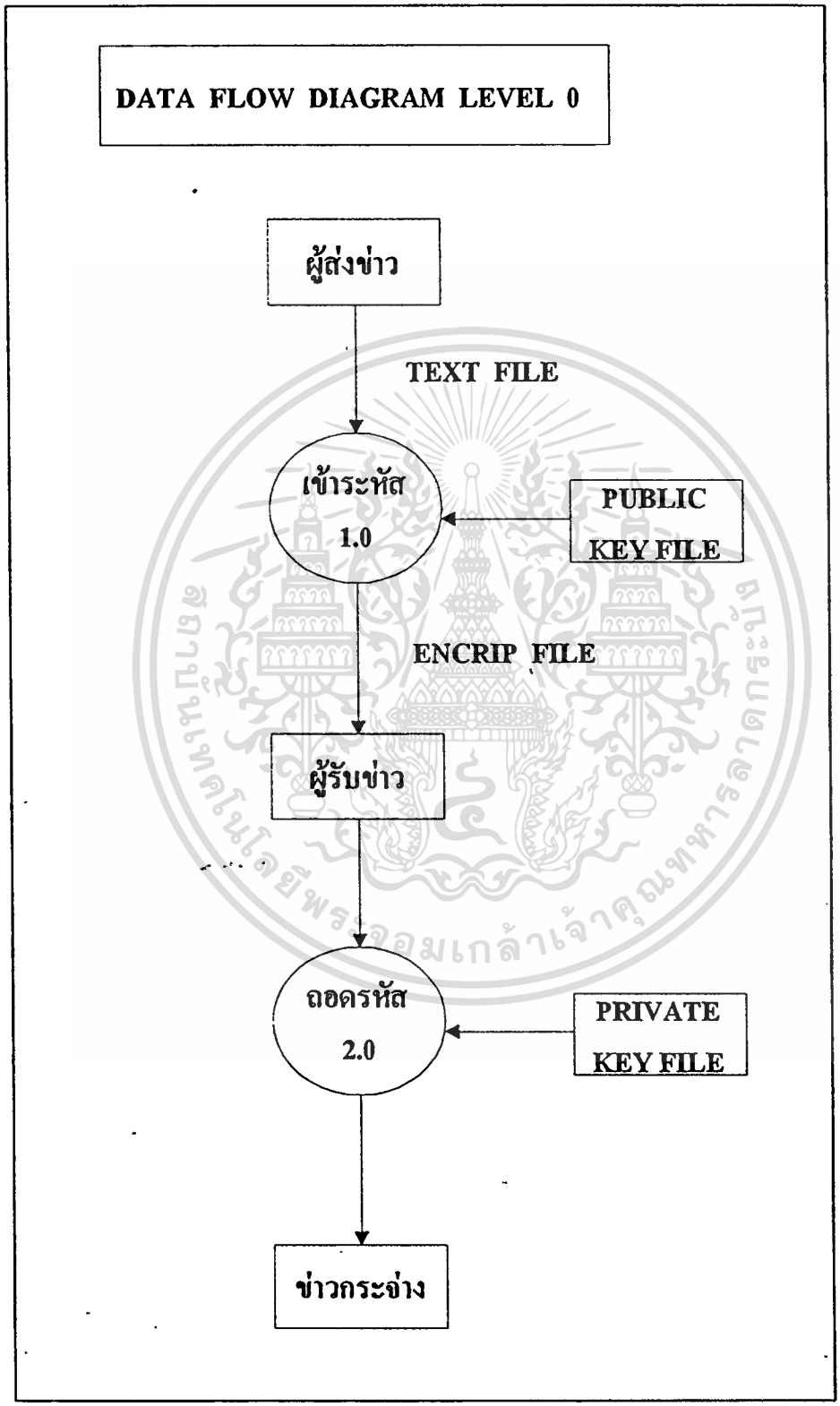
3.4.4.1 ส่วนการเข้ารหัส (Encryption)

3.4.4.2 ส่วนการถอดรหัส (Decryption)

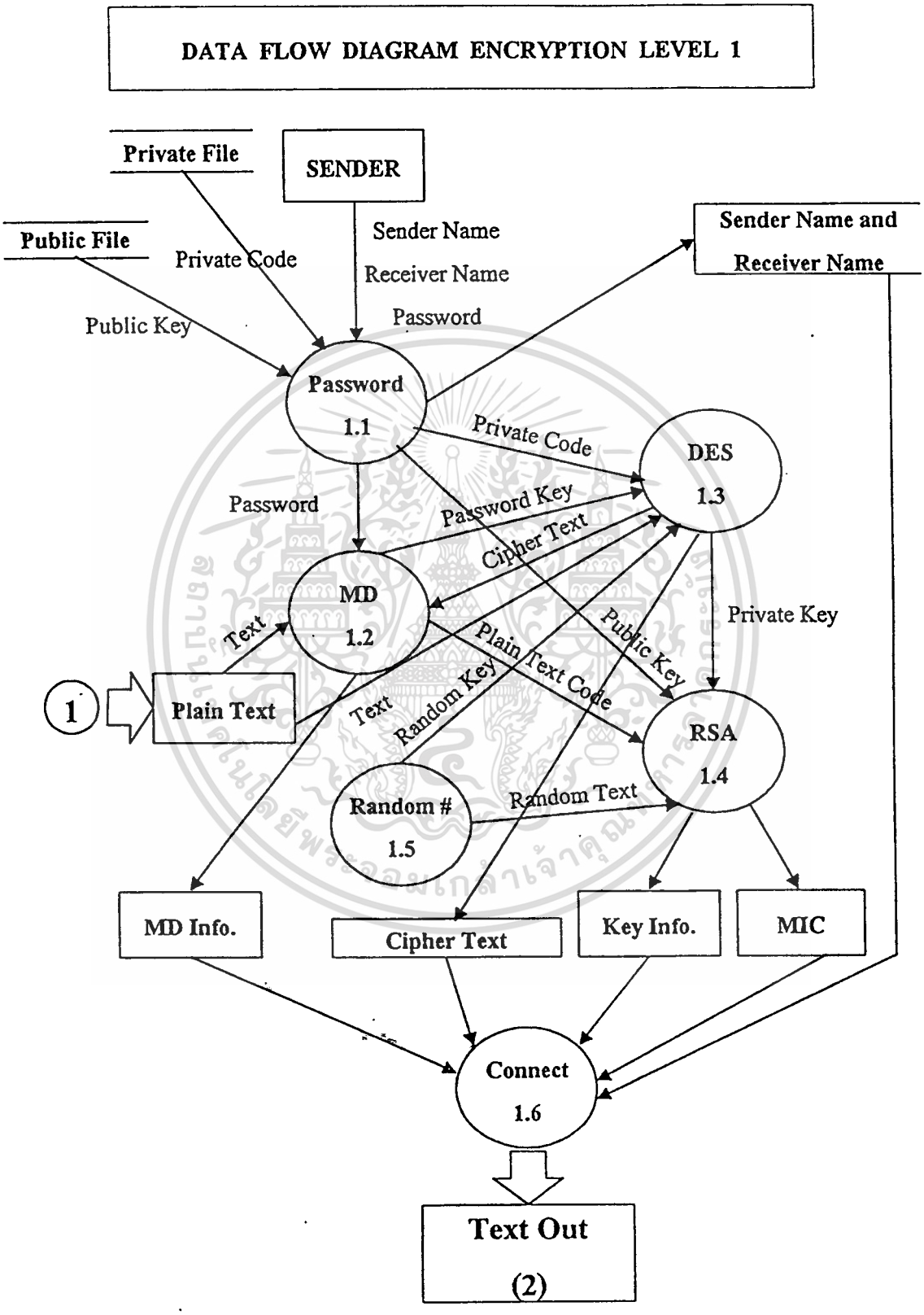
3.4.4.3 ส่วนการสร้างกุญแจ (Key Generator)

3.4.4.4 ส่วนการสร้างตัวเลขสุ่ม (Random Number Generator)

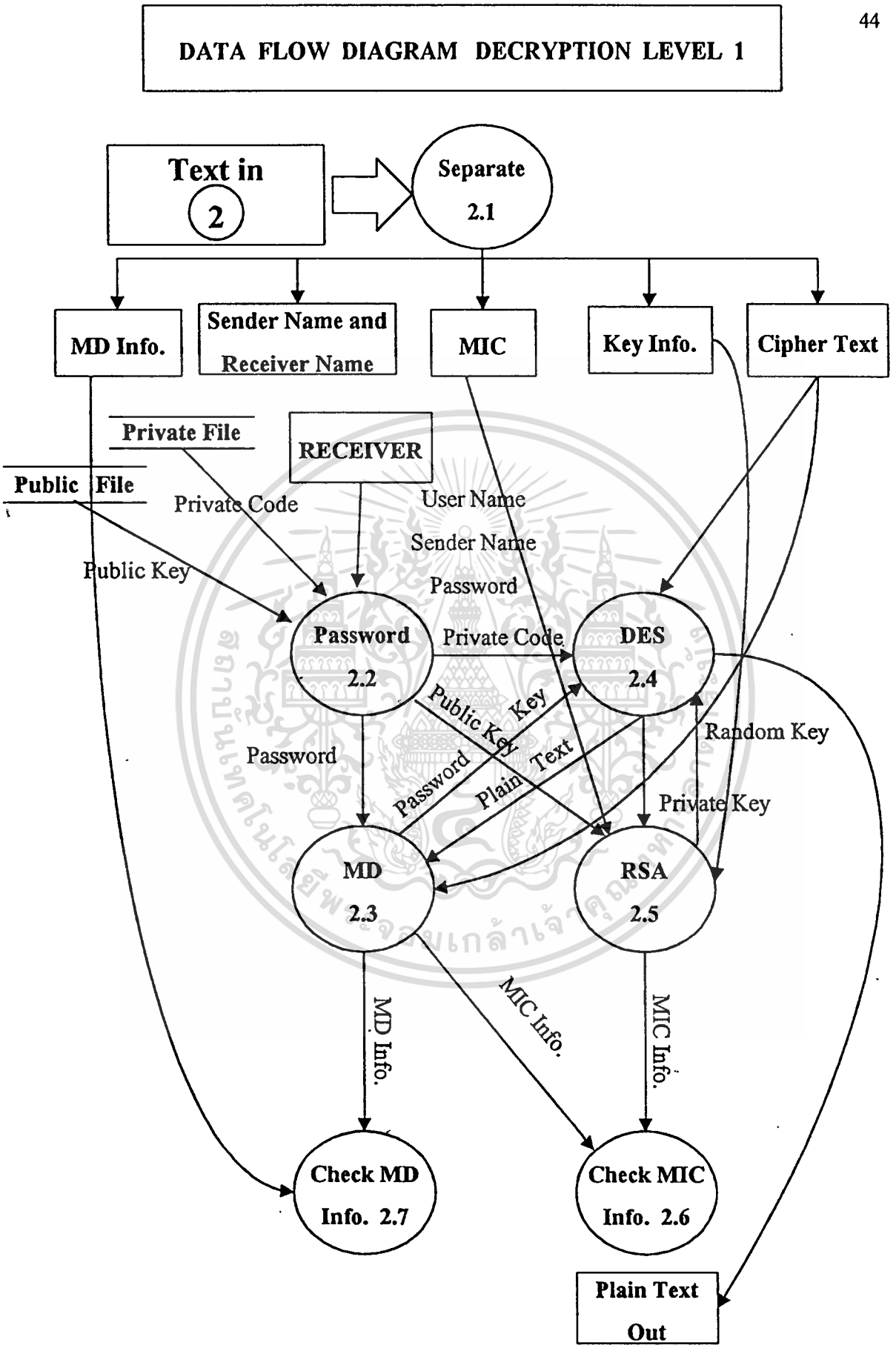
ดังรายละเอียดปรากฏตามดาต้าโฟลว์ ไดอะแกรม (ภาพที่ 16 17 และ 18)



ภาพที่ 16 Data Flow Diagram การรับ-ส่งข่าว



ภาพที่ 17 Data Flow Diagram การเข้ารหัส



ภาพที่ 18 Data Flow Diagram การถอดรหัส

3.5 พจนานุกรม ดาต้าโฟลว์ไดอะแกรม ระบบเข้า-ถอดรหัสที่นำเสนอใหม่

ชื่อกรรมวิธี 1.1 : Password

รายละเอียด : รับข้อมูล ชื่อผู้ส่ง (Sender Name) ชื่อผู้รับ (Receiver Name) และ รหัสผ่าน (Password) ของผู้ส่ง

: นำชื่อผู้ส่งไปหา Private Code จากแฟ้ม Private Code ส่งไปกรรมวิธี 1.3 (DES)

: ส่งรหัสผ่านไป กรรมวิธี 1.2 (MD5)

: นำชื่อผู้รับไปหา Public Key ในแฟ้มกุญแจส่วนตัว ส่งไปกรรมวิธี 1.4 (RSA)

: ส่ง Sender Name และ Password ไปกรรมวิธี 1.6 (Connect)

ชื่อกรรมวิธี 1.2 : MD5 (Massage Digest)

รายละเอียด : รับ Password จากกรรมวิธี 1.1 (Password) มาทำการเข้ารหัส ได้ผลลัพธ์เป็น Password Key ส่งไปเข้ากรรมวิธี 1.3 (DES)

: รับข้อมูล Plain Text มาทำการเข้ารหัส แล้วส่ง Plain Text Code ไปเข้ากรรมวิธี 1.4 (RSA)

: รับ Cipher Text จากกรรมวิธี 1.3 (DES) มาเข้ารหัส ได้ผลลัพธ์เป็น MD5 Info. ส่งไปกรรมวิธี 1.6 (Connect)

ชื่อกรรมวิธี 1.3 : DES (Data Encryption Standard)

รายละเอียด : รับ Private Code จากกรรมวิธี 1.1 (Password) และ Password Key จากกรรมวิธี 1.2 (MD5) มาทำการเข้ารหัสข้อมูล Private Code โดยใช้ Password Key เป็นกุญแจในการเข้ารหัส ได้ผลลัพธ์เป็น Private Key ส่งไปกรรมวิธี 1.4 (RSA)

: รับ Plain Text จากแฟ้ม Plain Text และ Random Key จากกรรมวิธี 1.5 (Random No.) มาเข้ารหัสข้อมูลโดยใช้ Random Key เป็นกุญแจเข้ารหัส ได้ผลลัพธ์เป็น Cipher Text ส่งไปกรรมวิธี 1.6 (Connect) และกรรมวิธี 1.2 (MD5)

ชื่อกรรมวิธี 1.4 : RSA

รายละเอียด : รับ Random Text จากกรรมวิธี 1.5 (Random #) และ Public Key ของผู้รับจากกรรมวิธี 1.1 (Password) ทำการเข้ารหัสข้อมูล Random Text โดยใช้ Public Key ของผู้รับเป็นกุญแจได้ผลลัพธ์เป็น Key Info. ส่งไปกรรมวิธี 1.6 (Connect)

: รับ Private Key ของผู้ใช้จากกรรมวิธี 1.3 (DES) และ Plain Text Code จากกรรมวิธี 1.2 (MD5) มาทำการเข้ารหัสข้อมูล Plain Text Code โดยใช้ Private Key ของผู้ใช้เป็นกุญแจ ได้ผลลัพธ์เป็น MIC ส่งไปกรรมวิธี 1.6 (Connect)

ชื่อกรรมวิธี 1.5 : Random No.

รายละเอียด : โมดูลใช้สร้างตัวเลขสุ่ม

: ส่ง Random Key ให้กรรมวิธี 1.3 (DES)

: ส่ง Random Text ให้กรรมวิธี 1.4 (RSA)

ชื่อกรรมวิธี 1.6 : Connect

รายละเอียด : รับ MD5 Info., Key Info., MIC, Sender Name and Receiver Name และ Cipher Text มาต่อกันเพื่อส่งเป็นข่าวออก

ชื่อกรรมวิธี 2.1 : Separate

รายละเอียด : แยกข้อมูล MD5 Info., Key Info., MIC, Sender Name and Receiver Name และ Cipher Text ออกจากกัน

: ส่ง MIC ไปให้ กรรมวิธี 2.5 (RSA).

: ส่ง MD5 Info. ไปกรรมวิธี 2.7 (Check MD5 Info.)

: ส่ง Key Info. ไป กรรมวิธี 2.5 (RSA)

: ส่ง Sender Name and Receiver Name ไปกรรมวิธี 2.2 (Password)

: ส่ง Cipher Text ไปกรรมวิธี 2.4 (DES)

: ส่ง Cipher Text ไปกรรมวิธี 2.3 (MD5)

ชื่อกรรมวิธี 2.2 : Password

รายละเอียด : รับ User Name (Receiver Name) และ Sender Name จากกรรมวิธี 2.1(Separate) และ Password ของผู้รับ

: นำ User Name ไปหา Private Code จากไฟล์ Private Code ส่งไปกรรมวิธี 2.4 (DES)

: ส่ง Password ไปกรรมวิธี 2.3 (MD5)

: นำ Sender Name ไปหา Public Key ในไฟล์ Public Key ส่งไปกรรมวิธีที่ 2.5 (RSA)

ชื่อกรรมวิธี 2.3 : MD5

รายละเอียด : รับ Password จากกรรมวิธี 2.2 (Password) มาทำการเข้ารหัส ได้ผลลัพธ์เป็น Password Key ส่งกรรมวิธี 2.4 (DES)

: รับข้อมูล Cipher Text จากกรรมวิธี 2.1(Separate) มาทำการเข้ารหัส ได้ผลลัพธ์เป็น MD5 Info. ส่งไปกรรมวิธี 2.7 (Check MD5 Info.)

: รับ Plain Text จากกรรมวิธี 2.4 (DES) มาทำการเข้ารหัสได้ผลลัพธ์เป็น MIC Info. ส่งไปกรรมวิธี 2.6 (Check MIC Info.)

