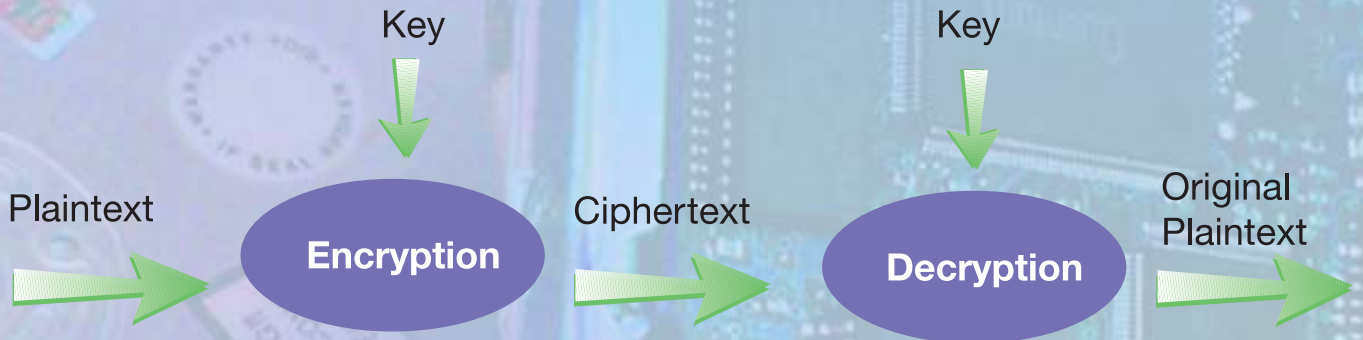


โทรศัพท์เข้ารหัสลับ



เครื่องโทรศัพท์เป็นอุปกรณ์สำหรับติดต่อสื่อสารที่สำคัญอย่างหนึ่งในชีวิตประจำวัน การติดต่อสื่อสารของแต่ละบุคคลก็มีจุดมุ่งหมายแตกต่างกัน เช่น สนทนาระหว่างเพื่อน คู่รัก ธุรกิจ การเมือง การทหาร เป็นต้น ซึ่งแต่ละบุคคลย่อมให้ความสำคัญในความลับของข้อความสนทนาไม่น้อยแตกต่างกันไป แต่ระบบโทรศัพท์ในปัจจุบัน ยังไม่มีการป้องกันการถูกดักฟังได้ดีพอ โดยเฉพาะระบบโทรศัพท์แบบใช้สาย จึงได้มีผู้คิดพัฒนาอุปกรณ์ป้องกันหรือแจ้งเตือนการถูกดักฟังในรูปแบบต่างๆ ขึ้น

วิธีการป้องกันการถูกดักฟังเสียงพูดทางโทรศัพท์วิธีการหนึ่งก็คือการเข้ารหัสลับเสียงพูด (Speech Encryption) ซึ่งหมายถึงกระบวนการเปลี่ยนแปลงข้อมูลเสียงที่สามารถฟังเข้าใจได้ให้อยู่ในรูปแบบที่ไม่สามารถฟังเข้าใจได้โดยใช้อัลกอริทึมทางคณิตศาสตร์ (Digital Ciphering) หากต้องการที่จะฟังเข้าใจข้อมูลเสียงนั้น จำเป็นต้องผ่านกระบวนการถอดรหัสลับเสียงพูด (Speech Decryption) เพื่อแปลงข้อมูลเสียงต้นฉบับนั้นกลับคืนมาทั้งกระบวนการเข้ารหัสลับและถอดรหัสลับนั้น จะต้องมีกำหนดกุญแจรหัส (Key) ที่ทราบกันเฉพาะระหว่างผู้คุยโทรศัพท์ทั้งสองฝ่าย ซึ่งกุญแจรหัสส่วนนี้ส่วนมากจะใช้ค่าตัวเลขจำนวนหลายหลัก และถูกนำมาใช้ใน Digital Ciphering

Digital Ciphering ในปัจจุบันมีอยู่หลายวิธี ได้แก่ DES, TDES, AES, BLOWFISH, IDEA, RSA, LUC เป็นต้น ซึ่งแต่ละวิธีก็จะมีระดับความสามารถในการปกป้องข้อมูลและความเร็วที่ใช้ในการคำนวณที่แตกต่างกัน

โครงการนี้เป็นการสร้างระบบขึ้นมาเพื่อจำลองการทำงานของโทรศัพท์เข้ารหัสลับ โดยใช้เครื่องคอมพิวเตอร์ 2 ชุดทำงานแทนเครื่องโทรศัพท์ของทั้งสองฝ่าย มีการรับส่งเสียงพูดผ่านการ์ดเสียง (Sound Card) และต่อโทรศัพท์โดยใช้โมเด็ม เมื่อต้องการเข้าสู่โหมดของการคุยความลับก็กดปุ่มเฉพาะ 1 ปุ่ม จากนั้นเครื่องคอมพิวเตอร์ของทั้งสองฝ่ายก็จะสร้างกุญแจรหัสและแลกเปลี่ยนระหว่างกันให้โดยอัตโนมัติ หลังจากกระบวนการแลกเปลี่ยนกุญแจรหัสเสร็จสิ้นแล้ว ทั้งสองฝ่ายก็จะเริ่มพูดคุยความลับกันได้

