

การสร้างสมภาคเชิงเส้นในการเข้ารหัสด้วยตัวเลข 10 หลัก Construction of Linear Congruences for Encoding with 10-digit Number

สุภาภรณ์ สดวกดี
Supaporn Saduakdee

สาขาวิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยราชภัฏจันทรเกษม
Program of Mathematics, Faculty of Science, Chandrakasem Rajabhat University
Email: aa_o_rr@hotmail.com

Received: 08 Aug 20

Revised: 21 Sep 20

Accepted: 22 Sep 20

บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อ 1) สร้างสมภาคเชิงเส้นในการเข้ารหัสด้วยตัวเลข 10 หลัก และแสดงเงื่อนไขที่ทำให้เลขโดดในแต่ละหลักของรหัสผลลัพธ์สองรหัสไม่ซ้ำกัน และ 2) แสดงรหัสผลลัพธ์ที่ได้จากสมภาคเชิงเส้นในการเข้ารหัสด้วยตัวเลข 10 หลักที่กำหนด การวิจัยนี้เป็นการวิจัยเชิงทฤษฎี โดยผู้วิจัยจะสร้างทฤษฎีบทและพิสูจน์ทฤษฎีบทเพื่อยืนยันว่าเป็นจริง แล้วสร้างสมภาคเชิงเส้นในการเข้ารหัสจากทฤษฎีบทที่ได้ ซึ่งใช้ความรู้ทางทฤษฎีจำนวนเรื่องสมภาค และสามารถนำผลการวิจัยไปประยุกต์ใช้ให้เกิดประโยชน์ในชีวิตจริง ผลการวิจัยพบว่า สมภาคเชิงเส้นในการเข้ารหัสที่สร้างขึ้น มีตัวแปรอิสระคือ จำนวนหลักของรหัสผลลัพธ์ และเลขโดดในแต่ละหลักของตัวเลข และตัวแปรตามคือ เลขโดดในแต่ละหลักของรหัสผลลัพธ์ และได้เงื่อนไขที่ทำให้เลขโดดในแต่ละหลักของรหัสผลลัพธ์สองรหัสไม่ซ้ำกัน นอกจากนี้ ยังได้รหัสผลลัพธ์จากสมภาคเชิงเส้นในการเข้ารหัสด้วยตัวเลข 10 หลักที่กำหนด และได้รหัสผลลัพธ์จากตัวเลขที่ซ้ำ 1 หลัก ซ้ำ l หลัก ไม่ซ้ำ 1 หลัก และไม่ซ้ำ l หลัก กับตัวเลขที่กำหนด เมื่อ l แทนจำนวนหลักของรหัสผลลัพธ์ ซึ่งผลเป็นไปตามเงื่อนไขที่ได้

คำสำคัญ: สมภาค สมภาคเชิงเส้น การเข้ารหัส

Abstract

Construction of Linear congruences for Encoding with 10-digit Number. the purposes of this research were 1) to construct the linear congruences for encoding with 10-digit numbers and represent the conditions which made the digits in each of the two output codes different and 2) to represent the output codes obtaining from the linear congruences for encoding with the specified 10-digit numbers. This research was theoretical research. The theorem would be constructed and proved to confirm that it was true. Subsequently, the linear congruences were established for encoding from the theorem using congruence, which was the Number Theory method. The results of this research would be utilized for real life. The results found that the linear congruences for encoding had the independent variables, and those were the number of digits of the output code. The digits and the dependent variable that was the digits in each digit of the output code obtained the conditions that made the digits in each of the two output codes different. Moreover, the output codes from the linear congruences for encoding with the specified 10-digit numbers and the output codes from 1 digit identical number, digits identical number, 1 digit different number and digits different number with the specified numbers when represented the number of digits of the output codes obtained.

Keywords: Congruence, Linear Congruence, Encoding

1. บทนำ

การสื่อสาร (Communication) หมายถึงกระบวนการส่งข่าวสารข้อมูลจากผู้ส่งข่าวสารไปยังผู้รับข่าวสาร มีวัตถุประสงค์เพื่อชักจูงให้ผู้รับข่าวสารมีปฏิกิริยาตอบสนองกลับมา โดยคาดหวังให้เป็นไปตามที่ผู้ส่งต้องการ องค์ประกอบหนึ่งของการสื่อสาร คือ การเข้ารหัส (encoding) เป็นการช่วยให้ผู้ส่งข่าวสารและผู้รับข่าวสารมีความเข้าใจตรงกันในการสื่อความหมาย จึงมีความจำเป็นต้องแปลงความหมายนี้ การเข้ารหัสจึงหมายถึงการแปลงข่าวสารให้อยู่ในรูปพลังงานที่พร้อมจะส่งไปในสื่อกลาง ทางผู้ส่งมีความเข้าใจตรงกันระหว่างผู้ส่งและผู้รับ หรือมีรหัสเดียวกัน การสื่อสารจึงเกิดขึ้นได้ กระบวนการสื่อสาร (Communication Process) โดยทั่วไปเริ่มต้นจากผู้ส่งข่าวสาร (Sender) ทำหน้าที่เก็บรวบรวมแนวความคิดหรือข้อมูล จากแหล่งข้อมูลต่างๆ เมื่อต้องการส่งข่าวไปยังผู้รับข่าวสาร ก็จะแปลงแนวความคิดหรือข้อมูลที่เกี่ยวข้องออกมาเป็นตัวอักษรนำเสียง สี การเคลื่อนไหว ฯลฯ ซึ่งเรียกว่าข่าวสาร (Message) จะได้รับการใส่รหัส (Encoding) แล้วส่งไปยังผู้รับข่าวสาร (Receivers) ผ่านสื่อกลาง (Media) ในช่องทางการสื่อสาร (Communication Channels) ประเภทต่าง ๆ หรืออาจจะถูกส่งจากผู้ส่งข่าวสารไปยังผู้รับข่าวสารโดยตรง ผู้รับข่าวสาร เมื่อได้รับข่าวสารแล้วจะถอดรหัส (Decoding) ตามความเข้าใจและประสบการณ์ในอดีต หรือสภาพแวดล้อมในขณะนั้น และมีปฏิกิริยาตอบสนองกลับไปยังผู้ส่งข่าวสาร [1]

