# วิทยาการเข้ารหัสลับด้วยสมบัติของเมทริกซ์และกลุ่มของผลคูณโดยตรงภายนอก

# Cryptography by Using Matrix Properties and External Direct Product Group Properties

นพรัตน์ ไวโรจนะ กมลรัตน์ สมบุตร สุธิดา พรมภักดิ์ และสุพิชชา สุขารมณ์*
หลักสูตรคณิตศาสตร์ประยุกต์ คณะวิทยาศาสตร์และเทคโนโลยี
มหาวิทยาลัยราชภัฏวไลยอลงกรณ์ ในพระบรมราชูปถัมภ์
* ผู้นิพนธ์หลัก (Corresponding Author) E-mail: Popiano133@gmail.com

**บทคัดย่อ**

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อการศึกษาวิธีการเข้ารหัสโดยใช้เมทริกซ์และสมบัติของผลคูณโดยตรงภายนอก รวมถึงเทคนิคพิเศษที่ต้องใช้เทคนิคบางประการในการหาคำตอบ ซึ่งผู้สนใจสามารถสร้างกุญแจการเข้ารหัสเพื่อใช้รักษาความปลอดภัยของข้อความเองได้ โดยใช้โค้ดตัวอักษรที่อยู่ในเซต z_3×z_67^*ประกอบไปด้วย ตัวอักษรภาษาไทย ตัวอักษรภาษาอังกฤษ และสัญลักษณ์พิเศษ รวมทั้งหมด 201 ตัวอักษร อย่างไรก็ตาม งานวิจัยนี้เป็นการต่อยอดจากวิจัยของ นางสาวนารีรัตน์ พูลสวัสดิ์ เรื่อง การเข้ารหัสด้วยพีชคณิต ที่ผู้วิจัยได้สร้างกุญแจมีตัวอักษรเพียง z_149 และเพื่อให้สามารถแยกตัวอักษรได้ง่ายขึ้น ผู้วิจัยได้แบ่งตัวอักษรในรูปของคู่อันดับเป็น 3 กลุ่ม ทำให้ง่ายต่อการจำโค้ดตัวอักษร แต่ด้วยเทคนิคพิเศษในการเข้ารหัส จึงทำให้การเข้ารหัสนั้นยากกว่าการเข้ารหัสแบบธรรมดาและเป็นแนวทางการรักษาความปลอดภัยในการสื่อสารข้อมูลที่เป็นความลับขององค์กร

**คำสำคัญ:** วิทยาการเข้ารหัสลับ, สมบัติของเมทริกซ์, การรักษาความปลอดภัย

**Abstract**

This research aims to study how to encode using matrix and external direct product group. Special techniques are required to use some tricks to finding the answer. Which can generate an encryption key to secure your own text? The character code is set $Z_3 \times Z_{67}^*$ comprises letters, Thai. English alphabet and special symbols total of 201 characters, however, this research extending from the research of Miss. Nareerat Poonsawat. Re: Cryptography in an Algebraic. The researchers created a key character only $Z_{149}$ and separate letters easier. The researchers divided the letters in the form of order into 3 groups. Make it easy to remember code but with special encoding. As a result, the

encryption is more difficult than conventional encryption. And as a guide Security in data communication the organization is confidential information.

**Keywords:** Cryptography, Matrix properties, Security system

**บทนำ**

การรักษาความปลอดภัยของข้อมูลข่าวสาร หรือการรักษาความลับ มีมาตั้งแต่มนุษย์เริ่มมีการติดต่อสื่อสารกัน โดยคาดหวังว่าสิ่งที่ตนเองต้องการเปิดเผยได้ถูกจำกัดบนขอบเขตที่ตนเองต้องการ ซึ่งสิ่งสำคัญที่จะต้องถูกปกป้องคือ “สาระของข้อมูลข่าวสาร” ต่อมาการสื่อสารของมนุษย์ได้ถูกพัฒนาไปตามเทคโนโลยีที่ทันสมัย การรักษาความปลอดภัยของข้อมูล จึงต้องกว้างขวางออกไปให้ครอบคลุมสื่อกลางที่ใช้นั้นด้วย ซึ่งปัจจุบันเราจะเห็นว่า มีเทคโนโลยีการรักษาความปลอดภัยใหม่ ๆ เกิดขึ้นเป็นจำนวนมาก โดยจะมีรูปแบบและวิธีการที่แตกต่างกันออกไป เพิ่มความซับซ้อนให้มากขึ้น เพื่อป้องกันภัยจากผู้ที่ไม่ประสงค์ดี การโจมตีของแฮกเกอร์แบบใหม่ ๆ และป้องกันภัยจากอาชญากรคอมพิวเตอร์ต่าง ๆ ที่เพิ่มขึ้นเป็นทวีคูณ ตัวอย่างเทคโนโลยีการรักษาความปลอดภัย อาทิเช่น การใช้หมึกเขียนชนิดพิเศษที่ต้องใช้เทคนิคบางประการในการทำให้ข้อมูลปรากฏ การใช้หีบหรือกล่องนิรภัย การใช้ระบบตอบรับเฉพาะบุคคลในการเข้าสู่ระบบ และการเข้ารหัส-ถอดรหัสของข้อมูล เป็นต้น

