

บรรณานุกรม

ดร.บรรจง หะรังษี. ความรู้เบื้องต้นของการเข้ารหัสข้อมูล. ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย.

http://www.thaicert.nectec.or.th/paper/encryption/intro_crypt.php, 2547.

บรรพต ดลวิทยากุล. การบีบอัดเอกสารเอชทีเอ็มแอล บนฝั่งเซิร์ฟเวอร์ด้วยการเข้ารหัสแบบฮัฟแมน. บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร, 2550.

ฐิริพงษ์ อำนาจ. ลายเซ็นดิจิทัลสำหรับอีเมลที่ส่งผ่านบนเว็บ : *Digital signature for Web-Based E-mail*. เชียงใหม่ : บัณฑิตวิทยาลัย มหาวิทยาลัยเชียงใหม่, 2548.

Aamer Nadeem, Dr M. Younus Javed. *A Performance Comparison of Data Encryption Algorithms*. First International Conference on 27-28 Aug. 2005. Page(s):84 – 89, 2005.

Chuanfeng Lv and Qiangfu Zhao. *Integration of Data Compression and Cryptography: Another Way to Increase the Information Security*. 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07), 2007.

Demijan Klinec, Carmit Hazayy, Ashish Jagmohan, Hugo Krawczyk, Tal Rabinz. *On Compression of Data Encrypted with Block Ciphers*. Data Compression Conference, 2009.

Mohammad Shirali-Shahreza and Sajad Shirali-Shahreza. *Sending Pictures by SMS*. *Advanced Communication Technology*. ICACT 2009. 11th International Conference on, 2009.

Thongpon Teerakanok and Sinchai Kamolphiwong. *Accelerating Asymmetric-Key Cryptography using Parallel-key Cryptographic Algorithm (PCA)*. Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology, 2009. ECTI-CON 2009. 6th International Conference on, 2009.

ภาคผนวก



ภาคผนวก ก

การติดตั้งโปรแกรมและการถอดถอนการติดตั้งโปรแกรม

ก.1 การติดตั้งโปรแกรม

ทรัพยากรของเครื่องคอมพิวเตอร์ที่ใช้ติดตั้งโปรแกรมต้องรองรับโปรแกรกดังต่อไปนี้

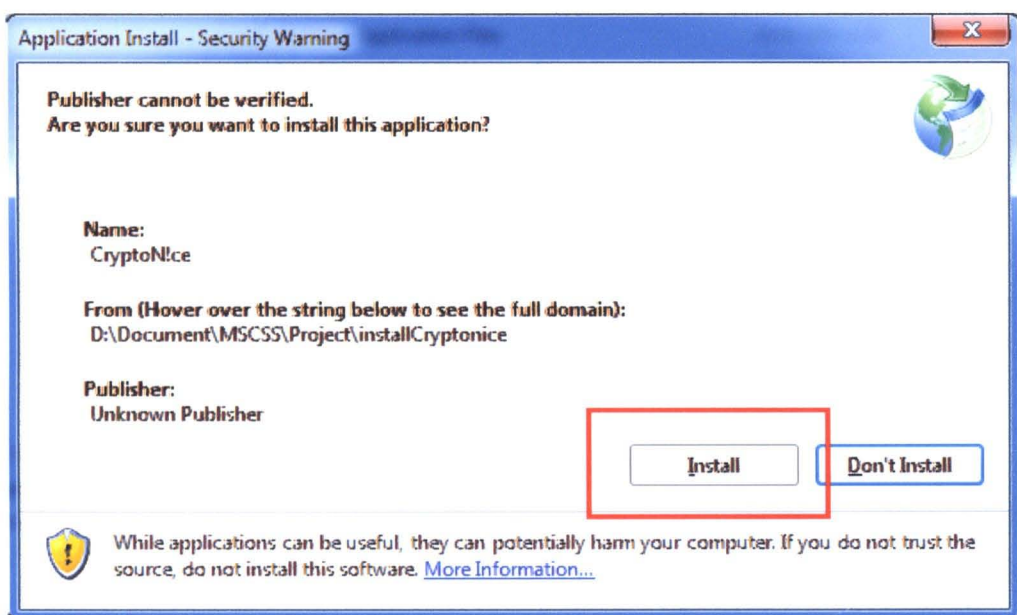
- 1) ระบบปฏิบัติการ วินโดวส์ เอ็กซ์พี (Windows XP) หรือสูงกว่า
- 2) .NET Framework 3.5 หรือสูงกว่า

การติดตั้งโปรแกรม CryptoN!ce สามารถดำเนินการโดยติดตั้งจากไฟล์ setup.exe ของโปรแกรมที่อยู่ในแฟ้ม installCryptonice ดังรูป

Name	Date modified	Type	Size
Application Files	19/6/2555 1:24	File folder	
autorun.inf	19/6/2555 1:28	Setup Information	1 KB
CryptoNice.application	19/6/2555 1:28	ClickOnce Applica...	6 KB
setup.exe	19/6/2555 1:28	Application	457 KB

