การเข้าและถอดรหัสด้วยอัลกอริทึม DES และ AES สำหรับภาษาไทยแบบ Unicode 16 บิต

Data Encryption and Decryption Using DES and AES Algorithm for Thai Unicode 16 bits

สุมิตรา เด่นกองพล (Sumitrra Denkongpon)* ธนานนท์ กลิ่นแก้ว (Tananon Klinkaew)**
ดร.พุธษดี ศิริแสงตระกูล (Dr.Pusadee Seresangtakul)***

บทคัดย่อ

ปัจจุบันการเข้ารหัสข้อมูลถูกนำมาใช้ในงานด้านความปลอดภัยเพิ่มมากขึ้น โดยที่ดีอีเอส 56 บิต และเออีเอส 128 บิต เป็นอัลกอริทึมแบบสมมาตร โดยที่เออีเอสเป็นอัลกอริทึมที่ได้รับความนิยมและยอมรับอย่างแพร่หลายในการนำมาใช้งาน ซึ่งแต่ละอัลกอริทึมเหล่านี้แต่จะมีปัญหาในการแสดงผลภาษาไทย ดังนั้นงานวิจัยชิ้นนี้จึงนำเสนอวิธีการเพื่อให้สามารถเข้ารหัสภาษาไทยตามมาตรฐาน unicode ขนาด 16 บิตด้วยอัลกอริธึม AES และ DES โดยเพิ่มเทคนิคการจับคู่ตารางเทียบเพื่อการแสดงผลอักษรไทยอย่างถูกต้อง ซึ่งมาตรฐาน Unicode นี้กำหนดให้มีค่าเลขฐานสิบหกสำหรับแสดงอักขระไทย อยู่ในช่วง 0E00 ถึง 0E7F เพื่อทดสอบประสิทธิภาพการทำงานของวิธีการที่นำเสนอ ผู้วิจัยได้ทำการพัฒนาโปรแกรมประยุกต์เพื่อจำลองการทำงานของอัลกอริทึมดังกล่าว โดยการนำเข้าข้อความภาษาไทยที่ขนาดความยาว 4 กิโลไบท์ 10 กิโลไบท์ และ 14 กิโลไบท์ เพื่อทำการทดสอบประสิทธิภาพสองประเด็นหลัก คือความถูกต้องและความเร็วของการเข้าและการถอดรหัส ซึ่งในแง่ของความถูกต้องนั้นวิธีการที่นำเสนอมีความสามารถในการถอดรหัสและแสดงผลภาษาไทยได้ถูกต้องแม่นยำ เมื่อนำผลการทดสอบความเร็วในการเข้าและถอดรหัสที่ได้มาวิเคราะห์ ผลปรากฏว่า เวลาที่ใช้ในการทำงานของดีอีเอสเร็วกว่าเออีเอสอัลกอริทึม และทั้งเออีเอสและดีอีเอสมีลักษณะแปรผันตามขนาดของข้อความที่นำเข้ามา ซึ่งมีความสัมพันธ์แบบเชิงเส้น หมายความว่าเวลาที่ใช้ในการทำงานเพิ่มมากขึ้นตามขนาดข้อความที่นำเข้านั่นเอง

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. This research presents the ASE and DES algorithm for 16-bits Unicode Thai characters in the range of 0E00 to 0E7F. In the study the table matching technique has been added to decrypt and encrypt the Thai characters. In order to evaluate the efficiency of the proposed method an application program was developed to simulate the operation of the proposed method.

* *นักศึกษา หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ คณะวิทยาศาสตร์ มหาวิทยาลัยขอนแก่น*
** *นักศึกษา หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ คณะวิทยาศาสตร์ มหาวิทยาลัยขอนแก่น*
*** *ผู้ช่วยศาสตราจารย์ ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยขอนแก่น*

The main issues in testing were accuracy and speed of encryption and decryption. In terms of accuracy, the proposed method has the ability to decrypt the Thai language precisely. In terms of speed, Thai text collected from tales, general and academic papers with lengths of 4 kilobytes, 10 kilobytes and 14 kilobytes was introduced to test the accuracy of the algorithm. The test results showed that the time spent 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.

