บทที่ 2

แนวความคิดพื้นฐานเกี่ยวกับการเข้ารหัสข้อมูล

2.1 ประวัติความเป็นมาของการเข้ารหัสข้อมูล

การเข้ารหัสลับกระทำเพื่อปกปิดข้อมูลที่มีความสำคัญให้เป็นความลับ โดยการเปลี่ยนรูปแบบของข้อมูลให้อยู่ในรูปแบบอื่น ซึ่งได้มีการใช้กันมาตั้งแต่สมัยอียิปต์โบราณเมื่อประมาณกว่า 4000 ปีมาแล้วและได้มีการพัฒนาวิธีการมาเป็นรูปแบบต่าง ๆ ซึ่งสามารถแบ่งได้กว้าง ๆ เป็น 2 ระบบ (Meyer and Matyas, 1982) คือ ระบบการเข้ารหัสข้อมูลด้วยการใช้พจนานุกรม (Code system) และระบบการเข้ารหัสลับ (Cryptographic System หรือ Cipher System) ในระบบการเข้ารหัสข้อมูลด้วยพจนานุกรม จะต้องมีพจนานุกรม (Code book หรือ Dictionary) เพื่อใช้ในการเข้ารหัสในระดับคำ วลี หรือประโยคของข้อมูลเนื้อแท้* (plaintext) ให้ออกมาเป็นข้อมูลเข้ารหัส (ciphertext) ส่วนระบบการเข้ารหัสลับ จะเป็นการเข้ารหัสในระดับที่เป็นตัวอักษรแต่ละตัวหรือในระดับบิตแต่ละบิตและจะต้องมีค่าคีย์ที่เป็นความลับ ข้อมูลเนื้อแท้และคีย์จะต้องผ่านการดำเนินการเพื่อให้ได้ผลลัพธ์ออกมาแตกต่างจากของเดิม เพื่อปกปิดข้อมูลที่แท้จริงไว้

เนื่องจากระบบการเข้ารหัสข้อมูลด้วยการใช้พจนานุกรม ต้องการหน่วยความจำเป็นจำนวนมากเพื่อใช้สำหรับเก็บพจนานุกรม และต้องใช้เวลามากในการค้นหา คำ วลี หรือประโยคนั้น และถ้าหากพจนานุกรมเล็กเกินไปจะไม่สามารถเข้ารหัสได้ทุก ๆ คำ จึงทำให้วิธีนี้มีข้อจำกัดไม่เหมาะกับการนำมาใช้เพื่อการเข้ารหัสข้อมูลสำหรับข้อมูลจำนวนมาก ๆ ส่วนระบบการเข้ารหัสลับ สามารถนำไปใช้งานได้สะดวก และมีความยืดหยุ่นมากกว่า แต่อย่างไรก็ตามวิธีการพื้นฐานของระบบการเข้ารหัสลับ เช่น วิธีการแทนที่ข้อมูล (Substitution Cipher) หรือวิธีการสลับตำแหน่งของข้อมูล (Transposition หรือ Permutation cipher) ซึ่งในสมัยก่อนวิธีการเหล่านี้ได้รับการยอมรับว่าทำให้ข้อมูลมีความปลอดภัย แต่เมื่อมาถึงยุคสมัยนี้

* หมายถึง ข้อมูลที่ต้องการนำมาเข้ารหัส

ความเจริญทางด้านเทคโนโลยีได้ก้าวหน้าขึ้นมากและมีการนำคอมพิวเตอร์มาใช้ ทำให้การทำงานหรือการแก้ปัญหาต่าง ๆ ทำได้ในเวลาอันรวดเร็ว ทำให้วิธีการเหล่านี้ไม่มีความปลอดภัยเพียงพอสำหรับข้อมูลที่มีความสำคัญ จึงต้องหาวิธีการที่ทำให้มีความปลอดภัยสำหรับข้อมูลมากยิ่งขึ้น แต่วิธีการพื้นฐานเหล่านี้ก็ยังได้ถูกนำมาใช้เป็นส่วนหนึ่งของระบบการเข้ารหัสลับที่นิยมใช้กันในปัจจุบัน

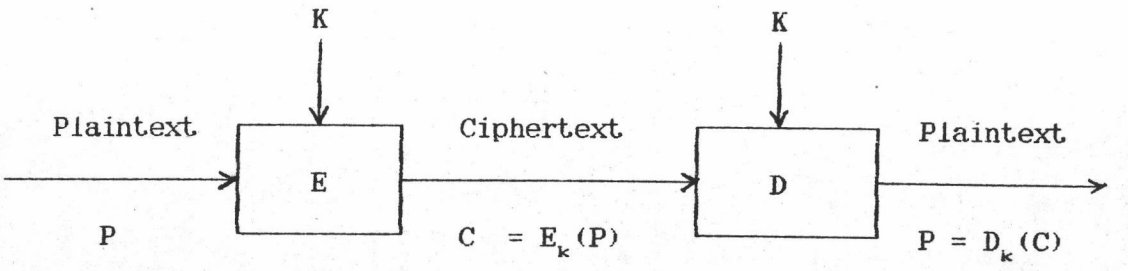
2.2 ระบบการเข้ารหัสลับ (Cryptographic System หรือ Cipher System)

Cryptography เป็นวิชาการที่ว่าด้วยการเข้ารหัสเพื่อปกปิดข้อมูลให้เป็นความลับ คำนี้มาจากภาษากรีก KRIPTO แปลว่า การซ่อน (Hidden) และ GRAFIA แปลว่า สิ่งที่ถูกเขียนขึ้นมา (Something which is written) (Patterson, 1987) ส่วนประกอบที่สำคัญของระบบการเข้ารหัสลับประกอบด้วย 2 ส่วน คือ อัลกอริทึมสำหรับการเข้ารหัสลับ (Cryptographic Algorithm) และ คีย์สำหรับการเข้ารหัสลับ (Cryptographic Key)

อัลกอริทึมสำหรับการเข้ารหัสลับ (Cryptographic Algorithm) คือ ขั้นตอนหรือวิธีการในการเข้ารหัสข้อมูลให้เป็นความลับ ภายในระบบจะมีการดำเนินการหลักอยู่ 2 ส่วน (รูปที่ 2.1) ส่วนแรก คือ **การดำเนินการเข้ารหัส (Encryption หรือ Encipherment)** เป็นการเปลี่ยนข้อมูลเนื้อแท้ให้เป็นข้อมูลเข้ารหัส โดยต้องมีคีย์สำหรับการเข้ารหัสลับส่งผ่านเข้าไปในส่วนการดำเนินการนี้ และ และส่วนที่สอง คือ **การดำเนินการถอดรหัส (Decryption หรือ Decipherment)** เป็นการเปลี่ยนข้อมูลเข้ารหัสให้กลับเป็นข้อมูลเนื้อแท้เหมือนเดิม และจะต้องมีคีย์ที่ใช้สำหรับการถอดรหัสลับเช่นเดียวกัน