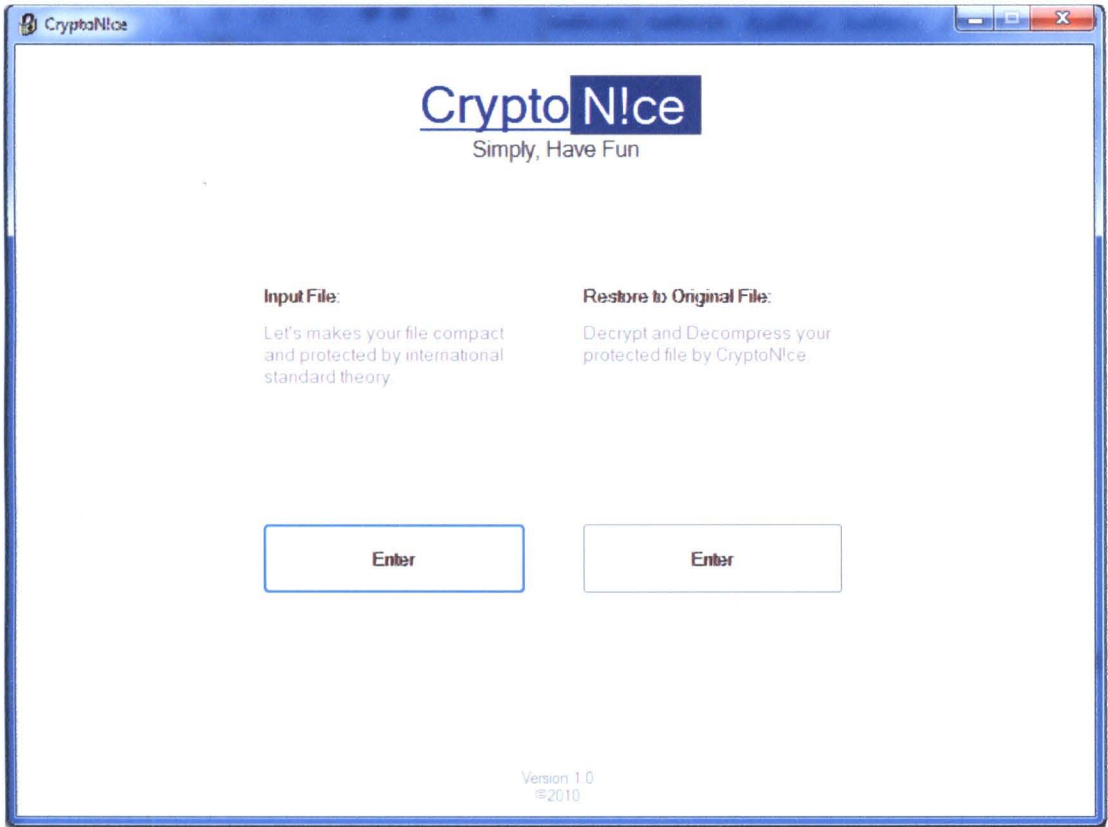
รูป ก.1 ไฟล์ติดตั้งโปรแกรม

เมื่อทำการเปิดไฟล์ setup.exe ก็จะเข้าสู่กระบวนการติดตั้งโปรแกรม ดังรูป



รูป ก.2 เริ่มกระบวนการติดตั้งโปรแกรม

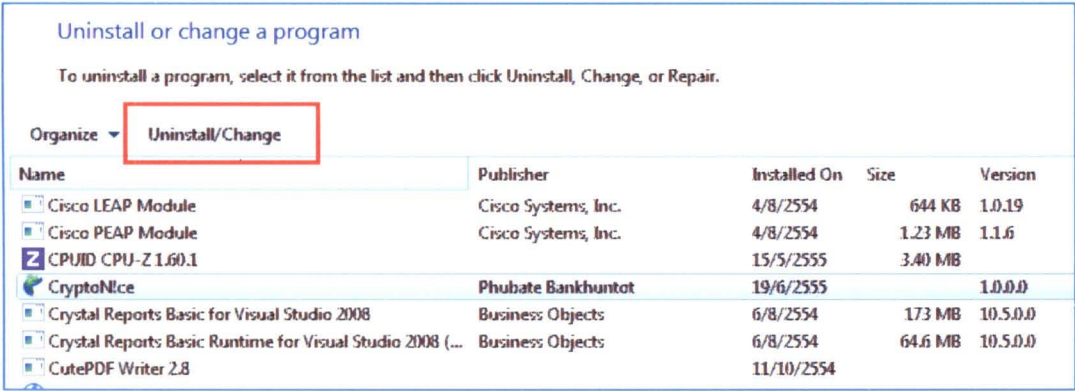
เมื่อกลุ่ม Install โปรแกรมก็จะถูกติดตั้งลงในเครื่องคอมพิวเตอร์ และเมื่อโปรแกรม CryptoN!ce ปรากฏขึ้นมา ก็แสดงว่าการติดตั้งเสร็จสมบูรณ์แล้ว