จากงานวิจัยได้มีการพัฒนาแนวคิดเริ่มต้นมาจาก เลสเตอร์ เอส ฮิลล์ เขาได้เสนอแนวคิดการเข้ารหัสและการถอดรหัส ด้วยความรู้ด้านพีชคณิต ซึ่งสามารถใช้ได้กับข้อมูลที่เป็นภาษาอังกฤษเท่านั้น ต่อมานารีรัตน์ พูนสวัสดิ์ (2562) ได้พัฒนาแนวคิดของเลสเตอร์ เอส ฮิลล์ (1929) โดยการทำให้สามารถเข้ารหัสและถอดรหัสของข้อมูลได้ทั้งข้อมูลที่เป็นภาษาอังกฤษ ภาษาไทย และสัญลักษณ์พิเศษ จากนั้นคณะผู้วิจัยได้นำแนวคิดข้างต้น มาต่อยอดโดยการใช้ความรู้ทางด้านเมทริกซ์ และสมบัติของกลุ่มของผลคูณโดยตรงภายนอก รวมถึงทฤษฎีอื่น ๆ ที่เกี่ยวข้อง เพื่อเพิ่มความซับซ้อนในการเข้ารหัส ทำให้การเข้ารหัสนั้นมีความปลอดภัยมากกว่าเดิม

**วัตถุประสงค**

1. เพื่อศึกษาวิธีการเข้ารหัสโดยใช้เมทริกซ์และสมบัติกลุ่มของผลคูณโดยตรงภายนอก
2. เพื่อสร้างโค้ดตัวอักษรที่อยู่ในเซต z_3×z_67^* โดยประกอบไปด้วยตัวอักษร ภาษาไทย ภาษาอังกฤษ และสัญลักษณ์พิเศษ รวมทั้งหมด 201 ตัว

**วิธีการวิจัย**

ขั้นตอนในการเข้ารหัสและการถอดรหัส ดังนั้นจึงขอนำเสนอสารข้อมูลที่ได้ศึกษาตามลำดับดังต่อไปนี้

1. กำหนดข้อมูลตัวอักษรและคีย์รหัสเป็นกลุ่มสามกลุ่ม คือ ภาษาไทย ภาษาอังกฤษ สัญลักษณ์พิเศษ
2. รับข้อมูลที่เป็นประโยค
3. นำตัวอักษรมาแปลงเป็นตัวเลขกลุ่มละสองชุด และสามชุดโดยใช้กุญแจที่สร้างขึ้นในบทที่ 3
4. ตรวจสอบค่าดีเทอร์มิแนนต์ของเมทริกซ์นั้น ๆ ต้องไม่เท่ากับศูนย์
5. นำตัวอักษรที่แปลงได้มาเข้ารหัสและถอดรหัส

**ตารางที่ 1** กำหนดตัวอักษรภาษาไทยให้มีความสัมพันธ์กับตัวเลข

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ก (2,0) | ข (2,1) | ฃ (2,2) | ค (2,3) | ฅ (2,4) | ฆ (2,5) | ง (2,6) | จ (2,7) | ฉ (2,8) | ช (2,9) | ซ (2,10) | ฌ (2,11) |
| ญ (2,12) | ฎ (2,13) | ฏ (2,14) | ฐ (2,15) | ฑ (2,16) | ฒ (2,17) | ณ (2,18) | ด (2,19) | ต (2,20) | ถ (2,21) | ท (2,22) | ธ (2,23) |
| น (2,24) | บ (2,25) | ป (2,26) | ผ (2,27) | ฝ (2,28) | พ (2,29) | ฟ (2,30) | ภ (2,3) | ม (2,32) | ย (2,33) | ร 2,34) | ล (2,35) |
| ว (2,36) | ศ (2,37) | ษ (2,38) | ส (2,39) | ห (2,40) | ฬ (2,41) | อ (2,42) | ฮ (2,43) | ะ (2,44) | า (2,45) | ิ (2,46) | ี (2,47) |
| ึ (2,48) | ื (2,49) | ุ (2,50) | ู (2,51) | เ (2,52) | แ (2,53) | ำ (2,54) | ไ (2,55) | ใ (2,56) | โ (2,57) | ็ (2,58) | ์ (2,59) |
| ๆ (2,60) | ฯ (2,61) | ั (2,62) | ่ (2,63) | ้ (2,64) | ๊ (2,65) | ๋ (2,66) | | | | | |