เทคโนโลยีการเข้ารหัสหรือวิทยาการการเข้ารหัสนั้นเริ่มเป็นที่รู้จักกันมาตั้งแต่สมัยโรมันพัฒนาจากแนวคิดเกี่ยวกับพื้นฐานในการรักษาความปลอดภัยของข้อมูลอิเล็กทรอนิกส์และพัฒนาเรื่อยมาจนถึงปัจจุบัน ซึ่งกลายเป็นกระบวนการทางคณิตศาสตร์ในการเข้ารหัส โดยการสร้างสิ่งที่อยู่ในรูปตัวอักษร อักขระ ตัวเลข หรือสัญลักษณ์ใด ๆ ขึ้นมา และเรียกสิ่งนั้นว่า กุญแจ (key) และใช้กุญแจเป็นกลไกสำคัญในการเข้ารหัสและถอดรหัส [2] ดังนั้น การที่มีการเข้ารหัสที่หลากหลายรูปแบบจึงมีความจำเป็นสำหรับการเลือกใช้งานได้อย่างเหมาะสมและหลากหลาย รวมถึงเมื่อต้องการใช้การเข้ารหัสในการสื่อสารที่มีความซับซ้อนเพื่อเพิ่มความน่าเชื่อถือในเรื่องความปลอดภัยของข้อมูล ยังสามารถเลือกใช้การเข้ารหัสหลาย ๆ รูปแบบประกอบกันได้

จากความจำเป็นของการเข้ารหัสดังกล่าว ผู้วิจัยจึงสนใจที่จะศึกษากระบวนการทางคณิตศาสตร์ในการเข้ารหัส โดยการสร้างสมภาคเชิงเส้นในการเข้ารหัส เพื่อนำเสนอรูปแบบการเข้ารหัสอีกรูปแบบหนึ่งที่เป็นประโยชน์ในการสื่อสาร และเพื่อให้ได้การเข้ารหัสจากสมภาคเดียวกันอย่างเป็นระบบ รวมถึงนำไปประยุกต์ใช้ในการแก้ปัญหาต่าง ๆ ได้ โดยมีวัตถุประสงค์ คือ 1) เพื่อสร้างสมภาคเชิงเส้นในการเข้ารหัสด้วยตัวเลข 10 หลัก และแสดงเงื่อนไขที่ทำให้เลขโดดในแต่ละหลักของรหัสผลลัพธ์สองรหัสไม่ซ้ำกัน และ 2) เพื่อแสดงรหัสผลลัพธ์ที่ได้จากสมภาคเชิงเส้นในการเข้ารหัส

ด้วยตัวเลข 10 หลักที่กำหนด สำหรับขอบเขตของการวิจัย ผู้วิจัยจะศึกษาการสร้างสมภาคเชิงเส้นในการเข้ารหัสด้วยตัวเลข 10 หลัก ที่ทำให้ได้รหัสผลลัพธ์ 10 หลัก 8 หลัก 6 หลัก และ 4 หลัก โดยใช้ความรู้ในวิชาทฤษฎีจำนวนเรื่องสมภาค และให้นิยามศัพท์เฉพาะ ดังนี้

ตัวเลข 10 หลัก หมายถึง ตัวเลข 10 ตัวเรียงกันโดยที่ตัวเลขแต่ละหลักได้จากเลขโดด 0-9 และอาจซ้ำกันได้

ตัวเลข 10 หลักที่กำหนด หมายถึง ตัวเลข 10 หลักชุดใดชุดหนึ่งที่ผู้วิจัยกำหนดขึ้น

รหัสผลลัพธ์ หมายถึง รหัส 10 หลัก 8 หลัก 6 หลัก และ 4 หลัก ที่ได้จากสมภาคเชิงเส้นที่ผู้วิจัยสร้างขึ้นโดยการแทนค่าเลขโดดจากตัวเลข 10 หลัก

สมภาคเชิงเส้นในการเข้ารหัส หมายถึง สมภาคเชิงเส้นที่ผู้วิจัยสร้างขึ้นเพื่อใช้ในการเข้ารหัสด้วยตัวเลข 10 หลัก ที่ทำให้ได้รหัสผลลัพธ์

ผู้วิจัยได้ศึกษาบทนิยาม ทฤษฎีบทเกี่ยวกับสมภาค และงานวิจัยที่เกี่ยวข้อง ดังนี้

บทนิยาม ให้ a และ b เป็นจำนวนเต็ม และ m เป็นจำนวนเต็มบวก จะกล่าวว่า a สมภาค (congruence) กับ b มอดุโล m ก็ต่อเมื่อ $m \mid (a-b)$ เขียนแทนด้วย $a \equiv b \pmod{m}$