ส่วนคีย์สำหรับการเข้ารหัสลับ (Cryptographic Key) คือ ข้อมูลที่ถูกเก็บเป็นความลับเพื่อใช้ในขณะที่ดำเนินการเข้าและถอดรหัสลับ คีย์นี้มีความสำคัญมากจะต้องเก็บเป็นความลับ เนื่องจากถ้าหากว่ารู้ค่าของคีย์แล้วก็จะสามารถถอดรหัสข้อมูลได้ทันที

จากรูปที่ 2.1 E คือ การดำเนินการเข้ารหัสลับข้อมูล และ D คือ การดำเนินการถอดรหัสลับข้อมูล P คือ ข้อมูลเนื้อแท้ ที่ต้องใส่เข้าในส่วนดำเนินการเข้ารหัส หรือได้จากการดำเนินการถอดรหัส C คือข้อมูลเข้ารหัส เป็นผลลัพธ์จากการดำเนินการเข้ารหัส และ K คือ คีย์สำหรับการเข้ารหัสลับ



รูปที่ 2.1 แสดงการดำเนินการเข้ารหัสลับและการดำเนินการถอดรหัสลับ

จะเห็นว่าระบบการเข้ารหัสลับที่จะสามารถป้องกันข้อมูลให้ปลอดภัยได้ จะขึ้นอยู่กับคีย์และอัลกอริทึม โดยที่คีย์จะต้องถูกเก็บเป็นความลับและอัลกอริทึมสำหรับการเข้ารหัสลับจะต้องมีการออกแบบที่ดี มีขั้นตอนวิธีการทำงานที่ซับซ้อนและสามารถป้องกันข้อมูลได้อย่างมีประสิทธิภาพ แม้ว่าจะมีการลักลอบรู้ข้อมูลที่เข้ารหัสแล้ว แต่จะไม่สามารถถอดรหัสออกได้ว่าข้อมูลที่แท้จริงคืออะไร หรือถ้าจะสามารถถอดรหัสได้ ก็ต้องใช้ระยะเวลานานและใช้ทรัพยากรต่าง ๆ เป็นจำนวนมาก เช่น ใช้หน่วยความจำเป็นจำนวนมาก จนทำให้ไม่สามารถที่จะหาข้อมูลนั้นได้ จึงทำให้ข้อมูลมีความปลอดภัย

ทาง National Bureau of Standards (NBS) ได้เสนอคุณสมบัติของอัลกอริทึมสำหรับการเข้ารหัสลับ (Meyer and Matyas, 1982) ไว้ดังนี้

1. อัลกอริทึม ที่จะออกแบบจะต้องมีความสมบูรณ์ ชัดเจน และ ไม่คลุมเคลือ
2. ต้องทราบว่าอัลกอริทึมนี้ มีความสามารถในการป้องกันข้อมูลได้แค่ไหน ต้องทราบระยะเวลาในการประมวลผล และ จำนวนขั้นตอนการทำงานที่ใช้ในการค้นหาคีย์
3. ประสิทธิภาพในการป้องกันข้อมูลจะขึ้นอยู่กับคีย์ที่จะต้องเก็บเป็นความลับเท่านั้น ไม่ใช่เป็นเพราะอัลกอริทึมที่ถูกเก็บเป็นความลับ
4. ในการทำงานของอัลกอริทึมเพื่อเข้ารหัสลับ จะต้องไม่กระทบกระเทือนต่อการทำงานของผู้ใช้ (user) คือ ต้องให้ผู้ใช้สามารถทำงานได้ตามปกติ

ในการศึกษาค้นคว้าเพื่อหาวิธีในการเข้ารหัสลับ เพื่อให้ได้วิธีที่มีประสิทธิภาพและสามารถป้องกันข้อมูลให้ปลอดภัย ได้มีนักวิชาการเสนอแนวความคิดในหลายรูปแบบ ซึ่งสามารถที่จะแบ่งระบบเกี่ยวกับการเข้ารหัสลับ โดยจำแนกตามลักษณะของคีย์สำหรับการเข้ารหัสที่ใช้ในอัลกอริทึมได้ 2 ประเภท คือ

2.2.1 ระบบการเข้ารหัสลับแบบสัญนิยม (Conventional Cryptographic System) หรือ Symmetric System)

อัลกอริทึมของระบบการเข้ารหัสแบบสัญนิยมนี้ คีย์ที่ใช้สำหรับการดำเนินการเข้ารหัสลับ และ การดำเนินการถอดรหัสลับข้อมูลจะต้องเหมือนกัน คือเป็นคีย์เดียวกัน หรือถ้าไม่เหมือนกัน คีย์หนึ่งจะสามารถถูกคำนวณจากอีกคีย์หนึ่งได้ และคีย์นี้จะต้องถูกเก็บเป็นความลับ ความเข้มแข็งของระบบการเข้ารหัสแบบสัญนิยม อยู่ที่ขั้นตอนการทำงานของอัลกอริทึมที่มีประสิทธิภาพ และค่าคีย์ที่เป็นความลับ

ตัวอย่างของอัลกอริทึมของระบบการเข้ารหัสลับแบบสัญนิยมที่นิยมกัน และนำมาใช้เพื่อป้องกันข้อมูลที่มีความสำคัญอย่างกว้างขวาง คือ อัลกอริทึมเดส (Data Encryption Standard Algorithm (DES)) ซึ่งจะได้กล่าวถึงต่อไป

2.2.2 ระบบการเข้ารหัสลับแบบคีย์สาธารณะ (Public Key System หรือ Asymmetric System)

