ทฤษฎีรหัสบนจำนวน c-Jacobsthal

Coding theory on c-Jacobsthal number

บุญยงค์ ศรีพลแผ้ว[1], สมคิด อินเทพ[2]*

Boonyong Sriponpaew[1], Somkid Intep [2]*

[1]ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยบูรพา

[1]Department of Mathematics, Faculty of Science, Burapha University

[2]ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยบูรพา

[2]Department of Mathematics, Faculty of Science, Burapha University

* E-mail: intep@buu.ac.th

บทคัดย่อ

ในบทความนี้ เราแนะนำ Q-เมทริกซ์ จากจำนวน c-Jacobsthal และวิธีเข้ารหัสและถอดรหัสจาก Q-เมทริกซ์ นอกจากนั้น เราได้ทำการสร้างความสัมพันธ์ระหว่างสมาชิกของเมทริกซ์รหัส การตรวจจับและการแก้ไขข้อผิดพลาดสำหรับทฤษฎีรหัสนี้ ค่าความสามารถในการแก้ไขข้อผิดพลาดของรหัสคือ 93.33%

คำสำคัญ: เข้ารหัส ถอดรหัส c-Jacobsthal

Abstract

In this manuscript, we introduce Q-matrix from c-Jacobsthal numbers and a method for coding and decoding messages from this Q-matrix. In addition, we construct the relations between the code matrix elements, error detection and correction for this coding theory. Correction ability of this method is 93.33%.

Keywords: Coding, decoding, c-Jacobsthal

บทนำ

ทฤษฎีการถอดรหัส (Coding theory) เป็นการศึกษาคุณสมบัติของรหัสและนำไปปรับใช้อย่างเหมาะสม เพื่อให้เข้ากับสถานการณ์ต่าง ๆ ไม่ว่าจะเป็นการบีบอัดข้อมูล วิทยาการเข้ารหัสลับ การตรวจหาและแก้ไขข้อผิดพลาดการส่งและการเก็บข้อมูล รหัสจะถูกนำไปใช้ประโยชน์ในสาขาวิชาต่าง ๆ เช่น ทฤษฎีสารสนเทศ วิศวกรรมไฟฟ้า ภาษาศาสตร์ และวิทยาการคอมพิวเตอร์

ในทุกวันนี้ ความปลอดภัยของข้อมูลกลายเป็นสิ่งสำคัญมากขึ้น ในแง่การส่งข้อมูลผ่านทางช่องทางการสื่อสาร ขั้นตอนวิธีการเข้าและถอดรหัสเป็นสิ่งที่สำคัญมากที่จะช่วยในการเพิ่มความปลอดภัยของข้อมูล ซึ่งได้มีนักคณิตศาสตร์ได้เริ่มนำจำนวนสำคัญทางคณิตศาสตร์มาประยุกต์ในการสร้างทฤษฎีการเข้าและถอดรหัส ในปี 2006 Stakov ได้เสนอทฤษฎีรหัสตัวใหม่ที่สร้างจากเมทริกซ์ฟิโบนักชี (Fibonacci matrix) ในปี 2009 Basu & Prasad ได้เสนอความสัมพันธ์ทั่วไประหว่างสมาชิกของเมทริกซ์รหัสสำหรับทฤษฎีรหัสฟิโบนักชี ต่อมามีนักคณิตศาสตร์หลายท่านได้พัฒนาทฤษฎีรหัสบนจำนวนอื่น ๆ ทางคณิตศาสตร์ซึ่งทำให้ขั้นตอนวิธีการเข้าและถอดรหัสมีความปลอดภัยมากขึ้น (Prasad, 2016; Tas, Ucar & Ozgur, 2017)

ในทางคณิตศาสตร์ลำดับ Jacobsthal เป็นลำดับของจำนวนจริงที่ถูกตั้งชื่อตามนักคณิตศาสตร์ชาวเยอรมัน Ernst Jacobsthal โดยมีการนิยามตามความสัมพันธ์เวียนเกิดดังนี้

$$J_n = J_{n-1} + 2J_{n-2}, \quad n = 2,3,4,...$$

โดยที่ $J_0 = 0$ และ $J_1 = 1$

โดยลำดับนี้มีความสำคัญในสาขาคอมพิวเตอร์ในการเปลี่ยนทิศทางของขั้นตอนการดำเนินการของโปรแกรม โดยใช้ในกระบวนการแยกคำสั่งแบบมีเงื่อนไขในไมโครคอนโทรลเลอร์ (Microcontroller) ซึ่งระบบการแยกคำสั่งมีรูปแบบเป็น 1, 3, 5, 11, 21, … กรณี สำหรับหน่วยความจำ 2, 3, 4, 5, 6, … บิต ตามลำดับ ซึ่งจำนวนกรณีดังกล่าวเป็นลำดับ Jacobsthal (Kyppo, 2019)

