VARIABLE LENGTH DATA ENCRYPTION

JOSEPH K. NILAAD

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE
(COMPUTER SCIENCE)

IN
FACULTY OF GRADUATE STUDIES
MAHIDOL UNIVERSITY
1996

ชื่อวิทยานิพนธ์ การเข้ารหัสข้อมูลที่มีขนาดแปรผัน

ผู้วิจัย โจเซฟ เค นิลาสน์

ปริญญา วิทยาศาสตรมหาบัณฑิต (คอมพิวเตอร์)

คณะกรรมการควบคุมวิทยานิพนธ์

ดำรัส วงศ์สว่าง Ph.D.

เจริญศรี มิตรภานนท์ Ph.D.

ศุภชัย ตั้งวงศ์ศานต์ Ph.D.

วันที่สำเร็จการศึกษา 11 ตุลาคม พ.ศ. 2539

บทคัดย่อ

การเข้ารหัสข้อมูลที่มีขนาดแปรผันคือการเข้ารหัสข้อมูลที่ให้ขนาดของข้อมูลแปรผันหลังจากที่ได้ทำการเข้ารหัสแล้ว ปรัชญาของการเข้ารหัสข้อมูลที่มีขนาดแปรผันนั้นคือให้มีความง่ายต่อการทำความเข้าใจ ให้ผลลัพธ์ของการเข้ารหัสที่รวดเร็ว และมีคุณสมบัติของความน่าจะเป็นไปได้ ในทางทฤษฎีการเข้ารหัสข้อมูลที่ให้ขนาดแปรผันจะสามารถป้องกันข้อมูลได้อย่างถาวร วิธีการที่ทำการเข้ารหัสทำได้อย่างรวดเร็วเพราะว่าใช้เวลาน้อยกว่า 5 สัญญาณนาฬิกา

การเข้ารหัสข้อมูลเป็นสิ่งที่สำคัญมากในระบบการทำงานของคอมพิวเตอร์เพื่อป้องกันข้อมูลไม่ให้บุคคลที่ไม่ได้รับอนุญาตเข้าถึงข้อมูล ผลจากการที่มีคอมพิวเตอร์ส่วนบุคคลได้ทำให้การเข้ารหัสข้อมูลเป็นที่นิยมใช้แพร่หลาย การเข้ารหัสข้อมูลที่มีและใช้งานอยู่ในปัจจุบันนี้สามารถถูกเจาะเข้ารหัสได้โดยเครื่องทางทฤษฎีที่มีชื่อว่า TURING ยกเว้นแต่การเข้ารหัสข้อมูลที่มีชื่อว่า ONE-TIME PAD นอกจากจะสามารถถูกเจาะเข้ารหัสได้แล้ววิธีการเข้ารหัสข้อมูลเหล่านั้นยังมีขั้นตอนการเข้ารหัสข้อมูลที่สลับซับซ้อน ให้ผลลัพธ์ช้า และมีคุณสมบัติตามแบบที่กำหนดไว้แล้ว ในการใช้งานจริงนั้นการเข้ารหัสข้อมูลที่มีขนาดแปรผันที่นำเสนอในวิทยานิพนธ์นี้สามารถทำการป้องกันข้อมูลได้ดีเทียบเท่าหรือดีกว่าการเข้ารหัสข้อมูลที่ดีที่สุดและมีใช้อยู่ทั่วไปในปัจจุบัน

Thesis Title	Variable Length Data Encryption
Name	Joseph K. Nilaad
Degree	Master of Science (Computer science)
Thesis supervisory Committee	
	Damras Wongsawang, Ph.D.
	Jarernsri L. Mitrpanont, Ph.D.
	Supachai Tangwongsan, Ph.D.
Date of Graduation	11 October B.E. 2539 (1996)

ABSTRACT

Variable Length Data Encryption (VLDE) is a cryptosystem that gives variable length of ciphertext. Its philosophies are simple, fast and probabilistic. By Information Theory, it is unconditionally secure with its probabilistic character. It is extremely fast because less than 5 clock cycles needed for encryption and decryption process.

Cryptography is playing a vital role in modern computing. With the advent of personal computer, cryptography is being used widely. All available algorithms are breakable with Turing Machine with the exception of "One-time Pad" algorithm. In addition those algorithms are complicated, slow and deterministic. Actual implementation of VLDE is as secure as the best available algorithm, if not better.