แนวความคิดเกี่ยวกับระบบการเข้ารหัสลับแบบคีย์สาธารณะได้ถูกเสนอขึ้นมาครั้งแรกโดย Diffie และ Hellman (Diffie and Hellman, 1976) จากบทความ "New Directions in Cryptograpy" ในปี 1976 เป็นแนวความคิดใหม่สำหรับการเข้ารหัสลับ โดยที่ในระบบจะมีคีย์สำหรับการเข้ารหัสลับอยู่ 2 คีย์ที่ใช้คู่กัน ซึ่งคีย์ทั้งสองจะมีค่าแตกต่างกัน แต่จะมีความสัมพันธ์กัน คีย์หนึ่งใช้ในการดำเนินการเข้ารหัสลับเรียกว่าคีย์สาธารณะ (Public Key) เป็นคีย์ที่ไม่เป็นความลับเป็นที่รู้กันทั่วไป ส่วนอีกคีย์หนึ่งใช้สำหรับการดำเนินการถอดรหัสเรียกว่า คีย์ที่เป็นความลับ (Secret Key) เป็นคีย์ที่ถูกเก็บไว้เป็นความลับ หลักการสำคัญของระบบการเข้ารหัสลับแบบคีย์สาธารณะ คือ วิธีการคำนวณหาค่าคีย์สาธารณะ และคีย์ที่เป็นความลับ คีย์ทั้งสองมักจะคำนวณมาจากฟังก์ชันทางคณิตศาสตร์ที่ซับซ้อนและมีความสัมพันธ์กัน และที่สำคัญ คือ การรู้ค่าคีย์สาธารณะจะต้องไม่สามารถที่จะคำนวณค่าคีย์ที่เป็นความลับได้ ดังนั้นผู้ที่ทราบคีย์สาธารณะจะสามารถทำการเข้ารหัสลับข้อมูลได้ แต่จะมีเพียงเจ้าของหรือผู้ที่รู้ค่าคีย์เท่านั้นที่จะสามารถถอดรหัสข้อมูลออกได้

อัลกอริทึมต่าง ๆ ที่ใช้ระบบการเข้ารหัสแบบคีย์สาธารณะที่สำคัญ คือ อัลกอริทึมอาร์เอสเอ (Rivest-Shamir-Adleman Algorithm) และอัลกอริทึมแนฟแซ็ค (Knapsack Algorithm)

2.2.3 ข้อสังเกตเกี่ยวกับระบบการเข้ารหัสแบบสัญนิยมและคีย์สาธารณะ

จากการศึกษาระบบการเข้ารหัสลับทั้งสองวิธีพบว่า ระบบการเข้ารหัสแบบคีย์สาธารณะจะทำงานช้ากว่า และต้องการขนาดของหน่วยความจำมากกว่าระบบการเข้ารหัสแบบสัญนิยม ตัวอย่างเช่น ชิป (chip) 1 ตัวที่ใช้เพื่อทำงานของอัลกอริทึมอาร์เอสเอ จะทำงานได้ในช่วง 100 ถึง 1000 บิตต่อวินาที ด้วยเทคโนโลยีในปี 1979 ในขณะที่อัลกอริทึมเดส สามารถทำงานได้ 1 เมกกะบิตต่อวินาที หรือในกรณีของอัลกอริทึมแนพแซค จะต้องใช้หน่วยความจำประมาณ 50 กิโลบิต ในขณะที่อัลกอริทึมเดส ต้องการเพียง 2 กิโลบิตเท่านั้น (Hellman, 1979)

แต่อย่างไรก็ตาม การเข้ารหัสลับแบบระบบคีย์สาธารณะมีข้อดี คือสามารถแก้ปัญหาเกี่ยวกับเรื่องการจัดการคีย์ เช่น ในการส่งข้อมูลที่เป็นความลับติดต่อกันระหว่าง 2 องค์กร จะต้องมีข้อตกลงในการเลือกใช้คีย์ที่จะนำมาเข้ารหัสข้อมูล ซึ่งคีย์นี้จะต้องถูกส่งไปยังผู้รับข้อมูลเสียก่อนด้วยวิธีการที่ปลอดภัย เช่น ส่งไปตามช่องสัญญาณ (Channel) ที่ปลอดภัย หรือส่งโดยการลงทะเบียน เป็นต้น เนื่องจากการรักษาคีย์ให้เป็นความลับจะเป็นปัญหาใหญ่สำหรับระบบการเข้ารหัสแบบสัญนิยม เพราะมีความเสี่ยงสูงในการที่คีย์จะถูกขโมยไปได้ ต้องเสียทั้งเวลาและค่าใช้จ่าย ซึ่งในธุรกิจบางประเภทต้องการความรวดเร็วจะเสียเวลาไม่ได้ แต่เราสามารถใช้ระบบคีย์สาธารณะเพื่อแก้ปัญหานี้ คือทำการเข้ารหัสข้อมูลเนื้อแท้ด้วยคีย์สำหรับเข้ารหัสลับ และทำการเข้ารหัสคีย์นี้ด้วยคีย์สาธารณะของผู้รับข้อมูล แล้วจึงส่งข้อมูลและคีย์ที่เข้ารหัสแล้วไปให้ผู้รับ ส่วนทางผู้รับเมื่อได้รับข้อมูลพร้อมทั้งคีย์ที่ถูกเข้ารหัสอยู่ก็จะทำการถอดรหัสคีย์ด้วยคีย์ที่เป็นความลับของตัวเอง จะได้คีย์สำหรับถอดรหัสข้อมูล แล้วจึงนำคีย์นี้มาถอดรหัสข้อมูลจะได้ข้อมูลเนื้อแท้ที่ส่งมา จะเห็นว่าเป็นการส่งข้อมูลไปพร้อมกับคีย์ในคราวเดียวกัน ทำให้ไม่ต้องเสียเวลาที่จะต้องส่งคีย์ไปก่อน และทำให้คีย์มีความปลอดภัยมากขึ้น

ดังนั้นจะเห็นว่า ระบบการเข้ารหัสแบบคีย์สาธารณะ จะเป็นส่วนประกอบที่เพิ่มขึ้นมาเพื่อช่วยแก้ปัญหาเรื่องการจัดการคีย์มากกว่าจะเป็นการแทนที่ระบบการเข้ารหัสแบบสัญนิยม (Hellman, 1979)

ในปัจจุบันนี้อัลกอริทึมของระบบการเข้ารหัสแบบสัญนิยมที่เป็นที่ยอมรับและมีการนำไปประยุกต์ใช้กับงานต่าง ๆ อย่างกว้างขวาง คือ อัลกอริทึมเดส ได้มีนักวิชาการและผู้เชี่ยวชาญในด้านต่าง ๆ ทำการตรวจสอบและพิจารณาการทำงานของอัลกอริทึมเดสอย่างละเอียด เพื่อทดสอบถึงประสิทธิภาพ ความสามารถในการป้องกันข้อมูลให้ปลอดภัย และหาจุดอ่อนและข้อบกพร่องต่าง ๆ ของอัลกอริทึม แต่ก็ไม่สามารถหาจุดอ่อนที่สำคัญที่จนทำให้อัลกอริทึมเดสนี้ไม่ได้รับการยอมรับ ซึ่งจะได้กล่าวถึงอัลกอริทึมเดสในรายละเอียดในหัวข้อต่อไป

2.3 อัลกอริทึมเดส (Data Encryption Standard : DES)