คำสำคัญ : การเข้ารหัส การเข้ารหัสภาษาไทย ดีอีเอส เออีเอส ยูนิโคต
Key Words : Encryption, Thai encryption, DES, AES, Unicode

บทนำ

ปัจจุบันการแลกเปลี่ยนข้อมูลข่าวสารได้มีการประยุกต์ใช้งานกว้างขวางมากขึ้นไม่ว่าจะเป็นการสื่อสารบนระหว่างเครื่องคอมพิวเตอร์ หรือ โทรศัพท์เคลื่อนที่โดยมีการคำนึงถึงความปลอดภัยในระหว่างการใช้งานแลกเปลี่ยนข้อมูล วิธีการป้องกันไม่ให้ข้อความที่ต้องการสื่อสารนั้นมีการเปลี่ยนแปลงแก้ไขหรือเปิดเผยข้อมูลก่อนถึงมือผู้รับจึงได้มีการเพิ่มวิธีการเข้ารหัสข้อมูล (Encryption) (Trappe and Washington, 2006) จึงเป็นทางเลือกหนึ่งของการเพิ่มความปลอดภัยข้อมูลยิ่งขึ้น รูปแบบการเข้ารหัสข้อมูลแบ่งเป็น 2 กลุ่มหลัก คือ การเข้ารหัสแบบสมมาตร (Symmetric Encryption หรือ Secret Key) และการเข้ารหัสแบบอสมมาตร (Asymmetric Encryption หรือ Public-Key Encryption)โดยนำข้อความ (Plain Text) ที่ต้องการส่งมาทำการเข้ารหัสด้วยลูกกุญแจ (Encryption) จะได้ข้อความที่ถูกเข้ารหัส (Cipher Text) หากมีการเข้ารหัสโดยใช้กุญแจแบบสมมาตรเป็นการเข้ารหัสและถอดรหัสโดยการใช้กุญแจดอกเดียวกัน (Secret-Key) โดยอัลกอริทึมในการเข้ารหัสแบบสมมาตร ไม่ว่าจะเป็น DES ขนาด 56 บิต และ AES ขนาด 128 บิต

สำหรับประเทศไทยได้มีการใช้มาตรฐานรหัสภาษาไทยซึ่งมีอยู่หลากหลายไม่ว่าจะเป็น window-874 ซึ่งเป็นมาตรฐานการเข้ารหัสบนระบบปฏิบัติการของวินโดวส์ ส่วน tis-620 หรือ มอก.620 (ณัฐวุฒิ และคณะ, 2548) เป็นมาตรฐานของรหัสตัวอักษรซึ่งกำหนดโดยสำนักงานมาตรฐานอุตสาหกรรมหรือ สมอ.(TISI: Thai Industrial Standard Institute) และอีกมาตรฐานคือ Unicode เป็นมาตรฐานสากลใหม่ที่นำมาใช้ในการกำหนดหมายเลขสำหรับอักขระ ซึ่งมีความสามารถที่จะรองรับการเก็บอักษรทุกภาษาทั่วโลกได้ หาก Unicodeที่ใช้ มีการจัดเก็บแบบ 16 บิต นั้นจะเป็นการกำหนดตัวอักขระที่ใช้บ่อย ๆ เพื่อช่วยในการประหยัดเนื้อที่ในการจัดเก็บ โดยมีค่าอ้างอิงสำหรับภาษาไทย อยู่ในช่วง 0E01-0E5A

ในการเข้ารหัสแบบสมมาตรนั้นสามารถทำงานได้ทั้งบนฮาร์ดแวร์และซอฟต์แวร์ เพราะความสามารถในการประมวลผลอันรวดเร็วและเปิดเผยอัลกอริทึมจึงเป็นที่นิยมอย่างแพร่หลาย แต่อัลกอริทึมเหล่านี้นั้นใช้ตัวอักษรภาษาอังกฤษเป็นมาตรฐานในการเข้ารหัส หากต้องการนำอัลกอริทึมเหล่านี้มาใช้เพื่อสนับสนุนสำหรับการทำงานของซอฟแวร์ในการเข้าและถอดรหัสตัวอักษรภาษาไทยนั้น จำเป็นอย่างยิ่งที่ต้องเพิ่มขั้นตอนบางอย่างในการทำงานเขียนโปรแกรมเพื่อให้อัลกอริทึมแบบสมมาตรเหล่านั้นสามารถเข้ารหัสและถอดรหัสออกมาเป็นภาษาไทยได้

วราภรณ์ (2539) ได้ทำการวิจัยการเข้าและถอดรหัสสำหรับตัวอักษรภาษาไทย โดยใช้อัลกอริทึม Affine Transformation, Exponentiation และ RSA cipher โดยการนำเข้าข้อความภาษาไทยผ่านอัลกอริทึมเหล่านี้ จะได้ข้อความที่เข้ารหัสแล้วในรูปตัวเลข 0 ถึง 63 ซึ่งเป็นค่าอ้างอิงที่ใช้ในการวิจัย ซึ่งงานวิจัยดังกล่าวนั้น มีขีดจำกัดในเรื่องของขนาดข้อความที่นำ