**ตารางที่ 2** กำหนดตัวอักษรภาษาอังกฤษให้มีความสัมพันธ์กับตัวเลข

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| A (1,0) | B (1,1) | C (1,2) | D (1,3) | E (1,4) | F (1,5) | G (1,6) | H (1,7) | I (1,8) | J (1,9) | K (1,10) | L (1,11) |
| M (1,12) | N (1,13) | O (1,14) | P (1,15) | Q (1,16) | R (1,17) | S (1,18) | T (1,19) | U (1,20) | V (1,21) | W (1,22) | X (1,23) |
| Y (1,24) | Z (1,25) | a (1,26) | b (1,27) | c (1,28) | d (1,29) | e (1,30) | f (1,31) | g (1,32) | h (1,33) | i (1,34) | j (1,35) |
| k (1,36) | l (1,37) | m (1,38) | n (1,39) | o (1,40) | p (1,41) | q (1,42) | r (1,43) | s (1,44) | t (1,45) | u (1,46) | v (1,47) |

| w (1,48) | x (1,49) | y (1,50) | z (1,51) | ¥ (1,52) | ¤ (1,53) | $ (1,54) | £ (1,55) | ฿ (1,56) | Ç (1,57) | œ (1,58) | æ (1,59) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ẽ (1,60) | Ñ (1,61) | đ (1,62) | ỹ (1,63) | µ (1,64) | ä (1,65) | Ä (1,66) | | | | | |

**ตารางที่ 3** กำหนดตัวอักษรสัญลักษณ์พิเศษให้มีความสัมพันธ์กับตัวเลข

| › (0,0) | ‹ (0,1) | ≥ (0,2) | ≤ (0,3) | ≠ (0,4) | ≈ (0,5) | ~ (0,6) | ∞ (0,7) | √ (0,8) | = (0,9) | ∑ (0,10) | ∏ (0,11) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Δ (0,12) | ∂ (0,13) | ⅞ (0,14) | ⅝ (0,15) | ⅜ (0,16) | ⅛ (0,17) | ⅚ (0,18) | ⅙ (0,19) | # (0,20) | ‡ (0,21) | ¶ (0,22) | § (0,23) |
| Ω (0,24) | ₣ (0,25) | / (0,26) | \ (0,27) | ◊ (0,28) | ◌ (0,29) | % (0,30) | ‰ (0,31) | ‘ (0,32) | ’ (0,33) | “ (0,34) | ” (0,35) |
| , (0,36) | ▪ (0,37) | … (0,38) | — (0,39) | ± (0,40) | + (0,41) | - (0,42) | * (0,43) | ^ (0,44) | Ø (0,45) | ß (0,46) | ¿ (0,47) |
| ? (0,48) | – (0,49) | @ (0,50) | © (0,51) | ® (0,52) | ™ (0,53) | € (0,54) | ( (0,55) | ) (0,56) | [ (0,57) | ] (0,58) | ∫ (0,59) |
| ! (0,60) | ◎ (0,61) | & (0,62) | ; (0,63) | : (0,64) | ¦ (0,65) | \| (0,66) | | | | | |

การหาคู่ผกผันการบวกและการคูณ

การบวกและการคูณบนเซตของจำนวนจริงสอดคล้องกฎการเปลี่ยนหมู่และกฎการสลับที่ โดยมี (0,0) และ(0,1) เป็นเอกลักษณ์ภายใต้การบวกและการคูณตามลำดับ

นิยามตัวผกผันการบวก $(a,b)+(c,d)=(a+c\ ,b+d)$

นิยามตัวผกผันการคูณ $(a,b)\cdot(c,d)=(a+b\ ,c\cdot d)$

นิยาม $Z_3$ คือ เซตของเศษเหลือของการนำจำนวนเต็มมาหารด้วย 3 = {0, 1, 2}

นิยาม $Z_{67}$ คือ เซตของเศษเหลือของการนำจำนวนเต็มมาหารด้วย 67 = {0, 1, 2, ..., 66}

นิยาม $Z_{67}^*$ = Z67 - {0} = {1, 2, ..., 66}

นิยาม $Z_3 \times Z_{67}$ คือเซตของคู่อันดับที่มีตัวหน้าเป็นสมาชิกในเซต $Z_3$ และ ตัวหลังเป็นสมาชิกของ $Z_{67}$

= {(0, 0), (0, 1), ..., (0, 66)

(1, 0), (1, 1), ..., (1, 66)

(2, 0), (2, 1), ..., (2, 66)}

นิยาม $Z_3 \times Z_{67}^*$ คือเซตของคู่อันดับที่มีตัวหน้าเป็นสมาชิกในเซต $Z_3$ และ ตัวหลังเป็นสมาชิก

ของ $Z_{67}^{*}$

= {(0, 1), (0, 2), ..., (0, 66)
(1, 1), (1, 2), ..., (1, 66)
(2, 1), (2, 2), ..., (2, 66)}