ชื่อกรรมวิธี 2.4 : DES

รายละเอียด : รับ Private Code จากกรรมวิธี 2.2 (Password) และPassword Key จากกรรมวิธี 2.3 (MD5) มาทำการเข้ารหัสข้อมูล Private Code โดยใช้ Password Key เป็นกุญแจในการเข้ารหัส ได้ผลลัพธ์เป็น Private Key ส่งไปกรรมวิธี 2.5 (RSA)

: รับ Cipher Text จากกรรมวิธี 2.1(Separate) และ Random Key

จากกรรมวิธี 2.5 (RSA) มาทำการถอดรหัสขอมูล Cipher Text โดยใช้ Random Key เป็นกุญแจในการถอดรหัส ได้ผลลัพธ์เป็นข่าวกระจ่าง (Plain Text) ส่งไปยัง กรรมวิธี 2.3 (MD5) และ Text Out

ชื่อกรรมวิธี 2.5	:	RSA
รายละเอียด	:	รับ MIC จากกรรมวิธี 2.1(Separate) และ Public Key ของผู้ส่งจาก กรรมวิธี 2.2 (Password) มาทำการถอดรหัส MIC โดยใช้ Public Key ของผู้ส่งข่าวเป็นกุญแจได้ผลลัพธ์เป็น MIC Info. ส่งไปกรรมวิธี 2.6 (Check MIC)
	:	รับ Key Info. จากกรรมวิธี 2.1(Separate) และ Private Key ของผู้ใช้จากกรรมวิธี 2.4 (DES) มาทำการถอดรหัส Key Info. โดยใช้ Private Key ของผู้ใช้เป็นกุญแจได้ผลลัพธ์เป็น Random Key ส่งไปกรรมวิธี 2.4 (DES)
ชื่อกรรมวิธี 2.6	:	Check MIC
รายละเอียด	:	รับ MIC Info. จากกรรมวิธี 2.5 (RSA) และ MIC Info. จากกรรมวิธี 2.3 (MD5) นำทั้งสองมาตรวจสอบเปรียบเทียบ ถ้าตรงกันแสดงว่าข่าวที่ถอดรหัสถูกต้อง
ชื่อกรรมวิธี 2.7	:	Check MD5 Info.
รายละเอียด	:	รับ MD5 Info. จากกรรมวิธี 2.1(Separate) และ MD5 Info. จากกรรมวิธี 2.3 (MD5) นำทั้งสองมาตรวจสอบเปรียบเทียบ ถ้าตรงกันแสดงว่าข่าวที่รับเข้าถูกต้อง
ชื่อคาต้าโฟลว์	:	Sender Name, Receiver Name, Password
รายละเอียด	:	ชื่อผู้ส่ง ชื่อผู้รับ รหัสผ่านของผู้ส่ง
จากกรรมวิธี	:	ข่าวและการส่งข่าว
ไปกรรมวิธี	:	1.1 Password

ชื่อคาต้าโฟลว์ : Private Code
รายละเอียด : ส่ง Private Code ของผู้ส่ง
จากกรรมวิธี : แฟ้มข้อมูล Private File
ไปกรรมวิธี : 1.1 Password

ชื่อคาต้าโฟลว์ : Public Key
รายละเอียด : Public Key ของผู้รับ
จากกรรมวิธี : แฟ้มข้อมูล Public File
ไปกรรมวิธี : 1.1 Password

ชื่อคาต้าโฟลว์ : Private Code
รายละเอียด : Private Code ของผู้ส่ง
จากกรรมวิธี : 1.1 Password
ไปกรรมวิธี : 1.3 DES

ชื่อคาต้าโฟลว์ : Public Key
รายละเอียด : Public Key ของผู้รับ
จากกรรมวิธี : 1.1 Password
ไปกรรมวิธี : 1.4 RSA

ชื่อคาต้าโฟลว์ : Password
รายละเอียด : รหัสผ่าน
จากกรรมวิธี : 1.1 Password
ไปกรรมวิธี : 1.2 MD5

ชื่อคาต้าโฟลว์ : Password Key
รายละเอียด : Password Key ของผู้ส่ง
จากกรรมวิธี : 1.2 MD5
ไปกรรมวิธี : 1.3 DES

ชื่อคาต้าโฟลว์	:	Plain Text Code
รายละเอียด	:	Plain Text Code
จากกรรมวิธี	:	1.2 MD5
ไปกรรมวิธี	:	1.4 RSA

ชื่อคาต้าโฟลว์	:	Cipher Text
รายละเอียด	:	ข่าวเข้ารหัส
จากกรรมวิธี	:	1.3 DES
ไปกรรมวิธี	:	1.2 MD5

ชื่อคาต้าโฟลว์	:	Random Text
รายละเอียด	:	ตัวเลขสุ่ม
จากกรรมวิธี	:	1.5 Random No.
ไปกรรมวิธี	:	1.4 RSA

ชื่อคาต้าโฟลว์	:	Random Key
รายละเอียด	:	ตัวเลขสุ่ม
จากกรรมวิธี	:	1.5 Random No.
ไปกรรมวิธี	:	1.3 DES

ชื่อคาต้าโฟลว์	:	Private Key
รายละเอียด	:	Private Key ผู้ส่ง
จากกรรมวิธี	:	1.3 DES
ไปกรรมวิธี	:	1.4 RSA

ชื่อคาต้าโฟลว์	:	Text
รายละเอียด	:	ข่าวที่จะส่ง
จากกรรมวิธี	:	แฟ้มข้อมูล Plain Text
ไปกรรมวิธี	:	1.2 MD5

ชื่อดาต้าโฟลว์	:	Text
รายละเอียด	:	ข่าวที่จะส่ง
จากกรรมวิธี	:	แฟ้มข้อมูล Plain Text
ไปกรรมวิธี	:	1.3 DES
ชื่อดาต้าโฟลว์	:	Sender Name and Receiver Name
รายละเอียด	:	ชื่อผู้ส่ง และ ชื่อผู้รับ
จากกรรมวิธี	:	1.1 Password
ไปกรรมวิธี	:	1.6 Connect
ชื่อดาต้าโฟลว์	:	MD5 Info.
รายละเอียด	:	MD5 Info.
จากกรรมวิธี	:	1.2 MD5
ไปกรรมวิธี	:	1.6 Connect
ชื่อดาต้าโฟลว์	:	MIC
รายละเอียด	:	Message Integrity Check
จากกรรมวิธี	:	1.4 RSA
ไปกรรมวิธี	:	1.6 Connect
ชื่อดาต้าโฟลว์	:	Key Info.
รายละเอียด	:	Key Information
จากกรรมวิธี	:	1.4 RSA
ไปกรรมวิธี	:	1.6 Connect
ชื่อดาต้าโฟลว์	:	Cipher Text
รายละเอียด	:	ข่าวเข้ารหัส
จากกรรมวิธี	:	1.3 DES
ไปกรรมวิธี	:	1.6 Connect

ชื่อคาต้าโฟลว์	:	Sender Name and Receiver Name
รายละเอียด	:	ชื่อผู้ส่ง และ ชื่อผู้รับ ของข่าวที่รับเข้า
จากกรรมวิธี	:	2.1 Separate
ไปกรรมวิธี	:	2.2 Password

ชื่อคาต้าโฟลว์	:	MD5 Info.
รายละเอียด	:	MD5 Info. ของข่าวที่รับเข้า
จากกรรมวิธี	:	2.1 Separate
ไปกรรมวิธี	:	2.7 Check MD5 Info.

ชื่อคาต้าโฟลว์	:	MIC
รายละเอียด	:	MIC ของข่าวที่รับเข้า
จากกรรมวิธี	:	2.1 Separate
ไปกรรมวิธี	:	2.5 RSA

ชื่อคาต้าโฟลว์	:	Key Info.
รายละเอียด	:	Key Info. ของข่าวที่รับเข้า
จากกรรมวิธี	:	2.1 Separate
ไปกรรมวิธี	:	2.5 RSA

ชื่อคาต้าโฟลว์	:	Cipher Text
รายละเอียด	:	ข่าวเข้ารหัส
จากกรรมวิธี	:	2.1 Separate
ไปกรรมวิธี	:	2.3 MD5

ชื่อคาต้าโฟลว์	:	Cipher Text
รายละเอียด	:	ข่าวเข้ารหัส
จากกรรมวิธี	:	2.1 Separate
ไปกรรมวิธี	:	2.4 DES

ชื่อดาต้าโฟลว์	:	User Name, Sender Name, Password
รายละเอียด	:	ชื่อผู้ใช้(ผู้รับ) ชื่อผู้ส่ง รหัสผ่าน
จากกรรมวิธี	:	ข่าวเข้าและการส่งข่าว
ไปกรรมวิธี	:	2.2 Password

ชื่อดาต้าโฟลว์	:	Private Code
รายละเอียด	:	Private Code ของผู้ใช้(ผู้รับ)
จากกรรมวิธี	:	แฟ้มข้อมูล Private File
ไปกรรมวิธี	:	2.2 Password

ชื่อดาต้าโฟลว์	:	Public Key
รายละเอียด	:	Public Key ของผู้ส่ง
จากกรรมวิธี	:	แฟ้มข้อมูล Public File
ไปกรรมวิธี	:	2.2 Password

ชื่อดาต้าโฟลว์	:	Private Code
รายละเอียด	:	Private Code ของผู้ใช้(ผู้รับ)
จากกรรมวิธี	:	2.2 Password
ไปกรรมวิธี	:	2.4 DES

ชื่อดาต้าโฟลว์	:	Public Key
รายละเอียด	:	Public Key ของผู้ส่ง
จากกรรมวิธี	:	2.2 Password
ไปกรรมวิธี	:	2.5 RSA

ชื่อดาต้าโฟลว์	:	Password
รายละเอียด	:	รหัสผ่านของผู้ใช้(ผู้รับ)
จากกรรมวิธี	:	2.2 Password
ไปกรรมวิธี	:	2.3 MD5

ชื่อดาต้าโฟลว์	:	Plain Text
รายละเอียด	:	ข่าวที่ถอดรหัสแล้ว
จากกรรมวิธี	:	2.4 DES
ไปกรรมวิธี	:	2.3 MD5

ชื่อดาต้าโฟลว์	:	Plain Text
รายละเอียด	:	ข่าวที่ถอดรหัสแล้ว
จากกรรมวิธี	:	2.4 DES
ไปกรรมวิธี	:	ข่าวออก

ชื่อดาต้าโฟลว์	:	Private Key
รายละเอียด	:	Private Key ของผู้ใช้ (ผู้รับ)
จากกรรมวิธี	:	2.4 DES
ไปกรรมวิธี	:	2.5 RSA

ชื่อดาต้าโฟลว์	:	Random Key
รายละเอียด	:	ตัวเลขสุ่ม (ของผู้ส่ง)
จากกรรมวิธี	:	2.5 RSA
ไปกรรมวิธี	:	2.4 DES

ชื่อดาต้าโฟลว์	:	MIC Info.
รายละเอียด	:	MIC Info.
จากกรรมวิธี	:	2.5 RSA
ไปกรรมวิธี	:	2.6 Check MIC Info.

ชื่อดาต้าโฟลว์	:	Password Key
รายละเอียด	:	Password Key
จากกรรมวิธี	:	2.3 MD5
ไปกรรมวิธี	:	2.4 DES

ชื่อคาด้าโฟลว์ : MIC Info

รายละเอียด : MIC Info

จากกรรมวิธี : 2.3 MD5

ไปกรรมวิธี : 2.6 Check MIC Info.

ชื่อคาด้าโฟลว์ : MD5 Info.

รายละเอียด : MD5 Info.

จากกรรมวิธี : 2.3 MD5

ไปกรรมวิธี : 2.7 Check MD5 Info

3.6 การสร้างกุญแจของอาร์เอสเอ

การสร้างกุญแจของอาร์เอสเอ ใช้ โมดูล ชื่อ DoGenerateKeys () ของ RSAREF เมื่อเรียกโมดูล จะทำการ สร้าง Public Key และ Private Key บนโครงสร้าง R_RSA_PUBLIC_KEY และ R_RSA_PRIVATE_KEY โดยกำหนดโครงสร้างไว้ล่วงหน้าคือ

```
R_RSA_PUBLIC_KEY
        unsigned int bits;
        unsigned char modulus [MAX_RSA_MODULUS_LEN];
        unsigned char exponent [MAX_RSA_MODULUS_LEN];

R_RSA_PRIVATE_KEY
        unsigned int bits;
        unsigned char modulus [MAX_RSA_MODULUS_LEN];
        unsigned char publicExponent [MAX_RSA_MODULUS_LEN] ;
        unsigned char exponent [MAX_RSA_MODULUS_LEN];
        unsigned char prime [2] [MAX_RSA_PRIME__LEN];
        unsigned char primeExponent [2] [MAX_RSA_PRIME_LEN];
        unsigned char coefficient [MAX_RSA_PRIME_LEN];
```

เมื่อเสร็จจาก โมดูล แล้วทำการ บันถึกข้อมูลตามโครงสร้างลง แฟ้มข้อมูล

3.7 อัลกอริทึมที่สำคัญของระบบ

3.7.1 อัลกอริทึม Gen_Initial_Random

```
Dimension Key (64)
        i = 0
        j = 0
While i < 256
        If HitKeyboard ()
                Key( j ) = Hex( i )
                j  = j +1
        Endif
        i = i +1
        If      i = 256
                i = 0
        Endif
        If      j > 63
        Exit loop
        End if
    End
    Write_Key_To_File (Key,"Initial_Random_Key_File")
```

3.7.2 อัลกอริทึม Make_Random_Key

```
Dimension  Array_Key (64)
Open "Initial_Random_Key_File"  As Input
Read_File_To_Array ("Initial_Random_Key_File",Array_Key)
Random_Key = MD5 (Array_Key)
Write_Key_To_File(Random_Key,"Initial_Random_Key_File")  4 Times.
```

3.7.3 อัลกอริทึม Control

```
Gen_Initial_Random ( )
Message
        " 0. Exit
          1. Encrypt
          2. Decrypt
          3. Key
          4. Encrypt File with Password
          5. Decrypt File with Password "
Selection : Get_selection
Do case
        case    Get_Selection = '0'
                Exit Program
        case    Get_Selection = '1'
                Encryption ( )
        case    Get_Selection = '2'
                Decryption( )
        case    Get_Selection = '3'
                Make_key ( )
        case    Get_Selection = '4'
                Encrypt_With_ password()
        case    Get_Selection = '5'
                Decrypt_With_Password()
Endcase
```

3.7.4 อัลกอริทึม Encryption

```
Input Sender_Name
If Not_Found_In_System_3_Time
```

```
    Exit Program
Endif
Input Sender_Password
IF Wrong_Password_ 3_Time
    Exit Program
Endif
Input Receive_Name
If Not_Found_Receiver_In_System_3_Time
    Exit Program
Endif
Input Plaintext
IF Not_Found_Plaintext_3_Time
    Exit Program
Endif
Input Encrypted_File
Open "Sender_Private_Key_File"  As Input
Open "Receiver_Public_Key_File" As Input
Password_Key = MD5 (Sender_Password)
Read Data_Private_Key From "Sender_ Private_Key"
Sender_Private_Key =DES_Decrypt (Data_Private_Key, Password_Key)
Make_Random_Key ( )
Open "Temp" As Output
While !eof("PlainText")
Read  Char_8_bytes   From "Plaintext"
Cipher_8 = DES_Encypt ( Char_8_bytes , Random_Key)
Write  Cipher_8   To  "Temp"
End
MD5_Info = MD5(Temp)
Close "Temp"
Read Receiver_Public_Key From  "Receiver_Public_Key_File"
```

```
Key_Info = RSA_Encrypt (Receiver_Public_Key, Random_Key)
Plaintext_Pass_MD5 = MD5 (Plaintext)
MIC = RSA_Encrypt (Plaintext_Pass_MD5, Sender_Private_Key)
Open "Encrypted_File" As Output
MD5_Info_822=RFC822_Encode(MD5_Info)
MIC_822 = RFC822_Encode (MIC)
Key_Info_822 = RFC822_Encode (Key_Info)
Open "Temp" As Input
Open "Ciphertext" As Output
While !eof("Temp")
        Read Data_temp_16_bytes From "Temp"
        Ciphertext_822 = RFC822_Encode (Data_temp_16_bytes)
        Write Ciphertext_822 To "Ciphertext"
End.
Write MD5_info_822,Sender_Name, MIC_822, Receiver_Name,
Key_Info_822 To "Encrypted_File"
Write "Ciphertext" To "Encrypted_File"
Close "Sender_Private_Key_File",
        "Receiver_Public_Key_File",
        "Encrypted_File",
        "Temp",
        "Cliphertext".
```

3.7.5 อัลกอริทึม Decryption

```
Input Encrypt_File
If Not_Found_Encrypted_File_3_Time
        Exit Program
Endif
Open "Encrypted_File" As Input
```

```
Read MD5_info_822,Sender_Name, MIC_822, Receiver_Name, Key_Info_822  From
"Encrypted_File"
If Empty_File
        Exit Program
Endif
Open 'Ciphertext" As Output
Whie !eof("Encrypted_File")
    Read Ciphertext_1_Line  From "Encrypted_File"
        Write Ciphertext_1_Line To "Ciphertext"
End
Close "Ciphertext"
Wirte Sender_Name, Receiver_Name to Screen
Input Receiver_Password
If Wrong_Password_3_Time
        Exit Program
Endif
Input Plaintext_File
MD5_Info= RFC822_Decode (MD5_Info_822)
MIC = RFC822_Decode (MIC_822)
Key_Info = RFC822_Decode (Key_Info_822)
Open "Ciphertext"  As Input
Open "Temp"  As Output
While !eof("Ciphertext")
   Read  Data_Ciphertext_16_bytes  From "Ciphertext"
   Cipher = RFC822_Decode (Data_Ciphertext_16_bytes)
   Write Cipher  To "Temp"
End
Close  "Ciphertext", "Temp"
Open "Sender_Public_Key_File" As Input
Read Sender_Public_Key
```

```
Check_MIC1 = RSA_Decrypt (MIC, Sender_Public_Key)
Open " Receiver_Private_Key_File" As Input
Read data_Private_Key From " Receiver_Private_Key_File"
Password_Key = MD5 (Receiver_Password)
Receiver_Private_Key = DES_Decrypt (Data_Private_Key, Password_Key)
Random_Key = RSA_Decrypt(Key_Info, Receiver_Private_Key)
Open "Temp" As Input
Open "Plaintext_Fie" As Output
While !eof("Temp")
        Read Char_8_bytes From "Temp"
        Plain_8 = DES_Decypt ( Char_8_bytes , Random_Key)
        Write Plain_8 To "Plaintext_File"
End
Check_MIC2 = MD5 (Plaintext)
IF Check_MIC1 <> Check_MIC2
    Exit Program
        Endif
Close   "Sender_Public_Key_File",
        "Receiver_Private_Key_File",
        "Plaintext_File",
        "Temp".
```

บทที่ 4

การทดลอง และ ผลการทดลอง

จากการวิเคราะห์และออกแบบการทำงานในบทที่ 3 นำมาทดลองปฏิบัติเพื่อให้เป็นไปตามวัตถุประสงค์ของการวิจัย คือสามารถติดต่อข่าวสารระหว่างหน่วยในกองทัพบกได้อย่างมีประสิทธิภาพ และมีความปลอดภัยจากการถูกโจรกรรมหรือลักลอบถอดรหัส

4.1 การทดลอง

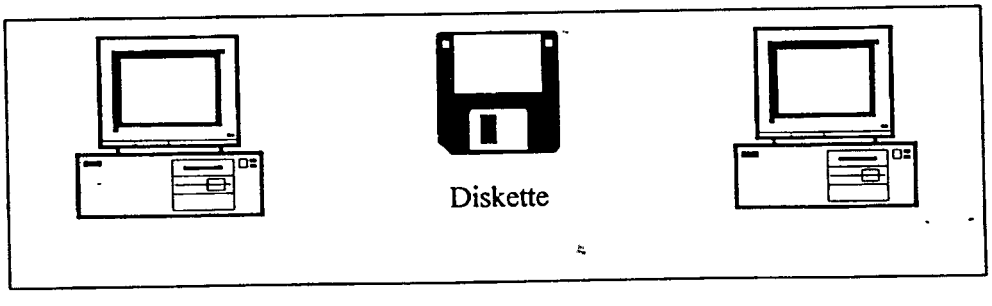
สามารถแบ่งการทดลองออกเป็น 2 ส่วนคือ

4.1.1 ส่วนการติดต่อสื่อสาร (Communication and Transfer Files)

หมายถึงกรรมวิธีใดๆก็ตามที่จะสามารถนำข่าวสารจากต้นทาง ไปถึงปลายทางได้โดยถูกต้องสมบูรณ์ ข้อมูลข่าวสารที่ใช้ในระบบนี้ จะอยู่ในรูปของแฟ้มข้อมูล (File) ในส่วนของการสื่อสารนี้เพื่อสนองนโยบายประหยัดของกองทัพบกและรัฐบาล จึงจะใช้อุปกรณ์การสื่อสารเท่าที่มีทั้งหมดของกองทัพบกมาใช้ให้เกิดประโยชน์สูงสุด โดยสามารถใช้การติดต่อสื่อสารได้ทั้งสิ้น 5 วิธี ดังนี้