มาเข้ารหัส และค่าที่ใช้อ้างอิงในการเข้ารหัสนั้นขาดความเป็นมาตรฐานสากล เพราะเป็นตัวเองที่จัดตั้งขึ้นเองเพื่อใช้งานเฉพาะ

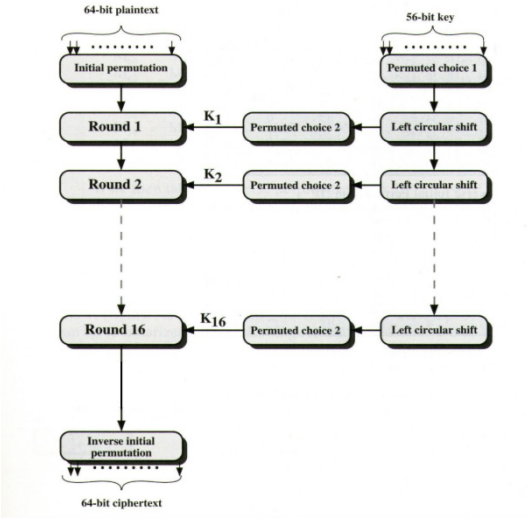
เนื่องจาก Unicode เป็นมาตรฐานสากล สามารถรองรับอักษรทุกภาษา และรองรับการทำงานแบบหลายภาษาได้ การวิจัยนี้นำเสนอการเข้ารหัสภาษาไทยตามมาตรฐาน Unicode 16 บิต เพื่อให้แสดงผลภาษาไทยได้อย่างถูกต้อง โดยใช้อัลกอริธึม AES และ DES และทำการพัฒนาโปรแกรม การเข้ารหัสและถอดรหัสสำหรับภาษาไทย เพื่อทดสอบความถูกต้องของวิธีการที่นำเสนอ

ทฤษฎีและแนวคิดที่เกี่ยวข้อง

ขั้นตอนในการดำเนินงานได้ดังนี้ศึกษาทฤษฎีการเข้ารหัสของ DES และ ศึกษามาตรฐานการเข้าและถอดรหัสภาษาไทย รวมไปถึง Unicode ขนาด 16-บิตและทำการพัฒนาโปรแกรมการเข้าและถอดรหัสด้วยอัลกอริทึม DES และ AES สำหรับภาษาไทย โดยเพิ่มกระบวนวิธี mapping กับตาราง Unicode เพื่อให้สามารถแสดงผลภาษาไทยได้อย่างถูกต้อง ทดสอบและวัดประสิทธิภาพการทำงานของวิธีการที่นำเสนอด้วยโปรแกรมที่พัฒนาขึ้นโดยวัดประสิทธิภาพความถูกต้องและวัดประสิทธิภาพเวลาที่ใช้ในการประมวลการทำงานกับขนาดข้อมูลที่แตกต่างกัน

การเข้าและถอดรหัสด้วยอัลกอริธึม Data Encryption Standard: DES

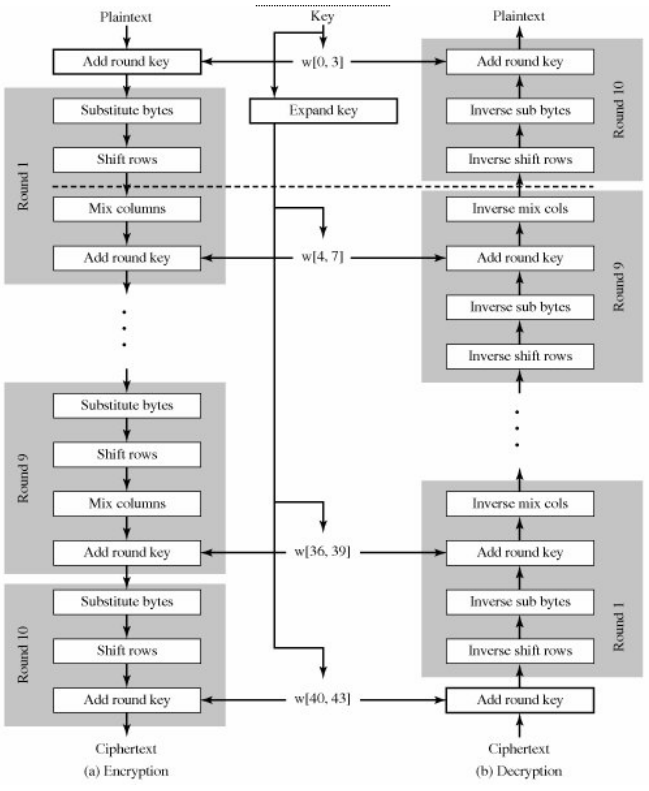
DES (Victor, 2007) เป็นอัลกอริทึมที่ใช้ในการเข้าและถอดรหัสแบบ Block Cipher (Federal Information Processing Standards Publications, 1999) ซึ่งจะทำการแบ่งข้อมูลออกเป็น block แล้วนำไปทำการเข้ารหัสทำการนำเข้าชุดข้อมูลแบบบล็อกขนาด 64 บิต และใช้กุญแจขนาด 56 บิต มีจำนวนรอบในการทำงานเท่ากับ 16 รอบ เพื่อสร้างกุญแจย่อยให้มีจำนวน 16 ดอก โดยระหว่างการเข้ารหัสนั้นแต่ละรอบการทำงานจะมีกุญแจขนาด 48 บิต การทำงานดังภาพที่ 1