สัญลักษณ์ (a, b) แทน ตัวหารร่วมมากของ a และ b

ทฤษฎีบท 1.1 ให้ a, b และ c เป็นจำนวนเต็ม และ m เป็นจำนวนเต็มบวก จะได้ว่า

ถ้า $a \equiv b \pmod{m}$ แล้ว $ac \equiv bc \pmod{m}$

ทฤษฎีบท 1.2 ให้ a, b และ c เป็นจำนวนเต็ม และ m เป็นจำนวนเต็มบวก จะได้ว่า

ถ้า $ab \equiv ac \pmod{m}$ และ $(a, m) = 1$

แล้ว $b \equiv c \pmod{m}$

ในปี พ.ศ. 2553 คมสัน สิงห์ศิริยุทธ [3] ได้ยกตัวอย่างการนำทฤษฎีจำนวนไปประยุกต์ใช้แก้ปัญหาต่าง ๆ ดังนี้ RSA Encryption เป็นการเข้ารหัสข้อมูลที่ดีวิธีหนึ่ง ซึ่งเป็นที่นิยมนำมาใช้ในการเข้ารหัสข้อมูลที่สำคัญผ่านเครือข่ายอิเล็กทรอนิกส์ และได้รับความน่าเชื่อถือในเรื่องความปลอดภัยของข้อมูลสูง การเข้ารหัสข้อมูลแบบ RSA Encryption มีขั้นตอนดังนี้

1. สร้างกุญแจสาธารณะ (public key) คือ n, e และกุญแจส่วนตัว (private key) คือ n, d

2. สร้างสมการการเข้ารหัสข้อมูล (encryption) คือ

$$C = M^e \pmod{n} \text{ หรือ } C = M^d \pmod{n}$$

3. สร้างสมการการถอดรหัสข้อมูล (decryption) คือ

$$M = C^d \pmod{n} \text{ หรือ } M = C^e \pmod{n}$$

โดยที่ M เป็น Plain Text และ C เป็น Cipher Text

อีกตัวอย่างที่น่าสนใจคือ กำหนดให้ผู้ใช้อคอมพิวเตอร์จะต้องมีรหัสผ่าน (password) มีความยาวตั้งแต่ 6 ถึง 8 โดยที่ตัวอักษรแต่ละตัวสามารถเป็นตัวอักษรภาษาอังกฤษ (A-Z; a-z) หรือตัวเลข (0-9) และจะต้องมีตัวเลขอย่างน้อยหนึ่งตัว จะได้ จำนวนรหัสผ่านของผู้ใช้ที่เป็นไปได้ทั้งหมด คือ

$$P = P_6 + P_7 + P_8$$

โดยที่ P_6 , P_7 และ P_8 แทน จำนวนรหัสผ่านของผู้ใช้งานที่มีความยาวเท่ากับ 6, 7 และ 8 ตามลำดับ

ในปี พ.ศ. 2555 ปรัชญา ไชยเมือง, สุชาติ คุ่มมะณี และสมนึก พ่วงพรพิทักษ์ [4] ได้ออกแบบ BASE64 S/Key OTP ที่มีฐานการสร้าง OTP แบบ S/Key และใช้การแปลงรหัสแบบ BASE64 นอกจากนี้ BASE64 S/KEY OTP ยังได้เปรียบเทียบการทำงาน กับ S/Key OTP, HOTP และ TOTP ผลการประเมินชี้ให้เห็นถึงประสิทธิภาพที่เพิ่มขึ้นจากการใช้ BASE64 S/KEY OTP

ในปี พ.ศ. 2558 อรรถพล สุวรรณษา และคณะ [5] ได้เสนอการวิเคราะห์ปัญหาของ OTP และเสนอการปรับปรุงอัลกอริทึมของ OTP นอกจากนี้ ยังได้พัฒนา Mobile OTP ร่วมกับระบบ Web Service ที่สนับสนุน OTP สุดท้ายนี้ ได้มีการทดสอบและประเมินผลประสิทธิภาพของระบบที่ออกแบบและพัฒนา พบว่า สามารถทำงานได้อย่างมีประสิทธิภาพและเป็นที่น่าพึงพอใจ

ในปี พ.ศ. 2561 ธันยชนก เกตุพิทยา [6] ได้ศึกษาการรับรู้ประโยชน์ของรหัสผ่าน การรับรู้ความยากง่ายในการใช้งานรหัสผ่าน และทัศนคติต่อการตั้งรหัสผ่านที่มีผลต่อการตัดสินใจใช้รหัสผ่านที่ปลอดภัยของพนักงานบริษัทเอกชนในตลาดหลักทรัพย์ พบว่า มีผลต่อการตัดสินใจใช้รหัสผ่านที่ปลอดภัยของพนักงานบริษัทเอกชนในตลาดหลักทรัพย์อย่างมีนัยสำคัญทางสถิติ ที่ระดับ 0.05

จากงานวิจัยที่ศึกษา ผู้วิจัยจะศึกษาการสร้างรหัสผลลัพธ์ 10 หลัก 8 หลัก 6 หลัก และ 4 หลัก จากตัวเลข 10 หลักโดยใช้สมภาคเชิงเส้น และแสดงเงื่อนไขที่ทำให้เลขโดดในแต่ละหลักของรหัสผลลัพธ์สองรหัสไม่ซ้ำกัน นอกจากนี้ ผู้วิจัยจะแสดงรหัสผลลัพธ์โดยการแทนค่าเลขโดดจากตัวเลข 10 หลักที่กำหนดลงในสมภาคเชิงเส้นในการเข้ารหัสที่สร้างขึ้น โดยแสดงรหัสผลลัพธ์ 10 หลัก 8 หลัก 6 หลัก หรือ 4 หลักที่ได้จากตัวเลข 10 หลักที่กำหนด และรหัสผลลัพธ์ที่ได้จากตัวเลขที่ซ้ำและไม่ซ้ำกับตัวเลขที่กำหนด

2. วิธีการวิจัย

การวิจัยนี้เป็นการวิจัยเชิงทฤษฎี โดยผู้วิจัยจะสร้างทฤษฎีบทและพิสูจน์ทฤษฎีบทเพื่อยืนยันว่าเป็นจริง แล้วสร้างสมภาคเชิงเส้นในการเข้ารหัสจากทฤษฎีบทที่ได้ ซึ่งใช้ความรู้ทางทฤษฎีจำนวนเรื่องสมภาค และสามารถนำผลการวิจัยไป