4.1.1.1 วิธีที่ 1 แบบมีหลักฐานถาวร (ภาพที่ 19)

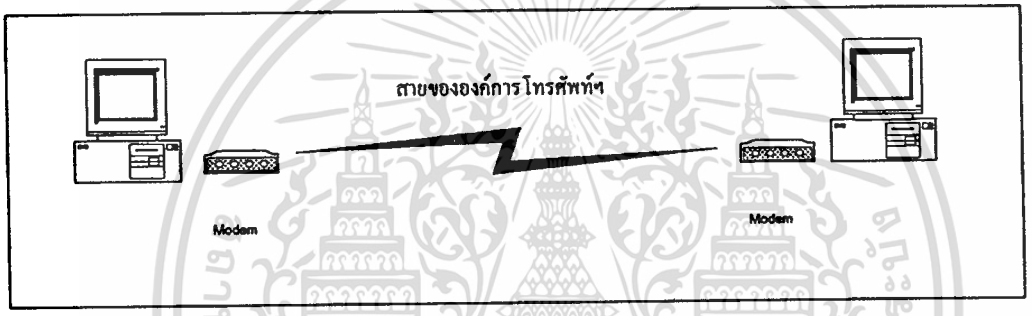
- นำข่าวที่จะส่งมาทำการเข้ารหัส
- นำข่าวที่เข้ารหัสแล้วเก็บลงไว้ในแผ่นดิสเก็ตในรูปของแฟ้มข่าว
- ส่งแผ่นดิสเก็ตให้ผู้รับข่าว
- เมื่อผู้รับได้แฟ้มข่าวแล้วนำมาถอดรหัสผลที่ได้คือข่าวต้นฉบับที่ส่งมา



ภาพที่ 19 แบบมีหลักฐานถาวร

4.1.1.2 วิธีที่ 2 ใช้เครือข่ายโทรศัพท์ขององค์การโทรศัพท์ฯ (ภาพที่ 20)

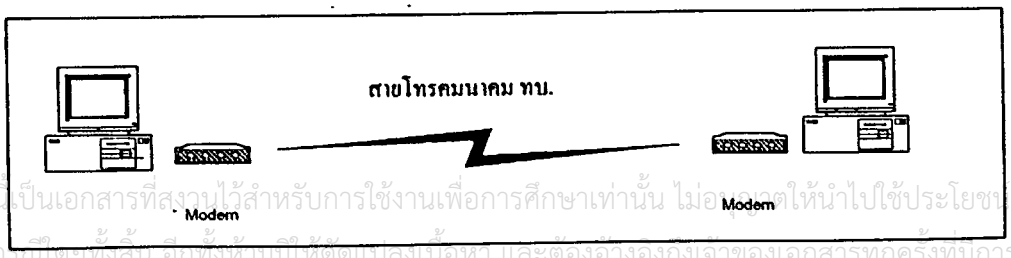
- นำข่าวที่จะส่งมาทำการเข้ารหัส
- นำข่าวที่เข้ารหัสแล้วเก็บเป็นแฟ้มข่าว
- ใช้โมเด็มเชื่อมต่อสัญญาณโทรศัพท์ โดยใช้ระบบสาย ขององค์การโทรศัพท์ฯ
- เมื่อเชื่อมต่อสัญญาณโทรศัพท์กับเครื่องรับได้แล้ว ทำการส่งแฟ้มข่าวไปตามสายโทรศัพท์
- เมื่อผู้รับได้แฟ้มข่าวแล้วนำมาถอดรหัส ผลที่ได้คือข่าวต้นฉบับที่ส่งมา



ภาพที่ 20 ใช้เครือข่ายขององค์การโทรศัพท์ฯ

4.1.1.3 วิธีที่ 3 ใช้เครือข่ายโทรคมนาคมของกองทัพบกผ่านระบบสาย (ภาพที่ 21)

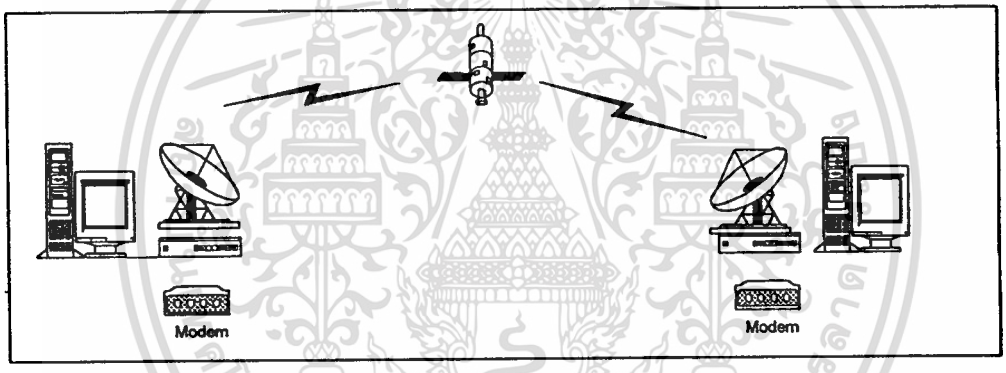
- นำข่าวที่จะส่งมาทำการเข้ารหัส
- นำข่าวที่เข้ารหัสแล้วเก็บเป็นแฟ้มข่าว
- ใช้ โมเด็มเชื่อมต่อสัญญาณโทรศัพท์โดยใช้ระบบสายโทรศัพท์ของกองทัพบก
- เมื่อเชื่อมต่อสัญญาณโทรศัพท์กับเครื่องรับได้แล้ว ทำการส่งแฟ้มข่าวไปตามสัญญาณโทรศัพท์
- เมื่อผู้รับได้แฟ้มข่าวแล้วนำมาถอดรหัส ผลที่ได้คือข่าวต้นฉบับที่ส่งมา



ภาพที่ 21 ใช้เครือข่ายโทรคมนาคมของกองทัพบกผ่านระบบสาย

4.1.1.4 วิธีที่ 4 ใช้เครือข่ายโทรคมนาคมของกองทัพบกผ่านระบบดาวเทียม (ภาพที่ 22)

- นำข่าวที่จะส่งมาทำการเข้ารหัส
- นำข่าวที่เข้ารหัสแล้วเก็บลงไว้ในรูปของแฟ้มข่าว
- ใช้โมเด็มเชื่อมต่อสัญญาณโทรศัพท์ของกองทัพบก โดยผ่านระบบดาวเทียม
- เมื่อเชื่อมต่อสัญญาณโทรศัพท์กับเครื่องรับได้แล้ว ทำการส่งแฟ้มข่าวไปตามสัญญาณโทรศัพท์
- เมื่อผู้รับได้แฟ้มข่าวแล้วนำมาถอดรหัส ผลที่ได้คือข่าวต้นฉบับที่ส่งมา

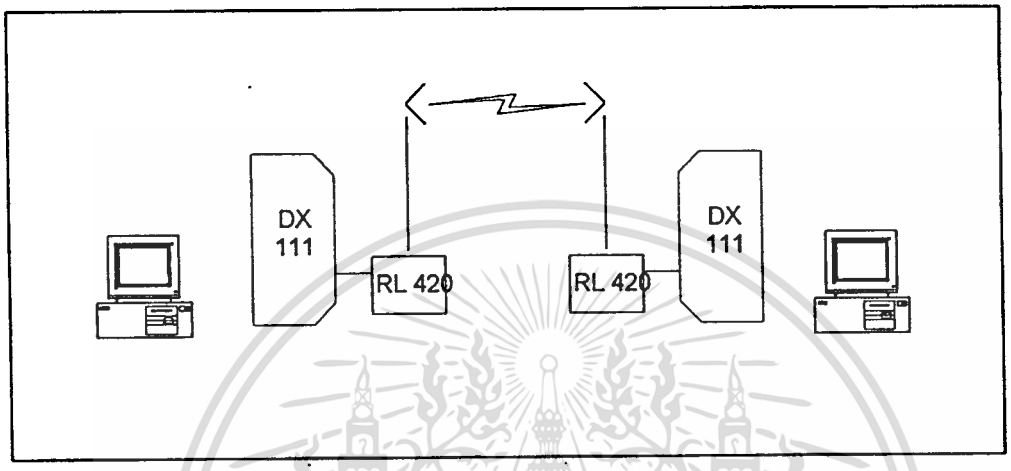


ภาพที่ 22 ใช้เครือข่ายโทรคมนาคมของกองทัพบกผ่านระบบดาวเทียม

4.1.1.5 วิธีที่ 5 ใช้เครือข่ายโทรศัพท์ผ่านระบบวิทยุถ่ายทอดสนามของกองทัพบก (ภาพที่ 23)

- นำข่าวที่จะส่งมาทำการเข้ารหัส
- นำข่าวที่เข้ารหัสแล้วเก็บลงไว้ในรูปของแฟ้มข่าว
- ใช้โมเด็มเชื่อมต่อสัญญาณโทรศัพท์โดยใช้ระบบวิทยุถ่ายทอดสนามของกองทัพบกด้วยการนำคอมพิวเตอร์และโมเด็มมาเชื่อมต่อกับตู้สลับสายอัตโนมัติทางทหาร แบบ DX-111 ซึ่งเชื่อมต่อกับชุดวิทยุถ่ายทอด (FM) แบบ RL-420 แล้วทำการติดต่อกับชุดวิทยุถ่ายทอดสนามปลายทางที่เชื่อมกับระบบคอมพิวเตอร์เหมือนกันอีกชุดหนึ่ง

- เมื่อเชื่อมต่อสัญญาณโทรศัพท์กับเครื่องรับได้แล้ว ทำการส่งไฟล์ข่าวเข้ารหัสไปตามสัญญาณโทรศัพท์
- เมื่อผู้รับได้แฟ้มข่าวแล้วนำมาถอดรหัส ผลที่ได้คือข่าวต้นฉบับที่ส่งมา



ภาพที่ 23 ใช้เครือข่ายโทรศัพท์ผ่านระบบวิทยุถ่ายทอดสนามของกองทัพบก

4.1.2 ส่วนการเข้า-ถอดรหัส (Encryption and Decryption)

หมายถึงส่วนของการพัฒนาระบบโปรแกรมในการเข้าและถอดรหัส ให้มีความซับซ้อน เพื่อการรักษาความปลอดภัยและความถูกต้องสูงสุด เนื่องจากระบบการทำงานนี้ใช้วิธีการเข้าและถอดรหัสในระดับของบิทข้อมูล จึงทำให้สามารถเข้า-ถอดรหัสได้ทุกรูปแบบของข้อมูล รายละเอียดการทำงานของโปรแกรมตามผนวก ก.

4.1.2.1 อุปกรณ์ที่ใช้ในการทดลอง

- Computer 386, RAM 16 MB, Hard Disk 100 MB
- Software รับข้อมูล Pro Com Plus, Turbo C Version 2 ขึ้นไป
- โมเด็ม ความเร็ว 28.8 Kbps
- ชุดวิทยุถ่ายทอดสนาม (วิทยุ RL –420 , ตู้สลับสายสนาม DX – 111)

4.1.2.2 วิธีการสื่อสารที่ใช้ในการทดลอง (โดยทำการทดลองครั้งละวิธี)

- ระบบเครือข่ายโทรศัพท์ขององค์การโทรศัพท์แห่งประเทศไทย
- ระบบเครือข่ายโทรคมนาคมของกองทัพบก
- ระบบเครือข่ายฝึกร่วมของหน่วยทหารสื่อสารทั่วประเทศ

4.1.2.3 การทดลอง

จากการทดลองได้ทดสอบกับข้อมูลในรูปแบบต่างๆ ดังนี้

- Text File
- Page Maker File
- Microsoft Word File
- Excel File
- Picture File (*.BMP , *.JPG , *.GIF)
- Visio File
- Execute File (*.EXE)
- Command File (*.COM)

4.1.2.4 ผลการทดลอง

ผลการทดลองปรากฏว่าสามารถเข้าและถอดรหัสกับข้อมูลรูปแบบต่างๆ ได้อย่างถูกต้องและมีความปลอดภัยสูง เพราะมีความซับซ้อนในการเข้ารหัสสูงและจะยกเลิกการถอดรหัสทันทีที่มีการเปลี่ยนแปลงใดๆเกิดขึ้นกับแฟ้มเข้ารหัส ในที่นี้ได้แสดงตัวอย่าง การเข้าและถอดรหัสไว้ 2 รูปแบบ คือ Text File และ Picture File เพราะเป็นรูปแบบข่าวสารที่กองทัพบกใช้มากที่สุด

<u>ตัวอย่างที่ 1</u> ข้อมูลข่าวสารชื่อ L4_1.TXT มีรายละเอียดดังปรากฏตามภาพที่ 24

Additional Information about FoxPro for MS-DOS
Remember that information in online help is the most current
information available.
There are three types of installation for FoxPro for MS-DOS:
Normal Installation, Administrative Installation and Workstation
Installation. Instructions for Normal Installation are in the
FoxPro Installation and Configuration manual. For information
about Administrative and Workstation Installation, see
INSTALL.TXT on FoxPro for MS-DOS Disk 1.
The directory FOXPRO25\GOODIES\LCKUPDAT contains files that allow
you to update PLBs built using the FoxPro 2.0 Library Construction
Kit for use with FoxPro 2.5 for MS-DOS. If you obtained your PLBs
from another source, such as a software supplier or online
service, contact that source for updated libraries that work with
FoxPro 2.5. To use these files, follow the directions in the
LCKUPDAT.TXT file located in the FOXPRO25\GOODIES\LCKUPDAT
directory.

ภาพที่ 24 รายละเอียด แฟ้ม L4_1.TXT

ข้อมูลข่าวสาร L4_2.TXT เข้ารหัสเก็บไว้ในแฟ้มที่ชื่อ C4_2.TXT ดังภาพที่ 25

THE ROYAL THAI ARMY

ENCRIPTION PROGRAM

VERSION 1.0

1. MD5-INFO : BA0599748FD67B64

2. Originator-ID: Chat

3. MIC-Info: RSA-MD5,RSA,

Y7UsrvM1cYNYeZhKPTtupw+yIBLLc5pFzUiEA91AyJQjS44jleMwv1RyBS34rpeQ

xVWowGYKFuh059hnsr8Z+JBrXuWXA9tMJQjpSFTrVGg=

4. Recipient-ID: Amry

5. Key-Info: RSA,

KAzWrprs/emW9Wu78ZT6lEclOFNmZqjn62Q3P1KgVdqk5R1EF+sucje5W7tPiBhA

fEE/NiEPPJxdsYowZUt80VHzSf/gDI7wTgiZWOHFyN7oTSGC2KUL+vgjyj+VVfis

VJXUTqP+6oE0M48pljaHaR3f4o+xFQLZds0gh7w=

p5t5K64ozDixxwJ/ZM1uTtMx9Gsn2mgG5j/Ly5hsH6Z7WtARopMzm3AgRz6wiMWu

kfE3uHveKDR+uhMk1YZO6Pm74yhjdqepvNoLyM02ZiFYlBTNDxHi0kAcuDnc1cfv

tgzfuyFFepwVzoafZGVOinFx3yGufbH0/z2NCJrz7ZZRS0RS+PQpmizX1p0L8khW

17kzmV27Cyk2BkcWX6W2forjcxbj4QpR5fbXOfkIXZP0IDg3EzGJLoAeB1wG2MKv

bKQAsTv4UqhZVmXBQq+cQWowkVfWJa6XM1NUg8RASorFGnY6FVM3flAeZBwv/6s4

z1+hSUv6SNrH4cs+9svDcGav313DzGg5X1Xc/1YSmhX3YAKXfw6OFzPV0sg69VW1

0ja/BmQb6rN6Ea8wlvVq6MITgomSff6ZM49m6oI18iB1mF9qt947mX+7c4djnFX

eHaDM6Veod6drD4WL4YPC8iJQ7FfZ+XGjQgYXWW8+KuwJKhLltD3jJY+0Z/qqjtQ

xhimFWsefT6C68xOvASGVhkeiQvR2Tf/Aq+zLvsQ0gTykB7cm3s7UgrJpAK9V+yy

dqNAD63xQY6ZvTDTmWaYdkcUp1wyjn+/lsT+X+VtQPx6h2H5fLbNCHdCUyDPEr12

zDnaWWqewU9rRh0HwtKoG6SLbS21WqGOuw8+hQBK3375v4JVQK/2wmjibv0GHfou

/5iNzHZMjea71a/To7z69EFGSfioq9OJR/vVcuMW+aELc4w3ZCIh69hVLgyT+0+

7RdtS53CvEdupYSi1YC2AOYD0817wQBXryMG2cZg7TtEJ81FlyMs4y8CLrhn5g8a

o61VXDMAGlM3x5S+2oYLYWV+f3/7+tkQ0rBXARxyGEZOyhhbKAQr1C61VnZIk56J

o6ryxJiHaM9rUCNApBdcExMqP2M87/d4UP+bdQ0ms/Q9/yJvRDMlm/7RKkoZi8V

CRS/Yi+vG4mu1+GEBz1xc1ETIHtzuofgLfPM2c7ot3tKz0f/GDTyhI8z3/HFLLjP

ilzLgg5MqbLD+L2ngqODPVvEmpQtyokXv03xpx8Bu0FssWkEvS/3sL8bzwwquMYN

NkWjzotKwOYNJ8U2qkqlXn1MQBaPn3ywz1kvkVm9WDgEzlh91Wl26JzqLRrh5SU4

BH96G0KtKrrRm7DO9dill7AKL6NxqcYgRYDDizO1+72F44ieFoVVTOBHg4SQALph

yvKnm9p0JZ8dQoot+kS+B3JTNdGQQatT82lvV5+t2+RXIk7xkupGmCe/2uGKc8Ov

qn6Wt4niRYINhkmPCVC/brO/T1iUmuZOs1FAa2ujl04q1lw6t9Cb74O1JlxnyJEp

nAGFQBfvBcPNXil1f4xELwf8WWQCmJZktxbRQhaElvOjuLTAKhCnWYoL0+oXsYx5

***** END MESSAGE *****

ภาพที่ 25 รายละเอียด แฟ้ม C4_1.TXT

นำแฟ้มเข้ารหัสชื่อ C4_1.TXT มาถอดรหัสเก็บไว้ในแฟ้มที่ชื่อ D4_1. ดังปรากฏในภาพที่ 26

Additional Information about FoxPro for MS-DOS
Remember that information in online help is the most current information available.
There are three types of installation for FoxPro for MS-DOS: Normal Installation, Administrative Installation and Workstation Installation. Instructions for Normal Installation are in the FoxPro Installation and Configuration manual. For information about Administrative and Workstation Installation, see INSTALL.TXT on FoxPro for MS-DOS Disk 1.
The directory FOXPRO25\GOODIES\LCKUPDAT contains files that allow you to update PLBs built using the FoxPro 2.0 Library Construction Kit for use with FoxPro 2.5 for MS-DOS. If you obtained your PLBs from another source, such as a software supplier or online service, contact that source for updated libraries that work with FoxPro 2.5. To use these files, follow the directions in the LCKUPDAT.TXT file located in the FOXPRO25\GOODIES\LCKUPDAT directory.