2.3.1 ประวัติความเป็นมาของอัลกอริทึมเดส

เนื่องจากผลกระทบจากการพัฒนาเทคโนโลยี ทำให้องค์กรต่าง ๆ เริ่มตระหนักถึงความปลอดภัยของข้อมูลมากยิ่งขึ้น มีการพัฒนาวิธีการในการเข้ารหัสมากมาย แต่ยังมีปัญหาเรื่องการติดต่อสื่อสารกันเพราะต่างก็ใช้วิธีการในการเข้ารหัสและใช้อุปกรณ์ที่แตกต่างกัน จึงได้มีความพยายามที่จะสร้างมาตรฐานสำหรับการดำเนินการเข้ารหัสลับข้อมูลขึ้น โดยมีหน่วยงานที่รับผิดชอบ คือ National Bureau of Standards (NBS) โดยในปี 1972 NBS ได้ชักชวนให้มีการเสนออัลกอริทึมสำหรับการเข้ารหัสลับเพื่อใช้ในการป้องกันข้อมูลที่ส่งผ่านเครือข่ายการสื่อสาร หรือข้อมูลที่เก็บไว้ในสื่อต่าง ๆ เช่น พวกจานแม่เหล็ก หรือ เทป เป็นต้น แต่อัลกอริทึมที่เสนอมายัง NBS มีคุณสมบัติไม่ตรงตามที่ NBS ได้กำหนดไว้ จนกระทั่งในปี 1974 บริษัท ไอบีเอ็ม (International Business Machine) ได้เสนออัลกอริทึมให้กับ NBS ซึ่งมีคุณสมบัติตรงกับที่ทาง NBS ได้กำหนดไว้ อัลกอริทึมนี้ คือ อัลกอริทึมลูไซเฟอร์ (Lucifer Encryption) ทาง National Security Agency (NSA) และกลุ่มผู้เชี่ยวชาญได้ทำการศึกษาอัลกอริทึมนี้อย่างละเอียดและได้มีการปรับเปลี่ยนให้เหมาะสมจนได้เป็นอัลกอริทึมใหม่ออกมามีชื่อว่าอัลกอริทึมเดส (Data Encryption Standard (DES)) และได้รับการยอมรับให้เป็นมาตรฐานเมื่อวันที่ 23 พฤศจิกายน ค.ศ. 1976

ถึงแม้ว่า อัลกอริทึมเดสจะได้รับการยอมรับให้เป็นมาตรฐานตั้งแต่ปี ค.ศ. 1976 แต่เพิ่งจะมีการนำมาใช้งานในด้านธุรกิจการค้าอย่างกว้างขวางเมื่อไม่นานมานี้เอง ตัวอย่างเช่น HBO (Home Box Office) มีการเข้ารหัสข้อมูลที่เป็นสัญญาณของสายเคเบิลทีวีเป็นครั้งแรก โดยใช้อัลกอริทึมเดส ส่วน CIRRUS International Banking Network มีการนำอุปกรณ์สำหรับการเข้ารหัสที่ใช้วิธีการของอัลกอริทึมเดส มาใช้กับระบบฝากถอนเงินแบบอัตโนมัติ (Electronic Funds Transfer) นอกจากนี้อัลกอริทึมเดสได้ถูกปรับเปลี่ยนให้เป็นมาตรฐานสำหรับ Inter-agency Electronic Funds Transfer โดยรัฐบาลสหรัฐอเมริกา เมื่อปี 1984 (Cooper, 1989)

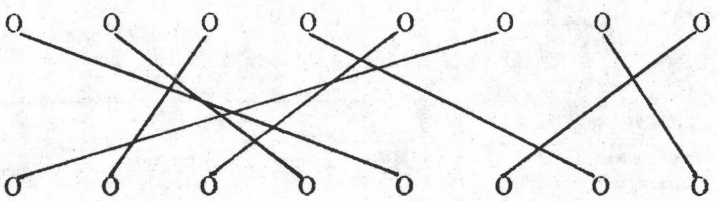
2.3.2 หลักการในการเข้ารหัสของอัลกอริทึมเดส

อัลกอริทึมเดส ได้นำหลักการของการเข้ารหัสแบบพื้นฐานมาใช้ คือ วิธีการจัดลำดับตำแหน่งของบิต (Permutation หรือ Transposition Cipher) วิธีการแทนที่ข้อมูล (Substitution Cipher) และโดยทางคณิตศาสตร์ คือวิธีการมอดดูโล 2 (Addition Modulo 2) หรือ การเอกซ์คลูซีฟออร์ (Exclusive-Or)(Davies and Price, 1984) (รายละเอียดของอัลกอริทึมเดสดู (NBS, 1977))

การจัดลำดับตำแหน่งของบิต สามารถกระทำได้ใน 3 ลักษณะ คือ

1. การจัดลำดับตำแหน่งของบิตของข้อมูลให้อยู่ในรูปแบบใหม่ (Permutation) เมื่อจัดเสร็จแล้วยังคงมีจำนวนบิตเท่าเดิม มีลักษณะดังรูป

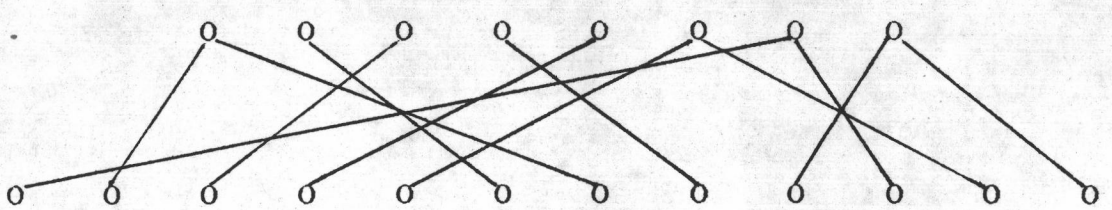
ข้อมูลเข้า



ข้อมูลออก

2. การจัดลำดับตำแหน่งของบิตของข้อมูลใหม่ โดยมีการใช้บางบิตของข้อมูลซ้ำ (Expanded Permutation) เมื่อจัดเสร็จจะมีจำนวนบิตเพิ่มขึ้น มีลักษณะดังรูป

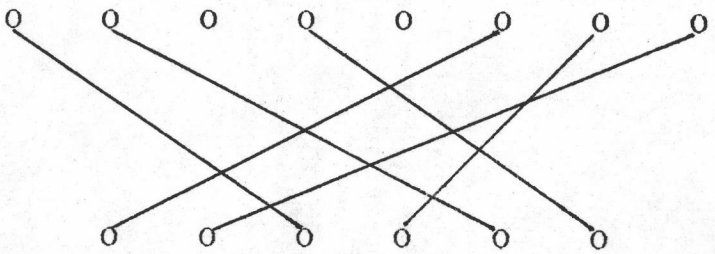
ข้อมูลเข้า



ข้อมูลออก

3. การจัดลำดับตำแหน่งของบิตของข้อมูลใหม่โดยนำบางบิตของข้อมูลเท่านั้นที่มาจัดลำดับและบางบิตจะไม่นำมาใช้ (Permuted Choices) เมื่อจัดเสร็จแล้วจะมีจำนวนบิตลดลง มีลักษณะดังรูป