ภาพที่ 1 แสดงการทำงานของอัลกอริทึม DES โดยการนำเข้าข้อมูลขนาด 64 บิต และกุญแจขนาด 54 บิต (Lai, 2009)

การเข้ารหัสและถอดรหัสด้วยอัลกอริธึม Advance Encryption Standard: AES

AES (Federal Information Processing Standards Publications, 2001) เป็นอัลกอริทึมที่ถูกคิดค้นและพัฒนาโดย Rijmen and Daemen หรือเรียกกันทั่วไปว่า Rijndael มีการใช้เทคนิคขนาดของคีย์ (Key Size) และขนาดของข้อมูล (Block Size) ซึ่งขนาดของคีย์สามารถเลือกได้เป็น 128 บิต 192 บิต และ 256 บิต AES แสดงได้แสดงในภาพที่ 2



ภาพที่ 2 โครงสร้างการเข้ารหัสและถอดรหัสอัลกอริทึมเออีเอส

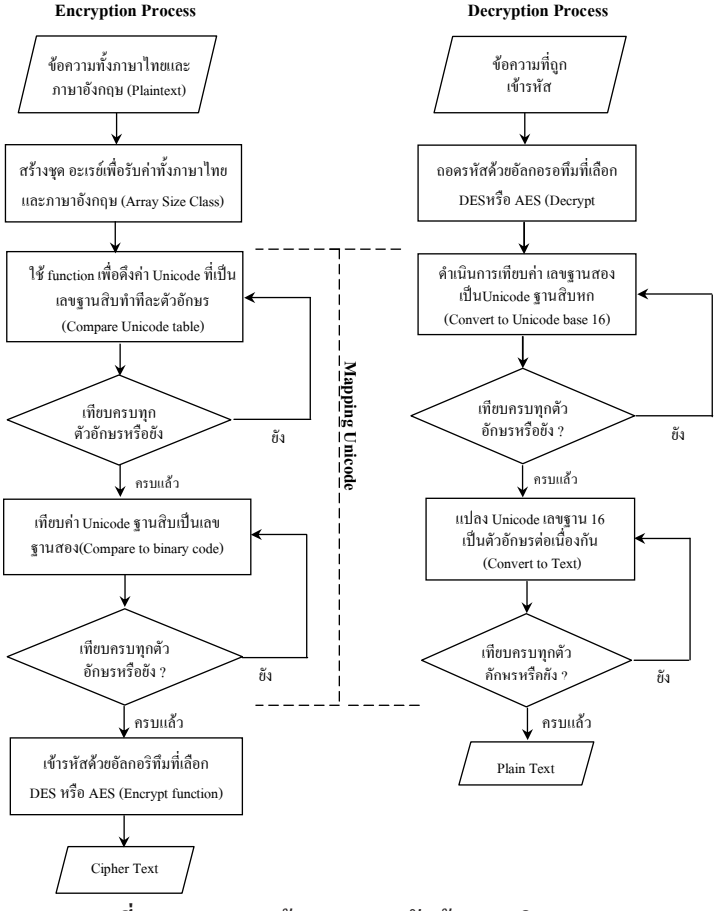
วิธีการดำเนินงานวิจัย

ในการเข้าและถอดรหัสสำหรับภาษาไทยด้วยอัลกอริธึม DES และ AES นี้เพื่อให้สามารถถอดรหัสและแสดงผลภาษาไทยได้อย่างถูกต้อง ผู้วิจัยได้สร้างตาราง Unicode (Davis, 1999) อ้างอิงสำหรับอักษรในภาษาไทยทั้ง 90 ตัว ซึ่งข้อมูลที่จัดเก็บในตารางอ้างอิง