ภาพที่ 26 รายละเอียด แฟ้ม D4_1.TXT

จากการเปรียบเทียบแฟ้ม L4_1.TXT กับ D4_1.TXT- ในลักษณะไบท์ต่อไบท์ ปรากฏว่าเท่ากันทุกประการ

ตัวอย่างที่ 2 ข้อมูลข่าวสารชื่อ L4_2.TXT มีรายละเอียดดังภาพที่ 27

บันทึกข้อความ
ส่วนราชการ สส.ทบ. (กองวิชาการ โทร.๕๑๕๐)
ที่กห.๐๕๐๕.๖/

วันที่ 22 พ.ค.๔๐

เรื่อง จัดหาซอฟต์แวร์ที่ใช้ในการสร้างระบบช่วยซ่อมบำรุงอุปกรณ์สื่อสาร
เสนอ พธ.ทบ.

๑. ตามที่ ทบ. ได้อนุมัติหลักการให้ สปช.ทบ. ดำเนินการจัดทำระบบช่วยซ่อมบำรุงอุปกรณ์สื่อสารด้วยคอมพิวเตอร์ สำหรับ งป.๔๐ เป็นจำนวนเงิน ๑,๐๐๐,๐๐๐.- บาท เพื่อเป็นค่าใช้จ่ายในการจัดซื้อซอฟต์แวร์ ที่ใช้ในการ สร้างระบบระบบช่วยซ่อมบำรุงฯ

๒. ดังนั้นเพื่อให้การจัดทำระบบบัญชีเงินราชการด้วยคอมพิวเตอร์ สามารถดำเนินการตามแผนงาน ที่ได้กำหนดไว้ จึงขอให้ พธ.ทบ. ดำเนินการจัดหาซอฟต์แวร์ที่ใช้ในการสร้างระบบช่วยซ่อมบำรุงอุปกรณ์สื่อสาร โดยมีคุณสมบัติตาม รายละเอียดที่แนบ และเมื่อได้ตัวผู้ดำเนินการแล้ว กรุณาแจ้งให้ สปช.ทบ. ทราบ เพื่อจะได้เสนอขออนุมัติ ทร. ต่อไป

จึงเสนอมาเพื่อโปรดดำเนินการต่อไป

(ลงชื่อ) พล.ต.
ผช.ปช.ทบ.ทำการแทน
ปช.ทบ.

ภาพที่ 27 รายละเอียด แฟ้ม L4_2.TXT

ข้อมูลข่าวสารL4_2.TXT นำมาเข้ารหัสเก็บไว้ในแฟ้มที่ชื่อ C4_2.TXT มีรายละเอียดดังภาพที่ 28

THE ROYAL THAI ARMY

ENCRIPTION PROGRAM

VERSION 1.0

1. MD5-INFO : 5E7BEFE3FE6F0339

2. Originator-ID: Amry

3. MIC-Info: RSA-MD5,RSA,

a3Su/wpHXHSEmE14ymqSRxVv7f+3dtsJUzOCYs2oh5GkuUdjvE9OaNefXS1yeaRN

zrME9csPJXZe4qlXjw7SOWy2ACrnkYFyG4j7nxr0a7cOiPoHSirWGpmahn2PFcdv

gIK0i6zzNCORI3/aI7Sss20wKM04/7tqgAmCi6/47MY=

4. Recipient-ID: Nor

5. Key-Info: RSA,

pny/TYgb8VFl4OVd9DKxQTRr51zqRgBHoZrm8856yTiUd1V9QQgY7Khgeg8xLrn6

C584anEjLRe2LqPCNzRfrhhbgx8gsxWnVnCd

MtG9oO+Gpd7T+Y4EysykJMMfovGi2n38SOt9JTpwHqh7nXcrcktruKzIZZf4KmJ0

SySQ+VeGlD5aLbTzRtjtvqAbhidIUyffRXxnfKM2G/vccPXt991pc0gLTbxyYwNA

wu0DdOOdOFMuq0DlvLprd8/bW/Rn2rV138kZaZtc5EQVYwoTUniYZ8q+6AMI1L8y

AW/ytGhZPuf9tCRIje1uzR3+B3uI9s+/3t44dh594W6OgaBs+pUyTJzKZYs/UOLA

YbOw7dT95JHajLSjrf86GoM3B+S+r3v4w/82ZavnOZzvoC539epB7fjwfeQI/JOm

CoYA+MMAGJhyAfl9B/QmdnfljCQ3OEb2hZxUM7AS9CGHa80ePyNgAZocJG+4ERrv

T5acvPbli/jA/uDfo93ItnawOKCvDlTPcoLCr9QF74BLQNbqUTKA7kYumEIk7kzr

DT/k2koOVdo9R2RnwvKOsKoigIuydt4mAuUgaEBuDrd5cB5faTY+GqUOdF3dpmpP

Dz0QoSP/S5rA0Q95l2wv60x+9zLOuOkoh+Lk1BxCkUX6q+JkQiqElkmFTFAl5irf

SHbzcYVUeZEYKulMGN4arHtIF+v3L2dxwfnqJKYb9Z9cWMn8iLRzQNAKaP8Yqdtn

cNXDal43Lq/mzzHc+bpvkAHiuHPl3BNbaP7eaV+me3see1Zen4DGWf3oR88k87Hh

N/qNznRCZBFpnA6lBbdHB3zcrjFxHavbl0D1eIDyP+axKsqanoG6nl0FZnwgazwl

mStus4nk50sKa9NS4OID5O98QSh/3ntZpUp7RQPtS0NMEM95GjgU5T0yl9aR3cAY

wzMZKJ+ivyJ/Oe5rTXCsNM2iiNhuIKtCzmrJD42pcIN6dDzQlz4XMX48j74slXAa

4ZlXTPwgU9zlBTkDN4b3n8kz4F0cr3XRlFRs9rPNneILa3TEc98NZF0qSvNyOOiv

bvUlnzmbcqTXMO4qCou2rdQl+8rvHTduHOKaj+jMqtYrhvBtDngmOVootdDhGwYM

3b9fUn5srdZ6ZIEzXc14pwipYpWwJJXf82bZ175oN15qFAiupDhzZfYBB0pIE6Z7

fg8VkLI75O4eJEzPxcteWlg2cwnYx6Btne3hA5wt+rBp3uW4STfT1cguRwi4wmSx

liabipig/+AdU4SGoGxfeepkwa92MQDP4BJJNLXcJ5gretqaZG9vsmHg56ssIohr

c/yqJY+cR/AfTqseu36e/qS8Z7lmA4JVXt0SVEjt811aPUZU5OTQBH1iUIEedkD4

S8FyoDYKJvKToXQy1/bXOHiS3HBqF59ThkFf7Rbb25adkCdngn7dgA==

ภาพที่ 28 รายละเอียด แฟ้ม C4_2.TXT

นำแฟ้มเข้ารหัสชื่อ C4_2.TXT มาถอดรหัสเก็บไว้ในแฟ้มที่ชื่อ D4_2.TXT มีรายละเอียดดังภาพที่ 29

บันทึกข้อความ
ส่วนราชการ สส.ทบ. (กองวิชาการ โทร.๕๑๕๐)
ที่กห.๐๕๐๕.๖/

วันที่ 22 พ.ค.๔๐

เรื่อง จัดหาซอฟต์แวร์ที่ใช้ในการสร้างระบบช่วยซ่อมบำรุงอุปกรณ์สื่อสาร
เสนอ พธ.ทบ.

๑. ตามที่ ทบ. ได้อนุมัติหลักการให้ สปช.ทบ. ดำเนินการจัดทำระบบช่วยซ่อมบำรุงอุปกรณ์สื่อสารด้วยคอมพิวเตอร์ สำหรับ งป.๔๐ เป็นจำนวนเงิน ๑,๐๐๐,๐๐๐.- บาท เพื่อเป็นค่าใช้จ่ายในการจัดซื้อซอฟต์แวร์ ที่ใช้ในการ สร้างระบบระบบช่วยซ่อมบำรุงฯ

๒. ดังนั้นเพื่อให้การจัดทำระบบบัญชีเงินราชการด้วยคอมพิวเตอร์ สามารถดำเนินการตามแผนงาน ที่ได้กำหนดไว้ จึงขอให้ พธ.ทบ. ดำเนินการจัดหาซอฟต์แวร์ที่ใช้ในการสร้างระบบช่วยซ่อมบำรุงอุปกรณ์สื่อสาร โดยมีคุณสมบัติตามรายละเอียดที่แนบ และเมื่อได้ตัวผู้ดำเนินการแล้ว กรุณาแจ้งให้ สปช.ทบ. ทราบ เพื่อจะได้เสนอขออนุมัติ ทร. ต่อไป

จึงเสนอมาเพื่อโปรดดำเนินการต่อไป

(ลงชื่อ) พล.ต.

ผช.ปช.ทบ.ทำการแทน
ปช.ทบ.

ภาพที่ 29 รายละเอียด แฟ้ม D4_2.TXT

จากการเปรียบเทียบระหว่างแฟ้ม L4_2.TXT กับ D4_2.TXT ในลักษณะไบท์ต่อไบท์ ปรากฏว่าเท่ากันทุกประการ

<u>ตัวอย่างที่ 3</u> ข้อมูลข่าวสารชื่อ L4_3.TXT มีรายละเอียดดังภาพที่ 30

```
จาก                 ผบ.พล.ม2.
ถึง                 ผบ.พล.ม21.
หมู่วันเวลา 170900 ก.พ. 41
        ให้เคลื่อนกำลังไปยังพิกัด TQ 6847 ในวัน จ-3 เวลา 1200.
```

ภาพที่ 30 รายละเอียด แฟ้ม L4_3.TXT

ข้อมูลข่าวสารL4_3.TXT นำมาเข้ารหัสเก็บไว้ในแฟ้มที่ชื่อ C4_3.TXT มีรายละเอียดดังภาพที่ 31

```
THE ROYAL THAI ARMY
    ENCRIPTION PROGRAM
    VERSION 1.0
1. MD5-INFO   :  29C1807693A049BC
2. Originator-ID: Nor
3. MIC-Info: RSA-MD5,RSA,
TZQlUrXKgIsMqiGLzzrc37hJMQbYij8JV1po8YByz2LgvhUCjpSwH2dr/StOmNpN
zhW2nvHV6b2dBN9xTey3OeDc/w9dnj7SQlo+ldSqj0k=
4. Recipient-ID: Chat
5. Key-Info: RSA,
COwVYhh9QvNDWOHSQ89w5EhKxNNy/l55qZcYOXP3o+s+JuSncWZU0KaNeIZMlgpB
y7krLe3USb2DE2/FYJrEADQD+toaS/1PGsE=

TlVJ/ndBwKomxMaF95f84qwvNjeWldZkhqZ/hzbGZPdzmssD/TdZEnbEL9WDpaVD
2kVGMwZjMq7VB21lDdrkgN/Vhp9w0ivQeMCDFi5by8gODJky4mSJJQvBeueEDwm7
hf6EdeWYhfVv5EHdgQ/+UJ3Fgt/Ogl49yN3Ia37UFPYVkpizrPEdfLhbTYd1bCq6
slsr2TbfZy/o/2wzfp7E4n8FBpOxzxplO1NL9srhP3XGnpqynd6XRA==
    ***** END MESSAGE *****
```

ภาพที่ 31 รายละเอียด แฟ้ม C4_3.TXT

นำแฟ้มเข้ารหัสชื่อ C4_3.TXT มาถอดรหัสเก็บไว้ในแฟ้มที่ชื่อ D4_3.TXT มีรายละเอียดดังภาพที่ 32

จาก ผบ.พล.ม2.
ถึง ผบ.พล.ม21.
หมู่วันเวลา 170900 ก.พ. 41
ให้เคลื่อนกำลังไปยังพิกัด TQ 6847 ในวัน ว-3 เวลา 1200.

ภาพที่ 32 รายละเอียด แฟ้ม D4_3.TXT

จากการเปรียบเทียบระหว่างแฟ้ม L4_3.TXT กับ D4_3.TXT ในลักษณะไบท์ต่อไบท์ ปรากฏว่าเท่ากันทุกประการ

<u>ตัวอย่างที่ 4</u> ข้อมูลข่าวสารชื่อ L4_4.TXT มีรายละเอียดดังภาพที่ 33

จาก ผบ.พัน ช.111
ถึง ผบ. พัน ช.ชบร.หนัก.
หมู่วันเวลา 151200 มี.ค. 41
ให้เตรียมอะไหล่สำหรับซ่อมบำรุง ชั้น 3 รสพ.21 จำนวน 2 คัน

ภาพที่ 33 รายละเอียด แฟ้ม L4_4.TXT

ข้อมูลข่าวสาร L4_4.TXT นำมาเข้ารหัสเก็บไว้ในแฟ้มที่ชื่อ C4_4.TXT มีรายละเอียดดังภาพที่ 34

```
THE ROYAL THAI ARMY
    ENCRIPTION PROGRAM
     VERSION 1.0
1. MD5-INFO   :   1A64346D01F82C91
2. Originator-ID: Chat
3. MIC-Info: RSA-MD5,RSA,
JlyUJxuzJtz2hadEMbzTQc1HxlGrbGPfKYTRNG2/9kCNEeJVjxt1e5Sub6slUQkU
77+KfRt6w77nZv9zDuOYSnz6JRguJvljwXf89UpcpZo=
4. Recipient-ID: Nor
5. Key-Info: RSA,
ZwTCWDDH45leWor0USIuJhNvED1yASD9GiSd8ceUPMNJz+6DrcDkgSOJSEV44yGa
diUnbVmeXVgBOxDgES+WHbdyYbmW0sll0vh9

G4Ker9NXGVgoCCEFApzoR9ZOMFwJXfZwOCanstz/YkqdV6ckjq40JinpJQvDJ5Jn
9yGsk16KwAvdoxsMYiRC8Qx5Hx6dsBdIeUlY5UZJhUdqbJ6N+QeE3RfHZ9nTskYS
94pchLf3hHFXACJxZAFYqVnu58n08GGGUHINuW8nbgspBQOiKPZlP5QQ8L7/PSdI
V5xMbWqeLzGUWp3SzKDZXLAWTDO7z+hyXwnzKF+WDsToj1rfin1kjUDhYOfFO5SaA
CJ6TNjX3+zk=
   ***** END MESSAGE *****
```

ภาพที่ 34 รายละเอียด แฟ้ม C4_4.TXT

นำแฟ้มเข้ารหัสชื่อ C4_4.TXT มาถอดรหัสเก็บไว้แฟ้มที่ชื่อ D4_4.TXT มีรายละเอียดดังภาพ ที่ 35

```
จาก                 ผบ.พัน ช.111
ถึง                 ผบ. พัน ช.ขบร.หนัก.
หมู่วันเวลา  151200 มี.ค. 41
          ให้เตรียมอะไหล่สำหรับซ่อมบำรุง ชั้น 3 รสพ.21 จำนวน 2 คัน
```

ภาพที่ 35 รายละเอียด แฟ้ม D4_4.TXT

จากการเปรียบเทียบระหว่างแฟ้ม L4_4.TXT กับ D4_4.TXT ในลักษณะไบท์ต่อไบท์ ปรากฏว่าเท่ากันทุกประการและเมื่อพิจารณาแฟ้มเข้าทุกแฟ้ม จะเห็นได้ว่าเป็นการยากที่จะทำความเข้าใจหรือลักลอบถอดรหัส ซึ่งเป็นไปตามวัตถุประสงค์ที่ตั้งไว้ทุกประการ

ตัวอย่างที่ 5 ข้อมูลรูปภาพ FLOWER.BMP ปรากฏในภาพที่ 36 และ ข้อมูลเข้ารหัส CFLOWER ปรากฏในภาพที่ 37

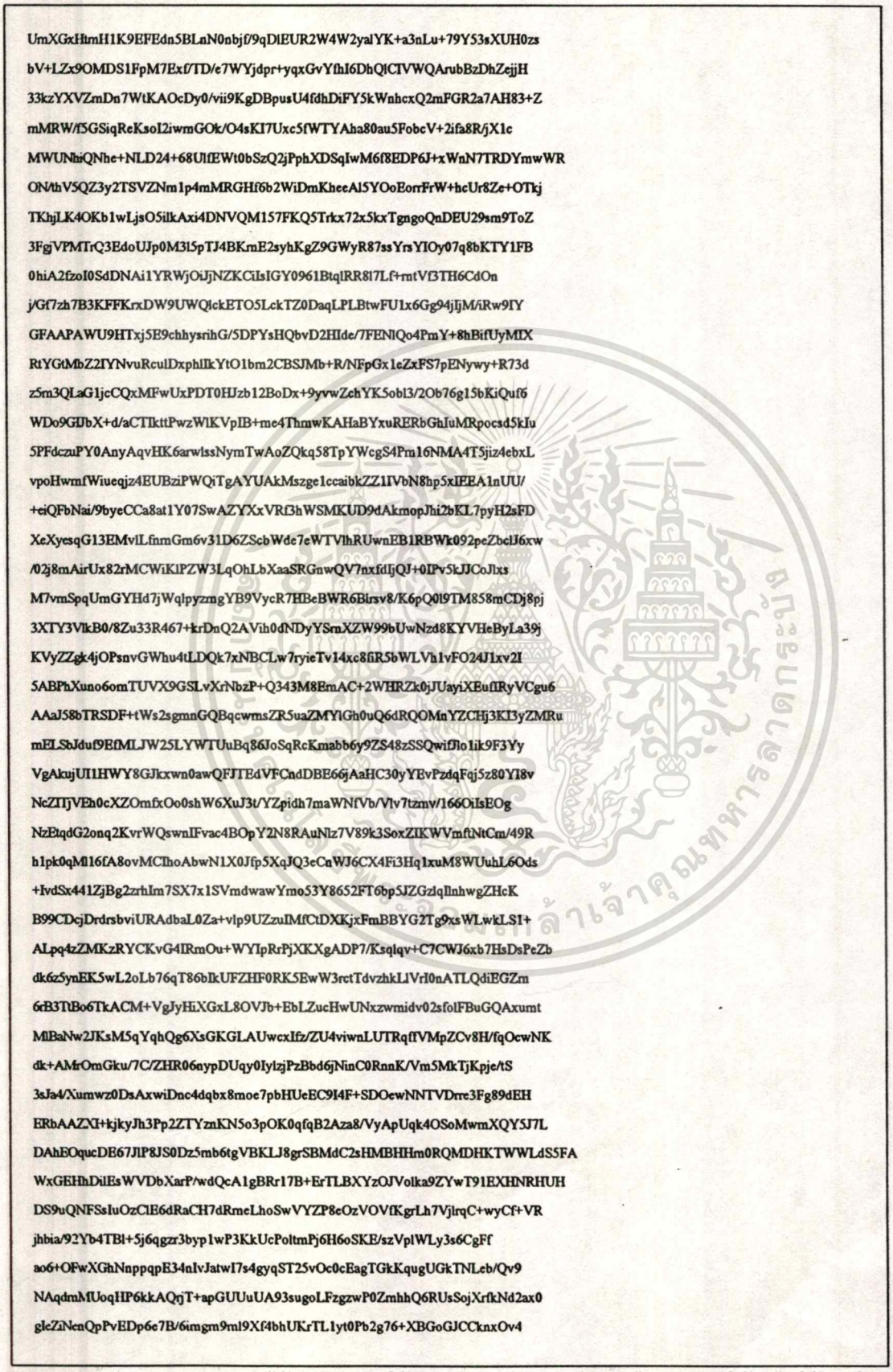
ภาพที่ 36 แฟ้มรูปภาพ FLOWER.BMP


```
THE ROYAL THAI ARMY
    ENCRIPTION PROGRAM
      VERSION 1.0
1. MD5-INFO   :  3C2AE64004901C4F
2. Originator-ID: Nor
3. MIC-Info: RSA-MD5,RSA,
eGg2ups4VQkk9nsZ6cABrpXx5XYPpcOPfnyz/E63WDGH11I2uK7TfRwDXRBswdfX
oTybmNZgGPbNXcDrig1RcpmaOpJV/wPAod5dC9kipcU=
4. Recipient-ID: Amry
5. Key-Info: RSA,
Ne/jpEDm59f1MOSqWIPQobMdE0+OQm57pcB8l/fjAa+oRj6CXKN2yM3XB0h005W
ZYhNYt9xMFfr2xEeYb0tnhzLIrW2xQBpkBL9tw+trQbfO/J9SxDo46/jMT1Gq1jX
EyIHOIIh7ZxOhW0nEDd2bU05n00y9aa/3CLC1pmw=
```