รูป ก.3 โปรแกรม CryptoN!ce ติดตั้งเสร็จสมบูรณ์

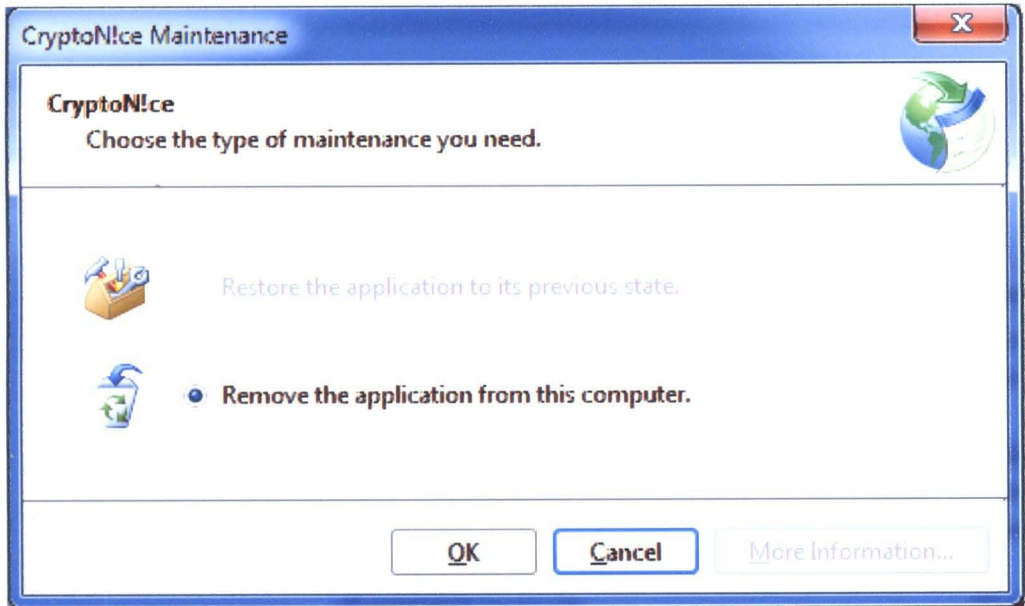
ก.2 การถอดถอนการติดตั้งโปรแกรม

เมื่อต้องการที่จะถอดถอนการติดตั้งโปรแกรม ผู้ใช้สามารถดำเนินการถอดถอนโปรแกรมได้ดังเช่นโปรแกรมอื่นๆ คือการ Add/Remove Program จากระบบปฏิบัติการที่ใช้



รูป ก.4 การถอดถอนโปรแกรม CryptoN!ce

ทำการเลือกโปรแกรม CryptoN!ce ที่ต้องการถอดถอนโปรแกรม แล้วกดปุ่ม Uninstall/Change ก็จะปรากฏหน้าต่างการถอดถอนโปรแกรม ดังรูป



รูป ก.5 หน้าต่างการถอดถอนโปรแกรม CryptoN!ce

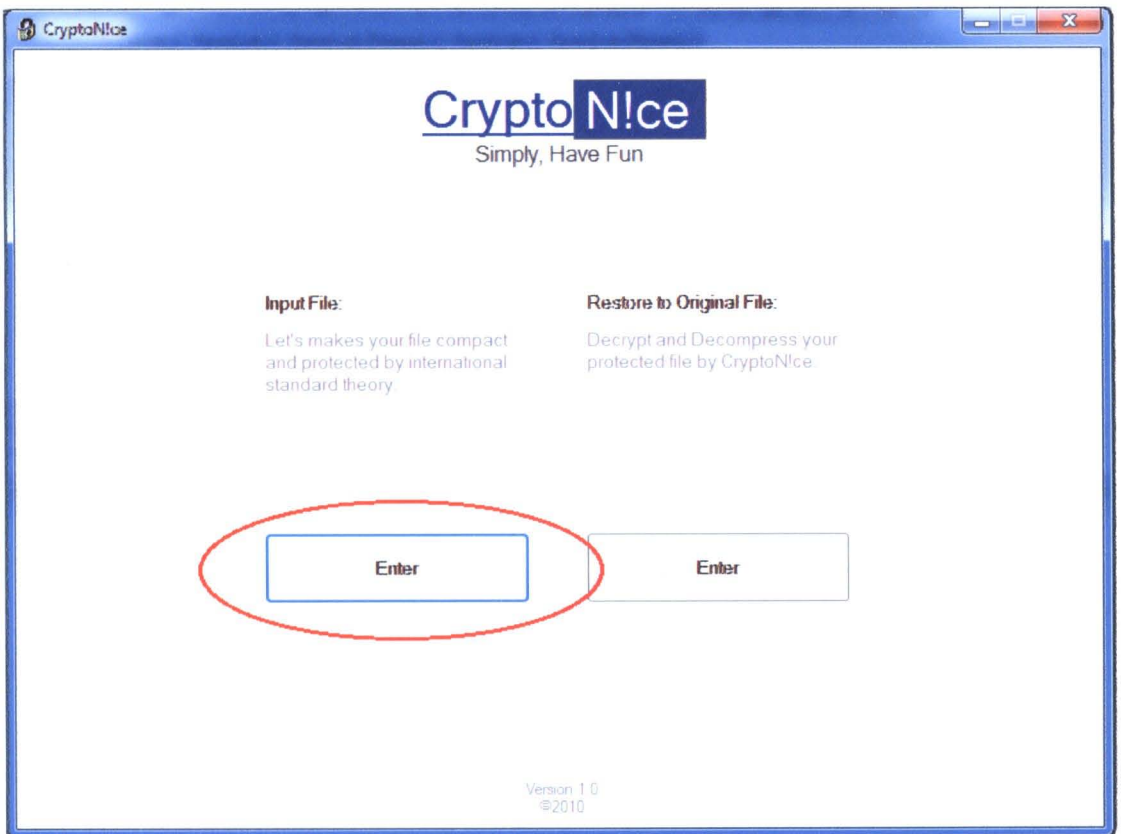
เมื่อกดปุ่ม OK ก็จะเป็นการถอดถอนโปรแกรม CryptoN!ce ออกจากเครื่องคอมพิวเตอร์อย่างสมบูรณ์