โดยอักขระแต่ละตัวในตารางอ้างอิงจะประกอบด้วย 4 แถวคือ แถวแรกแทนอักขระภาษาไทย แถวที่ 2 แทนรหัส ASCII ฐานสิบ สำหรับภาษาไทยขนาด 1 ไบต์ มีค่าระหว่าง 161–250 แถวที่ 3 แทนรหัส Unicode ฐานสิบขนาด 2 ไบต์ และแถว 4 แทนรหัส Unicode ในรูปฐานสิบหก ขนาด 2 ไบต์ (มีค่าระหว่าง 0E01–0E5A) ดังแสดงในตารางที่ 1 เพื่อให้สามารถถอดรหัสและแสดงผลกลับเป็นภาษาไทยอย่างถูกต้อง จะทำการ mapping ข้อมูลก่อนเข้ารหัส และข้อมูลที่ผ่านการถอดรหัสในรูปของรหัส ASCII กับค่าในตารางเปรียบเทียบที่สร้างขึ้น เพื่อดึงค่า Unicode ของตัวอักษรในเลขฐาน 16 มาเพื่อแสดงผล สามารถแสดงขั้นตอนการประมวลผลดังภาพที่ 3

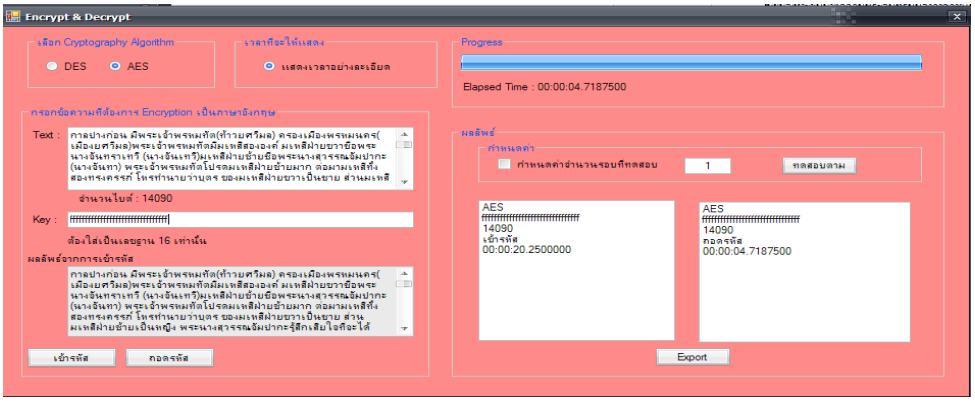
การทดสอบการเข้ารหัสและถอดรหัสภาษาไทยโดยอัลกอริธึม AES และ DES ผู้วิจัยได้ทำการพัฒนาโปรแกรมเพื่อทดสอบการเข้ารหัสและถอดรหัสสำหรับภาษาไทยโดยใช้ภาษา C# ทำงานภายใต้ระบบปฏิบัติการ windows XP แสดงดังภาพที่ 4