ภาพที่ 37 ข้อมูลเข้ารหัส CFLOWER

/Ya1w7/MDgkURA3+Y69RqG1HMoEhKrYRlMAQiTQ75EMnxZ45izPmlYGEAK417HXS
SK47jl3MbnHenZ5QCzCEIreRQKs/Snh878tyTJxdcW3RAKN0jdUD0JrMzAGQpOFn
A8b7nZKvDEAK28UUmZnjnRpq+KgORy93Vmr53FZzcPrNS/MuslQbhsbP9DuCaLCt
TerUoAuPHBXygfVnVMNoV3n0U5fLCk+ihJeiluIyHi3tXS3rQVsvmX/50ZG3C4d5
n9k/GBReK2fauGKW+J6n6XGm+r3uUi8o+JNJO6iwWsc91E82C/AKdql83TEhPw7S
tLD2XRRpe2FS973CmBlMioIUlnyNB6ifm+wSXbksPAV73VbR+PjjYXUw4RDeql8u
PJGER5espMxbn9GnVUUvT9u2ZtAuIxFtGT/KwFKA9pVCzvJt+a6o1+kzLNtBV9ce
RGxXGbFqM7Ad79OFDPw7/PNj/tvoFCTkeduHOvTDy9yGMmxu7KxIVGzzbl9eL9rk
vpAari7FyvSz9PmNiI0mAeqCK0YITfcGZir7HnStDOYaIcmffFaa9xDcFFCNA8oL
U2H8KkD9HH8xpuOjyM0FG26Kyu3fdt0nezleyvuGnZeiAWN3qIhK05JcFNFB92Vf
b2wpPOgAGu2SxPqDbAomaieCoOW134oo34OQceJ4xIRwAwgxaYAnx6vhlhzkbhMd
J1OkQgUsvqmjB3uQko7Yi0Tb5q5QmZslqpXNH0A0XALY18r4K/FTsY9w1xF5JXb+
bKOHSi70Wp/hOzMMKxm8Oy4DabOvVNV7i6llu5NxC1ViK+kv+B3hXvNICIi3/RmE
AxYjEh1r6qLUgEW/E2FNhRJjxwOtZLLaJav4decQl6hLrh0dR7laHqBChTe50E1r
mhMLLiB0APXN6RxtOr4Smq0ieNqj/PXyzKatc853vNVFOU7/LEoAxwNnmPw5n960
8v9cKXrb9ElCW/Ar16JpEMxNCP1rf7yUFpb3+F05c2fkHpc0im2FBiYjFHXYhZ8N
OLtn/zB+qhwW6qJ8aUX3cqzP09SmmtqSSjuNWADF+KsB/Qf12Sda2mLxuqcypy/D
9sUaZ2aUYH2p9ZAi5EtKCXM2+bWQIjtUfrdj8+K5hyrkZ5jXGJbKwjit5BpwaiWe
G5TlpzxTs7uUyjRWeal9B4/9g+8XPou7T0uMG6K5YftV3LVxCBq49MZPJ0d0LV1s
/RGWOuqzjvXiCVZ4YGpXpq/EGLs6y4pp5TdxT7JSnSyh9fc9013GoFlUALasJnhl
rG6syAr0uurp8WShFr6KVbUgunbJ2Z2afw7vRIDgRPubBN2al54iSMykd97hlEH3
YkyL7c65lXJtRuFj9q08dlyl6mnnJaNVAF9Uhg6qGAvflwx2nABW8EzbQ+jVhxcl
6x1Qz30HEcB1Jn6akuy+QRvsHmZ54aCMKNA5Dqs5PPxNYPsE+hUi9VsAhuIB1nd6
aFHznThxAQ+MKRQvr28CUG0TOM7JG3kr/zZZ8ELHu/sNaVvkO1bCkQ7jCDUqcXTj
XRZL+SJRrD9RE7V6iQqHRa0wjhSkrXAFqLdtI/V5+d5GxWdA0pKB4oo/nH1QQbg7
+SYVqg1FaSNHUs1/QGFX0kpiFYRgqYpb53OMKr/MfYfKhK38LTenj6xWqLs1ziob
O/MKNjoB2WMvAg2nYfjp0WDdRp4bhrU+oNCElbKpAJPm3aq/dYDyqS0YiuAaSWq4
JhOKpK9GZtexRtbn8u1XHZ7Nk36BiuedW9bNZob2jrNpKZ0ciHqX26mED7xrJAqY
REu8Dmz/Beup3duCnJhI1hE8y5NXjNCYJ/MJmuCudA+dQ2AwmMqOI8XGcHz/T3Xl
A48KRVBKjRhAHxUtMjCvtL70SPqrUCmXcppZ0RD3kRJAaXDOZQm9aLfkLibuaWPU
gJqkUQ8WaUVmigup9CGrDO/Gawjy+TRFoKL5aOTwustbpz5zsbZd44aY7+Nh/1xI
cr+YuwbSH9t2q7oTrJyCTWNEbdL50mZFrAbK3N1xMNv1x87EuPvxm4iIkJRdgpkF
IltTbeDbV9hvRK3TcJ7AyYT78G40jdcLNg6lcsW0mgCq3TyDhLz37ppvkqY0+Pj/
djKp/57cIpkTe1WdVzjzC1eHWvWQQcF2ZUA81156FdBHbGbmjDEh61bb6zDjXTNT
/R82ZddtS8PxhpQhv19sCqF5cM7iH3mukCZ2au6vr3+Z0aKv8SQ5l8varpDpf7Ie
Cy+l4EeapAX/bZolplqiDVGw6ysd7Qkc1f1tRrb+6TCWgbFOnPh7QwPpMIBMyTF+
AFF1+5bCHpWHbC1W86SdzIqkHTyq8lu+z3TW8vgFj60tdotFYnPnvQLy5X1/Qf7I
1K9RqD7B8kkwz7sIBiBs8XfWfasEOrPggJoEgKtJKGB8zEHew0klsdQt8OuzBI3f
CEUSK3C1QzLEIAn1ulJlwO8+UkvAeNm6uLkGl30CYO5AW6WFz9olDOiCLEN9BGbN
LxG1yn1x81TbTRLcquCKCt/f/IFspXXM77p2RUXowsiMy3ZfbhuGgcUtVCD1ZY7
lMlaNuGs17umML8s8Kv3FncB3chr/MPvpO9CyBsdaEu7wd1pUihi1ErwCsVA+fR5
f9iQGhD2kqB1O2/OGLrkHjxe006s08jqiSrvu8+V30lBadIH5JtRQn3xNVTBIDPP
scPsF9LPLI2rbswKo5Mzw4FbP9gz4GZLrF2TZu/fRDxB0t68JHdWKpwR7Z3tbbhj
ysx5BU9q2gBJ1DvK/VG/qLNIvZaPKptZHRVLVvkgwhAbIcVyWkXpVSlll31JTQvx

ภาพที่ 37 (ต่อ) ข้อมูลเข้ารหัส CFLOWER



ภาพที่ 37 (ต่อ) ข้อมูลเข้ารหัส CFLOWER

28EiclubX83j2Xj/72ic+ic1/UgDfG2CGHmW/Qu3nVBaDlnTHu//yDsIlrPXCNO
v7w+mkL1XyHjPQubb/cdnlkRUwYcSXON3cuntvCUZrpt39zMHTcLhy/L2/w72cnr
SsIUp+WFjS1N/FTDaz1OxbHdvOcQxMegAYxdgQD3XwaCRAf18qRX6dtsnp/XrfHT
AJviBwgWM57W6Ipf1kw3nRaKFLKTZ9nRozn8dJfryUAxmT0nB83/NjAWxQVyr3Md
acPLnDZMti+UfBytTKw6yxUwc0God7xywPBdygFFGYmoWAimEvJs34zMYEfgO3Gw
xB7zg8+lyQRQDhyYRWiE4XGja/lLbxwQH9LJPei/2nN1PBI1BlNoDDr3tXSgxEwj
QyiYahS9eZThoKZUPy8Q/hrpsBlGgtm/Dsxs1jHLVk6WcWOMtZywRjfdO8ivZAya
57S+48W1MFfLrtKEziCoUrlZ/yoV9i1LVR/kMjLkaMHXoH/LPsukq3gWv9TXlj+R
vA1tRb9P6Rsh6P1g1bZe7mU5ux61Jew9Mj38hiAbs0m9vwnlYn16CqdVtjsXFYo4
Zw6wLgSv8kxort5Q1aEjrkgprcsS9KGA6s/Nvwluk92uz2du1mdr6i8++i1v2E8J
u/H2+wyjPGdtJVE69JWjnqYayZcKFnSfZlvlJsIV8ZviyoXAPWK1euKhVeI98t/a
753fiMrkA3Y3cimdL/klbmONu8l3qiCOMqI1DGlYhOeDBkXy4Jd4uEYAV4TboFoT
9l0uSV+sXMoUE+PH/8bIG98dl+EyaFw+K/NkSa2vUVi6DzQUR0g6jJJUXjC3waWL
uOhGPx53OgAPhbX2AEymXrstkLNslFw7QQOPG6kZEK/TQuDdS5m9mh6oLVoZdAOv
tKmJ3TfOXaZm4/lQQNReZ9oTC/E5csio8h8CGsVM/E7rNlD+xqjxBjQyOD48lZQ7
Mm3pH47ZR0DNWcTEG+72XfH/Vj1B733JZE6EavnnvrAeXUDrARQZWPCMDXO3urbf
PU0zH0SCtgT90IpGrKTN2ZA5l4j2DZzCCjTue09ONvFvssKHWPb1L/y7NpaShryK
+54AiLs7ss8GYjPWCyDKUlU2B2EsszBzVpdYLOmky6bxvO17o4R/tc6nxslNYNs2
Lt9KlaBy9vh+/nxw2dJt0NwZQHsevdP6+ADKzZ+46a/gT65byB4wASRQfYFykfh+
kLthbWdIsx/x+lmTRrssuStHWTV8EB7Q7fW9+tqiJx/AoaYGoyRJ3hWYzXz8G5cD
qGtUkmMOoOC7v7dwhxHwBHKQMGMBl3vYrGwRBfrjzxQBFXdxLSS9TQ0fZw32conR
un07nNl01N34Ykh01TfWyxpFMnx/DBz3dTL+SVP/Ob6PI/mOff+0eXXVmNypvk1T
L50upfFrVSielvZoFjmuFMJqh1KSbw3/hI14PU2wLNBb2rZNhMTiZH5Hzlc3obua
eoI3vUhP2tTvYecI7R18tsKucGU2IsjuXlEouaPWNmBXoMrfDMdzLGo/ZHlRdXyA
qqHJFVC8orvgT7aVDxijPh32XuBZ4ucMJ50HvGDY6MOKpdNx4T+W4E6POH3Tsg/y
L/IeATmGZEJj8Zn1LfaD6Nu9sjoLNhDZb6bNTRUMqpDqS8vtgz+TrFg12SYG9ud6
wTtHHd2X1bKREXA5Cebtn/vyfHGi75csC3p4i/pPPa1FWxgFsjMJiaCfaljHZH+X
QFoBC6FYchJbadp0dfO/m7BvbIjzrHb2MAkPjwLwCLOiIcxXvQWhoXzK0Kt75C1B
091Sp8G2kZJkLbD9uAdoy6fy2wTwTpV9thYUS1W9hTFDgFBBsIJiWFyqFoKbvIvz
e7k4CyvpcEkI3we1sO7sBMD9B6agXPTQQK/kHi1nb2g4sgXGSgqhDn+uXrg4/Lop
gANLwdCkVwmVEpfd5JZOyXbUjUk1+Fe2+dbjHOJNxc1e7vw2EXQWsq4imGqcpVZU
EnvluS0jViyZr+GfLGdlXOjHkDtPgCCFwEVrAWYyK2XsDczSx6pdbayOts9aW6BS
wKOfUOLcIuSEh5A0F7dTvWvHgLDvExU2D092sdxaOWL590QJBg7Ej7Qy9ag2Gk8H
Jc03MTnCt3rNoT8ljOe9zU6CsxSlnkHVMO/gpu1qq3g7qnsxHZxssdiUd2yD1gfa
BcjySHIhRybsSu04AXMXwqDeg50fW9c4RGKRv31a4F/CXKP1jYCe9d5soMmtbtqN
ML5l8Y71kdw4PfF6yRJDfZ2pom7z1jAOKtnCkYXij6w4JUibTfd+nFa37Z5kd3sJ
afqD8SW7XtlubLzBhzC1fZZCL6hzaTNHJ2lGCTYOArD/qdQ9N4ObV8W5Cmv0lVSp
n3c3AlbrMuviza8mgZezQ5WwQy8QR2O3KdWqDYWEFtnC4UvoB42M+pIEnR/yJmvv
OYY6QdnDlld5aYluNvw5ufEGkQJD6P0URSMBjT2L2zdNx8wSoBPZ68ZflvOJTD9Z
2x/IEiWj0NlEk2FZVcbMpZWiFAN0hAKVUwsXOM8WYzsCk2sLu42E6bSpmghaF9bO
O0L+4jI82nZch/H4dVW33MYqB4cpXFrzwWVXAP8sYuhbS6/mGIb0drLd/BkbtHJa
yMfRbOfJ2NnUwdxEnQAjN1B0AQY6BKA4D3Cub3XheV2zzudWk0cDgUkX3Zrcvn0jS
hN3RRlDEKono/TX24HUhQFjWUj/g2hdNVg+IqjIeENq0tDKTxSM7Y9KWrfSlJYhS
HpyyV9lnBwS/hVqChc+vWGH9V7EgJBg55GNZsRsorEYUJ1bhxnoHD/qVxEdUXVZ
SlYngio+ardIRhrg2hc9u2RdUkMngVAkmYgTYIjOu59VyJvOC2alA9HLiY+wqgt
qf2QESDoLzHcj7N67Rql1EdEvyOcs9ET3HjGoEhlnsDntfBt5KR/uE5u4jlXVPt0

ภาพที่ 37 (ต่อ) ข้อมูลเข้ารหัส CFLOWER

b/LcshYRyR84kXyeoODg0zv8Dkxy+HEr02s7+jH2i6yaDh0ILXPTmiBzVQJTt9Tx
LeaJlduLl2MDoD5ArCRwSs7Q99L+2lvE/NNC+BoYTuwTuPW0bTfTH6FKjpkLgY7T
GyNNSlAegRtL0CQdH94HU+MvXMbrufQie38rqp8vfp9xbLZ3j4ZnE638dSZLqUZh
9J6fk6WddlJs/icUMH+SGblm8onnnPsUH0bokml4yiUQb0Ip8wbjTKL/Dhljipg5
J+jfru86+qgd90e6WO/Ovw2ToyHIqNUvda6KFavcmAkC8GzV7z200MLWS+sfe9sp
o60gyhGowBoSk3i2/JjkcqOsrjBuPGMyp6bJbmsqDhAqlVjTVqwUwQMELIQmh8LI
H3hYFXpSUxVaPVonOU3sK9YKd1mvOPYbPD79oWK7kgIGB0319oBauC5l6ifArn4B
vwDf6CNe3vaIyUp6BtC4IZB0GKwJwXKVcpALkKCd/ljRTGMxMs145Eh8ZYVJw7yB
2HoxEfsQdrpyN69X5Vf4kUvXFwIbvihCLqQbXTTaSlaN5gFTEdMSJNndfp5NCfw8
GM5+WoiiHxnljkTPMdjml0OHCON4E7+xeNiDdLGMQyIr+aE1y2VUwxEvkbWyMgHV
+26lOXaPPU5bqCpZEwIPiZVNGK6QNwwU0L8aS23J8dPA3XG8oWdN935zh8kEkvs4
fCzbPOigISSGqfwQawMx07SqvzIe9W4K2ZEIJAyJOTi5JqcWD1nMyjpwvMNv4unE
qj884l5KPlUZ116bzkhpQ1G/KCScmqq8mH5ARKtVo40AvA7S8c5MqhvE3UvRoFXs
UBSAaSD1PIsWyv+oeFxMAVWWvVTH3JZYDITLu5OxO+co4GQIFK47iltGjixgfkfT
GG2U2ph4W8yyWSnCfE8yyreDjkqMMdvUMxHY8xuirOYCkLclZBYLxQ53+LJuAU1q
SOVOafQbIc1TXbdtuObyVOdldeQLzmXXCfYlr5zMvctxySay2PgfHGqKVCqEvZrK
imaQ7WskM2Owtxj7hycTaO8lZZAMzahIV8Y+gy6xN78kP5yvG3sEuT7Ay0uzc6eH
8hsb8pRI05zFqsEiwn8FyyMfetgyOdUYnM3lhPDprGoeL20pTHqfmp1vi1Bn8Fbm
ldLu3FKrEP0g0KgOfRYQoQPOjeKNoOJCrbpRx5qB5xhijKdGFZ8V2vYVl3IjiuOi
TAzHq9gDVqYnHekuR5/4GWVwZ7IRIvpePGh8m+WaEQFWdBbsmT35muL0qDr1LRd
/CMsD7Ucm9DPFfTXK1AcH8AeUY4aoLGRwYtDIQfdumu2VDTj8Kw2jvpD+SacDuVL
zSPhYJ4mreS7VjmcJqIAV9AmJOrB8OPDDqu6YfhDICr+ti9clClqZP/0CsBOZY3z
BpnKu25CnCDJvqbZ3M57k0rPRsSpAPsLyutPZw+uCttZL8wEE6zyY5h5prlQkSAY
67seXmHxZjZKv0aZXJO/QMoWtdQ4BMpiIAyjQgopSy+PALmn2tsTxdWYD2pC5yfX

***** END MESSAGE *****

ภาพที่ 37 (ต่อ) ข้อมูลเข้ารหัส CFLOWER

นำแฟ้มเข้ารหัสชื่อ CFLOWER มาถอดรหัสเก็บไว้ในแฟ้มที่ชื่อ DFLOWER.BMP ปรากฏดังภาพที่ 38

ภาพที่ 38 ภาพ แฟ้ม DFLOWER.BMP

จากการเปรียบเทียบรูปภาพแฟ้ม FLOWER.BMP กับ DFLOWER.BMP ปรากฏว่าเหมือนกันทุกประการ และเมื่อพิจารณาแฟ้มเข้ารหัส CFLOWER จะเห็นได้ว่าเป็นการยากที่จะทำความเข้าใจหรือลักลอบถอดรหัส ซึ่งเป็นไปตามวัตถุประสงค์ที่ตั้งไว้ทุกประการ

4.2 ผลการทดลอง

จากการทดลองปรากฏผล ดังนี้

4.2.1 ส่วนการสื่อสารข้อมูล

ได้ทดลองรับ-ส่งข้อมูลผ่านระบบเครือข่ายต่างๆ ดังตารางที่ 11

การทดลองรับ-ส่งแฟ้มข้อมูลเข้ารหัส

ต้นทาง	ปลายทาง	เครือข่ายที่ใช้รับ-ส่งข้อมูล	ความเร็วของเครือข่าย (Bps)	หน่วยทดสอบ
Server สส.	Server บก.ทบ.	ผ่านดาวเทียม TDMA	19200	ศูนย์โทร ฯ
Server สส	Terminal กวก. สส.	5 ตัว ทบ.	9600	กวก.สส.
Server สส.	Terminal ส.101	วิทยุถ่ายทอด 1 hop ผ่าน 5 ตัว ทบ.	1200	ส.101
Server สส.	Terminal ส.13	วิทยุถ่ายทอด 1 hop ผ่าน 5 ตัว ทบ.	1200	ส.13
Server สส.	Terminal ส.102	วิทยุถ่ายทอด 1 hop ผ่าน 5 ตัว ทบ.	1200	ส.102
Server สส.	Terminal กวก. สส.	สัญญาณจากตู้ DX ผ่าน 5 ตัว ทบ.	1200	รร.ส.สส.