**ตารางที่ 4** ตารางค่าของตัวผกผันการบวกและตัวผกผันการคูณของตัวอักษรภาษาไทย

| ตัวอักษร | ตัวผกผันการบวก | ตัวผกผันการคูณ | ตัวอักษร | ตัวผกผันการบวก | ตัวผกผันการคูณ |
|---|---|---|---|---|---|
| ก | A | - | ร | ≥ | C |
| ข | Ä | B | ล | § | X |
| ฃ | ä | I | ว | € | $ |
| ค | µ | T | ศ | ◌ | d |
| ต | ỹ | R | ษ | % | e |
| ฆ | đ | B | ส | ( | £ |
| ง | ñ | ฿ | ห | & | đ |
| จ | ẽ | W | ฬ | ⅝ | S |
| ฉ | æ | Q | อ | √ | I |
| ช | œ | P | ฮ | ™ | ¤ |
| ซ | Ć | V | ะ | ‘ | ɡ |
| ฌ | ฿ | Ñ | า | ≤ | D |
| ญ | £ | C | ิ | © | z |
| ฎ | $ | F | ี | ∑ | K |
| ฏ | ¤ | Y | ึ | ∞ | H |
| ฐ | ¥ | J | ื | / | a |
| ฑ | z | V | ุ | ; | ỹ |
| ฒ | y | E | ู | ß | u |
| ณ | x | p | เ | ] | œ |
| ด | w | ẽ | แ | * | r |
| ต | v | Ć | ำ | ’ | k |
| ถ | u | Q | ไ | — | n |
| ท | t | µ | ใ | ~ | G |
| ธ | s | J | โ | # | U |

| ตัวอักษร | ตัวผกผันการบวก | ตัวผกผันการคูณ | ตัวอักษร | ตัวผกผันการบวก | ตัวผกผันการคูณ |
|---|---|---|---|---|---|
| น | r | O | ๘ | ® | ¥ |
| บ | q | Æ | ์ | ₣ | z |
| ป | p | X | ๆ | ⅙ | T |
| ผ | o | F | ฯ | ∏ | L |
| ฝ | n | M | | ± | o |
| พ | m | L | ' | @ | y |
| ฟ | l | M | ้ | ¶ | W |
| ภ | k | N | ๗ | ’ | h |
| ม | j | S | ๋ | \| | Ä |
| ย | i | ä | | | |

**ตารางที่ 5** ตารางค่าของตัวผกผันการบวกและตัวผกผันการคูณของตัวอักษรภาษาอังกฤษ

| ตัวอักษร | ตัวผกผันการบวก | ตัวผกผันการคูณ | ตัวอักษร | ตัวผกผันการบวก | ตัวผกผันการคูณ |
|---|---|---|---|---|---|
| A | ก | - | i | ย | ข |
| B | ๋ | ข | j | ม | ธ |
| C | ๗ | ร | k | ภ | ำา |
| D | ้ | า | l | ฟ | พ |
| E | ' | ฒ | m | พ | ฟ |
| F | ั | ผ | n | ฝ | ไ |
| G | ฯ | ใ | o | ผ | ั |
| H | ๆ | ึ | p | ป | ณ |
| I | ์ | อ | q | บ | ฉ |
| J | ๘ | ฐ | r | น | แ |
| K | โ | ึ | s | ธ | ม |
| L | ใ | ฯ | t | ท | ค |
| M | ไ | ฝ | u | ถ | ข |
| N | ำา | ภ | v | ต | ซ |
| O | แ | น | w | ด | จ |
| P | เ | ช | x | ณ | ป |

| ตัวอักษร | ตัวผกผัน การบวก | ตัวผกผัน การคูณ | ตัวอักษร | ตัวผกผัน การบวก | ตัวผกผัน การคูณ |
|---|---|---|---|---|---|
| Q | ง | ถ | y | ฒ | ' |
| R | ๆ | ศ | z | ฑ | ิ |
| S | ็ | ฬ | ¥ | ฐ | ็ |
| T | ็ | ๆ | ¤ | ฏ | ฮ |
| U | ็ | โ | $ | ฎ | ว |
| V | ิ | ฑ | £ | ญ | ส |
| W | า | ้ | ฿ | ฌ | ง |
| X | ะ | ล | Ç | ซ | ต |
| Y | ฮ | ฏ | œ | ช | เ |
| Z | อ | ์ | æ | ฉ | บ |
| a | ฬ | ็ | ë | จ | ด |
| b | ห | ฆ | ñ | ง | ฌ |
| c | ส | ญ | d̲ | ฆ | ห |
| d | ษ | ศ | ỹ | ศ | ๆ |
| e | ศ | ษ | µ | ค | ท |
| f | ว | ฎ | ä | ฃ | ย |
| g | ล | ะ | Ä | ข | ' |
| h | ร | ็ | | | |