ข้อมูลเข้า



ข้อมูลออก

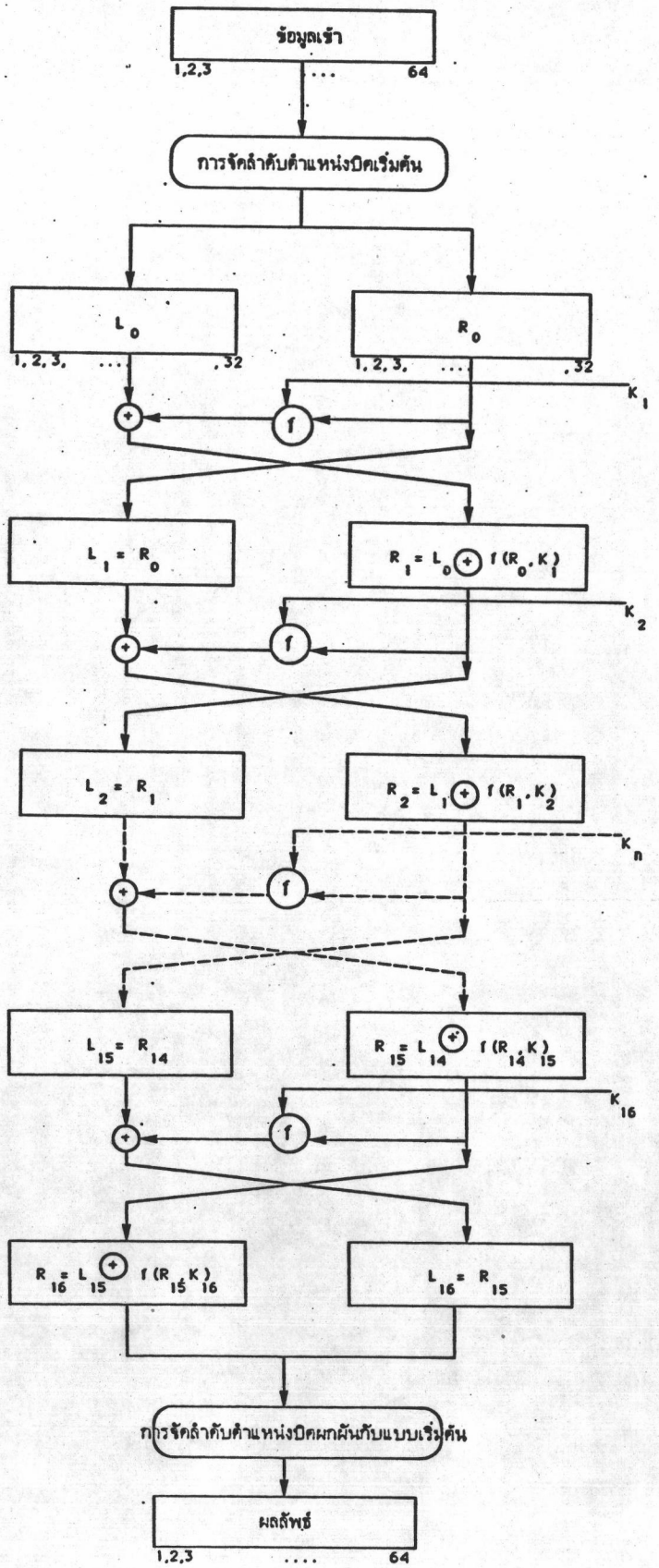
ส่วนวิธีการแทนที่ข้อมูล (Substitution Cipher) จะเป็นการแทนที่ข้อมูลเดิมด้วยข้อมูลใหม่

2.3.3 <u>ขั้นตอนการทำงานของอัลกอริทึมเดส</u>

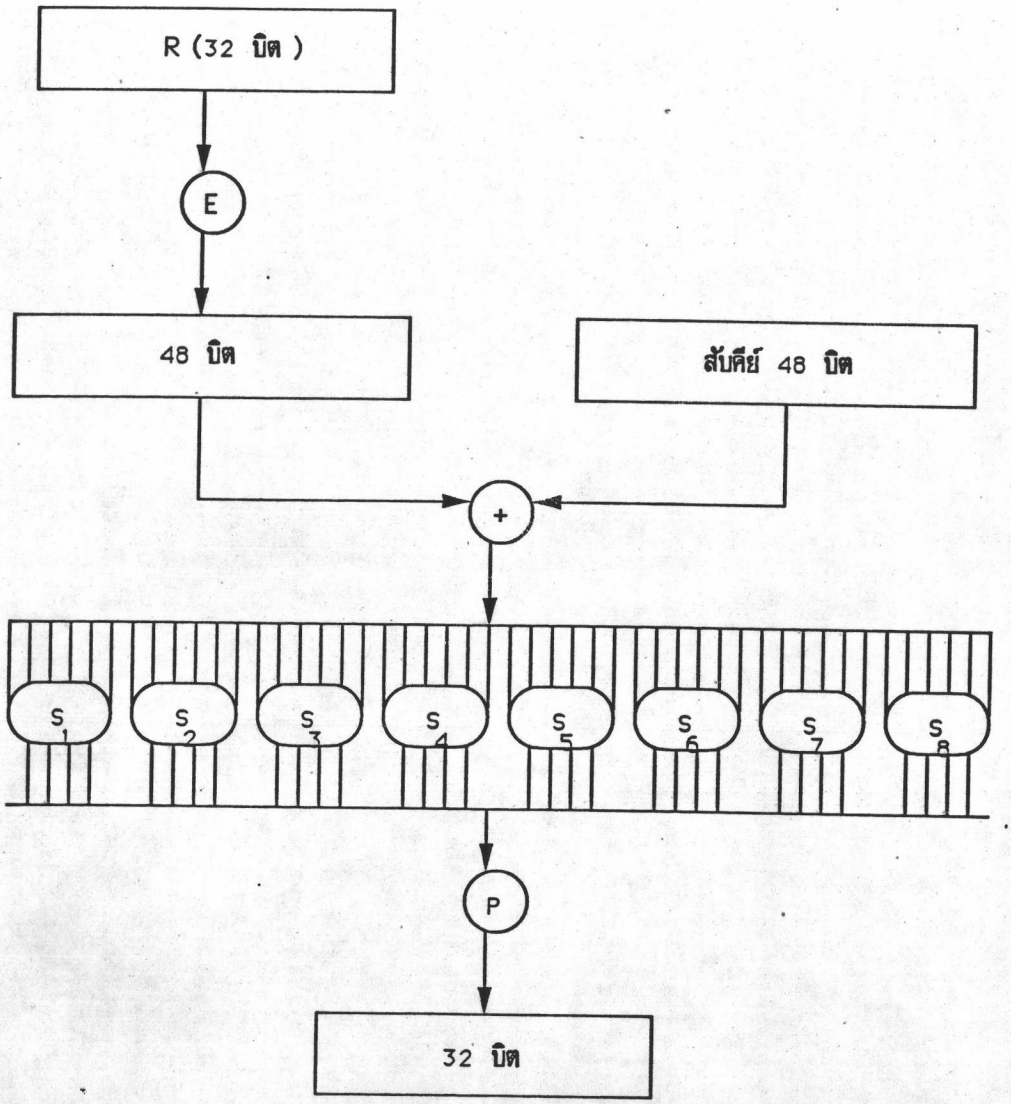
การเข้ารหัสข้อมูลโดยใช้อัลกอริทึมเดส ข้อมูลจะถูกแบ่งเป็นกลุ่ม ๆ ละ 64 บิต มีคีย์สำหรับการเข้ารหัสลับขนาด 64 บิต แต่มีการตัดพาริตี้บิตออกไป 8 บิต ดังนั้นจะเหลือ 56 บิต และได้ผลลัพธ์คือข้อมูลที่เข้ารหัสแล้วขนาด 64 บิต