ตารางที่ 11 การทดลองรับ-ส่งแฟ้มข้อมูลเข้ารหัส

จากการทดลองรับ-ส่งแฟ้มข้อมูลเข้ารหัสไปโดยผ่านระบบเครือข่ายต่างๆ ของกองทัพบก ผลปรากฏว่าสามารถ รับ-ส่ง แฟ้มข้อมูลเข้ารหัสได้

4.2.2 ส่วนการเข้า-ถอดรหัส

จากการทดลองด้วยข้อมูลหลายรูปแบบ ดังตารางที่ 12

ข้อมูลที่ใช้ในการทดลอง

ชนิดของข้อมูล	จำนวนที่ทดสอบ
TEXT FILE	20
PAGE MAKER FILE	10
MICROSOFT WORD FILE	10
EXCEL FILE	10
PICTURE FILE (*.BMP , *.JPG , *.GIF)	10
VISIO FILE	5
EXECUTE FILE(*.EXE)	5
COMMAND FILE(*.COM)	5

ตารางที่ 12 ข้อมูลที่ใช้ในการทดลอง

ผลปรากฏว่าเมื่อส่งข้อมูลรูปแบบต่างๆ ที่เข้ารหัสจากต้นทางมายังปลายทางแล้ว สามารถนำแฟ้มข้อมูลเข้ารหัสดังกล่าว มาทำการถอดรหัสได้ผลลัพธ์ตรงกับแฟ้มข้อมูลเริ่มต้นทุกประการ และใช้เวลาในการเข้าและถอดรหัสโดยเฉลี่ยประมาณ 1 นาที

บทที่ 5
สรุปผลการวิจัยและข้อเสนอแนะ

5.1 สรุปผลการวิจัย

ในการรบ การติดต่อสื่อสารถือเป็นเรื่องจำเป็นและสำคัญมาก ในการติดต่อสื่อสารระหว่างกันนั้น การรักษาความปลอดภัยทางการสื่อสารถือเป็นเรื่องสำคัญ เพราะถ้าข้าศึกทราบถึงข่าวที่ส่งถึงกัน ข้าศึกจะนำข่าวนั้นไปใช้ประโยชน์ทางยุทธวิธีได้

ปัจจุบันกองทัพบกใช้วิธีการเข้ารหัสด้วยมือโดยเจ้าหน้าที่ ซึ่งทำให้เกิดปัญหาความล่าช้าและความผิดพลาดในการปฏิบัติงานของเจ้าหน้าที่ ส่วนเครื่องมือเข้ารหัสที่มีขายอยู่โดยทั่วไปก็มีราคาแพง ไม่มีการเปิดเผยเทคโนโลยี และมีกฎหมายของประเทศผู้ผลิตควบคุมอยู่ การจัดซื้อจัดหาจึงกระทำได้ยาก นอกจากนี้ ยังมีปัญหาเรื่องความเข้ากันไม่ได้ของเครื่องมือแต่ละรุ่น หรือแต่ละชนิด และฝ่ายตรงข้ามก็สามารถหาซื้อเครื่องมือเดียวกันได้ อันจะทำให้เกิดจุดอ่อนด้านความมั่นคง

ฉะนั้นจากเหตุผลข้างต้น กองทัพบกจึงน่าที่จะทำการพัฒนาการเข้ารหัสข่าวของตนขึ้นเองโดยใช้คอมพิวเตอร์ช่วยเสริมให้การเข้ารหัสรวดเร็วและซับซ้อนมากยิ่งขึ้น รวมทั้งสามารถสร้างกุญแจรหัสส่วนตัวสำหรับผู้ใช้แต่ละคน ทำให้ยากต่อการถูกลักลอบถอดรหัส นอกจากนี้ ระบบคอมพิวเตอร์ยังสามารถจะนำไปเชื่อมต่อเข้ากับระบบสายโทรศัพท์และวิทยุถ่ายทอดสนามในการรับ-ส่งข่าวเพื่อประโยชน์ในการรักษาความปลอดภัยในการสื่อสาร และช่วยประหยัดงบประมาณของชาติได้อีกด้วย

จากการศึกษาการเข้า-ถอดรหัสที่มีใช้ในปัจจุบันปรากฏว่าการเข้ารหัสที่มีการพิสูจน์อย่างกว้างขวางว่ามีความน่าเชื่อถือมากที่สุด 2 ระบบ คือเดส และ อาร์เอสเอ แต่ทั้งสองระบบต่างก็มีจุดอ่อน และจุดแข็งที่แตกต่างกันไป ดังนั้น การวิจัยเพื่อพัฒนาระบบการเข้ารหัสที่จะนำเสนอใหม่แก่กองทัพบกจึงนำระบบทั้งสองมาปรับปรุงและประยุกต์เข้าด้วยกันในการทำงาน

ระบบเข้า-ถอดรหัสที่พัฒนาขึ้นใหม่นี้ ได้นำข่าวกระจ่างที่จะส่งมาเข้ารหัสด้วยวิธีการกุญแจลับ (DES) ซึ่งเป็นวิธีที่มีประสิทธิภาพในการรักษาความปลอดภัยสูงเป็นที่น่าเชื่อถือได้ และมีความสะดวกรวดเร็วในการใช้งาน แต่มีจุดอ่อน คือ มีระบบการใช้กุญแจที่ยุ่งยาก ต้องเก็บกุญแจ

เป็นความลับ ใช้กุญแจจำนวนมาก และการที่มีผู้รู้รหัสกุญแจหลายคนจึงลดประสิทธิภาพในการรักษาความปลอดภัย ทำให้มีความจำเป็นต้องเปลี่ยนกุญแจบ่อยครั้ง

ด้วยเหตุนี้ จึงนำระบบกุญแจสาธารณะ (RSA) มาประยุกต์ใช้ร่วมกับเดสเพราะแม้ว่าอาร์เอสเอจะใช้เวลาในการเข้า-ถอดรหัสนานกว่าเดส แต่มีการจัดการกุญแจที่สะดวกต่อการใช้กว่า รหัสเดสมาก คือผู้ใช้แต่ละคนจะมีกุญแจเพียงกุญแจเดียวที่จะต้องรักษาไว้เป็นความลับ และใช้กุญแจจำนวนน้อยกว่าทำให้มีประสิทธิภาพในการรักษาความปลอดภัยสูง

ระบบที่พัฒนาขึ้นนี้เพิ่มการรักษาความปลอดภัยด้วยการนำแนวความคิดเรื่องลายนิ้วมือลายเซ็นดิจิตอล และจดหมายอีเล็คโทรนิคส์มาประยุกต์งานร่วมกับเครื่องมือสื่อสารที่ใช้อยู่ในกองทัพบก เพื่อทำให้ระบบการรับ-ส่งข่าวมีการรักษาความปลอดภัยที่ดีขึ้น โดยเพิ่มการรับรองข่าวสารและการป้องกันมิให้ผู้ที่ไม่เกี่ยวข้องสามารถอ่านข่าวสารได้ การทำงานของระบบที่พัฒนาใหม่นี้ จะเข้ารหัสข่าวด้วยกุญแจรหัสเดสที่สร้างขึ้นใหม่ในแต่ละครั้ง หลังจากนั้นจึงนำกุญแจไปเข้ารหัสอาร์เอสเออีกชั้นหนึ่งแล้วส่งไปพร้อมกับข่าวเข้ารหัส ผู้รับข่าวจะไม่ได้ทราบกุญแจถอดรหัสล่วงหน้า แต่สามารถใช้กุญแจส่วนตัวของตนถอดรหัสอาร์เอสเอเพื่อรับทราบกุญแจสำหรับใช้ในการถอดรหัสเดส เพื่อให้ได้ข่าวกระจ่างต้นฉบับ นอกจากนี้ ยังมีการสร้างลายนิ้วมือดิจิตอลของข้อมูลที่ส่งเพื่อใช้ตรวจสอบความถูกต้องของข้อมูลนั้นๆ ทั้งก่อนและหลังการเข้ารหัส

การรักษาความปลอดภัยของการเข้า-ถอดรหัสข่าวนอกจากจะต้องคำนึงถึงการรักษาความปลอดภัยของกุญแจรหัสแล้ว ยังจะต้องใช้ระบบเข้า-ถอดรหัสที่ผ่านการพิสูจน์ทางคณิตศาสตร์อย่างเป็นทางการแล้วว่ามีความปลอดภัย นอกจากนี้ ระบบเข้า-ถอดรหัสที่ดีต้องมีความซับซ้อนมากจนไม่สามารถทำการลอบถอดรหัสได้ในระยะเวลาอันสั้น จะได้ประโยชน์จากเงื่อนไขของเวลาที่จะทำให้ข่าวสารนั้นหมดความสำคัญลงไป

เมื่อเปรียบเทียบระยะเวลาที่ใช้ในการเข้า-ถอดรหัส ระหว่างการเข้า-ถอดรหัสด้วยมือที่ใช้อยู่ในปัจจุบัน กับระบบการเข้า-ถอดรหัสที่พัฒนาขึ้น จะเห็นได้ว่าระบบการเข้า-ถอดรหัสที่พัฒนาขึ้นใช้ระยะเวลาในการเข้า-ถอดรหัสน้อยกว่า การเข้า-ถอดรหัสด้วยมือมาก โดยการเข้ารหัสข้อมูลรูปแบบต่างๆ ที่นำมาทำการทดลองใช้เวลาโดยเฉลี่ยเพียง 1 นาที ในขณะที่การเข้า-ถอดรหัสด้วยมือโดยเจ้าหน้าที่ใช้เวลาโดยเฉลี่ยถึง 15 นาที นอกจากนี้ ยังมีความเป็นไปได้สูงที่การเข้า-ถอดรหัสด้วยมืออาจใช้ระยะเวลานานกว่า 15 นาที ทั้งนี้ ขึ้นอยู่กับความชำนาญของเจ้าหน้าที่ ความซับซ้อนของ

รหัส และความยาวของข้อมูล นอกจากนี้ ข้อมูลบางชนิด เช่น รูปภาพ ไม่สามารถทำการเข้า-ถอดรหัสด้วยมือได้

จากการทดลองสรุปได้ว่าระบบการเข้า-ถอดรหัสที่พัฒนาขึ้น สามารถเพิ่มประสิทธิภาพของเข้า-ถอดรหัสข้อมูลในกองทัพบกได้ โดยนอกจากจะลดระยะเวลาที่ใช้ในการเข้า-ถอดรหัสแล้ว ระบบที่พัฒนาขึ้นยังสามารถเข้า-ถอดรหัสข้อมูลได้หลายรูปแบบ มีความถูกต้องแม่นยำกว่าการเข้า-ถอดรหัสด้วยมือ มีความน่าเชื่อถือในการรักษาความปลอดภัยเนื่องจากลักลอบถอดรหัสได้ยาก

นอกจากนี้ ระบบการเข้า-ถอดรหัสที่พัฒนาขึ้นยังมีการเพิ่มการรักษาความปลอดภัย โดยสามารถพิสูจน์ทราบผู้รับ-ผู้ส่งได้ และตรวจสอบได้ว่าข้อมูลที่เข้ารหัสแล้วถูกลักลอบเปลี่ยนแปลงแก้ไขหรือไม่

5.2 ข้อเสนอแนะ

ระบบเข้า-ถอดรหัสที่พัฒนาขึ้นนี้ มิได้ป้องกันการ การลักลอบนำข่าวเก่าที่เคยส่งไปแล้วมาส่งใหม่ในระบบอีกครั้งหนึ่ง อันจะทำให้ผู้รับเกิดความเข้าใจที่ผิดพลาดได้ กรณีนี้สามารถแก้ไขได้โดยให้มีการลงวันเวลากำกับในการส่งข่าวทุกครั้ง

ในระบบที่ทำการพัฒนาขึ้นใหม่มีการตรวจสอบความถูกต้องของข้อมูลเข้ารหัสด้วย MD5 Info. ซึ่งบอกได้ว่าเนื้อข่าวที่ทำการเข้ารหัสแล้วถูกแก้ไขเปลี่ยนแปลงหรือไม่ ทั้งนี้ โอกาสที่ฝ่ายตรงข้ามจะส่งข่าวเข้ารหัสปลอมมาพร้อมกับ MD5 Info. ปลอม เพื่อเป็นการลวง นั้น กระทำได้ยาก เนื่องจากการถอดรหัสยังต้องผ่านกระบวนการอื่นๆ ด้วย และในระบบยังมี MIC ทำหน้าที่ตรวจสอบความถูกต้องของข่าวที่ถอดรหัสแล้วอีกชั้นหนึ่ง ดังนั้น จึงมีโอกาสน้อยมากที่จะเกิดกรณีเช่นนี้ขึ้นได้ อย่างไรก็ดี หากมีความจำเป็นก็สามารถเสริมการทำงานของ MD5 Info. ได้ด้วยการนำ MD5 Info. มาเข้ารหัสอาร์เอสเอด้วยกุญแจสาธารณะของผู้รับก่อนที่จะส่งไป

นอกจากนี้ จุดที่จะสามารถเพิ่มการรักษาความปลอดภัยให้แก่ระบบที่พัฒนาขึ้นได้อีกคือ การลบแฟ้มข้อมูลชั่วคราวที่ระบบสร้างขึ้นโดยอัตโนมัติ ทิ้งไปทุกครั้งก่อนที่จะออกจากระบบ

แม้ว่าระบบที่พัฒนาขึ้นจะสามารถเพิ่มประสิทธิภาพการเข้า-ถอดรหัสของกองทัพบกได้อย่างเป็นผล แต่ก็ยังไม่สามารถนำมาใช้ได้อย่างเต็มที่เนื่องจากระเบียบราชการที่ใช้อยู่ในปัจจุบันไม่ยอมรับการลงลายเซ็นดิจิตอล คือต้องมีการลงลายมือชื่อเป็นลายลักษณ์อักษรเท่านั้น

ระบบเข้า-ถอดรหัสที่ดีควรจะมีระบบการรักษาความปลอดภัยอื่นๆ ประกอบด้วย เนื่องจากยังมีสถานการณ์ที่ระบบเข้า-ถอดรหัสเพียงประการเดียวไม่สามารถรักษาความลับไว้ได้เช่น

- การเข้ารหัสไม่สามารถป้องกันมิให้ข้อมูลถูกลบไปได้
- ผู้ที่ลักลอบใช้สามารถจะปรับแก้โปรแกรมเข้ารหัส ให้รับกุญแจซึ่งมิใช่กุญแจที่บันทึกไว้ หรืออาจเก็บข้อมูลที่เข้ารหัสไว้ในแฟ้มข้อมูลพิเศษ เพื่อจะลองถอดรหัสในอนาคตได้
- ผู้ที่ลักลอบอาจเข้าถึงข้อมูลได้ก่อนที่จะเข้ารหัส หรือหลังจากที่ถอดรหัสแล้ว

ระบบเข้า-ถอดรหัสที่นำเสนอนี้ นอกจากจะเป็นการเพิ่มประสิทธิภาพในการรักษาความปลอดภัยของการรับ-ส่งข่าวแล้ว ยังเป็นก้าวแรกในการนำระบบคอมพิวเตอร์มาประยุกต์ใช้ในการเข้า-ถอดรหัสของกองทัพบกไทย การที่ระบบนี้เน้นการปรับปรุงและพัฒนาซ็อฟต์แวร์เป็นพื้นฐานของการเพิ่มประสิทธิภาพในการทำงาน ดังนั้น ระบบจึงมีศักยภาพที่จะพัฒนาต่อไปได้ด้วยการปรับปรุงซ็อฟต์แวร์ และการใช้ฮาร์ดแวร์ที่มีสมรรถนะสูงขึ้น

บรรณานุกรม

Biham, E. and Ali Shamir. Differential Cryptanalysis of the Full 16-Round DES, Lecture at Workshop on Cryptanalysis. Washington, D.C., March 1992.

Cooper, James Arlin. Computer and Communications Security : Strategies for the 1990's, Singapore : McGraw-Hill Book Company, 1989.

Fahn, Paul. Answer to Frequently Asked Question about Today's Cryptography, Redwood City California : RSA Laboratories, 1993.

Forcht, Karen A. Computer Security Management, Palo Alto, California : Thompson Information/ Publishing Group. 1992.

Garfinkel, Simson and Gene Spafford. Practical Unix Security, Chicago, Illinois : O'Rielly & Associates, Inc., 1993.

Information Standards Division, Center for Standards, Joint Interoperability and Engineering Organization. US Message Text Format (USMTF) Interoperability Program, Briefing Presented to Royal Thai Supreme Command. U.S.A. : 12 June 1997.

Schneier, Bruce. Applied Cryptography, New York, New York : John Wiley & Sons, Inc., 1994.

Schneier, Bruce. E-mail Security ; How to Keep Your Electronic Messages Private, New York, New York : John Wiley & Sons, Inc., 1995.

Stinson, Douglas. Cryptography Theory and Practice, Hong Kong : CRC Press, 1995.

Tsudik, G. Message Authentication in One-way Hash Function, paper Presented at the Symposium on Computer Security. Florence, Italy, May 1992.

U.S. Commamnder in Chief Pacific (USCINCPAC). Military Intelligence, Report of Thailand/ U.S. Command and Control Interoperability Board. Phuket, Thailand :3-7 September 1997.

กรมยุทธศึกษาทหารบก. หลักนิยมการสื่อสารทางยุทธวิธี (รศ 24-5). กรุงเทพฯ : 2530.

โรงเรียนทหารสื่อสาร, กรมการทหารสื่อสาร. หลักนิยมการสื่อสาร. กรุงเทพฯ : 2538.

โรงเรียนทหารสื่อสาร, กรมการทหารสื่อสาร. การปฏิบัติการสื่อสารทางยุทธวิธี. กรุงเทพฯ : 2540.

ภาคผนวก

ผนวก ก.