**ตารางที่ 6** ตารางค่าของตัวผกผันการบวกและตัวผกผันการคูณของตัวอักษรสัญลักษณ์พิเศษ

| ตัวอักษร | ตัวผกผัน การบวก | ตัวผกผัน การคูณ | ตัวอักษร | ตัวผกผัน การบวก | ตัวผกผัน การคูณ |
|---|---|---|---|---|---|
| › | › | - | “ | ’ | ≥ |
| ‹ | \| | ‹ | ” | ‘ | § |
| ≥ | ¦ | “ | , | ‰ | € |
| ≤ | : | Ø | ▪ | % | ◌ |
| ≠ | ; | ⅛ | … | ◌ | % |
| ≈ | & | \ | — | ◊ | ( |
| ~ | ◎ | ) | ± | \ | & |

| ตัวอักษร | ตัวผกผันการบวก | ตัวผกผันการคูณ | ตัวอักษร | ตัวผกผันการบวก | ตัวผกผันการคูณ |
|---|---|---|---|---|---|
| ∞ | ! | ? | + | / | ⅝ |
| √ | ∫ | - | - | ₣ | √ |
| = | ] | ⅝ | * | Ω | ™ |
| ∑ | [ | ¿ | ^ | § | ‘ |
| ∏ | ) | ◎ | Ø | ¶ | ≤ |
| △ | ( | ◊ | ß | ‡ | © |
| ∂ | € | ‰ | ¿ | # | ∑ |
| ⅞ | ™ | Ω | ? | ⅙ | ∞ |
| ⅝ | ® | = | – | ⅝ | / |
| ⅜ | © | ‡ | @ | ⅛ | ; |
| ⅛ | @ | ≠ | © | ⅜ | ß |
| ⅚ | – | + | ® | ⅝ | ] |
| ⅙ | ? | ! | ™ | ⅞ | * |
| # | ¿ | [ | € | ∂ | ’ |
| ‡ | ß | ⅜ | ( | △ | — |
| ¶ | Ø | : | ) | ∏ | ~ |
| § | ^ | ” | [ | ∑ | # |
| Ω | * | ⅞ | ] | = | ® |
| ₣ | - | ∫ | ∫ | √ | ₣ |
| / | + | – | ! | ∞ | ⅙ |
| \ | ± | ≈ | ◎ | ~ | ∏ |
| ◊ | — | △ | & | ≈ | ± |
| ◌ | … | ▪ | ; | ≠ | @ |
| % | ▪ | … | : | ≤ | ¶ |
| ‰ | , | ∂ | ¦ | ≥ | ’ |
| ‘ | ” | ^ | \| | ‹ | \| |
| ’ | “ | ¦ | | | |

การสร้างกุญแจ

ในการสร้างกุญแจ จำเป็นต้องมีการสร้างกุญแจสำหรับการเข้ารหัส (Private key) และกุญแจ

สำหรับการถอดรหัส (Public key) มาใช้คู่กันเสมอ ซึ่งมีขั้นตอนการหากุญแจดังนี้

1) เลือกกุญแจในการเข้ารหัส

$$k = \begin{bmatrix} C & ฆ \\ ข & H \end{bmatrix} = \begin{bmatrix} (1,2) & (2,5) \\ (2,1) & (1,7) \end{bmatrix}$$

**หมายเหตุ:** ในการเลือกคู่อันดับสำหรับการสร้างกุญแจ ควรเลือกคู่อันดับที่ไม่มี 0 เป็นตัวประกอบ เนื่องจากจะทำให้ค่า $\det = 0$ นั่นคือ ไม่สามารถหาเมทริกซ์ผกผันได้

2) หาเมทริกซ์ $k^{-1}$ ซึ่งเป็นกุญแจสำหรับการถอดรหัส โดยการแก้ระบบสมการเชิงเส้นดังต่อไปนี้

$$\begin{bmatrix} (1,2) & (2,5) \\ (2,1) & (1,7) \end{bmatrix} => \begin{bmatrix} x & y \\ z & w \end{bmatrix} \begin{bmatrix} (1,2) & (2,5) \\ (2,1) & (1,7) \end{bmatrix} = \begin{bmatrix} (0,1) & (0,0) \\ (0,0) & (0,1) \end{bmatrix}$$

$(1,2)x + (2,1)y = (0,1)$.....(1)

$(2,5)x + (1,7)y = (0,0)$.....(2)

$(1,2)z + (2,1)w = (0,0)$.....(3)

$(2,5)z + (1,7)w = (0,1)$.....(4)

$(2,34) \times (1); (0,1)x + (1,34)y = (2,34)$.....(5)

$(1,27) \times (2); (0,1)x + (2,55)y = (1,0)$.....(6)

$(6) - (5); (1,21)y = (-1,-34)$

$(1,21)y = (2,33)$

$(2,16)(1,21)y = (2,16)(2,33)$

$(0,1)y = (1,59)$

$y = (1,59)$

แทนค่า y ใน (1) ;

$(1,2)x + (2,1)(1,59) = (0,1)$

$(1,2)x + (0,59) = (0,1)$

$(1,2)x = (0,1) - (0,59)$

$(1,2)x = (0,1) + (0,8)$

$(1,2)x = (0,9)$

$(2,34)(1,2)x = (2,34)(0,9)$

$(0,1)x = (2,38)$

$x = (2,38)$

$(2,34) \times (3); (0,1)z + (1,34)w = (2,0)$.....(7)