ในงานวิจัยนี้จะกล่าวถึงลำดับ c-Jacobsthal ซึ่งนิยามมาจากลำดับ (k,c)-Jacobsthal (Marques & Trojovsky, 2019) โดยที่ $k = 2$ ซึ่งมีนิยามดังต่อไปนี้

$$J_n = J_{n-1} + cJ_{n-2}, \quad n = 2,3,4,...$$

โดยที่ $J_0 = 0, J_1 = 1$ และ $c > 0$

เราสร้างวิธีการเข้ารหัสและถอดรหัสโดยใช้ Q-เมทริกซ์ ของลำดับ c-Jacobsthal พร้อมทั้งวิธีการตรวจสอบและแก้ไขข้อผิดพลาดของรหัส และคำนวณค่าความสามารถในการแก้ไขข้อผิดพลาดของรหัส ซึ่งจะเห็นได้ว่าเราสามารถมองเป็นกรณีทั่วไปจากทฤษฎีรหัสฟิโบนักชี $(c = 1)$ และจากการที่ c สามารถเลือกเป็นจำนวนเต็มบวกใด ๆ ทำให้สามารถเพิ่มความปลอดภัยในการคาดเดาของการโจรกรรมทางข้อมูลมากขึ้น

วัตถุประสงค์การวิจัย

1) เพื่อสร้างวิธีการเข้ารหัสและถอดรหัสจากจำนวน c-Jacobsthal
2) เพื่อตรวจสอบและแก้ไขข้อผิดพลาดของรหัส และคำนวณค่าความสามารถในการแก้ไขข้อผิดพลาดของรหัส

วิธีดำเนินการวิจัย

จากความสัมพันธ์เวียนเกิดของลำดับ c-Jacobsthal

$$J_n = J_{n-1} + cJ_{n-2}$$

เราสามารถสร้าง Q-เมทริกซ์ ได้ดังนี้

$$Q=\begin{bmatrix}1 & c\\ 1 & 0\end{bmatrix}=\begin{bmatrix}J_2 & cJ_1\\ J_1 & cJ_0\end{bmatrix}$$

และกำลัง n ของเมทริกซ์ Q คือ

$$Q^n=\begin{bmatrix}J_{n+1} & cJ_n\\ J_n & cJ_{n-1}\end{bmatrix}$$

โดยที่ $\det(Q^n)=(-c)^n$

ถ้าเราแทนค่าข้อความเริ่มต้นในรูปเมทริกซ์ไม่เอกฐานขนาด 2×2 ดังนี้

$$M=\begin{bmatrix}m_1 & m_2\\ m_3 & m_4\end{bmatrix}$$

โดยที่ m_i เป็นจำนวนเต็มที่ไม่ติดลบ

และสำหรับจำนวนเต็มบวก n ใด ๆ เราสามารถทำการเข้ารหัส โดยการคูณด้วยเมทริกซ์ Q^n จากด้านขวา

$$M\times Q^n=\begin{bmatrix}e_1 & e_2\\ e_3 & e_4\end{bmatrix}=E$$

และส่งข้อความที่เป็นรหัสผ่านช่องทางการสื่อสาร และทำการถอดรหัส โดยการคูณเมทริกซ์ E ด้วย Q^{-n} ดังนี้

$$E\times Q^{-n}=\begin{bmatrix}e_1 & e_2\\ e_3 & e_4\end{bmatrix}\times Q^{-n}=M$$

เราสามารถพิสูจน์ได้ว่า สำหรับค่า n ที่มากพอ

$$\frac{e_1}{e_2}\approx r \text{ และ } \frac{e_3}{e_4}\approx r$$

โดยที่ r เป็นค่าคงที่ ซึ่งเราสามารถนำความสัมพันธ์นี้ มาตรวจสอบและแก้ไขข้อผิดพลาดของรหัสได้ พร้อมทั้งใช้วิธีการนับเพื่อหาค่าความน่าจะเป็นของค่าความสามารถในการแก้ไขข้อผิดพลาดของรหัส