ตารางที่ 1 แสดงค่า Unicode สำหรับ การแสดงผลภาษาไทย

ก 161 3585 E01	ข 162 3586 E02	ฃ 163 3587 E03	ค 164 3588 E04	ฅ 165 3589 E05	ฆ 166 3590 E06	ง 167 3591 E07	จ 168 3592 E08	ฉ 169 3593 E09	ช 170 3594 E0A
ซ 171 3595 E0B	ฌ 172 3596 E0C	ญ 173 3597 E0D	ฎ 174 3598 E0E	ฏ 175 3599 E0F	ฐ 176 3600 E10	ฑ 177 3601 E11	ฒ 178 3602 E12	ณ 179 3603 E13	ด 180 3604 E14
ต 181 3605 E15	ถ 182 3606 E16	ท 183 3607 E17	ธ 184 3608 E18	น 185 3609 E19	บ 186 3610 E1A	ป 187 3611 E1B	ผ 188 3612 E1C	ฝ 189 3613 E1D	พ 190 3614 E1E
ฟ 191 3615 E1F	ภ 192 3616 E20	ม 193 3617 E21	ย 194 3618 E22	ร 195 3619 E23	ฤ 196 3620 E24	ล 197 3621 E25	ฦ 198 3622 E26	ว 199 3623 E27	ศ 200 3624 E28
ษ 201 3625 E29	ส 202 3626 E2A	ห 203 3627 E2B	ฬ 204 3628 E2C	อ 205 3629 E2D	ฮ 206 3630 E2E	ฯ 207 3631 E2F	ะ 208 3632 E30	ั 209 3633 E31	า 210 3634 E32
ำ 211 3635 E33	ิ 212 3636 E34	ี 213 3637 E35	ึ 214 3638 E36	ื 215 3639 E37	ุ 216 3640 E38	ู 217 3641 E39	ฺ 218 3642 E3A	□ 219 3643 E3B	□ 220 3644 E3C
□ 221 3645 E3D	□ 222 3646 E3E	฿ 223 3647 E3F	เ 224 3648 E40	แ 225 3649 E41	โ 226 3650 E42	ใ 227 3651 E43	ไ 228 3652 E44	ๅ 229 3653 E45	ๆ 230 3654 E46
็ 231 3655 E47	่ 232 3656 E48	้ 233 3657 E49	๊ 234 3658 E4A	๋ 235 3659 E4B	์ 236 3660 E4C	ํ 237 3661 E4D	๎ 238 3662 E4E	๏ 239 3663 E4F	๐ 240 3664 E50
๑ 241 3665 E51	๒ 242 3666 E52	๓ 243 3667 E53	๔ 244 3668 E54	๕ 245 3669 E55	๖ 246 3670 E56	๗ 247 3671 E57	๘ 248 3672 E58	๙ 249 3673 E59	๚ 250 3674 E5A



ภาพที่ 3 แสดงการเข้าและถอดรหัสด้วยเทคนิค mapping



ภาพที่ 4 โปรแกรมทดสอบการเข้าและถอดรหัส ข้อความภาษาไทย

การทดสอบและวัดประสิทธิภาพการทำงาน

เพื่อทำการทดสอบประสิทธิภาพการทำงานของการเข้ารหัส DES และ AES สำหรับภาษาไทย เนื่องจากงานวิจัยมุ่งเน้นความถูกต้องในการเข้ารหัสและถอดรหัสสำหรับภาษาไทยเป็นหลักนั้น ผู้วิจัยจะทำการทดสอบออกเป็น 2-ประเด็น คือ ความถูกต้องในการเข้ารหัสและถอดรหัสภาษาไทยเป็นประเด็นหลัก และความเร็วในการเข้ารหัสตามแนวทางของ Nadeem *et al* (2005) ซึ่งทำการทดสอบโดยการนำเข้าข้อมูลที่มีขนาดต่างกัน และตรวจสอบความถูกต้องสมบูรณ์ในการถอดรหัสข้อความที่นำเข้า ส่วนประเด็นที่สองในการทดสอบการเข้ารหัสและถอดรหัสแต่ละครั้งจะทำการบันทึกเวลาเพื่อทำหาค่าเฉลี่ยของเวลาในการเข้าและถอดรหัสของชุดข้อมูลที่มีขนาดความยาวแตกต่างกัน

ในการวัดประวัดประสิทธิภาพความถูกต้องและความเร็วในการเข้ารหัสและถอดรหัสภาษาไทย โดยอัลกอริทึมที่นำเสนอ ผู้วิจัยได้ทำการเข้ารหัสข้อความภาษาไทยที่นำมาจากนิทานพื้นบ้าน บทความทั่วไปและบทความเชิงวิชาการ ที่ขนาดความยาว 4 กิโลไบท์ 10 กิโลไบท์ และ14 กิโลไบท์ อย่างละ 5 ชุด ทำการทดสอบการเข้ารหัสและถอดรหัสโดยโปรแกรมที่พัฒนาขึ้น ผลการทดลองสามารถถอดรหัสและแสดงผลภาษาไทยได้ถูกต้องตรงกับข้อความต้นฉบับทุกประการ ส่วนเวลาเฉลี่ยในการเข้ารหัสและถอดรหัสโดย DES Algorithm และ AES Algorithm สามารถแสดงได้ดังตารางที่ 2, 3 และ 4

ตารางที่ 2 แสดงค่าเวลาที่ใช้ในการเข้าและถอดรหัสชุดข้อความภาษาไทย โดย DES Algorithm และเวลาเฉลี่ย