ภาคผนวก ข

คู่มือการใช้โปรแกรม

ข.1 การนำเข้าข้อมูล

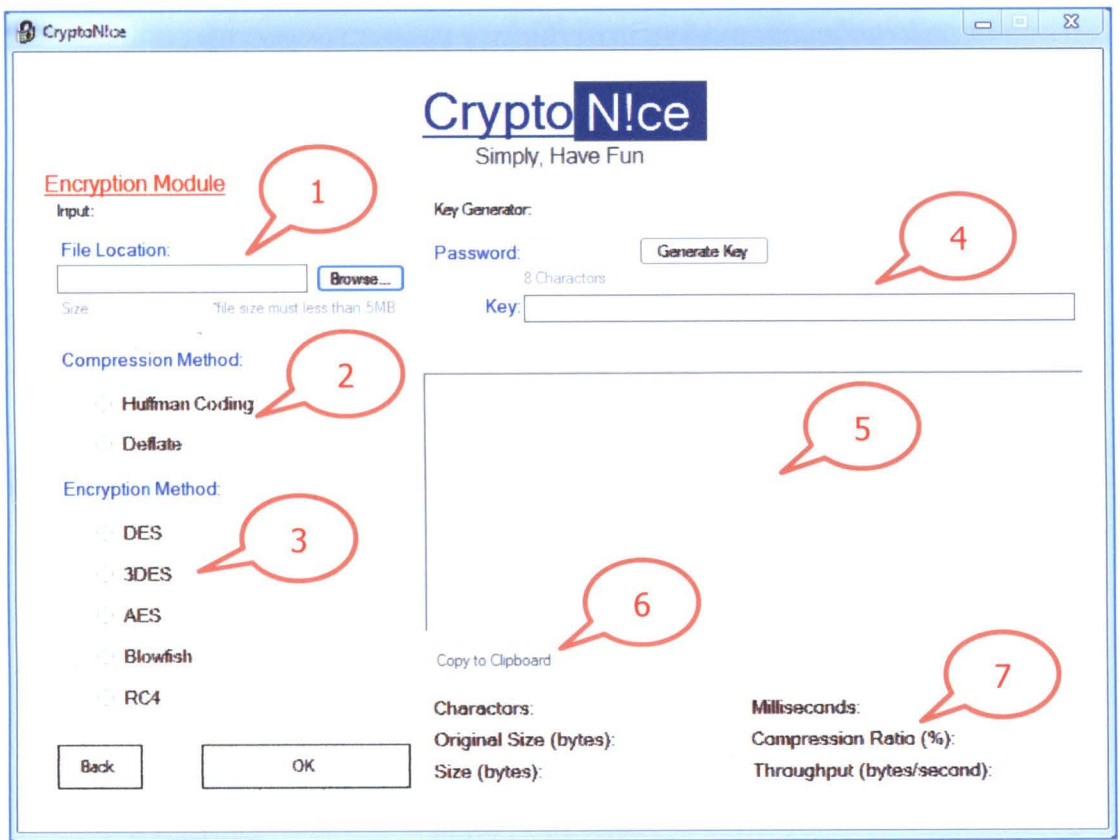
เมื่อเปิดโปรแกรม CryptoN!ce ขึ้นมาแล้ว ในส่วนของการนำเข้าข้อมูล ผู้ใช้สามารถเลือกเข้าใช้งานได้จากปุ่มด้านซ้ายมือ ดังรูป



รูป ข.1 การใช้งานนำเข้าข้อมูล

ในส่วนของการนำเข้าข้อมูล จะเป็นส่วนที่ให้ผู้ผู้ใช้ได้เลือกไฟล์ที่ต้องการจะนำไปบีบอัดและเข้ารหัส ซึ่งผู้ใช้งานสามารถที่จะเลือกได้ว่า ต้องการบีบอัดและเข้ารหัสด้วยอัลกอริทึมแบบใด โดยไฟล์ที่จะนำเข้าสู่กระบวนการนี้ได้นั้น ผู้ใช้สามารถเลือกใช้ไฟล์ประเภทใดก็ได้ แต่ต้องมีขนาดไม่เกินกว่า 5 เมกกะไบต์