ผลการวิจัย

เพื่อความสะดวกในการพิสูจน์เราทำการแสดงการพิสูจน์สมบัติพื้นฐานของค่า Q-เมทริกซ์ และค่าของลิมิตของสัดส่วน J_{n+1} และ J_n ดังนี้

ทฤษฎีบทที่ 1 สำหรับ n เป็นจำนวนเต็มบวกใด ๆ และ $Q=\begin{bmatrix}1 & c\\ 1 & 0\end{bmatrix}$ จะได้ว่า

$$Q^n=\begin{bmatrix}J_{n+1} & cJ_n\\ J_n & cJ_{n-1}\end{bmatrix}$$

พิสูจน์ เราจะใช้วิธีการอุปนัยทางคณิตศาสตร์

<u>ขั้นฐาน</u>

$$Q=\begin{bmatrix}1 & c\\ 1 & 0\end{bmatrix}=\begin{bmatrix}J_2 & cJ_1\\ J_1 & cJ_0\end{bmatrix}$$

ดังนั้น ขั้นฐานเป็นจริง

<u>ขั้นอุปนัย</u> สมมติว่า $Q^k=\begin{bmatrix}J_{k+1} & cJ_k\\ J_k & cJ_{k-1}\end{bmatrix}$

ดังนั้น

$$\begin{aligned}Q^{k+1}&=Q^kQ\\ &=\begin{bmatrix}J_{k+1} & cJ_k\\ J_k & cJ_{k-1}\end{bmatrix}\begin{bmatrix}1 & c\\ 1 & 0\end{bmatrix}\\ &=\begin{bmatrix}J_{k+1}+cJ_k & cJ_{k+1}\\ J_k+cJ_{k-1} & cJ_k\end{bmatrix}\\ &=\begin{bmatrix}J_{k+2} & cJ_{k+1}\\ J_{k+1} & cJ_k\end{bmatrix}\end{aligned}$$

ดังนั้น ทฤษฎีบทเป็นจริง

บทแทรกที่ 2 สำหรับ n เป็นจำนวนเต็มบวกใด ๆ จะได้ว่า

1) $\det(Q^n)=(-c)^n$
2) $J_{n+1}J_{n-1}-J_n^2=(-1)^nc^{n-1}$

พิสูจน์ สังเกตได้ว่า $\det Q=-c$

ดังนั้น $\det(Q^n)=(\det Q)^n=(-c)^n$

และจะได้ว่า

$$c(J_{n+1}J_{n-1}-J_n^2)=\det(Q^n)=(-c)^n$$

ซึ่งส่งผลให้ $J_{n+1}J_{n-1}-J_n^2=(-1)^nc^{n-1}$

ทฤษฎีบทที่ 3 สำหรับ n เป็นจำนวนเต็มบวกใด ๆ จะได้ว่า

$$J_n=\frac{(\sqrt{4c+1}+1)^n-(-\sqrt{4c+1}+1)^n}{2^n\sqrt{4c+1}}\quad\text{และ}\quad\lim_{n\to\infty}\frac{J_{n+1}}{J_n}=\frac{\sqrt{4c+1}+1}{2}$$

พิสูจน์ เราสามารถหาค่าลักษณะเฉพาะและเวกเตอร์ลักษณะเฉพาะของ Q-เมทริกซ์ ได้ดังนี้

$\lambda_1=\dfrac{1+\sqrt{4c+1}}{2}$ ซึ่งสอดคล้องกับเวกเตอร์ $v_1=\begin{bmatrix}\dfrac{1+\sqrt{4c+1}}{2}\\ 1\end{bmatrix}$

และ $\lambda_2 = \dfrac{1-\sqrt{4c+1}}{2}$ ซึ่งสอดคล้องกับเวกเตอร์ $v_2 = \begin{bmatrix} \dfrac{1-\sqrt{4c+1}}{2} \\ 1 \end{bmatrix}$