ขั้นตอนการทำงานของอัลกอริทึมเดส (รายละเอียดดู (NBS, 1977)) ดังแสดงไว้ในรูปที่ 2.2 - 2.4 มีวิธีการดังนี้ คือ

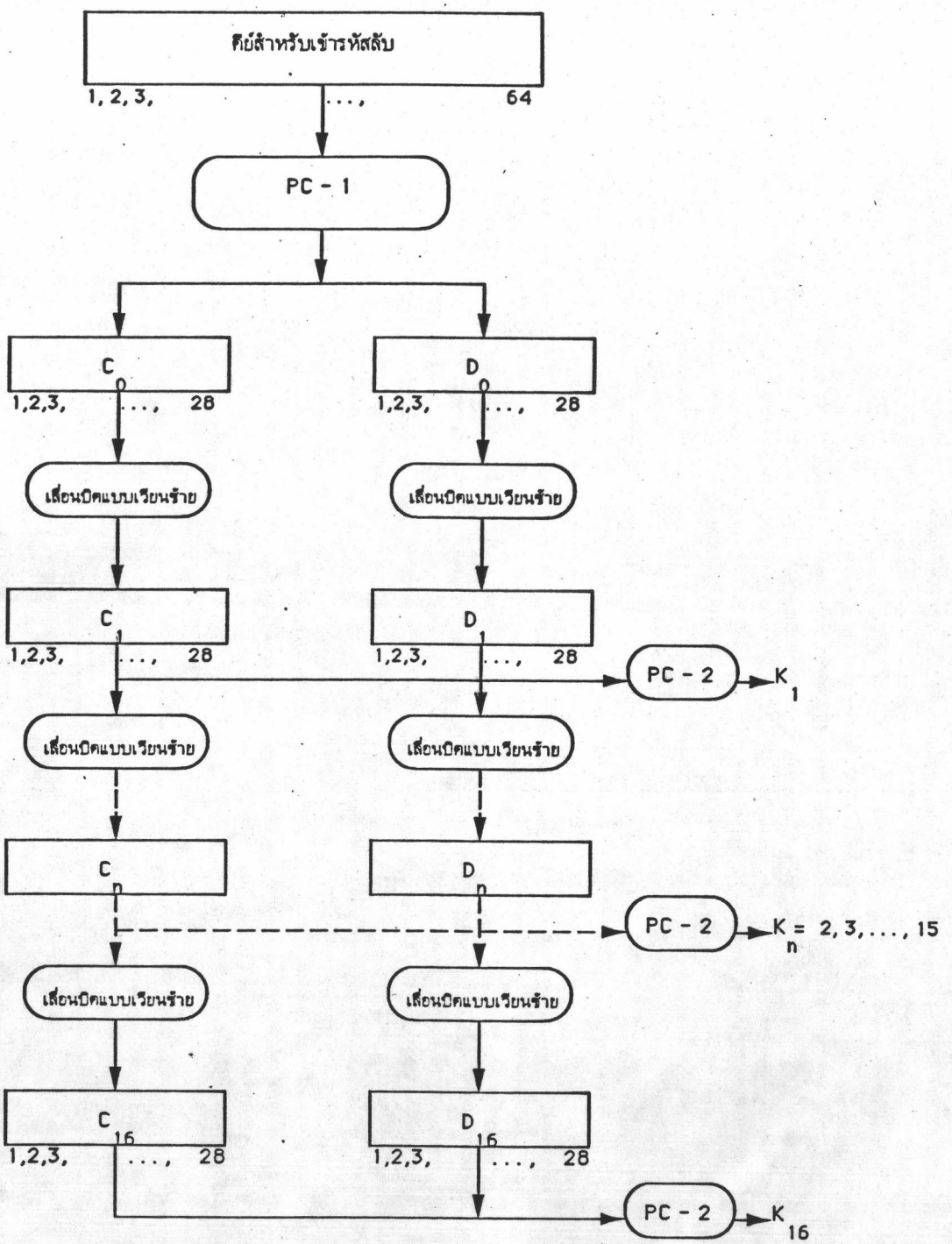
ข้อมูลเนื้อแท้ที่จะเข้ารหัสโดยใช้อัลกอริทึมเดส จะถูกนำมาผ่านการจัดลำดับตำแหน่งบิตเริ่มต้น (initial permuation) ดังรูปที่ 2.2 ได้ผลลัพธ์ออกมาจะถูกแบ่งเป็น 2 ส่วน คือ ส่วนซ้าย (L_0) และส่วนขวา (R_0) ส่วนละ 32 บิต ส่วนขวาจะถูกเปลี่ยนรูปแบบโดยผ่านฟังก์ชัน f ซึ่งเป็นนอนลีเนียร์ฟังก์ชัน (Non-linear function) มีค่าขึ้นอยู่กับค่าคีย์สำหรับการเข้ารหัสลับ ผลจากฟังก์ชัน f จะนำมาเอ็กซ์คลูซีฟออร์กับส่วนซ้าย ได้เป็นส่วนขวาใหม่ (R_1)



รูปที่ 2.2
แสดงขั้นตอนการทำงานของอัลกอริทึมเดส



รูปที่ 2.3 แสดงการทำงานของฟังก์ชั่น f



รูปที่ 2.4 แสดงการคำนวณค่าสับคีย์ (Subkey)