โดยส่วนประกอบของหน้าต่างโปรแกรม ดังรูป

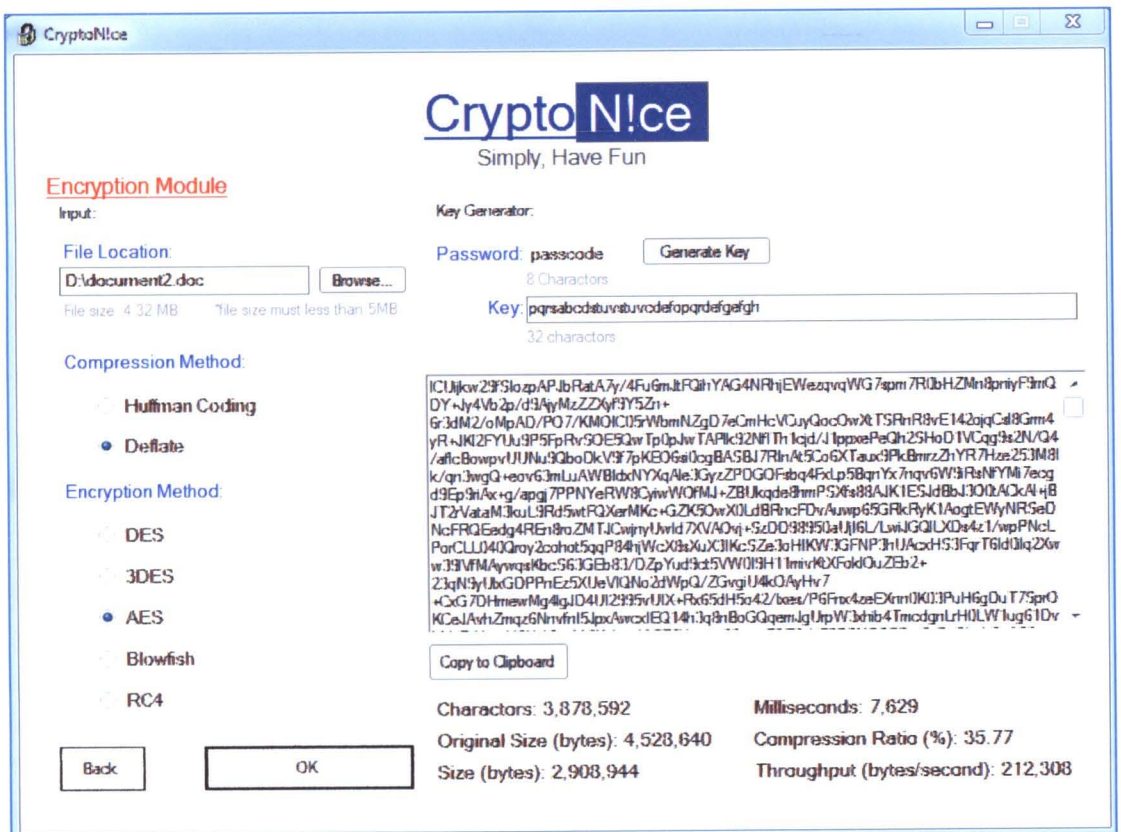


รูป ข.2 หน้าต่างโปรแกรมส่วนของการนำเข้าข้อมูล

- 1) ส่วนที่ให้ผู้ใช้งานสามารถ browse เลือกไฟล์ที่ต้องการนำเข้าข้อมูลได้ โดยจะเป็นไฟล์ประเภทใดก็ได้ แต่ต้องมีขนาดไม่เกิน 5 เมกกะไบต์
- 2) อัลกอริทึมในการบีบอัดข้อมูล ซึ่งสามารถเลือกได้ 2 แบบ คือ Huffman Coding และ Deflate
- 3) อัลกอริทึมในการเข้ารหัสลับข้อมูล ซึ่งสามารถเลือกได้ 5 แบบ คือ DES, 3DES, AES, Blowfish และ RC4
- 4) เมื่อผู้ใช้งานได้เลือกอัลกอริทึมในการเข้ารหัสลับแล้ว ผู้ใช้ต้องทำการระบุ key ที่เป็นเสมือนรหัสผ่านในการถอดรหัส ซึ่งในการระบุ key ในโปรแกรม CryptoN!ce นี้ ผู้ใช้ต้องระบุรหัสผ่านเป็นจำนวน 8 ตัวอักษร เมื่อผู้ใช้งานกดปุ่ม Generate Key โปรแกรมจะทำการ นำเอารหัสผ่านที่ผู้ใช้ระบุไปคำนวณและแปลงค่าให้อยู่ในรูปแบบที่สอดคล้องกับอัลกอริทึมที่เลือกโดยอัตโนมัติ
- 5) ส่วนแสดงผลข้อมูลที่ผ่านการบีบอัดและเข้ารหัสลับแล้ว ซึ่งจะแสดงผลออกมาในรูปแบบของตัวอักษร