ดังนั้นเราสามารถเขียน Q ในรูปของเมทริกซ์ทะแยงมุมได้ดังนี้

$$D = P^{-1}QP$$

โดยที่ $D = \begin{bmatrix} \dfrac{1+\sqrt{4c+1}}{2} & 0 \\ 0 & \dfrac{1-\sqrt{4c+1}}{2} \end{bmatrix}$ และ $P = \begin{bmatrix} \dfrac{1+\sqrt{4c+1}}{2} & \dfrac{1-\sqrt{4c+1}}{2} \\ 1 & 1 \end{bmatrix}$

จะได้ว่า $D^n = P^{-1}Q^nP$

ดังนั้น $Q^n = PD^nP^{-1}$

โดยที่ $D^n = \begin{bmatrix} \left(\dfrac{1+\sqrt{4c+1}}{2}\right)^n & 0 \\ 0 & \left(\dfrac{1-\sqrt{4c+1}}{2}\right)^n \end{bmatrix}$

จากการคำนวณ สามารถแสดงได้ว่า

$$\begin{bmatrix} J_{n+1} & cJ_n \\ J_n & cJ_{n-1} \end{bmatrix} = \begin{bmatrix} \dfrac{\left(1+\sqrt{4c+1}\right)^{n+1} - \left(1-\sqrt{4c+1}\right)^{n+1}}{2^{n+1}\sqrt{4c+1}} & \alpha \\ \dfrac{\left(1+\sqrt{4c+1}\right)^{n} - \left(1-\sqrt{4c+1}\right)^{n}}{2^{n}\sqrt{4c+1}} & \beta \end{bmatrix}$$

ดังนั้น $J_n = \dfrac{\left(1+\sqrt{4c+1}\right)^n - \left(1-\sqrt{4c+1}\right)^n}{2^n\sqrt{4c+1}}$

และ

$$\lim_{n\to\infty}\frac{J_{n+1}}{J_n} = \lim_{n\to\infty}\frac{\left(1+\sqrt{4c+1}\right)^{n+1} - \left(1-\sqrt{4c+1}\right)^{n+1}}{2^{n+1}\sqrt{4c+1}} \cdot \frac{2^n\sqrt{4c+1}}{\left(1+\sqrt{4c+1}\right)^n - \left(1-\sqrt{4c+1}\right)^n}$$

$$= \frac{1+\sqrt{4c+1}}{2}$$

ความสัมพันธ์ระหว่างสมาชิกของเมทริกซ์รหัส

จาก $E = M \times Q^n = \begin{bmatrix} m_1 & m_2 \\ m_3 & m_4 \end{bmatrix} \begin{bmatrix} J_{n+1} & cJ_n \\ J_n & cJ_{n-1} \end{bmatrix} = \begin{bmatrix} e_1 & e_2 \\ e_3 & e_4 \end{bmatrix}$

และ $Q^{-n} = \frac{1}{(-c)^n} \begin{bmatrix} cJ_{n-1} & -cJ_n \\ -J_n & J_{n+1} \end{bmatrix}$

โดยไม่เสียนัยทั่วไป สมมติ n เป็นจำนวนคู่ จะได้ว่า

$$M = E \times Q^{-n} = \frac{1}{c^n} \begin{bmatrix} ce_1 J_{n-1} - e_2 J_n & -ce_1 J_n + e_2 J_{n+1} \\ ce_3 J_{n-1} - e_4 J_n & -ce_3 J_n + e_4 J_{n+1} \end{bmatrix}$$

ดังนั้น จะได้ว่า

$$ce_1 J_{n-1} - e_2 J_n > 0 \quad (1)$$

$$-ce_1 J_n + e_2 J_{n+1} > 0 \quad (2)$$

$$ce_3 J_{n-1} - e_4 J_n > 0 \quad (3)$$

$$-ce_3 J_n + e_4 J_{n+1} > 0 \quad (4)$$

จาก (1) และ (2) เราสามารถแสดงได้ว่า

$$\frac{J_{n+1}}{cJ_n} > \frac{e_1}{e_2} > \frac{J_n}{cJ_{n-1}}$$

เมื่อ n มีค่ามาก จะได้ว่า

$$\frac{e_1}{e_2} \approx r$$

โดยที่ $r = \frac{1+\sqrt{4c+1}}{2c}$

ในทำนองเดียวกัน จาก (3) และ (4) เราสามารถสรุปได้ว่า สำหรับ n มีค่ามาก

$$\frac{e_3}{e_4} \approx r$$

การตรวจข้อผิดพลาดของรหัส

ในทฤษฎีรหัส การตรวจสอบและแก้ไขข้อผิดพลาดของรหัสเป็นเรื่องสำคัญที่ต้องพิจารณาเพราะในช่องทางการสื่อสารอาจจะมีการรบกวนเกิดขึ้น ซึ่งสิ่งที่ช่วยในการตรวจสอบ คือ ค่าดีเทอร์มิแนนท์ของเมทริกซ์

