ชื่อเรื่องการค้นคว้าแบบอิสระ การใช้แอดวานซ์เอนคริปชันสแตนดาร์ดสำหรับข้อความที่กำหนด

ผู้เขียน นายกัสสปะ สุขเอี่ยม

ปริญญา วิทยาศาสตรมหาบัณฑิต (วิทยาการคอมพิวเตอร์)

อาจารย์ที่ปรึกษาการค้นคว้าแบบอิสระ

ผู้ช่วยศาสตราจารย์ ดร. รัฐสิทธิ์ สุขะหุต

บทคัดย่อ

การค้นคว้าแบบอิสระเชิงวิทยานิพนธ์เรื่องการใช้แอดวานซ์เอนคริปชันสแตนดาร์ดสำหรับข้อความที่กำหนดมีวัตถุประสงค์เพื่อสร้างเครื่องมือสำหรับช่วยเข้ารหัสสำหรับข้อความที่กำหนด โดยใช้เทคนิค เออีเอส โดยระบบจะมีการแบ่งการทำงานอยู่ 2 ส่วนหลักด้วยกัน คือ ส่วนของการเข้ารหัสข้อความ และส่วนของการถอดรหัสข้อความ โดยการทำงานของการเข้าและถอดรหัสนั้น จะมีการกำหนดการใช้คีย์ร่วมกันของข้อความที่ต้องการเข้าและถอด กล่าวคือ หากผู้ใช้งานคนอื่นที่ไม่ทราบคีย์นั้นแล้ว จะไม่สามารถเข้าถึงข้อความนั้นๆได้

ระบบจะถูกออกแบบในลักษณะของ ยู เอ็ม แอล ซึ่งใช้ โปรแกรม เรชันนอล โรส 2000 และทำการพัฒนาโปรแกรมภายใต้ระบบปฏิบัติการวินโดวส์ 2000 ด้วยเครื่องมือเป็น โปรแกรม ซี พลัสพลัส บิวเดอร์ เดเวอร์ลอบเมนต์ เอนไวรอนเมนต์ เวอร์ชัน 6.0 โปรแกรมดังกล่าวให้ผลลัพธ์ที่มีประสิทธิภาพ และคุณภาพในระดับหนึ่ง คือ ประมาณ 89.8 % แต่ยังคงมีข้อจำกัดเรื่องของวิธีการและข้อมูลที่ต้องการนำมาเข้าและถอดรหัส ซึ่งหากมีการพัฒนาต่อไปโดยมีการเพิ่มขั้นตอนและวิธีการในการเข้ารหัส จะทำให้โปรแกรมมีประสิทธิภาพและคุณภาพมากยิ่งขึ้นด้วย

Independent Study Title Implementation of Advanced Encryption Standard for Specified Texts

Author Mr. Kasapa Sukeiam

Degree Master of Science (Computer Science)

Independent Study Advisor

Assistant Professor.Dr.Rattasit Sukhahuta

ABSTRACT

The Independent Study "Implementation of Advanced Encryption Standard for Specified Texts" conducted to support users for encrypt and decrypt Specified texts. The process was divided into two parts. First was encryption and the Second was decryption texts. In the process has to have key which make texts safe, prevent cipher text from the other persons who want to read its. Key will help to encrypt and decrypt texts. The algorithms for encryption is AES (Advanced Encryption Standard).

The system was designed using UML (Unified Modeling Language) developed with Rational Rose 2000 software and the system run on Microsoft Windows 2000 operation system with C++ Builder 6.0 developer tool .

The results of the study showed the efficiency and accuracy about 89.8% for encryption and decryption. The system still had some limits .Further development methods for encrypt picture data still required in order to improve an efficiency of future .