$(1,27) \times (4); (0,1)z + (2,55)w = (1,27)$.....(8)

$$(8) - (7); (1,21)w = (-1,27)$$

$$(1,21)w = (2,27)$$

$$(2,16)(1,21)w = (2,16)(2,27)$$

$$(0,1)w = (1,30)$$

$$w = (1,30)$$

แทนค่า w ใน (4) ;

$$(2,5)z + (1,7)(1,30) = (0,1)$$

$$(2,5)z + (2,9) = (0,1)$$

$$(2,5)z = (0,1) - (2,9)$$

$$(2,5)z = (0,1) + (1,58)$$

$$(2,5)z = (1,59)$$

$$(1,27)(2,5)z = (1,27)(1,59)$$

$$(0,1)z = (2,52)$$

$$z = (2,52)$$

จะเห็นว่า เมทริกซ์ผกผันของเมทริกซ์ k คือ

$$k^{-1} = \begin{bmatrix} (2,38) & (1,59) \\ (2,52) & (1,30) \end{bmatrix}$$

ตรวจสอบการเป็นเมทริกซ์ผกผัน

$$\begin{bmatrix} (2,38) & (1,59) \\ (2,52) & (1,30) \end{bmatrix}\begin{bmatrix} (1,2) & (2,5) \\ (2,1) & (1,7) \end{bmatrix} = \begin{bmatrix} (2,38)(1,2)+(1,59)(2,1) & (2,38)(2,5) & (1,59)(1,7) \\ (2,52)(1,2)+(1,30)(2,1) & (2,52)(2,5) & (1,30)(1,7) \end{bmatrix}$$

$$= \begin{bmatrix} (0,9)+(0,59) & (1,56)+(2,11) \\ (0,37)+(0,30) & (1,59)+(2,9) \end{bmatrix} = \begin{bmatrix} (0,1) & (0,0) \\ (0,0) & (0,1) \end{bmatrix}$$

จะเห็นว่า $(k^{-1})(k) = e$ นั่นคือ เมทริกซ์ผกผันที่ได้นั้นถูกต้อง

สรุปได้ว่า

กุญแจสำหรับการเข้ารหัส คือ

$$k = \begin{bmatrix} (1,2) & (2,5) \\ (2,1) & (1,7) \end{bmatrix}$$

กุญแจสำหรับการถอดรหัส คือ

$$k^{-1} = \begin{bmatrix} (2,38) & (1,59) \\ (2,52) & (1,30) \end{bmatrix}$$

**ผลและอภิปรายผลการวิจัย**

ตัวอย่างการเข้ารหัสและการถอดรหัส

การจะนำข้อมูลมาเข้ารหัสและถอดรหัสได้นั้น ต้องแบ่งตัวอักษรเป็นกลุ่ม กลุ่มละสองตัว(ตามขนาดของเมทริกซ์จัตุรัส) จากซ้ายไปขวา จากนั้นแปลงอักษรให้เป็นตัวเลขตามที่เรากำหนดไว้ข้างต้น จะ

ได้รูปแบบคำดังต่อไปนี้

ตัวอย่างที่ 1 ทำอะไรอยู่

การเข้ารหัส

ท ◌ำ อ ะ ไ ร อ ย ◌ู ◌่

(2,22) (2,54) (2,42) (2,44) (2,55) (2,34) (2,42) (2,33) (2,51) (2,63)

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ท | ◌ำ | อ | ะ | ไ | ร | อ | ย | ◌ู | ◌่ |
| (2,22) | (2,54) | (2,42) | (2,44) | (2,55) | (2,34) | (2,42) | (2,33) | (2,51) | (2,63) |

ทำอะ

$$k=\begin{bmatrix}(1,2) & (2,5)\\ (2,1) & (1,7)\end{bmatrix}\times\begin{bmatrix}(2,22) & (2,42)\\ (2,54) & (2,44)\end{bmatrix}=\begin{bmatrix}(1,46) & (1,36)\\ (1,65) & (1,15)\end{bmatrix}=\begin{bmatrix}u & k\\ \ddot{a} & P\end{bmatrix}$$

ไรอย

$$k=\begin{bmatrix}(1,2) & (2,5)\\ (2,1) & (1,7)\end{bmatrix}\times\begin{bmatrix}(2,55) & (2,42)\\ (2,34) & (2,33)\end{bmatrix}=\begin{bmatrix}(1,12) & (1,48)\\ (1,25) & (1,5)\end{bmatrix}=\begin{bmatrix}M & w\\ z & F\end{bmatrix}$$

◌ู ◌่

$$k=\begin{bmatrix}(1,2) & (2,5)\\ (2,1) & (1,7)\end{bmatrix}\times\begin{bmatrix}(2,51)\\ (2,63)\end{bmatrix}=\begin{bmatrix}(1,15)\\ (1,23)\end{bmatrix}=\begin{bmatrix}P\\ X\end{bmatrix}$$

ข้อความที่ได้จากการเข้ารหัส คือ uäkPMZwFPX

การถอดรหัส

u ä k P M Z w F P X

(1,46) (1,65) (1,36) (1,15) (1,12) (1,25) (1,48) (1,5) (1,15) (1,23)