- 6) ปุ่ม Copy to Clipboard ช่วยให้ผู้ใช้งานสามารถคัดลอกข้อมูลอักขรทั้งหมดที่แสดงในส่วนผลลัพธ์ เก็บค่าไว้ในหน่วยความจำให้ผู้ใช้งานนำไปใช้งานต่อได้ทันที
- 7) ส่วนที่แสดงค่าสถิติผลการทำงาน

เมื่อผู้ใช้งานทำการเลือกไฟล์ที่จะนำเข้า แล้วทำการกำหนดค่าต่างๆ ตามที่โปรแกรมต้องการเรียบร้อยแล้ว เมื่อกดปุ่ม OK โปรแกรมจะทำการบีบอัดและเข้ารหัสลับ แล้วแสดงผลลัพธ์ออกมาให้อยู่ในรูปแบบของตัวอักษร พร้อมทั้งแสดงค่าสถิติในการดำเนินการ ดังรูป

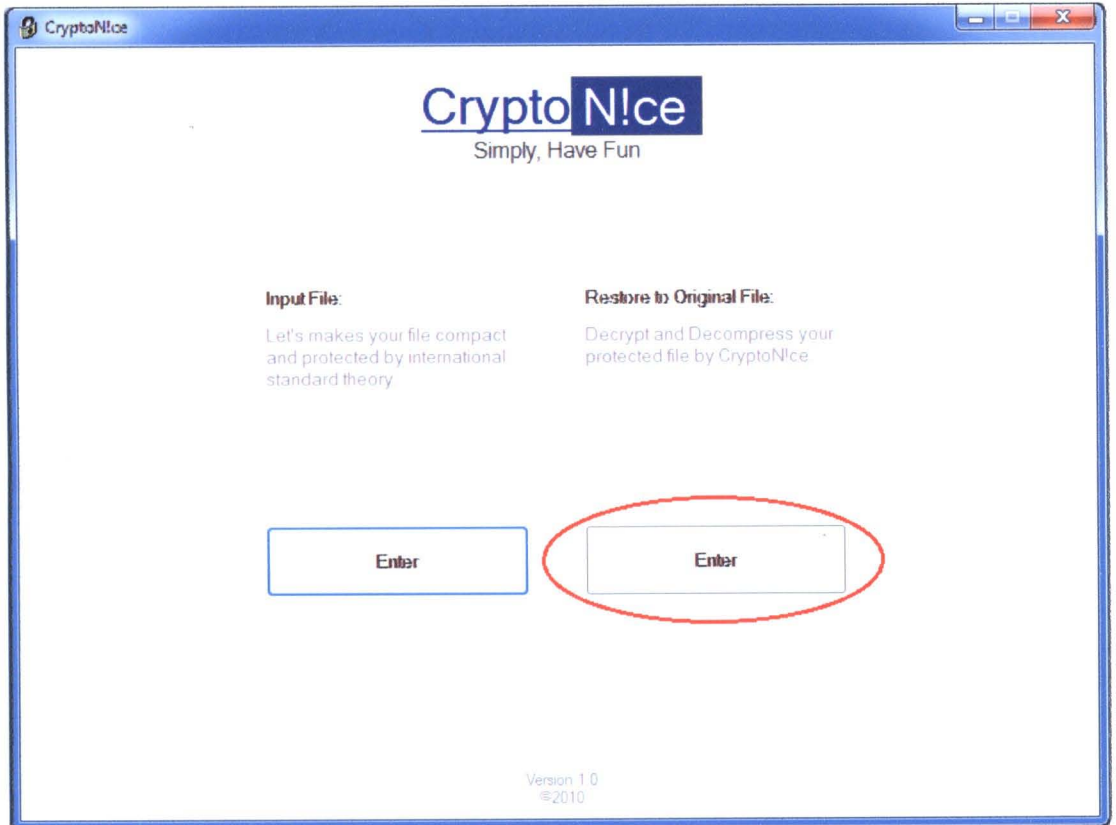


รูป ข.3 หน้าต่างแสดงผลการทำงานเมื่อเสร็จสิ้นกระบวนการนำเข้าข้อมูล

โดยหลังจากที่กระบวนการบีบอัดและเข้ารหัสลับเสร็จสิ้นแล้ว ผู้ใช้สามารถกดปุ่ม Copy to Clipboard เพื่อคัดลอกตัวอักษรทั้งหมดในส่วนของกล่องแสดงผลลัพธ์นั้น ไปใช้งานได้ทันที

ข.2 การถอดรหัสข้อมูลกลับมาเป็นไฟล์ต้นฉบับ

เมื่อเปิดโปรแกรม CryptoN!ce ขึ้นมาแล้ว ในส่วนของการถอดรหัสข้อมูลกลับมาเป็นไฟล์ต้นฉบับ จะอยู่ด้านขวา ดังรูป