การใช้โปรแกรม

Royal Thai Army

Encryption-Decryption Program

การใช้โปรแกรมกระทำโดย Run โปรแกรม RTA_ED โปรแกรมจะทำการสร้าง Random Key จำนวน 64 ชุด ชุดละ 2 ไบท์ เพื่อใช้ในการสุ่มเลือกบางชุดไปใช้ในการเข้ารหัสและสร้างรหัสลับของผู้ใช้ โดยการ Random แต่ละตัวจะเกิดขึ้นจากการเคาะ Key Board แต่ละครั้ง ดังภาพที่ ก-1

```
**** Generate random seed s and save to file temp ****
Press key like normal typing to generate  64 random numbers.
ad 11 65 d9 5b 17 19 8e 82 42 bd d5 9c 5b c0 54
21 15 5b 9c e0 26 67 b4 fb 41 7e c7 15 5f 87 d5
4b 95 d1 10 5e a6 f6 2e 78 c9 17 63 a4 f7 45 8c
41 26 85 91 e1 14 5b 96 da 23 68 ab ed 2c 23 23
Press Enter to continue.
```

ภาพที่ ก-1 การสร้าง Random Key

เมื่อผ่านการ Random Key เรียบร้อยแล้ว จะถูกนำสู่การทำงานตามเมนูโปรแกรมซึ่งมีรายการดังภาพที่ ก-2

```
        THE ROYAL THAI ARMY
        Encryption-Decryption Program
-------------------------------------------------------------

  0) Exit
  1) Encrypt file
  2) Decrypt file
  3) Key
  4) Encrypt file with password
  5) Decrypt file with password
-------------------------------------------------------------
                VERSION 1.0
-------------------------------------------------------------
Selection :
```

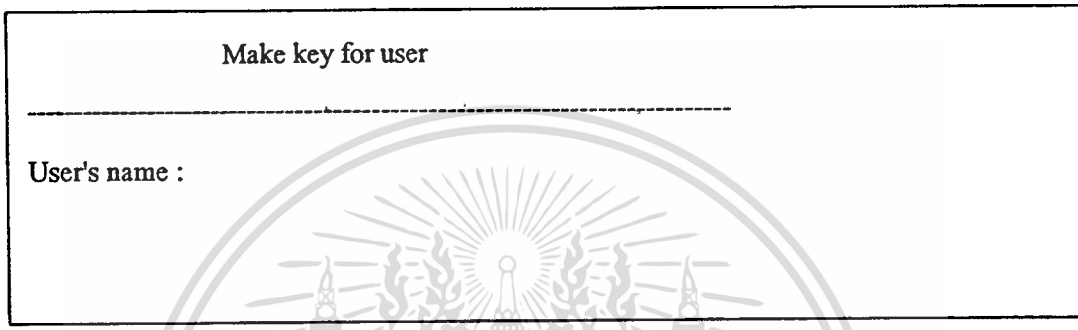
ภาพที่ ก-2 เมนูโปรแกรม

รายการตามเมนูมีดังนี้

0) Exit	หมายถึง การเลิกการทำงานโปรแกรม
1) Encrypt file	หมายถึง การเข้ารหัสโดยการสร้างแฟ้มเข้ารหัสขึ้นมาใหม่
2) Decrypt file	หมายถึง การถอดรหัสจากแฟ้มเข้ารหัสมาเป็นข้อมูลข่าว
3) Key	หมายถึง การสร้างกุญแจสำหรับผู้ใช้ระบบ
4) Encrypt file with password	หมายถึง การเข้ารหัสเพิ่มเพื่อเก็บไว้ใช้ส่วนตัว
5) Decrypt file with password	หมายถึง การถอดรหัสส่วนตัวเพื่อนำกลับมาใช้งาน

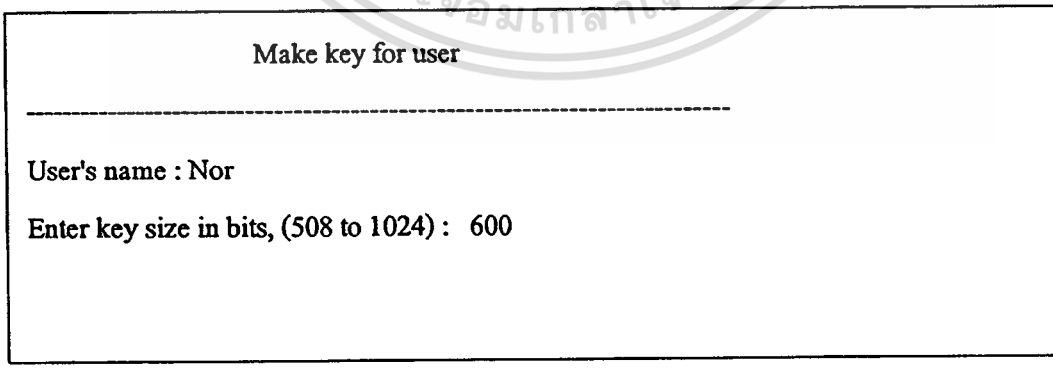
เลือกการทำงานข้อ 3. การสร้างกุญแจสำหรับผู้ใช้ระบบ

โปรแกรมจะให้กรอกชื่อผู้ใช้ที่ต้องการสร้างกุญแจ โดยมีข้อจำกัดว่าชื่อผู้ใช้ในระบบเดียวกันจะต้องไม่ซ้ำกัน แต่สามารสร้างชื่อผู้ใช้เดิมทับของเก่าได้ ดังภาพที่ ก-3



ภาพที่ ก-3 การสร้างกุญแจสำหรับผู้ใช้ระบบ

เมื่อใส่ชื่อผู้ใช้โปรแกรมจะถามขนาดของ Key ที่ต้องการสร้าง มีขนาดตั้งแต่ 508 – 1024 bits เพื่อใช้เป็นส่วนประกอบในการเข้ารหัสที่เรียกว่า Key-Info. ทำให้ส่วนประกอบส่วนนี้ของผู้ใช้แต่ละคนแตกต่างกัน ดังนั้น แฟ้มข้อมูลเดียวกันที่เข้ารหัสโดยผู้ใช้แต่ละคนจะได้แฟ้มเข้ารหัสที่แตกต่างกัน ดังภาพที่ ก-4



ภาพที่ ก-4 การใส่ขนาด Key ของผู้ใช้

การสร้างขนาด Key จะใช้เวลาที่แตกต่างกัน ขนาด Key ที่มีขนาดใหญ่จะใช้เวลามากกว่าขนาดเล็กโดยโปรแกรมจะแสดง Message บอกให้ทราบว่าโปรแกรมยังคงทำงานอยู่ ดังภาพที่ ก-5

```
                    Make key for user
------------------------------------------------------------------

User's name : Nor
Enter key size in bits, (508 to 1024) : 600
Working. This may take a long time. Please wait a while.
```

ภาพที่ ก-5 Message การรอการสร้าง Key

เมื่อสร้าง Key เรียบร้อย โปรแกรมจะให้ใส่รหัสผ่านส่วนตัวซึ่งเก็บไว้เป็นความลับเพื่อใช้ในการถอดรหัส การใส่รหัสผ่านนี้จะไม่ปรากฏให้เห็นเวลากรอก และมีผลกับอักษรเล็กใหญ่ ดังภาพที่ ก-

```
                    Make key for user
------------------------------------------------------------------

User's name : Nor
Enter key size in bits, (508 to 1024) : 600
Working. This may take a long time. Please wait a while.
Please enter pass phase carefully, and remember your pass phrase.
You don't have a second chance!
Pass phase can be any sentence of any length.
password :
Finished.
Press Enter to continue.
```

ภาพที่ ก-6 การใส่รหัสผ่านส่วนตัว

เลือกการทำงานข้อ 1. การเข้ารหัส(Encryption)

1. การเข้ารหัสมีข้อกำหนดดังนี้

1.1 ทั้งผู้ส่งและผู้รับจะต้องถูกสร้างไว้ในระบบเรียบร้อยแล้ว โปรแกรมจะไม่ยอมทำงานถ้าหาผู้ส่งและผู้รับไม่เจอ

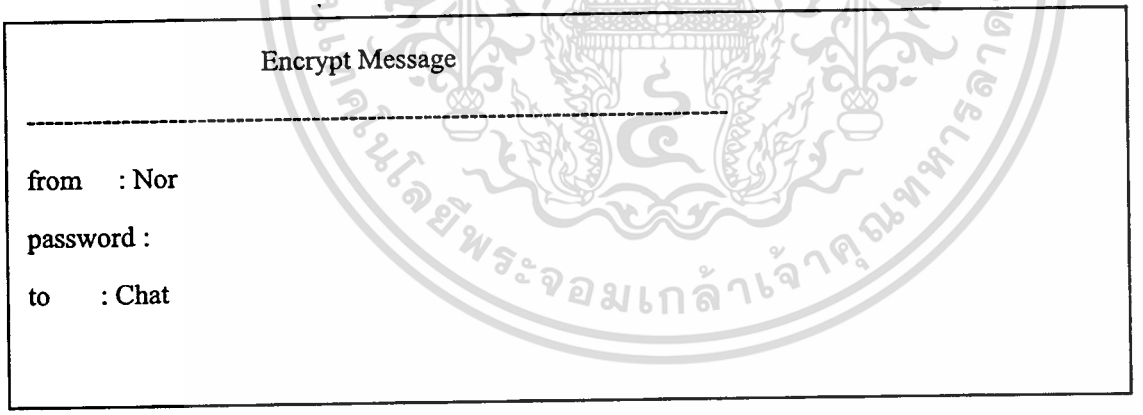
1.2 แฟ้มข้อมูลข่าวที่ต้องการเข้ารหัสต้องถูกสร้างไว้ก่อนหน้าแล้วโดยไม่จำกัดชนิดของแฟ้มว่าเป็นประเภทใด

2. มีขั้นตอนการทำงานคือ

2.1 กรอกชื่อผู้ส่ง

2.2 ใส่รหัสผ่านผู้ส่ง

2.3 กรอกชื่อผู้รับ ดังภาพ ก-7



ภาพที่ ก-7 การเข้ารหัสโดยการใส่ผู้ส่งและผู้รับ

2.4 ใส่ชื่อแฟ้มข้อมูลข่าวสารที่ต้องการเข้ารหัส (Plain Text)

2.5 ใส่ชื่อแฟ้มเข้ารหัสที่ต้องการสร้าง (Cipher Text) ดังภาพที่ ก-8

Encrypt Message

---

from : Nor

password :

to : Chat

Plaintext filename : L4_5.TXT

Ciphertext filename : C4_5.TXT

Press Enter to continue.

ภาพที่ ก-8 การใส่แฟ้มข้อมูลข่าวและแฟ้มเข้ารหัส

<u>ตัวอย่าง</u> แฟ้มข้อมูลข่าวสารที่ต้องการเข้ารหัส (Plain Text) ชื่อ L4_5.TXT ดังภาพที่ ก-9

จาก ผบ.พันช.111

ถึง ผบ. พันช.ซบร.หนัก.

หมู่วันเวลา 151200 มี.ค. 41

ให้เตรียมอะไหล่สำหรับซ่อมบำรุง ชั้น 3 รสพ.21 จำนวน 2 คัน

ภาพที่ ก-9 รายละเอียดแฟ้มข้อมูลข่าวสาร L4_5.TXT

ตัวอย่าง แฟ้มเข้ารหัส ชื่อ C4_5.TXT (เข้ารหัสจากแฟ้ม L4_5.TXT) ดังภาพที่ ก-10

THE ROYAL THAI ARMY

ENCRIPTION PROGRAM

VERSION 1.0

1. MD5-INFO : 7B04A887A48C264A

2. Originator-ID: Nor

3. MIC-Info: RSA-MD5,RSA,

l0QUit2Nfb4TwFb0XBbSXqL5i4+jWxeMtaB9c6vLugTo6qLe5EsZqhrlmS8TSDcF

4CTJp6MueT1DZ+xeEPwxgzVLxRXl/alTXz8f6m2YcII=

4. Recipient-ID: Chat

5. Key-Info: RSA,

Amnz0hnUUZOit0eXeiQnXuD/TVvHzG1FkQgNX+qApULJrN3iz1xqqcTVEWeLbSrn

yugLmFWg1pdVu6X4FwCBapBjbhzkOBr63Yg=

FTA9sILsXOamtcCP9kjHrsHTYUxUoslVy+Pf0srRxHxL8zacZOQufnKleQ5euJg4

b+ItqnFJRlnFzzrMVIDnPfMCieF8Jj7l2OUvtCwmg3udjMLR4YE4oAZxwzn7CJPl

siJCngy1Y4Hf6GYSeMfOq0JVJ1bBtb0ymwI2ZouVdCi04gHzhoMIK1E4TZ89Rbub

+KPMylGpKfn04Pn7t9XlGcTHzMF+5646pPcjUYll/gKwbAp0+rykXFyn+L+wMsMI

/2CPVfpmirk=

***** END MESSAGE *****

ภาพที่ ก-10 รายละเอียดแฟ้มเข้ารหัส C4_5.TXT

เลือกการทำงานข้อ 2. การถอดรหัส (Decryption)

1. การถอดรหัสมีข้อกำหนดดังนี้

1.1 ทั้งผู้ส่งและผู้รับจะต้องถูกสร้างไว้ในระบบเรียบร้อยแล้ว โปรแกรมจะไม่ยอมทำงานถ้าหาผู้ส่งและผู้รับไม่เจอ

1.2 แฟ้มเข้ารหัสที่ต้องการถอดรหัสต้องเป็นแฟ้มที่เข้ารหัสจากระบบนี้เท่านั้น

2. มีขั้นตอนการทำงานคือ

2.1 กรอกชื่อแฟ้มเข้ารหัส โปรแกรมจะแสดงชื่อผู้ส่ง(Sender Name) และชื่อผู้รับ (Receipt name) โดยอัตโนมัติ

2.2 ใส่รหัสผ่านผู้รับ ดังภาพที่ ก-11

Decrypt Message

---

filename : C4_5.txt

SenderName : Nor

Recipient : Chat

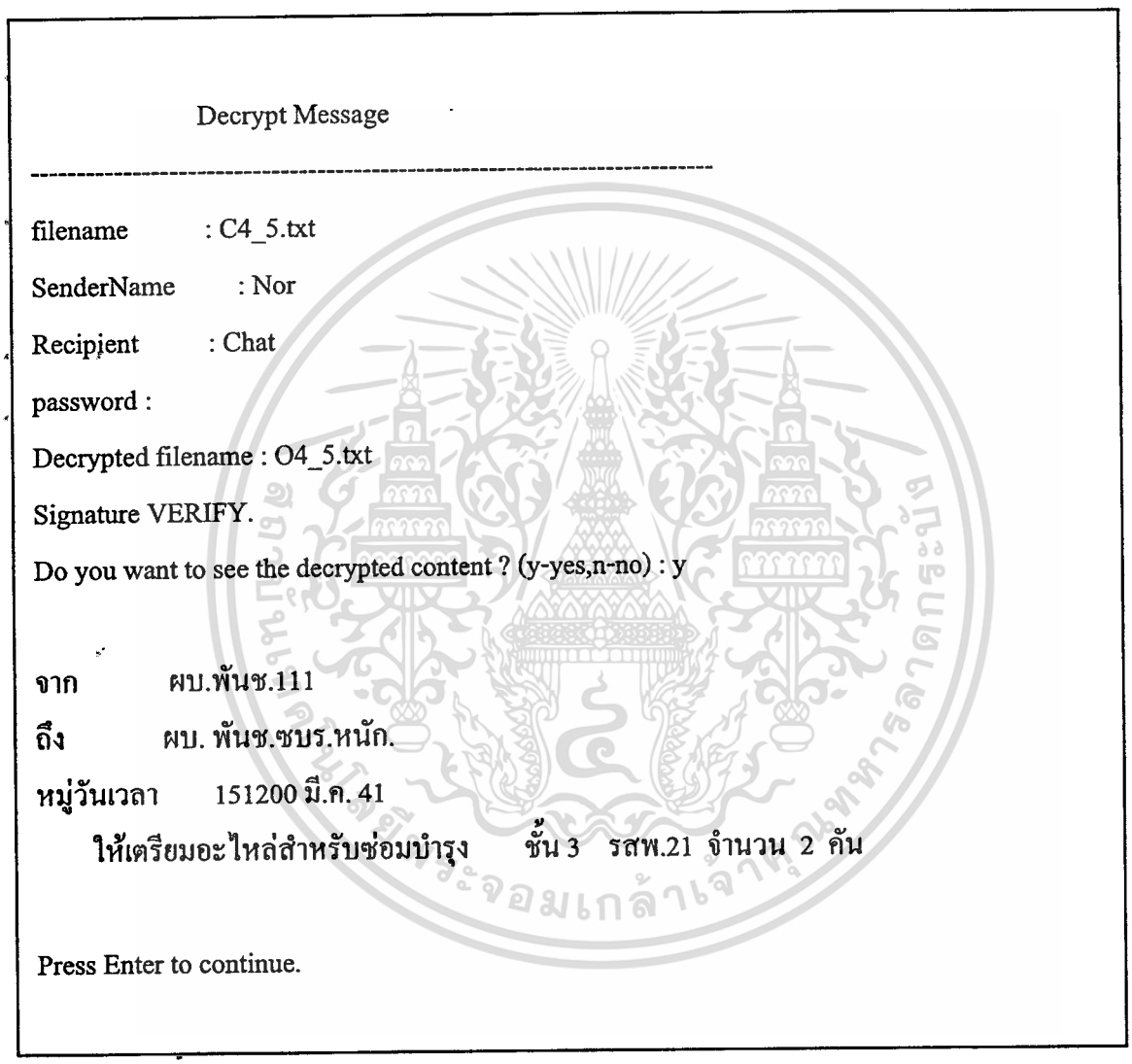
password :

ภาพที่ ก-11 การถอดรหัส

2.3 ใส่ชื่อแฟ้มเข้ารหัส หากมีการแก้ไขใดๆกับแฟ้มนี้การถอดรหัสจะถูกยกเลิกทันที

2.4 ใส่ชื่อแฟ้มข้อมูลข่าวสารที่ต้องการได้จากการถอดรหัส

2.5 โปรแกรมจะถามว่าต้องการแสดงผลการถอดรหัสทางจอภาพด้วยหรือไม่ ถ้าตอบ "Y" ผลจากการถอดรหัสจะแสดงออกมา และบันทึกผลนั้นในชื่อแฟ้มที่ใส่เข้าไป ดังภาพที่ ก-12



ภาพที่ ก-12 ขั้นตอนการถอดรหัสและผลลัพธ์

เลือกการทำงานข้อ 5. การเข้ารหัสด้วยรหัสผ่าน(Encryption with password)

การเข้ารหัสด้วยรหัสผ่านเป็นการเข้ารหัสโดยตรงกับแฟ้มข้อมูลต่างๆ ทั้งแฟ้มข้อมูลข่าวสารธรรมดาหรือแฟ้มที่ผ่านการเข้ารหัสแล้ว โดยการกำหนดรหัสผ่านโดยตรงเข้ากับแฟ้มเพื่อเป็นการเก็บแฟ้มนั้นๆไว้ใช้เฉพาะผู้ที่ทราบรหัสผ่านเท่านั้น แต่มีข้อจำกัดคือรหัสผ่านที่ใส่โดยตรงกับแฟ้มแต่ละแฟ้มจะต้องจำได้ไม่เช่นนั้นแฟ้มที่ผ่านการเข้ารหัสนี้จะไม่สามารถใช้ได้เลย การทำงานดังภาพที่ ก-13

```
Do encrypt file with password.
Input  filename : C4_5.TXT
Output filename : EC4_5.TXT
password :
```

ภาพที่ ก-13 ขั้นตอนการเข้ารหัสด้วยรหัสผ่าน

และตัวอย่าง การเข้ารหัสโดยใส่รหัสผ่าน กระทำกับแฟ้มที่ถูกเข้ารหัสมาแล้วได้ผลลัพธ์ตามภาพที่ ก-14

เลือกการทำงานข้อ 6. การถอดรหัสด้วยรหัสผ่าน(Decryption with password)