จากสมการ $M \times Q^n = E$

จะได้ว่า

$$\det E = (\det M) \times (-c)^n \quad (5)$$

ดังนั้น ถ้าค่าดีเทอร์มิแนนท์ของ E และ M ไม่สอดคล้องสมการ (5) เราสามารถสรุปได้ว่ารหัสเกิดข้อผิดพลาดขึ้น

การแก้ไขข้อผิดพลาดของรหัส

ในความเป็นจริงเราไม่สามารถพิจารณาว่าตำแหน่งไหนที่เกิดข้อผิดพลาดของรหัส เราทำได้แค่พิจารณาตามกรณีที่สมมติตามจำนวนตำแหน่งของข้อผิดพลาดของข้อมูล ดังนี้

กรณีที่ 1 มีข้อผิดพลาดของรหัสแค่ 1 ตำแหน่ง

โดยไม่เสียนัยทั่วไป ให้สมาชิกตัวแรกของเมทริกซ์ E เป็นตัวที่มีข้อผิดพลาด ดังนั้น เมทริกซ์ที่ผิดพลาด คือ

$$E' = \begin{bmatrix} u & e_2 \\ e_3 & e_4 \end{bmatrix}$$

โดยที่ u คือ รหัสที่ถูกเปลี่ยนแปลงไป และสมาชิกที่เหลือมีความถูกต้องของรหัส

จากสมการ $M \times Q^n = E$ จะได้ว่า ค่าดีเทอร์มิแนนท์ของทั้งสองข้างของสมการเท่ากัน

$$\det(M) \times (-c)^n = ue_4 - e_2e_3$$

ซึ่งเราสามารถแก้สมการหาค่า u ที่ถูกต้องได้ในรูป

$$u = \frac{\det(M) \times (-c)^n + e_2e_3}{e_4}$$

โดยการใช้ค่า u ที่ถูกต้องนี้ เราสามารถแก้ไขข้อผิดพลาดของรหัสใน 1 ตำแหน่งได้

กรณีที่ 2 มีข้อผิดพลาดของรหัส 2 ตำแหน่ง

สมมติตัวที่มีข้อผิดพลาดเป็นสมาชิกในแถวที่ 1 ของเมทริกซ์ E ดังนั้น เมทริกซ์ที่ผิดพลาด คือ

$$E' = \begin{bmatrix} u & v \\ e_3 & e_4 \end{bmatrix}$$

จากการเท่ากันของค่าดีเทอร์มิแนนท์ จะได้

$$ue_4 - ve_3 = (-c)^n \det(M) \tag{6}$$

เรารู้จากการพิสูจน์ว่า

$$\frac{u}{v} \approx r \tag{7}$$

เราสามารถเห็นได้ชัดเจนว่า สมการ (6) เป็นสมการไดโอแฟนไทน์ ซึ่งมีคำตอบจำนวนมาก เราสามารถหาคำตอบที่สอดคล้องกับสมการ (7) โดยการใช้ค่า u และ v ที่ถูกต้องนี้ เราสามารถแก้ไขข้อผิดพลาดของรหัสใน 2 ตำแหน่งได้

กรณีที่ 3 มีข้อผิดพลาดของรหัส 3 ตำแหน่ง

$$\begin{bmatrix} u & v \\ w & e_4 \end{bmatrix}$$

โดยการเท่ากันของดีเทอร์มิแนนท์ จะได้ว่า

$$ue_4 - vw = (-c)^n \det(M)$$

จาก $\frac{w}{e_4} \approx r$ เราสามารถลดรูปสมการดังกล่าวให้เหลือสมการไดโอแฟนไทน์สองตัวแปร และเนื่องจาก $\frac{u}{v} \approx r$ โดยกระบวนการที่เหมือนกันกับกรณีที่ 2 เราสามารถแก้สมการในกรณีที่มีข้อผิดพลาด 3 ตำแหน่งได้