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| u | ä | k | P | M | Z | w | F | P | X |
| (1,46) | (1,65) | (1,36) | (1,15) | (1,12) | (1,25) | (1,48) | (1,5) | (1,15) | (1,23) |

uäkP

$$k^{-1}=\begin{bmatrix}(2,38) & (1,59)\\ (2,52) & (1,30)\end{bmatrix}\times\begin{bmatrix}(1,46) & (1,36)\\ (1,65) & (1,15)\end{bmatrix}=\begin{bmatrix}(2,22) & (2,42)\\ (2,54) & (2,44)\end{bmatrix}=\begin{bmatrix}ท & อ\\ ◌ำ & ะ\end{bmatrix}$$

MZwF

$$k^{-1}=\begin{bmatrix}(2,38) & (1,59)\\ (2,52) & (1,30)\end{bmatrix}\times\begin{bmatrix}(1,12) & (1,48)\\ (1,25) & (1,5)\end{bmatrix}=\begin{bmatrix}(2,55) & (2,42)\\ (2,34) & (2,33)\end{bmatrix}=\begin{bmatrix}ไ & อ\\ ร & ย\end{bmatrix}$$

PX

$$k^{-1} = \begin{bmatrix} (2,38) & (1,59) \\ (2,52) & (1,30) \end{bmatrix} \times \begin{bmatrix} (1,15) \\ (1,23) \end{bmatrix} = \begin{bmatrix} (2,51) \\ (2,63) \end{bmatrix} = \begin{bmatrix} ง \\ ' \end{bmatrix}$$

ข้อความที่ได้จากการถอดรหัส คือ ทำอะไรอยู่

ตัวอย่างที่ 2 Memory

การเข้ารหัส

M e m o r y

(1,12) (1,30) (1,38) (1,40) (1,43) (1,50)

| M e | m o | r y |
|---|---|---|
| (1,12) (1,30) | (1,38) (1,40) | (1,43) (1,50) |

Memory

$$k = \begin{bmatrix} (1,2) & (2,5) \\ (2,1) & (1,7) \end{bmatrix} \times \begin{bmatrix} (1,12) & (1,38) & (1,43) \\ (1,30) & (1,40) & (1,50) \end{bmatrix} = \begin{bmatrix} (2,40) & (2,8) & (2,1) \\ (2,21) & (2,50) & (2,58) \end{bmatrix} = \begin{bmatrix} ห & ฉ & ข \\ ถ & ุ & ็ \end{bmatrix}$$

ข้อความที่ได้จากการเข้ารหัส คือ หถฉุข็

การถอดรหัส

ห ถ ฉ ุ ข ็

(2,40) (2,21) (2,8) (2,50) (2,1) (2,58)

| ห ถ | ฉ ุ | ข ็ |
|---|---|---|
| (2,40) (2,21) | (2,8) (2,50) | (2,1) (2,58) |

หถฉุข็

$$k^{-1} = \begin{bmatrix} (2,38) & (1,59) \\ (2,52) & (1,30) \end{bmatrix} \times \begin{bmatrix} (2,40) & (2,8) & (2,1) \\ (2,21) & (2,50) & (2,58) \end{bmatrix} = \begin{bmatrix} (1,12) & (1,38) & (1,43) \\ (1,30) & (1,40) & (1,50) \end{bmatrix} = \begin{bmatrix} M & m & r \\ e & o & y \end{bmatrix}$$

ข้อความที่ได้จากการถอดรหัส คือ Memory

**สรุปผลการวิจัย**

งานวิจัยนี้เป็นการสร้างกุญแจ (กุญแจเข้ารหัส) และกุญแจตัวผกผัน (กุญแจถอดรหัส) โดยผู้วิจัยได้ออกแบบเป็นเทคนิคเฉพาะ โดยการนิยามตัวผกผันการบวกและตัวผกผันการคูณใหม่ภายใต้การดำเนินการ $Z_3 \times Z_{67}^*$ เพื่อให้สามารถสร้างกุญแจได้มากขึ้น แต่หาผลลัพธ์จากการเข้ารหัสได้ยากยิ่งขึ้น ทำให้การเข้ารหัสนั้นมีความปลอดภัยมากยิ่งขึ้น นอกจากนี้ ผู้ที่สนใจสามารถสร้างกุญแจการเข้ารหัส รวมไปถึงแก้สมการเพื่อหากุญแจการถอดรหัส ซึ่งผู้อื่นไม่สามารถรับรู้ได้ อย่างไรก็ตาม ก็จะทำให้มีอักษรบางตัวที่ไม่สามารถนำมาสร้างกุญแจได้ อาทิเช่น ก , A , > ดังที่หมายเหตุไว้ข้างต้น จากการศึกษาพบว่า

กุญแจในการเข้ารหัส คือ

$$k = \begin{bmatrix} C & ฆ \\ ข & H \end{bmatrix} = \begin{bmatrix} (1,2) & (2,5) \\ (2,1) & (1,7) \end{bmatrix}$$