การถอดรหัสด้วยรหัสผ่านเป็นการถอดรหัสโดยตรงกับแฟ้มข้อมูลต่างๆ ทั้งแฟ้มข้อมูลข่าวสารธรรมดาหรือแฟ้มที่ผ่านการเข้ารหัสแล้ว โดยการกำหนดรหัสผ่านนั้นต้องตรงกับรหัสผ่านที่ใส่ตอนเข้ารหัสแฟ้ม การทำงานดังภาพที่ ก-15 และตัวอย่าง การถอดรหัสโดยใส่รหัสผ่าน ได้ผลลัพธ์ตาม ภาพที่ ก-16

```
SK47jl3MbnHenZ5QCzCEIreRQKs/Snh878tyTJxdcW3RAKN0jdUD0JrMzAGQpOFn
A8b7nZKvDEAK28UUmZnjnRpq+KgORy93Vmr53FZzcPrNS/MuslQbhsbP9DuCaLCt
U2H8KkD9HH8xpuOjyM0FG26Kyu3fdt0nezleyvuGnZeiAWN3qIhK05JcFNFB92Vf
bKOH5i70Wp/hOzMMKxm8Oy4DabOvVNV7i6llu5NxC1ViK+kv+B3hXvNICIi3/RmE
8v9cKXrb9ElCW/Ar16JpEMxNCPlrf7yUFpb3+F05c2fkHpc0lm2FBiYjFHXYhZ8N
OLtn/zB+qhwW6qJ8aUX3cqzP09SmmtqSSjuNWADF+KsB/Qf12Sda2mLxuqcypy/D
9sUaZ2aUYH2p9ZAi5EtKCXM2+bWQIjtUfrdj8+K5hyrkZ5jXGJbKwjit5BpwaiWe
G5TlpzxTs7uUyjRWeal9B4/9g+8XPou7T0uMG6K5YftV3LVxCBq49MZPJ0d0V1s
Cy+l4EeapAX/bZolplqiDVGw6ysd7Qkc1f1tRrb+6TCWgbFOnPh7QwPpMIBMyTF+
AFF1+5bCHpWHbClW86SdzIqkHTyq8lu+z3TW8vgFj60tdotFYnPnvQLy5X1/Qf7I
1K9RqD7B8kkwz7sIBiBs8XfWfasEOrPggJoEgKtJKGB8zEHew0klsdQt8OuzBI3f
LxG1yn1x81TbTRLcquCKCt/f//IFspXXM77p2RUXowsiMy3ZfbhuGgcUtVCD1ZY7
```

ภาพที่ ก-14 ผลลัพธ์การเข้ารหัสด้วยรหัสผ่านกระทำกับแฟ้มที่เข้ารหัสแล้ว(EC4_5.TXT)

```
Do decrypt file with password.
Input  filename : EC4_5.TXT
Output filename : DC4_5.TXT
password :
```

ภาพที่ ก-15 ขั้นตอนการถอดรหัสด้วยรหัสผ่าน

```
THE ROYAL THAI ARMY
ENCRIPTION PROGRAM
VERSION 1.0
1. MD5-INFO : 7B04A887A48C264A
2. Originator-ID: Nor
3. MIC-Info: RSA-MD5,RSA,
l0QUit2Nfb4TwFb0XBbSXqL5i4+jWxeMtaB9c6vLugTo6qLe5EsZqhrlmS8TSDcF
4CTJp6MueT1DZ+xeEPwxgzVLxRXl/alTXz8f6m2YcII=
4. Recipient-ID: Chat
5. Key-Info: RSA,
Amnz0hnUUZOit0eXeiQnXuD/TVvHzG1FkQgNX+qApULJrN3iz1xqqcTVEWeLbSm
yugLmFWg1pdVu6X4FwCBapBjbhzkOBr63Yg=

FTA9sILsXOamtcCP9kjHrsHTYUxUoslVy+Pf0srRxHxL8zacZOQufnKleQ5euJg4
b+ItqnFJRlnFzzrMVIDnPfMCieF8Jj7l2OUvtCwmg3udjMLR4YE4oAZxwzn7CJP1
siJCngy1Y4Hf6GYSeMfOq0JVJ1bBtb0ymwI2ZouVdCi04gHzhoMIK1E4TZ89Rbub
+KPMylGpKfn04Pn7t9XlGcTHzMF+5646pPcjUYlI/gKwbAp0+rykXFyn+L+wMsMI
/2CPVfpmirk=
***** END MESSAGE *****
```

ภาพที่ ก-16 ผลลัพธ์การถอดรหัสด้วยรหัสผ่าน (DC4_5.TXT)

ผนวก ข.

กระบวนการสังเคราะห์ข่าว

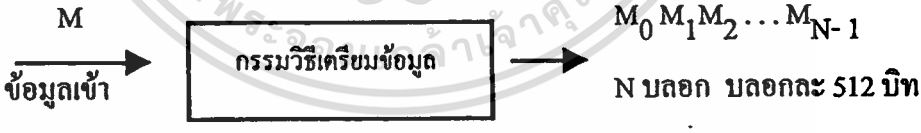
Message Digest 5 - MD5

กระบวนการสังเคราะห์ข่าว (Message Digest5 - MD5)

เป็นการเข้ารหัสอย่างง่ายแบบหนึ่ง แต่เป็นการเข้ารหัสทางเดียว (One-way Hash Function) มีหลักการทำงานคือ ข้อมูลเข้าไม่ว่าจะมีความยาวเท่าไรก็ตาม เมื่อผ่านกระบวนการสังเคราะห์ข่าวแล้ว จะได้ข้อมูลออกมามีความยาวเท่ากันเสมอ เช่น ข้อมูลเข้า 80 บิท ผ่านกระบวนการสังเคราะห์ข่าวแล้ว จะได้ข้อมูลออกมา 128 บิท ถ้า ข้อมูลเข้า 175 บิท ผ่านกระบวนการสังเคราะห์ข่าวแล้ว จะได้ข้อมูลออกมา 128 บิท เช่นกัน ข้อมูลออกแต่ละอันจะไม่เหมือนกัน

<u>หลักการทั่วไป</u>

- ข้อมูลเข้า (Input) มีความยาวกี่บิทก็ได้ ข้อมูลออก (Output) มีความยาว 128 บิทเสมอ
- เมื่อนำข้อมูลเข้าไปผ่านกรรมวิธีเตรียมข้อมูล (Initial Process) ได้ผลเป็นข้อมูล N บลอก ซึ่งแต่ละบลอกมีความยาว 512 บิท

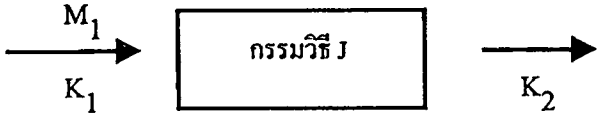


- กำหนดค่าเริ่มต้นของตัวเลข 128 บิท K_0 เป็น

  K_0 = 01 23 45 67 89 AB CD EF FE DC BA 98 76 54 32 10

- นำ M_0 (บลอกที่ 1) กับ K_0 ไปผ่านกรรมวิธี J ผลลัพธ์ที่ได้จะเป็นตัวเลข 128 บิท เรียกว่า K_1

- นำ M_1 (บลอกที่ 2) กับ K_1 ไปผ่านกรรมวิธี J ผลลัพธ์ที่ได้จะเป็นตัวเลข 128 บิท เรียกว่า K_2



- กระทำเช่นนี้ต่อๆ ไปจนถึงบลอกสุดท้าย คือ M_{N-1} กับ K_{N-1} ผลลัพธ์ที่ได้คือ P ซึ่งเป็น Hash Function ของข้อมูลที่ป้อนเข้า

<u>กรรมวิธีเตรียมข้อมูล</u>

- แบ่งข้อมูลที่ป้อนเข้าออกเป็นบลอก บลอกละ 512 บิท เศษที่เหลือคือบลอกสุดท้าย จะมีความยาวระหว่าง 0 ถึง 511 บิท
- เพิ่มเลข 1 เข้าไป 1 ตัว ดังนั้น บลอกสุดท้ายจะมีความยาว ระหว่าง1 ถึง 512 บิท
- หากบลอกสุดท้ายยาวมากกว่า 448 บิท จะต้องเพิ่มเลขศูนย์เข้าไปจนเต็มบลอก (512 บิท) แล้วจึงเพิ่มข้อมูลอีก 1 บลอก ดังนั้น เมื่อเสร็จขั้นตอนนี้บลอกสุดท้ายก็จะมีความยาวระหว่าง 0 ถึง 448 บิท
- ถ้าบลอกสุดท้ายยังมีความยาวน้อยกว่า 448 บิท ก็ให้เพิ่มเลขศูนย์เข้าไปจนครบ 448 บิท
- ใส่ตัวเลข 64 บิทสุดท้าย ซึ่งเป็นความยาวของข้อมูลที่ป้อนเข้า (MODULO 2^{64}) ก่อนที่จะมีการต่อเติม เมื่อผ่านขั้นตอนนี้บลอกสุดท้ายจะมีความยาว 512 บิทพอดี

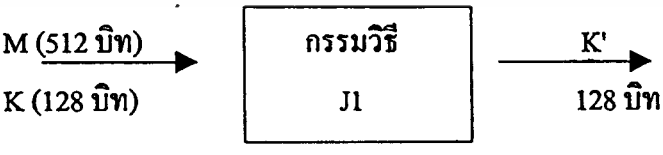
<u>กรรมวิธี J</u>

- ข้อมูลที่ป้อนเข้ามี 2 จำนวน คือ M ที่มีความยาว 512 บิท กับ K ที่มีความยาว 128 บิท ข้อมูลที่ได้ออกมา คือ J (M,K) ที่มีความยาว 128 บิท

- กรรมวิธี J แบ่งเป็น 4 กรรมวิธีย่อยที่กระทำต่อเนื่องกัน คือ กรรมวิธี J1 J2 J3 และ J4 หรือเรียกว่ากรรมวิธี J มี 4 ยก และแต่ละยกจะมีข้อมูลที่ป้อนเข้าคือ M และ K ส่วนข้อมูลที่ได้ออกมา คือ K' ที่มีความยาว 128 บิท และจะใช้เป็นค่า K สำหรับยกต่อไป

<u>กรรมวิธี J1</u>

- ข้อมูลที่ป้อนเข้ามี 2 จำนวน คือ Mที่มีความยาว 512 บิท กับ K ที่มีความยาว 128 บิท ส่วนข้อมูลที่ได้ออกมา คือ K' มีความยาว 128 บิท



- แบ่ง M (512 บิท) ออกเป็น 16 ส่วน ส่วนละ 32 บิท เท่าๆ กัน เรียกว่า $m_0\ m_1\ m_2 \ldots m_{15}$ และ แบ่ง K (128 บิท) ออกเป็น 4 ส่วน ส่วนละ 32 บิท เท่าๆ กัน เรียก ว่า a b c d

- ผ่านกระบวนการ16 ครั้ง โดยแต่ละครั้งใช้สูตร ดังนี้

$$x1 = x2 + ((F(x2, x3, x4) + x5 + x6) <<< x7)$$

ทั้งนี้ โดยที่ x1, x2, ... x7 แต่ละจำนวนเป็นตัวเลข 32 บิท และ x1 จะแทนค่า a b c หรือ d

- และ สำหรับครั้งต่อๆ ไป <<< x7 หมายถึงการหมุนบิท x7 ตำแหน่ง ค่าของ x1, x2, ... x7 ปรากฏใน ตาราง ที่ ข-1

No	xi	x2	x3	x4	x5	x6	x7
1	a	b	c	d	m_0	d76aa478	7
2	d	a	b	c	m_1	e8c7b756	12
3	c	d	a	b	m_2	242070db	17
4	b	c	d	a	m_3	c1bdceee	22
5	a	b	c	d	m_4	f57c0faf	7
6	d	a	b	c	m_5	4787c62a	12
7	c	d	a	b	m_6	a8304613	17
8	b	c	d	a	m_7	fd469501	22
9	a	b	c	d	m_8	698098d8	7
10	d	a	b	c	m_9	8b44f7af	12
11	c	d	a	b	m_{10}	ffff5bb1	17
12	b	c	d	a	m_{11}	895cd7be	22
13	a	b	c	d	m_{12}	6b901122	7
14	d	a	b	c	m_{13}	fd987193	12
15	c	d	a	b	m_{14}	a679438e	17
16	b	c	d	a	m_{15}	49b40821	22

ตาราง ที่ ข-1 กรรมวิธี J1

- ฟังก์ชั่น F (X, Y, Z) เป็น Non Linear Function ซึ่งเป็นปฏิบัติการทางลอจิกทีละบิท (Bitwise-Logic Operation) กับตัวแปร X Y และ Z ซึ่งเป็นตัวเลข 32 บิทโดยใช้สูตร ดังนี้

  F(X,Y,Z) = XY OR (NOT X)Z

  ซึ่งก็คือการปฏิบัติการ If X then Y else Z
- เมื่อผ่านกระบวนการครบ 16 ครั้งแล้ว นำค่า a b c b มารวมกันเป็นตัวเลข 128 บิท ได้ เป็นค่าของข้อมูลออก K'

<u>กรรมวิธี J2</u>

- โดยทั่วไปจะเหมือนกับกรรมวิธี J1 แตกต่างกันที่ตารางค่าของ x1, x2, ... x7 และ Non Linear Function เท่านั้น
- กระบวนการ 16 ครั้ง ใช้สูตร ดังนี้

  x1 = x2 + ((G(x2, x3, x4) + x5 + x6) <<< x7)

  ค่าของ x1 x2 ... x7 ปรากฏในตารางที่ ข-2
- ฟังก์ชั่น G (X, Y, Z) เป็นการปฏิบัติการ โดยใช้สูตร

  G(X,Y,Z) = XZ OR Y(NOTZ)

<u>กรรมวิธี J3</u>

- โดยทั่วไปก็จะเหมือนกับกรรมวิธี J1 แตกต่างกันที่ ตารางค่าของ x1, x2, ... x7 และ Non Linear Function เช่นกัน
- กระบวนการ 16 ครั้ง ใช้สูตร ดังนี้

  x1 = x2 + ((H(x2, x3, x4) + x5 + x6) <<< x7)

  ค่าของ x1, x2, ... x7 ปรากฏในตารางที่ ข-3
- ฟังก์ชั่น H(X, Y, Z) เป็นการปฏิบัติการ Non Linear Function โดยใช้สูตร ดังนี้

  H(X,Y,Z) = X XOR Y XOR Z

  ซึ่งคือการปฏิบัติการ Bitwise Parity

No	x1	x2	x3	x4	x5	x6	x7
1	a	b	c	d	m_1	f61e2562	5
2	d	a	b	c	m_6	c040b340	9
3	c	d	a	b	m_{11}	265e5a51	14
4	b	c	d	a	m_0	e9b6c7aa	20
5	a	b	c	d	m_5	d62f105d	5
6	d	a	b	c	m_{10}	02441453	9
7	c	d	a	b	m_{15}	d8a1e681	14
8	b	c	d	a	m_4	e7d3fbc8	20
9	a	b	c	d	m_9	21e1cde6	5
10	d	a	b	c	m_{14}	c33707d6	9
11	c	d	a	b	m_3	f4d50d87	14
12	b	c	d	a	m_8	455a14ed	20
13	a	b	c	d	m_{13}	a9e3e905	5
14	d	a	b	c	m_2	Fcefa3f8	9
15	c	d	a	b	m_7	676f02d9	14
16	b	c	d	a	m_{12}	8d2a4c8a	20

ตารางที่ ข-2 กรรมวิธี J2

No	x1	x2	x3	x4	x5	x6	x7
1	a	b	c	d	m_5	fffa3942	4
2	d	a	b	c	m_8	8771f681	11
3	c	d	a	b	m_{11}	6d9d6122	16
4	b	c	d	a	m_{14}	fde5380c	23
5	a	b	c	d	m_1	a4beea44	4
6	d	a	b	c	m_4	4bdecfa9	11
7	c	d	a	b	m_7	f6bb4b60	16
8	b	c	d	a	m_{10}	bebfbc70	23
9	a	b	c	d	m_{13}	289b7ec6	4
10	d	a	b	c	m_0	eaa127fa	11
11	c	d	a	b	m_3	d4ef3085	16
12	b	c	d	a	m_6	04881d05	23
13	a	b	c	d	m_9	d9d4d039	4
14	d	a	b	c	m_{12}	e6db99e5	11
15	c	d	a	b	m_5	1fa27cf8	16
16	b	c	d	a	m_2	c4ac5665	23

ตารางที่ ข-3 กรรมวิธี J3

กรรมวิธี J4

- โดยทั่วไปเหมือนกับกรรมวิธี J1 เช่นกัน แตกต่างกันที่ ตารางค่าของ x1, x2, ... x7 และ Non Linear Function
- กระบวนการ 16 ครั้ง ใช้สูตร ดังนี้

$$x1 = x2 + ((I(x2, x3, x4) + x5 + x6) <<< x7)$$

ค่าของ x1, x2, ... x7 ปรากฏตารางที่ ข-4

- ฟังก์ชั่น G(X, Y, Z) เป็นการปฏิบัติการ Non Linear Function โดยใช้สูตร ดังนี้

$$I(X,Y,Z) = Y \text{ XOR } (X \text{ OR } (\text{NOT } Z))$$

หมายเหตุ

- ตัวเลขในช่อง x6 เป็น Hexadecimal
- ตัวเลขในช่อง x6 คำนวณมาจาก Integer Part ของ

4294967296 abs(sine(i)) where i = 1, 2, ... i มีหน่วยเป็นเรเดียน

-4294967296 คือ 2^{32}

No	x1	x2	x3	x4	x5	x6	x7
1	a	b	c	d	m_0	f4292244	6
2	d	a	b	c	m_7	411aff97	10
3	c	d	a	b	m_{14}	ab9423a7	15
4	b	c	d	a	m_5	fc93a039	21
5	a	b	c	d	m_{12}	655b59c3	6
6	d	a	b	c	m_3	8f0ccc92	10
7	c	d	a	b	m_{10}	ffeff47d	15
8	b	c	d	a	m_1	85845dd1	21
9	a	b	c	d	m_8	6fa87e4f	6
10	d	a	b	c	m_{15}	fe2ce6e0	10
11	c	d	a	b	m_6	a3014314	15
12	b	c	d	a	m_{13}	4e0811a1	21
13	a	b	c	d	m_4	f7537e82	6
14	d	a	b	c	m_{11}	bd3af235	10
15	c	d	a	b	m_2	2ad7d2bb	15
16	b	c	d	a	m_9	eb86d391	21

ตารางที่ ข-4 กรรมวิธี J4

ประวัติผู้เขียน

พันตรีนรเศรษฐ์ พงษ์เจริญ เกิดเมื่อวันที่ 30 สิงหาคม 2509 ที่กรุงเทพมหานคร สำเร็จการศึกษาวิทยาศาสตร์บัณฑิต (สาขาวิศวกรรมไฟฟ้าสื่อสาร) จากโรงเรียนนายร้อยพระจุลจอมเกล้า รุ่นที่ 36 (เตรียมทหารรุ่นที่ 25) ปีการศึกษา 2531 และเข้ารับราชการในกองทัพบก ในตำแหน่งนายทหารซ่อมบำรุงสายและวิทยุถ่ายทอด ณ กองพันทหารสื่อสารซ่อมบำรุงเขตหลัง ค่ายกำแพงเพชรอัครโยธิน อำเภอกระทุ่มแบน จังหวัดสมุทรสาคร ต่อมาเมื่อปี พ.ศ. 2534 ได้ย้ายมารับราชการที่กรมการทหารสื่อสาร สะพานแดง กรุงเทพมหานคร ปัจจุบันดำรงตำแหน่งนายทหารประจำแผนกวิจัยและพัฒนา กองวิทยาการ กรมการทหารสื่อสาร