ส่วนในกรณีที่มีข้อผิดพลาด 4 ตำแหน่ง นั่นคือ E เป็นรหัสที่ผิดพลาดทุกตำแหน่งและไม่สามารถที่จะแก้ไขข้อผิดพลาดได้

เนื่องจากรหัสอาจเกิดข้อผิดพลาดขึ้นได้ ตั้งแต่การเกิดข้อผิดพลาด 1 ตำแหน่ง จนถึงเกิดข้อผิดพลาด 4 ตำแหน่ง ดังนั้น จำนวนวิธีการเกิดข้อผิดพลาดทั้งหมด เท่ากับ ${}^4C_1 + {}^4C_2 + {}^4C_3 + {}^4C_4 = 15$ วิธี โดยที่เราสามารถแก้ไขรหัสให้ถูกต้องได้ทุกวิธี ยกเว้นวิธีเดียวคือกรณีที่เกิดข้อผิดพลาดทั้ง 4 ตำแหน่ง $\left({}^4C_4 = 1\right)$ ดังนั้น ค่าความสามารถในการแก้ไขข้อผิดพลาดของรหัสจึงมีค่า เท่ากับ $\frac{14}{15} = 0.9333 = 93.33\%$

ตัวอย่างการเข้าและถอดรหัส

สำหรับการเข้าและถอดรหัสของการส่งข้อความ เริ่มแรกเราจะทำการใส่ข้อความที่ต้องการส่งลงในเมทริกซ์ขนาดเป็นเลขคู่ โดยเติม 0 ลงระหว่างคำ และเติม 0 ที่ท้ายประโยคจนกว่าเต็มเมทริกซ์ หลังจากนั้น ทำการแบ่งเมทริกซ์เป็นเมทริกซ์บล็อคขนาด 2×2 โดยกำหนดการแปลงตัวอักษรให้เป็นตัวเลขดังนี้

ตารางที่ 1 การแปลงตัวอักษร

ตัวอักษร	A	B	C	D	E	F	G	H	I	J	K	L	M	
ตัวเลข	1	2	3	4	5	6	7	8	9	10	11	12	13	
ตัวอักษร	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
ตัวเลข	14	15	16	17	18	19	20	21	22	23	24	25	26	0

สมมติว่า เราต้องการส่งข้อความคำว่า “NAKHON SAWAN MAP” ซึ่งเราสามารถกำหนดเมทริกซ์ข้อความได้ดังนี้

$$B = \begin{bmatrix} N & A & K & H \\ O & N & 0 & S \\ A & W & A & N \\ 0 & M & A & P \end{bmatrix}$$

ทำการแบ่งเมทริกซ์ให้เป็นเมทริกซ์บล็อคขนาด 2x2 และแปลงตัวอักษรให้เป็นตัวเลข ได้เป็น

$$B=\begin{bmatrix} M_1 & M_2 \\ M_3 & M_4 \end{bmatrix}$$

โดยที่ $M_1=\begin{bmatrix} 14 & 1 \\ 15 & 14 \end{bmatrix}, M_2=\begin{bmatrix} 11 & 8 \\ 0 & 19 \end{bmatrix}, M_3=\begin{bmatrix} 1 & 23 \\ 0 & 13 \end{bmatrix}, M_4=\begin{bmatrix} 1 & 14 \\ 1 & 16 \end{bmatrix}$

หลังจากนั้น ทำการเข้ารหัส โดยในที่นี้เรากำหนดให้ $c=3$ และ $n=2$ จะได้

$$M_i \times Q^n=\begin{bmatrix} e_{i1} & e_{i2} \\ e_{i3} & e_{i4} \end{bmatrix}=E_i,\ \ i=1,2,3,4$$

ดังนั้น $E_1=\begin{bmatrix} 57 & 45 \\ 74 & 87 \end{bmatrix},\ E_2=\begin{bmatrix} 52 & 57 \\ 19 & 57 \end{bmatrix},\ E_3=\begin{bmatrix} 27 & 72 \\ 13 & 39 \end{bmatrix},\ E_4=\begin{bmatrix} 18 & 45 \\ 20 & 51 \end{bmatrix}$