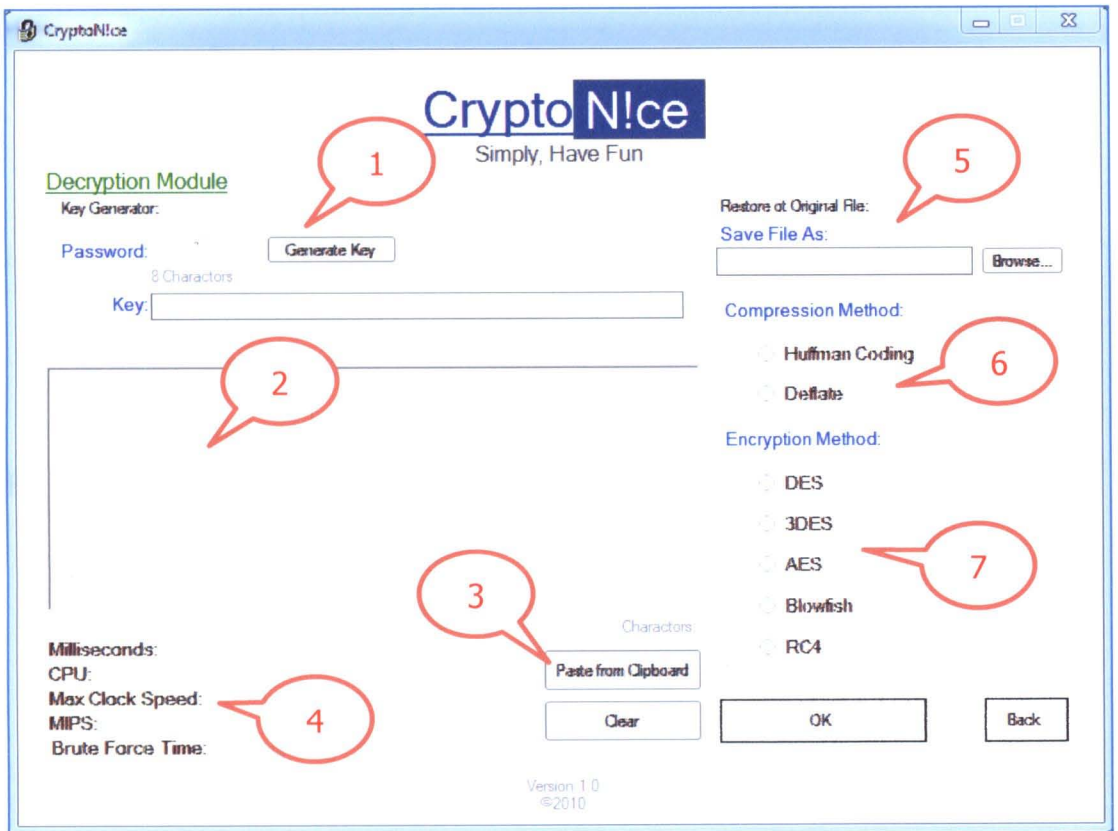
รูป ข.4 การใช้งานถอดรหัสข้อมูลกลับมาเป็นไฟล์ต้นฉบับ

ในส่วนนี้ จะเป็นการนำเอาตัวอักษรที่เป็นผลมาจากการบีบอัดและเข้ารหัสด้วยโปรแกรม CryptoN!ce มาทำการแปลงกลับไปเป็นไฟล์ต้นฉบับ โดยผู้ใช้งานต้องทำการคัดลอกตัวอักษรทั้งหมด มาให้ครบถ้วน และผู้ใช้งานต้องทำการระบุอัลกอริทึมในการบีบอัดและอัลกอริทึมในการเข้ารหัสลับ และรหัสผ่านในการสร้าง key ให้ตรงกับที่กำหนดค่าในการนำเข้าข้อมูลต้นฉบับ