ประยุกต์ใช้ให้เกิดประโยชน์ในชีวิตจริง ซึ่งมีวิธีดำเนินการวิจัยดังนี้

- 2.1 ศึกษาเอกสารความรู้เรื่องสมภาค
- 2.2 ศึกษางานวิจัยเกี่ยวกับการเข้ารหัส
- 2.3 ตั้งข้อคาดการณ์และวิเคราะห์ผลโดยการพิสูจน์เพื่อยืนยันว่าข้อคาดการณ์เป็นจริง
- 2.4 สร้างสมภาคเชิงเส้นในการเข้ารหัสด้วยตัวเลข 10 หลัก
- 2.5 แสดงเงื่อนไขที่ทำให้เลขโดดในแต่ละหลักของรหัสผลลัพธ์สองรหัสไม่ซ้ำกัน
- 2.6 แสดงรหัสผลลัพธ์โดยการแทนค่าเลขโดดจากตัวเลข 10 หลักลงในสมภาคเชิงเส้นในการเข้ารหัสที่สร้างขึ้น
- 2.7 ตรวจสอบความถูกต้องของผลสรุปที่ได้ และเรียงลำดับเนื้อหาให้สอดคล้องกัน

3. ผลการวิจัย

3.1 สมภาคเชิงเส้นในการเข้ารหัสด้วยตัวเลข 10 หลัก และเงื่อนไขที่ทำให้เลขโดดในแต่ละหลักของรหัสผลลัพธ์สองรหัสไม่ซ้ำกัน

เริ่มต้นผู้วิจัยได้สร้างทฤษฎีบทสำคัญและพิสูจน์ทฤษฎีบทเพื่อยืนยันว่าเป็นจริง เพื่อนำไปสู่การสร้างสมภาคเชิงเส้นในการเข้ารหัสด้วยตัวเลข 10 หลัก สองชุดใดๆ ที่ไม่ซ้ำกัน ซึ่งทำให้ได้รหัสผลลัพธ์สองรหัสที่ไม่ซ้ำกันด้วยดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 3.1 กำหนดให้ $n, n' \in \{0, 1, \dots, 9\}$, $c \in \mathbb{Z}$,
 $p \equiv cn \pmod{10}$ และ $p' \equiv cn' \pmod{10}$
 ถ้า $c \equiv 3 \pmod{10}$ หรือ $c \equiv 7 \pmod{10}$ หรือ $c \equiv 9 \pmod{10}$ แล้ว $p \neq p'$ ก็ต่อเมื่อ $n \neq n'$
พิสูจน์ ให้ $c \equiv 3 \pmod{10}$ หรือ $c \equiv 7 \pmod{10}$ หรือ $c \equiv 9 \pmod{10}$
 $(\Rightarrow)$ สมมติ $n = n'$
 นั่นคือ $n - n' = 0$
 จะได้ $10 | (n - n')$
 จะได้ว่า $n \equiv n' \pmod{10}$
 จากทฤษฎีบท 1.1 จะได้ $cn \equiv cn' \pmod{10}$
 นั่นคือ $p \equiv p' \pmod{10}$
 จะได้ $10 | (p - p')$
 เนื่องจาก $p \equiv cn \pmod{10}$ และ $p' \equiv cn' \pmod{10}$

จะได้ $p, p' \in \{0, 1, \dots, 9\}$

เนื่องจาก $10 \mid (p - p')$ จะได้ $p - p' = 0$

ดังนั้น $p = p'$

($\Leftarrow$) สมมติ $p = p'$

นั่นคือ $p - p' = 0$

จะได้ $10 \mid (p - p')$

จะได้ว่า $p \equiv p' \pmod{10}$

นั่นคือ $cn \equiv cn' \pmod{10}$

เนื่องจาก $c \equiv 3 \pmod{10}$ หรือ

$c \equiv 7 \pmod{10}$ หรือ $c \equiv 9 \pmod{10}$

จะได้ $(c, 10) = 1$

จากทฤษฎีบท 1.2 จะได้ $n \equiv n' \pmod{10}$

จะได้ว่า $10 \mid (n - n')$

เนื่องจาก $n, n' \in \{0, 1, \dots, 9\}$ จะได้

$$n - n' = 0$$

ดังนั้น $n = n'$

ผู้วิจัยสร้างสมภาคเชิงเส้นในการเข้ารหัสด้วยตัวเลข 10 หลัก เพื่อให้ได้รหัสผลลัพธ์ 10 หลัก 8 หลัก 6 หลัก และ 4 หลัก โดยสมภาค 1 อยู่ในพจน์ของ $n_{5-\frac{l}{2}+i}$ และสมภาค 2

อยู่ในพจน์ของ $n_{6+\frac{l}{2}-i}$ ดังนี้

สมภาค 1

$$p_i \equiv cn_{5-\frac{l}{2}+i} \pmod{10}$$

เมื่อ l แทน จำนวนหลักของรหัสผลลัพธ์ โดยที่ $l = 10, 8, 6$ หรือ 4

p_i แทน เลขโดดในหลักที่ i ของรหัสผลลัพธ์ สำหรับทุก $i = 1, 2, \dots, l$

$n_{5-\frac{l}{2}+i}$ แทน เลขโดดในหลักที่ $5 - \frac{l}{2} + i$ ของตัวเลข สำหรับทุก $i = 1, 2, \dots, 10$

c แทน จำนวนเต็มซึ่ง $c \equiv 3 \pmod{10}$ หรือ $c \equiv 7 \pmod{10}$ หรือ $c \equiv 9 \pmod{10}$