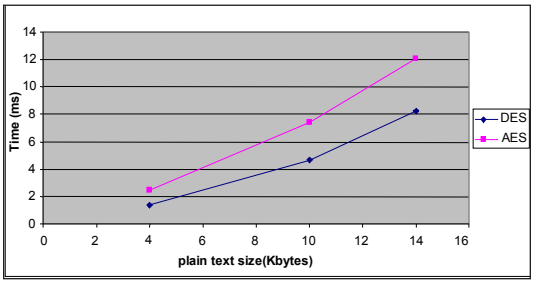
Time (ms)	ข้อความภาษาไทยขนาด 4 กิโลไบท์					ข้อความภาษาไทยขนาด 10 กิโลไบท์					ข้อความภาษาไทยขนาด 14 กิโลไบท์				
	ชุดที่ 1	ชุดที่ 2	ชุดที่ 3	ชุดที่ 4	ชุดที่ 5	ชุดที่ 1	ชุดที่ 2	ชุดที่ 3	ชุดที่ 4	ชุดที่ 5	ชุดที่ 1	ชุดที่ 2	ชุดที่ 3	ชุดที่ 4	ชุดที่ 5
Encrypt time	2.3438	2.1406	2.0313	2.2500	1.4844	9.4375	8.5781	8.1250	7.9375	7.2500	15.1406	15.3906	15.3281	15.2031	14.4375
Decrypt Time	0.4531	0.4219	0.5469	0.7656	1.2969	0.8125	1.1719	1.1406	1.2500	1.1094	1.7656	0.9063	1.5156	1.1719	1.2656
Average	**1.3984**	**1.2813**	**1.2891**	**1.5078**	**1.3906**	**5.1250**	**4.8750**	**4.6328**	**4.5938**	**4.1797**	**8.4531**	**8.1484**	**8.4219**	**8.1875**	**7.8516**
Average	**1.3734**					**4.6813**					**8.2125**				

ตารางที่ 3 แสดงค่าเวลาที่ใช้ในการเข้าและถอดรหัสชุดข้อความภาษาไทย โดย AES Algorithm และเวลาเฉลี่ย

Time (ms)	ข้อความภาษาไทยขนาด 4 กิโลไบท์					ข้อความภาษาไทยขนาด 10 กิโลไบท์					ข้อความภาษาไทยขนาด 14 กิโลไบท์				
	ชุดที่ 1	ชุดที่ 2	ชุดที่ 3	ชุดที่ 4	ชุดที่ 5	ชุดที่ 1	ชุดที่ 2	ชุดที่ 3	ชุดที่ 4	ชุดที่ 5	ชุดที่ 1	ชุดที่ 2	ชุดที่ 3	ชุดที่ 4	ชุดที่ 5
Encrypt Time	3.2813	2.9688	2.5781	2.9375	3.1563	11.8281	11.7188	11.3906	11.4531	10.0469	20.2500	19.5469	19.6875	19.6250	18.3281
Decrypt Time	2.2031	1.8432	1.9844	2.1406	1.8594	3.7969	3.3125	3.3594	4.1563	3.3438	4.7188	4.5625	4.8750	4.8438	4.5313
Average	**2.7422**	**2.4060**	**2.2813**	**2.5391**	**2.5078**	**7.8125**	**7.5156**	**7.3750**	**7.8047**	**6.6953**	**12.4844**	**12.0547**	**12.2813**	**12.2344**	**11.4297**
Average	**2.4953**					**7.4406**					**12.0969**				

ตารางที่ 4 แสดงค่าเวลาเฉลี่ยสำหรับอัลกอริทึม DES และ AES

Plaintext sizes (Kbytes)	Time (ms)	
	DES	AES
4	**1.3734**	**2.4953**
10	**4.6813**	**7.4406**
14	**8.2125**	**12.0969**



ภาพที่ 5 กราฟแสดงความสัมพันธ์ขนาดของข้อความที่นำเข้าเทียบกับเวลาที่ใช้ในการประมวลของแต่ละอัลกอริทึม