รูป ข.5 ข้อมูลตัวอักษรที่จะนำมาแปลงกลับไปเป็นไฟล์ต้นฉบับ

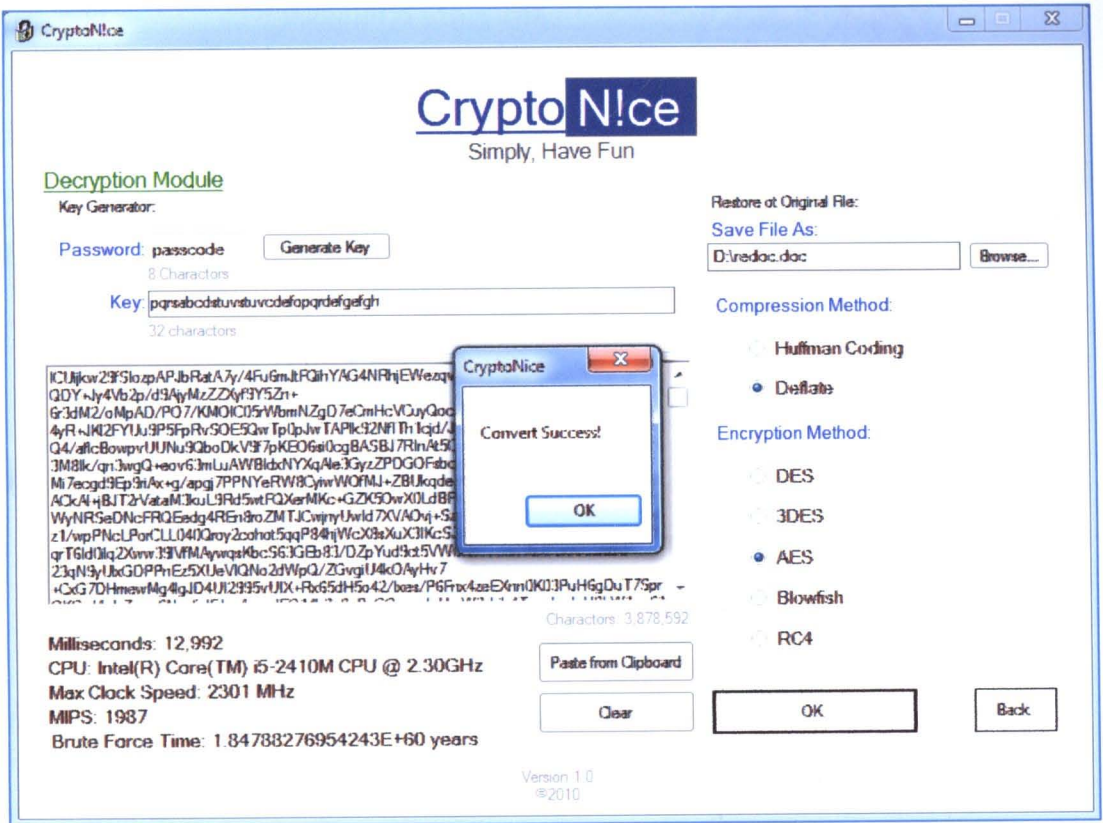
ส่วนประกอบของหน้าต่างโปรแกรมการแปลงกลับไปเป็นไฟล์ต้นฉบับ ดังนี้



รูป ข.6 หน้าต่างโปรแกรมส่วนของการแปลงกลับไปเป็นไฟล์ต้นฉบับ

- 1) ผู้ใช้ต้องระบุรหัสผ่านจำนวน 8 ตัวอักษรให้ตรงกับรหัสผ่านที่ทำการเข้ารหัสในครั้งแรก โดยเมื่อระบุรหัสผ่านแล้วทำการกดปุ่ม Generate Key โปรแกรมจะทำการแปลงรหัสนั้นเป็น Key ที่ใช้ร่วมกับอัลกอริทึมที่ใช้ในการเข้ารหัสโดยอัตโนมัติ
- 2) กล่องข้อความที่ให้ผู้ใช้งานสามารถวางตัวอักษรที่ทำการคัดลอกมา
- 3) ปุ่ม Paste from Clipboard ช่วยอำนวยความสะดวกให้ผู้ใช้งานสามารถวางข้อมูลที่คัดลอกเก็บไว้ในหน่วยความจำได้ทันที
- 4) ค่าแสดงผลการดำเนินการทำงาน
- 5) ให้ผู้ใช้เลือกที่อยู่ของไฟล์ที่จะบันทึกเมื่อแปลงกลับเป็นไฟล์ต้นฉบับแล้ว
- 6) อัลกอริทึมที่ใช้ในการคลายการบีบอัด
- 7) อัลกอริทึมที่ใช้ในการถอดรหัสลับ

เมื่อผู้ใช้งานข้อมูลตัวอักษรที่จะนำมาแปลงกลับเป็นไฟล์ต้นฉบับ และกำหนดค่าต่างๆ ตามที่โปรแกรมต้องการครบถ้วนแล้ว หากกระบวนการทำงานเสร็จสิ้น จะปรากฏผลลัพธ์ดังนี้



รูป ข.7 หน้าต่างแสดงผลการทำงานเมื่อเสร็จสิ้นกระบวนการแปลงกลับ ไปเป็นไฟล์ต้นฉบับ

ประวัติผู้เขียน

ชื่อ – สกุล

นายภูเบศวร์ แบนขุนทด



วัน เดือน ปี เกิด

31 สิงหาคม 2522

ประวัติการศึกษา

วิทยาศาสตรบัณฑิต (ภูมิศาสตร์)
มหาวิทยาลัยเชียงใหม่
ปี พ.ศ. 2544

ประวัติการทำงาน

- นักภูมิศาสตร์ บริษัท เอคิเอส แอนด์ คอมพิวเตอร์ จำกัด
- อาจารย์สาขาเทคโนโลยีสารสนเทศ
โรงเรียนพ่ายพเทคโนโลยีและบริหารธุรกิจ

ตำแหน่งงานปัจจุบัน

พนักงานปฏิบัติงาน สำนักหอสมุด มหาวิทยาลัยเชียงใหม่