สมภาค 2

$$p_i \equiv cn_{6+\frac{l}{2}-i} \pmod{10}$$

เมื่อ l แทน จำนวนหลักของรหัสผลลัพธ์ โดยที่ $l = 10, 8, 6$ หรือ 4

p_i แทน เลขโดดในหลักที่ i ของรหัสผลลัพธ์ สำหรับทุก $i = 1, 2, \dots, l$

$n_{6+\frac{l}{2}-i}$ แทน เลขโดดในหลักที่ $6 + \frac{l}{2} - i$ ของตัวเลข

สำหรับทุก $i = 1, 2, \dots, 10$

c แทน จำนวนเต็มซึ่ง $c \equiv 3 \pmod{10}$ หรือ $c \equiv 7 \pmod{10}$ หรือ $c \equiv 9 \pmod{10}$

จากสมภาคเชิงเส้นในการเข้ารหัส ทั้งสมภาค 1 และ สมภาค 2 และจากทฤษฎีบท 3.1 ทำให้ได้เงื่อนไขที่ทำให้ เลขโดดในแต่ละหลักของรหัสผลลัพธ์สองรหัสไม่ซ้ำกัน ดังบทแทรกต่อไปนี้

บทแทรก 3.2 กำหนดให้ $l = 10, 8, 6, 4$ สำหรับทุก

$i = 1, 2, \dots, l$ ให้ $n_{5-\frac{l}{2}+i}, n'_{5-\frac{l}{2}+i} \in \{0, 1, \dots, 9\}$ และ

$c \in \mathbb{Z}$ ซึ่ง $c \equiv 3 \pmod{10}$ หรือ $c \equiv 7 \pmod{10}$ หรือ $c \equiv 9 \pmod{10}$ จะได้ว่า

$$p_i \neq p'_i \text{ ก็ต่อเมื่อ } n_{5-\frac{l}{2}+i} \neq n'_{5-\frac{l}{2}+i}$$

บทแทรก 3.3 กำหนดให้ $l = 10, 8, 6, 4$ สำหรับทุก

$i = 1, 2, \dots, l$ ให้ $n_{6+\frac{l}{2}-i}, n'_{6+\frac{l}{2}-i} \in \{0, 1, \dots, 9\}$ และ

$c \in \mathbb{Z}$ ซึ่ง $c \equiv 3 \pmod{10}$ หรือ $c \equiv 7 \pmod{10}$ หรือ $c \equiv 9 \pmod{10}$ จะได้ว่า

$$p_i \neq p'_i \text{ ก็ต่อเมื่อ } n_{6+\frac{l}{2}-i} \neq n'_{6+\frac{l}{2}-i}$$

เนื่องจากสมภาค 1 และ 2 มีค่าคงตัว c โดยที่ c แทนจำนวนเต็มซึ่ง $c \equiv 3 \pmod{10}$ หรือ $c \equiv 7 \pmod{10}$ หรือ $c \equiv 9 \pmod{10}$ ดังนั้นสามารถแทนค่า c ที่เป็นไปตามเงื่อนไขได้หลายค่า ผู้วิจัยจึงนำเสนอสมภาคเชิงเส้นในการเข้ารหัสจากการแทนค่า c ทั้งหมด 12 แบบ โดยแทนค่า c ด้วยพจน์ของ i ในสมภาค 1 และ 2 ดัง Table 1 ซึ่งพบว่า เมื่อพิจารณา $c \equiv 3 \pmod{10}$ จะได้ p_i ที่ได้จากแบบ (1.1) และ (1.2) มีค่าเท่ากัน และ p_i ที่ได้จากแบบ (2.1) และ (2.2) มีค่าเท่ากัน เมื่อพิจารณา $c \equiv 7 \pmod{10}$ จะได้ p_i ที่ได้จากแบบ (1.3) และ (1.4) มีค่าเท่ากัน และ p_i ที่ได้จากแบบ (2.3) และ (2.4) มีค่าเท่ากัน และเมื่อพิจารณา $c \equiv 9 \pmod{10}$ จะได้ p_i ที่ได้จากแบบ (1.5) และ (1.6) มีค่าเท่ากัน และ p_i ที่ได้จากแบบ (2.5) และ (2.6) มีค่าเท่ากัน สำหรับทุก $i = 1, 2, \dots, l$

Table 1 Linear congruences for encoding by replacing C to the term of i

C	congruence 1	congruence 2
	(1.1) $p_i \equiv (10i + 3)n_{5-\frac{l}{2}+i} \pmod{10}$	(2.1) $p_i \equiv (10i + 3)n_{6+\frac{l}{2}-i} \pmod{10}$
$c \equiv 3 \pmod{10}$	(1.2) $p_i \equiv \begin{cases} (5i + 8)n_{5-\frac{l}{2}+i} \pmod{10}; \\ i \text{ เป็นจำนวนคี่} \\ (5i + 3)n_{5-\frac{l}{2}+i} \pmod{10}; \\ i \text{ เป็นจำนวนคู่} \end{cases}$	(2.2) $p_i \equiv \begin{cases} (5i + 8)n_{6+\frac{l}{2}-i} \pmod{10}; \\ i \text{ เป็นจำนวนคี่} \\ (5i + 3)n_{6+\frac{l}{2}-i} \pmod{10}; \\ i \text{ เป็นจำนวนคู่} \end{cases}$
	(1.3) $p_i \equiv (10i + 7)n_{5-\frac{l}{2}+i} \pmod{10}$	(2.3) $p_i \equiv (10i + 7)n_{6+\frac{l}{2}-i} \pmod{10}$
$c \equiv 7 \pmod{10}$	(1.4) $p_i \equiv \begin{cases} (5i + 12)n_{5-\frac{l}{2}+i} \pmod{10}; \\ i \text{ เป็นจำนวนคี่} \\ (5i + 7)n_{5-\frac{l}{2}+i} \pmod{10}; \\ i \text{ เป็นจำนวนคู่} \end{cases}$	(2.4) $p_i \equiv \begin{cases} (5i + 12)n_{6+\frac{l}{2}-i} \pmod{10}; \\ i \text{ เป็นจำนวนคี่} \\ (5i + 7)n_{6+\frac{l}{2}-i} \pmod{10}; \\ i \text{ เป็นจำนวนคู่} \end{cases}$
	(1.5) $p_i \equiv (10i + 9)n_{5-\frac{l}{2}+i} \pmod{10}$	(2.5) $p_i \equiv (10i + 9)n_{6+\frac{l}{2}-i} \pmod{10}$
$c \equiv 9 \pmod{10}$	(1.6) $p_i \equiv \begin{cases} (5i + 14)n_{5-\frac{l}{2}+i} \pmod{10}; \\ i \text{ เป็นจำนวนคี่} \\ (5i + 9)n_{5-\frac{l}{2}+i} \pmod{10}; \\ i \text{ เป็นจำนวนคู่} \end{cases}$	(2.6) $p_i \equiv \begin{cases} (5i + 14)n_{6+\frac{l}{2}-i} \pmod{10}; \\ i \text{ เป็นจำนวนคี่} \\ (5i + 9)n_{6+\frac{l}{2}-i} \pmod{10}; \\ i \text{ เป็นจำนวนคู่} \end{cases}$