และในส่วนขวาเดิมจะกลายเป็นส่วนซ้ายใหม่ (L_i) การดำเนินการนี้จะกระทำซ้ำ ๆ กัน 16 รอบ และหลังจากนั้นจะนำผลลัพธ์มาผ่านการจัดลำดับตำแหน่งของบิตแบบผกผันกับแบบเริ่มต้น (inverse initial permutation) จะได้ข้อมูลที่ถูกเข้ารหัสแล้วขนาด 64 บิต

ส่วนขั้นตอนการทำงานในฟังก์ชัน f ดังรูปที่ 2.3 ข้อมูลที่ใส่เข้ามาในฟังก์ชันนี้ คือส่วนขวา (R_0 หรือ $R_{(i-1)}$) มีขนาด 32 บิต จะมีการจัดลำดับตำแหน่งบิตของข้อมูลใหม่โดยมีการใช้บางบิตซ้ำ (expanded permutation)ขยายข้อมูลเป็น 48 บิต ($E(R_{(i-1)})$) แล้วนำมาเอ็กซ์คลูซีฟออร์กับสับคีย์ (Subkey) K_i i คือ รอบที่ทำงานในฟังก์ชัน f โดยที่ i = 1, 2, ..., 16 ได้ผลลัพธ์จะนำมาแบ่งเป็นกลุ่ม ๆ ละ 6 บิต จำนวน 8 กลุ่ม แล้วจึงนำแต่ละกลุ่มมาผ่านฟังก์ชัน S-box ได้ผลลัพธ์ออกมากลุ่มละ 4 บิต นำมารวมกันจะได้ผลลัพธ์ทั้งหมด 32 บิตเท่าเดิม แล้วนำมาจัดลำดับบิตใหม่ ผ่าน P

และในส่วนการคำนวณค่าสับคีย์ ดังรูปที่ 2.4 จะนำคีย์สำหรับการเข้ารหัสลับซึ่งเป็นคีย์ที่เก็บเป็นความลับขนาด 64 บิต นำมาจัดลำดับบิตใหม่ ผ่าน PC-1 ซึ่งมีการตัดพาริตี้บิตออกไป 8 บิต จะเหลือ 56 บิต นำมาแบ่งเป็น 2 ส่วน ๆ ละ 28 บิต แต่ละส่วนจะถูกนำมาเปลี่ยนลำดับตำแหน่งบิตใหม่โดยใช้การเลื่อนตำแหน่งบิตแบบหมุนเวียนไปทางซ้าย (circular left shift) ทีละ 1 บิต หรือ 2 บิต โดยในแต่ละรอบจะนำผลลัพธ์ทั้งสองส่วนมารวมกันได้ 56 บิต แล้วทำการจัดลำดับตำแหน่งบิตใหม่ โดยบางบิตจะไม่นำมาใช้ (permuted choices) โดยผ่าน PC-2 จะได้สับคีย์ขนาด 48 บิต กระบวนการนี้จะกระทำซ้ำกัน 16 รอบ ดังนั้น จะได้สับคีย์ 16 คีย์ คือ K_1, K_2, ..., K_{16} นำค่าสับคีย์แต่ละคีย์มาใช้ในฟังก์ชัน f

การดำเนินการเข้ารหัสและถอดรหัสโดยใช้อัลกอริทึมเดสจะเหมือนกัน แต่ต่างกันที่ในค่าสับคีย์ที่ใช้ในการถอดรหัส จะใช้ในลักษณะตรงกันข้ามกับที่ใช้ในการเข้ารหัส คือ ใช้สับคีย์ K_{16} ในรอบที่ 1 ใช้สับคีย์ K_{15} ในรอบที่ 2 เป็นเช่นนี้เรื่อยไป จนถึงรอบที่ 16 จะใช้สับคีย์ K_1

2.3.4 การวิเคราะห์โครงสร้างของอัลกอริทึมเดส

จะเห็นว่าโครงสร้างภายในของอัลกอริทึมเดส จะเป็นวงจรของการทำงานที่ซ้ำ ๆ กันถึง 16 รอบ ประกอบด้วยการจัดลำดับตำแหน่งบิตของข้อมูล การแทนที่ข้อมูล และการเอกซ์คลูซีฟออร์กับค่าคีย์สำหรับเข้ารหัสลับ ซึ่งการทำงานในวงจรนี้เรียกว่าฟังก์ชัน f ลักษณะการทำงานเป็นวงจรแบบนี้ ทำให้อัลกอริทึมสามารถทำงานได้อย่างมีประสิทธิภาพ (Diffie and Hellman, 1977) เพราะอัลกอริทึมที่ใช้วิธีการแทนที่ หรือวิธีการจัดลำดับตำแหน่งของข้อมูล

เพื่อเข้ารหัสเพียงอย่างใดอย่างหนึ่งจะสามารถถูกทำลายได้โดยง่าย Shannon (Shannon, 1949 quoted in Davies and Price, 1984) ได้เสนอว่าถ้านำวิธีการทั้งสองมาใช้ร่วมกัน จะทำให้อัลกอริทึมเข้มแข็งขึ้นยากแก่การทำลาย เนื่องจากการใช้วิธีการแทนที่ข้อมูลจะป้องกันความพยายามที่จะทำลายอัลกอริทึมที่ใช้ทฤษฎีทางคณิตศาสตร์ (Determistic Method และ Analytical Method) มาเพื่อวิเคราะห์อัลกอริทึม เช่น ความพยายามหาความสัมพันธ์ระหว่างข้อมูลเนื้อแท้ ข้อมูลเข้ารหัส และคีย์ ให้ออกมาเป็นสมการ จะทำไม่ได้ เพราะลักษณะการแทนที่ข้อมูลด้วยข้อมูลอื่นเป็นพวกนอนลีเนียร์ฟังก์ชัน (Non-linear function) ส่วนวิธีการจัดลำดับตำแหน่งบิตของข้อมูลใหม่ จะป้องกันความพยายามที่จะทำลายอัลกอริทึมที่ใช้วิธีการทางสถิติ (Statistical Method) มาเพื่อวิเคราะห์อัลกอริทึม เพื่อหาความสัมพันธ์ระหว่างข้อมูลเนื้อแท้ ข้อมูลเข้ารหัส และคีย์ ซึ่งอัลกอริทึมเดสก็ได้นำวิธีดังกล่าวมาใช้

