สุมิตรา เด่นกองพล. 2553. **การเข้าและถอดรหัสแบบ DES และ AES อัลกอริทึม สำหรับภาษาไทยแบบ Unicode ขนาด 16 บิต** . การศึกษาอิสระปริญญาวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ คณะวิทยาศาสตร์ มหาวิทยาลัยขอนแก่น.

อาจารย์ที่ปรึกษาการศึกษาอิสระ: ผู้ช่วยศาสตราจารย์ ดร. พุธษดี ศิริแสงตระกูล

บทคัดย่อ

ปัจจุบันการเข้ารหัสข้อมูลถูกนำมาใช้ในงานด้านความปลอดภัยเพิ่มมากขึ้น โดยที่ดีอีเอส 56 บิต และเออีเอส 128 บิต เป็นอัลกอริทึมแบบสมมาตร โดยที่เออีเอสเป็นอัลกอริทึมที่ได้รับความนิยมและยอมรับอย่างแพร่หลายในการนำมาใช้งาน ซึ่งแต่ละอัลกอริทึมเหล่านี้ในบางกรณีไม่สามารถรองรับในการใช้งานกับตัวอักษรไทยมากนัก ดังนั้นงานวิจัยชิ้นนี้จึงได้ทำการพัฒนาโปรแกรมประยุกต์เพื่อจำลองการทำงานของอัลกอริทึมดังกล่าว และเพิ่มเทคนิคการจับคู่ตารางเทียบการแสดงผลอักษรภาษาไทย เพื่อให้มีความสามารถเข้าและถอดรหัสสำหรับภาษาไทยได้ โดยการพัฒนาโปรแกรมดังกล่าวนั้นได้ทำการอ้างอิงมาตรฐานแบบยูนิโค้ด ขนาด 16 บิต ซึ่งมาตรฐานนี้ได้จัดให้มีค่าเลขฐานสิบหกสำหรับแสดงอักขระไทย อยู่ในช่วง 0E00 ถึง 0E7F ในส่วนของการทดสอบการทำงานของโปรแกรมประยุกต์ที่สร้างนั้นจะทำการทดสอบสองประเด็นหลัก คือความถูกต้องและความเร็วของการเข้าและถอดรหัส ซึ่งในแง่ของความถูกต้องนั้นโปรแกรมประยุกต์ที่สร้างมีความสามารถในการถอดรหัสเป็นภาษาไทยได้ถูกต้องแม่นยำ และในส่วนของความเร็วนั้นได้มีการนำเข้าข้อความภาษาไทยที่ขนาดความยาว 4 กิโลไบท์ 10 กิโลไบท์ และ 14 กิโลไบท์ มาทดสอบการทำงานของโปรแกรมประยุกต์ที่สร้าง เมื่อนำผลการทดสอบที่ได้มาวิเคราะห์ ผลปรากฏว่า เวลาที่ใช้ในการทำงานของดีอีเอสและเออีเอสอัลกอริทึมมีลักษณะแปรผันตามขนาดของข้อความที่นำเข้ามา ซึ่งมีความสัมพันธ์แบบเชิงเส้น หมายความว่าเวลาที่ใช้ในการทำงานเพิ่มมากขึ้นตามขนาดข้อความที่นำเข้านั่นเอง

Sumittra Denkongpon. 2010. **Data Encryption and Decryption Data Using DES and AES algorithm for Thai Unicode 16 bits**. Master of Science Independent Study in Information Technology, Faculty of Science, Khon Kaen University.

Independent Study Advisor : Asst.Prof. Dr.Pusadee Seresangtakul

ABSTRACT

Data encryption has become one of the most important factors in computer security. The DES 56-bit symmetric algorithm was developed in the 1970s and was replaced with the AES 128-bit symmetric algorithm in 2001. The DES 56-bit was very popular and widely accepted for many years but with the increase in computer attacks had to be upgraded to the AES 128bit algorithm. Neither these algorithms however provide support, at the software level, for Thai characters. This research has been developing an application to simulate the operation of both of these algorithms. The table matching technique to display Thai characters has been added to decrypt and encrypt Thai characters. The 16-bit Unicode standard was used as a reference in the development of the program because it was able to provide the necessary hexadecimal code to display the Thai characters in the range of 0E00 to 0E7F. The two main issues in testing the operation of the application program were accuracy and speed of encryption and decryption. In terms of accuracy, the application program has the ability to decrypt the Thai language precisely. In terms of speed, Thai text with lengths of 4 kilobytes, 10 kilobytes and 14 kilobytes were introduced to test the operation of application. The test results showed that the time spent in the working on the DES and AES algorithms varied according to the size of the text line, i.e. there was a linear relationship. This means that the time spent working on either encryption or decryption increased according to the length of the text.