3.2 รหัสผลลัพธ์ที่ได้จากสมภาคเชิงเส้นในการเข้ารหัสด้วยตัวเลข 10 หลักที่กำหนด

สำหรับ $l=10,8,6,4$ ผู้วิจัยจะแสดงรหัสผลลัพธ์ l หลัก โดยการแทนค่าเลขโดดจากตัวเลข 10 หลักที่กำหนดลงในสมภาค 1 และ 2 โดยกำหนด C ที่ใช้ในสมภาคดังกล่าว 7 แบบ ดังนี้

แบบที่ 1 ใช้ $c \equiv 3 \pmod{10}$

สำหรับหลักที่ $1,2,\dots,l$ ของรหัสผลลัพธ์

แบบที่ 2 ใช้ $c \equiv 7 \pmod{10}$

สำหรับหลักที่ $1,2,\dots,l$ ของรหัสผลลัพธ์

แบบที่ 3 ใช้ $c \equiv 9 \pmod{10}$

สำหรับหลักที่ $1,2,\dots,l$ ของรหัสผลลัพธ์

แบบที่ 4 ใช้ $c \equiv 3 \pmod{10}$

สำหรับหลักที่ $1,3,\dots,k$ ของรหัสผลลัพธ์ และ
ใช้ $c \equiv 7 \pmod{10}$

สำหรับหลักที่ $2,4,\dots,l$ ของรหัสผลลัพธ์

เมื่อ $k < l$

แบบที่ 5 ใช้ $c \equiv 9 \pmod{10}$

สำหรับหลักที่ $1,3,\dots,k$ ของรหัสผลลัพธ์ และ
ใช้ $c \equiv 3 \pmod{10}$

สำหรับหลักที่ $2,4,\dots,l$ ของรหัสผลลัพธ์

เมื่อ $k < l$

แบบที่ 6 ใช้ $c \equiv 7 \pmod{10}$
 สำหรับหลักที่ $1, 3, \dots, k$ ของรหัสผลลัพธ์ และ
 ใช้ $c \equiv 9 \pmod{10}$
 สำหรับหลักที่ $2, 4, \dots, l$ ของรหัสผลลัพธ์
 เมื่อ $k < l$
 แบบที่ 7 ใช้ $c \equiv 3 \pmod{10}$
 สำหรับหลักที่ $1, 4, \dots, k$ ของรหัสผลลัพธ์
 ใช้ $c \equiv 7 \pmod{10}$
 สำหรับหลักที่ $2, 5, \dots, k$ ของรหัสผลลัพธ์ และ
 ใช้ $c \equiv 9 \pmod{10}$
 สำหรับหลักที่ $3, 6, \dots, k$ ของรหัสผลลัพธ์
 เมื่อ $k \leq l$

จากการใช้สมภาค 1 และ 2 โดยกำหนดค่า c ทั้ง
 7 แบบ ดังนั้น ตัวเลขแต่ละตัวเลขจะทำให้ได้รหัสผลลัพธ์
 ที่แตกต่างกัน 14 รหัส

นอกจากนี้ จะแสดงรหัสผลลัพธ์ที่ได้จากตัวเลขที่ซ้ำ
 1 หลักให้เป็นหลักที่ $6 - \frac{l}{2}$ ซ้ำ l หลัก ให้เป็นหลักที่
 $6 - \frac{l}{2}$ ถึง $5 + \frac{l}{2}$ ไม่ซ้ำ 1 หลัก ให้เป็นหลักที่ $6 - \frac{l}{2}$ ไม่
 ซ้ำ l หลัก ให้เป็นหลักที่ $6 - \frac{l}{2}$ ถึง $5 + \frac{l}{2}$ กับตัวเลขที่
 กำหนด เพื่อยืนยันว่ารหัสผลลัพธ์ที่ได้เป็นไปตามบทแทรก 3.2
 และ 3.3 โดยตัวเลข 10 หลักที่กำหนด คือ 6742813950 และ
 เลขโดดในตัวเลข 10 หลักที่ขีดเส้นใต้แสดงถึงเลขโดดในหลักที่
 ซ้ำกับตัวเลข 6742813950 ดังต่อไปนี้

Table 2 The 10-digit output codes obtaining from the linear congruences for encoding with the 10-digit numbers