อภิปรายผล

จากการทดสอบทำงานการเข้าและถอดรหัสข้อความภาษาไทยที่มีขนาดความยาวที่แตกต่างกัน และมีความหลากหลายของคำภาษาไทย ด้วยอัลกอริทึม DES และ AES ซึ่งแบ่งประเด็นการทดสอบออกเป็นสองประเด็นคือ ประเด็นแรกจะทดสอบความถูกต้องในการเข้าและถอดรหัสข้อความ ผลปรากฏว่า มีความสามารถในการถอดรหัสออกมาได้อย่างถูกต้องแม่นยำตรงตามต้นฉบับข้อความแต่ละชุดที่นำเข้ามา และในส่วนประเด็นที่สองนั้นจะทดสอบถึงความเร็วในการเข้าและถอดรหัสข้อความด้วยอัลกอริทึม DES และ AES ผลปรากฏว่าค่าเวลาที่ได้สำหรับ อัลกอริทึม DES และ AES นั้น เพิ่มขึ้นตามขนาดข้อความที่นำเข้ามา หากพิจารณาในแง่ของความเร็ว DES อัลกอริทึมจะคำนวณได้เร็วกว่า เพราะมีความซับซ้อนและจำนวนบิตที่น้อยกว่า AES อัลกอริทึม หากพิจารณาในแง่ของความปลอดภัย AES อัลกอริทึมจะมีความปลอดภัยมากกว่าเพราะมีความซับซ้อนในการคำนวณมากกว่าและจำนวนบิตของกุญแจที่ยาวกว่า และเมื่อนำค่าเวลาเหล่านั้นมาทำการสร้างกราฟความสัมพันธ์ของแต่ละอัลกอริทึมจะได้ดังภาพที่ 5

สรุปผลการวิจัย

จากการใช้เทคนิควิธีการเทียบชุดข้อความที่นำเข้ากับตาราง Unicode เลขฐานสิบหกซึ่งเป็นมาตรฐานของภาษาไทย มาใช้ในการถอดรหัสเป็นภาษาไทย และในแง่ของการทดสอบความถูกต้องในการเข้าและถอดรหัสข้อความนั้น ผลปรากฏว่าโปรแกรมประยุกต์พัฒนาขึ้นสามารถถอดรหัสออกมาได้อย่างถูกต้องแม่นยำตรงตามต้นฉบับข้อความแต่ละชุดที่นำเข้ามา และในแง่ของการทดสอบความเร็วเวลาที่ประมวลผลการทำงานของแต่ละอัลกอริทึมนั้นแปรผันตรงตามขนาดข้อความที่นำเข้ามา สำหรับการศึกษานี้ เน้นเรื่องความถูกต้องในการเข้ารหัสและถอดรหัสด้วยเทคนิค AES และ DES ควรพิจารณาเทคนิคอื่นเพิ่มเติมอาทิเช่น triple-DES, Blowflish

และควรเปรียบเทียบประสิทธิภาพด้านอื่น ๆ เช่น CPU-workload เป็นต้น

เอกสารอ้างอิง

ณัฐวุฒิ อันทะราศรี และคณะ. 2548 . การสนับสนุนภาษาไทยอย่างเต็มรูปแบบโดย เว็บเมล์ “สยามทะเล”. The Joint Conference Computer Science and Software Engineering, November 17-18, 2005, 313-318.

วราภรณ์ กาญจนทวี. 2539. ขั้นตอนวิธีในการสร้างรหัสภาษาไทย (Algorithms in Thai Encryption). การประชุมทางวิชาของมหาวิทยาลัยเกษตรศาสตร์ ครั้งที่ 34. กรุงเทพฯ, 33-36.

Nadeem, A., Javed, MY. 2005. A Performance Comparison of Data Encryption Algorithms. IEEE, 84-89.

Victor, B. 2007. DES. [online] 2010 May 20. [cited 2007 August 7]. Available from http://www.it.uu.se/edu/course/homepage/security/p3vt07/bv/F3-8.PDF

Federal Information Processing Standards Publications (FIPS PUBS). 1999. Data Encryption Standard (DES). Retrieved May 20, 2010. from http://www.itl.nist.gov/fipspubs/fip46-2.htm

Federal Information Processing Standards Publications (FIPS PUBS). 2001. Advanced Encryption Standard(AES). Retrieved May 20, 2010. from http://csrc.nist.gov/archive/aes/index.html

Davis, M. 1999. Forms of Unicode. IBM developer and President of the Unicode Consortium, IBM Retrieved May 20, 2010. from http://icu- project.org/docs/papers/forms_of_unicode/

NutthNet Communication Network. [ม.ป.ป]. ตารางแสดงตัวอักษร ภาษาไทยและลำดับรหัส ASCII, Unicode บนระบบคอมพิวเตอร์. ค้นเมื่อ 20 พฤษภาคม 2553, จาก http://www.nutthnet.com/articles/charcode.php

Lai, TH. 2009. Modern Block Ciphers. [online] 2010 May 20.[cited 2009 April 15]. Available from http://www.cse.ohio-state.edu/~lai/651/3-DES.ppt

Trappe, W., Washington, L. 2006. Introduction to Cryptography with Coding Theory. United State of America: Pearson Prentice Hall.