จากโครงสร้างการทำงานของอัลกอริทึมในลักษณะดังกล่าว จะเห็นว่าข้อมูลแต่ละบิตของข้อมูลเข้ารหัสที่ได้จากอัลกอริทึมเดสเป็นฟังก์ชันของทุก ๆ บิตของข้อมูลเนื้อแท้ กับคีย์สำหรับการเข้ารหัสลับ และจะไม่สามารถหาความสัมพันธ์ของข้อมูลทั้งสามออกมาอยู่ในรูปของสมการทางคณิตศาสตร์ได้ ซึ่งจุดนี้เองทำให้อัลกอริทึมเดสมีความเข้มแข็งยากแก่การทำลาย นอกจากนี้ การทำงานที่เป็นวงจรถึง 16 รอบ ทำให้อัลกอริทึมเดสมีความซับซ้อน ถึงแม้จะรู้ข้อมูลเข้ารหัสก็จะไม่สามารถย้อนกลับไปหาข้อมูลเนื้อแท้ได้

ดังนั้นวิธีการที่จะทำลายอัลกอริทึมเดสที่มีโอกาสเป็นไปได้ คือการค้นหาคีย์ที่ใช้สำหรับเข้ารหัสลับโดยวิธีค้นแบบไล่เรียง (Exhaustive Search) เพราะเมื่อทราบคีย์ก็จะสามารถถอดรหัสข้อมูลได้ เนื่องจากขั้นตอนวิธีการของอัลกอริทึมเดสเป็นที่เปิดเผย ในการค้นหาคีย์นี้มีสมมติฐานว่า ผู้ที่จะทำลายอัลกอริทึมทราบข้อมูลเนื้อแท้และข้อมูลเข้ารหัสที่คู่กันบางส่วนแล้ว และคีย์ที่เป็นไปได้ทั้งหมดที่จะใช้ในการเข้ารหัสลับมีทั้งหมด 2^{56} หรือ 7×10^{16} คีย์ การค้นหาว่าคีย์ใดเป็นคีย์ที่แท้จริงที่ใช้ในการเข้ารหัส จะทำโดยการทดลองเข้ารหัสข้อมูลเนื้อแท้ที่ทราบค่าด้วยค่าคีย์ที่เป็นไปได้ ได้ผลลัพธ์แล้วเอามาเปรียบเทียบกับข้อมูลเข้ารหัสที่ทราบค่า ถ้าได้ข้อมูลเข้ารหัสตรงกัน แล้วคีย์ที่ใช้ในการทดลองเข้ารหัสลับคือคีย์ที่แท้จริง แต่ถ้าได้ผลลัพธ์ไม่ตรงกันก็ต้องทำการทดลองเข้ารหัสลับข้อมูลด้วยคีย์อื่น ๆ ต่อไปจนกว่าจะพบคีย์ที่ต้องการ ซึ่งการค้นหาค่าคีย์นี้อาจจะต้องใช้ระยะเวลานานกว่าจะพบคีย์ที่ใช้ในการเข้ารหัสที่แท้จริง ขึ้นอยู่กับความเร็วของเครื่องคอมพิวเตอร์ที่ใช้ในการประมวลผล

แต่อย่างไรก็ตาม เมื่ออัลกอริทึมเดสได้รับการยอมรับให้เป็นมาตรฐานจาก NBS ได้มีนักวิชาการหลายท่าน ได้ทำการตรวจสอบขั้นตอนการทำงานของเดสว่ามีความปลอดภัยเพียงพอหรือไม่ ตัวอย่างเช่น Diffie และ Hellman ได้เสนอความเห็นว่าขนาดความยาว

ของคีย์ที่ใช้ในอัลกอริทึม 56 บิต ยังให้ความปลอดภัยไม่เพียงพอ (รายละเอียดดูจาก (Diffie and Hellman, 1977) และได้แสดงให้เห็นว่า ถ้าใช้วิธีการที่จะค้นหาคีย์แบบไล่เรียง ซึ่งมีคีย์ที่เป็นไปได้ทั้งหมด 2^{56} คีย์ หรือ 7×10^{16} ดังที่ได้กล่าวมาแล้วนั้น และต้องมีการสร้างเครื่องมือพิเศษเพื่อใช้ค้นหาคีย์ จะทำให้หาค้นหาคีย์ที่ต้องการได้ภายในเวลา 1 วัน ซึ่งได้ประมาณค่าใช้จ่ายสำหรับเครื่องมือพิเศษนี้เป็นเงินประมาณ 20 ล้านดอลลาร์ ส่วนทางด้าน NBS ได้จัดให้มีการสัมมนา เกี่ยวกับความเป็นไปได้ในการสร้างเครื่องมือพิเศษใช้สำหรับค้นหาคีย์ (รายละเอียดดู (Meissner, 1976)) ซึ่งประกอบด้วยผู้เชี่ยวชาญด้านต่าง ๆ ได้ประมาณค่าใช้จ่ายของเครื่องมือนี้ประมาณ 72 ล้านดอลล่าร์และจะสามารถสร้างให้เสร็จได้ในภายในปี ค.ศ. 1990 และทางด้านบริษัทไอบีเอ็ม ก็ได้ประมาณค่าใช้จ่ายสำหรับเครื่องมือนี้เป็นเงินมากกว่า 220 ล้านดอลลาร์ ซึ่งการสร้างเครื่องมือนี้จะทำได้ยากมาก ต้องใช้ทรัพยากรต่าง ๆ เป็นจำนวนมาก และจุดนี้คือเหตุผลยืนยันว่าความยาวของคีย์ 56 บิต ยังให้ความปลอดภัยเพียงพอ

แต่อย่างไรก็ตามการพัฒนาทางด้านเทคโนโลยีที่มีความก้าวหน้าขึ้น ได้มีผลกระทบต่ออัลกอริทึมที่ใช้กันอยู่ ความเร็วของคอมพิวเตอร์ได้เพิ่มขึ้นจาก 10 MFLOP (million of floating point operations per second) จนปัจจุบันเป็น GFLOP (a billion of floating point operations per second) นอกจากนี้การประมวลผลแบบขนาน (Parallel Processing) และ การประมวลผลแบบเวคเตอร์ (Vector Processing) ได้รับการพัฒนาให้เป็นจริงมากขึ้น (Cooper, 1989) ดังนั้นโอกาสที่จะพบจุดอ่อนของอัลกอริทึมที่ใช้กันอยู่จะมีมาก และมีความวิตกกังวลว่าอัลกอริทึมที่มีการใช้อยู่ในปัจจุบันจะไม่สามารถป้องกันข้อมูลให้ปลอดภัยได้เพราะอาจจะถูกทำลายได้ จึงมีความจำเป็นจะต้องมีการพัฒนาอัลกอริทึมที่มีอยู่ให้มีประสิทธิภาพมากยิ่งขึ้น หรือต้องมีการสร้างอัลกอริทึมใหม่ที่สามารถป้องกันข้อมูลให้ปลอดภัยได้ดีกว่าของเดิมที่มีอยู่