Pattern	10-digit Number	Output code from the congruence 1	Output code from the congruence 2	Pattern	10-digit Number	Output code from the congruence 1	Output code from the congruence 2
1	6742813950	8126439750	0579346218	5	6742813950	4166237750	0519948238
	6305924718	8905762134	4312675098		6305924718	4905166194	2332875078
	6742813950	8126439750	0579346218		6742813950	4166237750	0519948238
	4742813950	2126439750	0579346212		4742813950	6166237750	0519948232
	4370561829	2910583467	7643850192		4370561829	6930589487	1623450172
2	6742813950	2984671350	2984671350	6	6742813950	2388691150	2587621654
	6305924718	2105348976	6798435012		6305924718	2705388372	6996415014
	6742813950	2984671350	2984671350		6742813950	2388691150	2587621654
	4742813950	8984671350	0531764898		4742813950	8388691150	0537724696
	4370561829	8190527643	3467250918		4370561829	8790547241	3869250316
3	6742813950	4368297150	0517928634	7	6742813950	8966699350	0919626338
	6305924718	4705186392	2936815074		6305924718	8105382994	4732415078
	6742813950	4368297150	0517928634		6742813950	8966699350	0919626338
	4742813950	6368297150	0517928636		4742813950	2966699350	0519726832
	4370561829	6730549281	1829450376		4370561829	2130543687	7423250972
4	6742813950	8924479350	0974376310				
	6305924718	8105742936	4718635092				
	6742813950	8924479350	0974376310				
	4742813950	2924479350	0571366818				
	4370561829	2110523663	7447850998				

Table 3 The 8-digit output codes obtaining from the linear congruences for encoding with the 10-digit numbers

Pattern	10-digit Number	Output code from the congruence 1	Output code from the congruence 2	Pattern	10-digit Number	Output code from the congruence 1	Output code from the congruence 2
1	6742813950	12643975	57934621	5	6742813950	32849915	57732661
	2716904583	13870254	45207831		2716904583	33470254	25601891
	0742813956	12643975	57934621		0742813956	32849915	57732661
	6342813950	92643975	57934629		6342813950	72849915	57732669
	6215794380	63517294	49271536		6215794380	83511274	29673596
2	6742813950	98467135	53176489	6	6742813950	96427735	51196883
	2716904583	97230856	65803279		2716904583	99210652	65803473
	0742813956	98467135	53176489		0742813956	96427735	51196883
	6342813950	18467135	53176481		6342813950	16427735	51196887
	6215794380	47593816	61839574		6215794380	49533612	67819578
3	6742813950	36829715	51792863	7	6742813950	18847775	53736829
	2716904583	39410652	25601493		2716904583	17470656	45603439
	0742813956	36829715	51792863		0742813956	18847775	53736829
	6342813950	76829715	51792867		6342813950	98847775	53736821
	6215794380	89531672	27613598		6215794380	67513696	41679534
4	6742813950	18663175	53974429				
	2716904583	17830856	45207239				
	0742813956	18663175	53974429				
	6342813950	98663175	53974421				
	6215794380	67597896	41231534				

Table 4 The 6-digit output codes obtaining from the linear congruences for encoding with the 10-digit numbers

Pattern	10-digit Number	Output code from the congruence 1	Output code from the congruence 2	Pattern	10-digit Number	Output code from the congruence 1	Output code from the congruence 2
1	6742813950	264397	793462	5	6742813950	662377	199482
	7543120689	293608	806392		7543120689	699608	408372
	5642813907	264397	793462		5642813907	662377	199482
	6792813950	764397	793467		6792813950	162377	199487
	6719284350	376429	924673		6719284350	978469	722613
2	6742813950	846713	317648	6	6742813950	886911	377246
	7543120689	817402	204718		7543120689	877804	204916
	5642813907	846713	317648		5642813907	886911	377246
	6792813950	346713	317643		6792813950	386911	377241
	6719284350	734681	186437		6719284350	714287	166839
3	6742813950	682971	179286	7	6742813950	242311	719446
	7543120689	679804	408976		7543120689	219604	808316
	5642813907	682971	179286		5642813907	242311	719446
	6792813950	182971	179281		6792813950	742311	719441
	6719284350	918267	762819		6719284350	338487	982639
4	6742813950	244793	713668				
	7543120689	213402	806798				
	5642813907	244793	713668				
	6792813950	744793	713663				
	6719284350	336621	984477				

Table 5 The 4-digit output codes obtaining from the linear congruences for encoding with the 10-digit numbers

Pattern	10-digit Number	Output code from the congruence 1	Output code from the congruence 2	Pattern	10-digit Number	Output code from the congruence 1	Output code from the congruence 2
1	6742813950	6439	9346	5	6742813950	8499	7326
	3592681407	6843	3486		3592681407	8823	9446
	5092813764	6439	9346		5092813764	8499	7326
	6746813950	8439	9348		6746813950	4499	7328
	6741382950	3946	6493		6741382950	9926	8473
2	6742813950	4671	1764	6	6742813950	4277	1968
	3592681407	4267	7624		3592681407	4469	7228
	5092813764	4671	1764		5092813764	4277	1968
	6746813950	2671	1762		6746813950	2277	1964
	6741382950	7164	4617		6741382950	7768	4219
3	6742813950	8297	7928	7	6742813950	6699	9726
	3592681407	8429	9248		3592681407	6223	3646
	5092813764	8297	7928		5092813764	6699	9726
	6746813950	4297	7924		6746813950	8699	9728
	6741382950	9728	8279		6741382950	3126	6673
4	6742813950	6631	9744				
	3592681407	6247	3684				
	5092813764	6631	9744				
	6746813950	8631	9742				
	6741382950	3144	6697				

จาก Tables 2, 3, 4 และ 5 พบว่า สามารถสร้างรหัสผลลัพธ์ 10 หลัก 8 หลัก 6 หลัก และ 4 หลักจากสมภาคเชิงเส้นในการเข้ารหัสด้วยตัวเลข 10 หลักที่กำหนด จากสมภาค 1 และ 2 และค่า C ทั้ง 7 แบบ นอกจากนี้ สำหรับ