กุญแจในการถอดรหัส คือ

$$k^{-1} = \begin{bmatrix} ษ & æ \\ เ & e \end{bmatrix} = \begin{bmatrix} (2,38) & (1,59) \\ (2,52) & (1,30) \end{bmatrix}$$

**กิตติกรรมประกาศ**

งานวิจัยฉบับนี้สำเร็จลงได้ด้วยดี เนื่องจากอาจารย์ที่ปรึกษา อาจารย์ ดร.นพรัตน์ ไวโรจนะ อาจารย์กมลรัตน์ สมบุตร ที่กรุณาให้คำปรึกษาตลอดจนแนวทางการปรับปรุงแก้ไขข้อบกพร่องต่าง ๆ ด้วยความเอาใจใส่อย่างดียิ่ง ผู้วิจัยตระหนักถึงความตั้งใจจริงและความทุ่มเทของอาจารย์และขอกราบขอบพระคุณเป็นอย่างสูงไว้ ณ ที่นี้

ผู้วิจัยขอกราบขอบพระคุณผู้เขียนตำราและหนังสือ ที่ได้ใช้เป็นเอกสารอ้างอิง ผู้วิจัยหวังว่างานวิจัยฉบับนี้จะมีประโยชน์อยู่ไม่มากก็น้อย จึงขอมอบส่วนดีทั้งหมดนี้ให้แก่เหล่าคณาจารย์ที่ได้ประสิทธิประสาทวิชาจนทำให้ผลงานวิจัยเป็นประโยชน์ต่อผู้ที่เกี่ยวข้อง สำหรับข้อบกพร่องต่าง ๆ ที่อาจจะเกิดขึ้นนั้น ผู้วิจัยขอน้อมรับผิดชอบเพียงผู้เดียว และยินดีที่จะรับฟังคำแนะนำจากทุกท่านที่เข้ามาศึกษา เพื่อเป็นประโยชน์ในการพัฒนางานวิจัยต่อไป

**เอกสารอ้างอิง**

Bootstrap. (2017). Re:Solving System of Linear Equations Using Matrix. Retrieved Septemper 6th, 2019, from https://www.opendurian.com/

BURNSIDE, W. (1897). Re: Theory of groups of finite order. University Press, Cambridge.

Chaweewan Rattanaprasert. (2008). Re: Algebra Plan in the Department of Mathematics. Department of Mathematics. Faculty of Science. Silpakorn University, Thailand.

Gallian, Joseph A. (2010). Re: Direct product. Retrieved August 7th, 2019, from https://en.wikipedia.org/wiki/Direct_product_of_groups

Jajalove. (2010). Re: Encode – Decode for Security of Information. Retrieved August 7th, 2019, from https://itm633.wordpress.com

J.S. Milne. (2019). Re: Group Theory. Retrieved August 5th, 2019, from https://www.jmilne.org/math/CourseNotes/GT.pdf

Lester S. Hill. (1929). Re: Cryptography in an Algebraic Alphabet. The American

Mathematical Monthly, Vol. 36, No. 6, pp. 306-312. https://www.jstor.org/stable/2298294?seq=1

OpenDurian, (2017). Re: Solving System of Linear Equations Using Matrix Retrieved August 3th, 2019, from https://www.opendurian.com/learn/solving_system_of_linear_equations_using_matrix/

Suwimon Phuphiphat. (2013). Re: Row operations. Retrieved August 7th, 2019, from https://suwimon030835.blogspot.com/2013/06/inverse.html.

Weisstein, (1999-2020). Re: GroupDirectProduct. Retrieved August 3th, 2019, from https://mathworld.wolfram.com/GroupDirectProduct.html

**Translate Thai References**

ฉวีวรรณ รัตนประเสริฐ. 2551. พีชคณิตแผนในภาควิชาคณิตศาสตร์. สาขาวิชาคณิตศาสตร์.คณะวิทยาศาสตร์. มหาวิทยาลัยศิลปากร.

สุวิมล ภูพิพัฒน์. 2556. การดำเนินงานแบบแถว. [ออนไลน์], เข้าถึงได้จาก: https://suwimon030835.blogspot.com/2013/06/inverse.html.(2562, 7 สิงหาคม).

ศุภากร กังพิสดาร. 2553. วิทยาการเข้ารหัสลับเพื่อความมั่นคงปลอดภัยของเครือข่าย. วิทยานิพนธ์วิทยาศาสตรมหาบัณฑิต. สาขาวิชาความมั่นคงทางระบบสารสนเทศ.คณะวิทยาการอละเทคโนโลยีสารสนเทศ. มหาวิทยาลัยเทคโนโลยีมหานคร.

นารีรัตน์ พูลสวัสดิ์. 2562. การเข้ารหัสด้วยพีชคณิต. สาขาวิชาคณิตศาสตร์ประยุกต์. คณะวิทยาศาสตร์และเทคโนโลยี.มหาวิทยาลัยราชภัฏวไลยอลงกรณ์ ในพระบรมราชูปถัมภ์ จังหวัดปทุมธานี.