และเมื่อข้อความที่เป็นรหัสถูกส่งถึงปลายทาง จะสามารถถูกถอดรหัส ได้เป็น

$$E_i \times Q^{-n}=\begin{bmatrix} e_{i1} & e_{i2} \\ e_{i3} & e_{i4} \end{bmatrix} \times Q^{-n}=M_i,\ \ i=1,2,3,4$$

ซึ่งจะได้เมทริกซ์รหัส M_i

และได้เมทริกซ์ข้อความ คือ

$$B=\begin{bmatrix} M_1 & M_2 \\ M_3 & M_4 \end{bmatrix}=\begin{bmatrix} 14 & 1 & 11 & 8 \\ 15 & 14 & 0 & 19 \\ 1 & 23 & 1 & 14 \\ 0 & 13 & 1 & 16 \end{bmatrix}$$

และเมื่อทำการแปลงตัวเลขให้เป็นตัวอักษรตามตารางการแปลงข้างต้น จะได้ข้อความที่ถูกส่งไปนั่นเอง

จากตัวอย่างข้างต้น เมื่อเราพิจารณา E_1 จะพบว่าอัตราส่วนของสมาชิกในแต่ละแถว เป็นดังนี้

ตารางที่ 2 อัตราส่วนของสมาชิกในแต่ละแถวของ E_1

n	e_1/e_2	e_3/e_4
2	1.2667	0.8506
5	0.7070	0.7537
6	0.8048	0.7756
10	0.7756	0.7684
15	0.7674	0.7675
20	0.7676	0.7676

จากตารางจะเห็นว่า เมื่อ n มีค่ามากขึ้น ค่าของอัตราส่วนของสมาชิกในแต่ละแถวจะมีค่าเข้าใกล้ 0.7676 มากขึ้น สำหรับเมทริกซ์ E อื่น ๆ ค่าของอัตราส่วนของสมาชิกในแต่ละแถวมีค่าเข้าใกล้ 0.7676 เมื่อ n มีค่ามากขึ้นเช่นเดียวกัน

อภิปรายผลการวิจัยและข้อเสนอแนะ

กระบวนการเข้ารหัสโดยใช้ Q-เมทริกซ์เป็นกระบวนการเข้ารหัสที่อยู่ในรูปของการคูณเมทริกซ์ ซึ่งสามารถไปประยุกต์ใช้ได้ง่ายกับการเขียนโปรแกรมสมัยใหม่ ในกรณีที่มีข้อมูลเป็นจำนวนมาก เราสามารถจัดการข้อความโดยแบ่งข้อความเป็นส่วน ๆ และรับข้อมูลได้ไม่จำกัด

ค่าความสามารถในการแก้ไขข้อผิดพลาดของรหัสของกระบวนการนี้ เท่ากับ 93.33% โดยที่สามารถแก้ไขข้อผิดพลาดของรหัสได้ถึง 3 ตำแหน่งจากทั้งหมด 4 ตำแหน่ง

กิตติกรรมประกาศ

ผู้วิจัยขอขอบคุณ คณะวิทยาศาสตร์ มหาวิทยาลัยบูรพา ที่สนับสนุนทุนวิจัย

เอกสารอ้างอิง

Basu, M. & Prasad, B. (2009). The generalized relations among the code elements for Fibonacci coding theory, *Chaos Solitons and Fractals, 41*(5), 2517-2525.

Kyppo, J. (2019). *Board games: throughout the history and multidimensional spaces*. New Jersey: World Scientific.

Marques, D. & Trojovsky, P. (2019). On characteristic polynomial of higher order generalized Jacobsthal numbers. *Advances in Difference Equations, 392*, 9 pages. https://doi.org/10.1186/s13662-019-2327-6.

Prasad, B. (2016). Coding theory on Lucas *p* numbers. *Discrete Mathematics Algorithms and Applications, 8*(4), 1650074(17 pages).

Stakhov, A. P. (2006). Fibonacci matrices, a generalization of “Cassini formula”, and a new coding theory. *Chaos Solitons & Fractals, 30*(1), 56-66.

Tas, N., Ucar, S. and Ozgur, N. Y. (2017). Pell coding and Pell decoding methods with some applications. Retrieved from https://arxiv.org/pdf/1706.04377.

วันที่รับบทความ 22 มิ.ย. 63, วันที่แก้ไขบทความ 11 พ.ย. 63, วันที่ตอบรับบทความ 29 ธ.ค. 63