$l=10,8,6,4$ ตัวเลข l หลักที่ซ้ำหลักที่ $6-\frac{l}{2}$ ซ้ำหลักที่

$6-\frac{l}{2}$ ถึง $5+\frac{l}{2}$ ไม่ซ้ำหลักที่ $6-\frac{l}{2}$ และไม่ซ้ำหลักที่

$6-\frac{l}{2}$ ถึง $5+\frac{l}{2}$ กับตัวเลขที่กำหนด ทำให้ได้รหัสผลลัพธ์

l หลัก จากสมภาค 1 ที่ซ้ำหลักที่ 1 ซ้ำหลักที่ 1 ถึง l ไม่ซ้ำหลักที่ 1 และไม่ซ้ำหลักที่ 1 ถึง l กับรหัสผลลัพธ์ที่ได้จากตัวเลขที่กำหนด และได้รหัสผลลัพธ์ l หลัก จากสมภาค 2 ที่ซ้ำหลักที่ l ซ้ำหลักที่ 1 ถึง l ไม่ซ้ำหลักที่ l และไม่ซ้ำหลักที่ 1 ถึง l กับรหัสผลลัพธ์ที่ได้จากตัวเลขที่กำหนด ตามลำดับซึ่งเป็นไปตามบทแทรก 3.2 และ 3.3

4. สรุปและอภิปรายผล

4.1 จากสมภาคเชิงเส้นในการเข้ารหัสที่ผู้วิจัยสร้างขึ้น ทำให้ทราบที่มาของรหัสผลลัพธ์อย่างเป็นระบบ โดยตัวเลข 10 หลักแต่ละชุด จะทำให้ได้รหัสผลลัพธ์ 10 หลัก 8 หลัก 6 หลัก และ 4 หลัก และแต่ละสมภาคทำให้ได้รหัสผลลัพธ์ที่แตกต่างกันเป็นจำนวนมาก ซึ่งรหัสผลลัพธ์ที่ต่างกันเหล่านี้ก็มีที่มาจากสมภาคเดียวกัน

4.2 ในการสร้างรหัสผลลัพธ์ 10 หลัก 8 หลัก 6 หลัก และ 4 หลัก จะได้รหัสที่แตกต่างกันทั้งหมด 10,000,000,000 รหัส 100,000,000 รหัส 1,000,000 รหัส และ 10,000 รหัส ตามลำดับ ซึ่งสมภาคเชิงเส้นในการเข้ารหัสที่ผู้วิจัยสร้างขึ้น ทำให้ได้รหัสที่แตกต่างกันครบทั้งหมด เพื่อให้สามารถนำรหัสผลลัพธ์ไปใช้ได้มากที่สุด

4.3 จากสมภาคเชิงเส้นในการเข้ารหัส ทั้งสมภาค 1 และ 2 ที่ผู้วิจัยสร้างขึ้น ทำให้ได้ว่า ตัวเลข 10 หลัก สองชุดใด ๆ ที่ไม่ซ้ำกัน จะทำให้ได้เลขโดดในแต่ละหลักของรหัสผลลัพธ์สองรหัสที่ไม่ซ้ำกันด้วยตามเงื่อนไขดังบทแทรก 3.2 และ 3.3

4.4 เนื่องจากข้อความที่ต้องการสื่อสารอาจอยู่ในรูปของตัวอักษร อักขระ หรือสัญลักษณ์ ดังนั้น อาจแปลงตัวอักษร อักขระ หรือสัญลักษณ์ ให้อยู่ในรูปของตัวเลข แล้วใช้สมภาคเชิงเส้นในการเข้ารหัส และเพื่อเพิ่มความซับซ้อนในการเข้ารหัส อาจใช้การเข้ารหัสหลาย ๆ รูปแบบประกอบกัน เช่น ใช้การเข้ารหัสในรูปแบบอื่นก่อน แล้วจึงใช้สมภาคเชิงเส้นในการเข้ารหัส หรือใช้สมภาคเชิงเส้นในการเข้ารหัสก่อน แล้วจึงใช้การเข้ารหัสในรูปแบบอื่น เป็นต้น

5. References

- [1] Composition of communication.
<https://sites.google.com/site/it504249220/xngkh-prakxb-khxng-kar-suxsar>. Accessed 18 June 2020. (in Thai)
- [2] Cryptographic.
[file:///C:/Users/HP%20i5/Downloads/%E0%B9%80%E0%B8%98_%E0%B9%80%E0%B8%98%E0%B8%92%E0%B9%80%E0%B8%98%E0%B8%83%E0%B9%80%E0%B8%99%258%20\(1\).pdf](file:///C:/Users/HP%20i5/Downloads/%E0%B9%80%E0%B8%98_%E0%B9%80%E0%B8%98%E0%B8%92%E0%B9%80%E0%B8%98%E0%B8%83%E0%B9%80%E0%B8%99%258%20(1).pdf). Accessed 18 June 2020. (in Thai)
- [3] Singhirannusorn, K. 2010. Discontinuous Mathematics Part 5–6. MY MATHS 63: 6–11. (in Thai)
- [4] Chaimuang, P., Khummanee, S. and Puangpornpitak, S. 2012. An Improvement of the S/key One Time Password (OTP) using a BASE64 Data Encodement. Journal of Information Technology 8(2): 1–7. (in Thai)
- [5] Suwansa, A., Puangpornpitak, S., Thamsirarak, P. and Khaeypudsa, A. 2015. Security Enhancement of One Time Password Technology, Bangkok, National Research Council of Thailand. (in Thai)
- [6] Ketpittaya, T. 2018. A Study of Security Password Benefit's Perception, Security Password Protection Difficulty's Perception, and Security Password Setting's Attitude Affecting Employees' Behavior on Security Password in Stock Exchange of Thailand. Independent research, M.B.A., Graduate School, Bangkok University. (in Thai)