วิทยาการเข้ารหัสลับและเทคโนโลยีบล็อกเชน

Cryptography and Blockchain Technology

ผู้ช่วยศาสตราจารย์ ดร. ชาญศักดิ์ ศรีสวัสดิ์สกุล

วท.ม. (ธุรกรรมอิเล็กทรอนิกส์) ปร.ด. (เทคโนโลยีสารสนเทศ)

คณะวิทยาการคอมพิวเตอร์ มหาวิทยาลัยราชภัฏอุบลราชธานี

วิทยาการเข้ารหัสลับและเทคโนโลยีบล็อกเชน

เขียนโดย ผู้ช่วยศาสตราจารย์ ดร. ชาญศักดิ์ ศรีสวัสดิ์สกุล
พิมพ์ครั้งที่ 1 พ.ศ. 2566

ราคา 349 บาท

ข้อมูลทางบรรณานุกรมของหอสมุดแห่งชาติ

ชาญศักดิ์ ศรีสวัสดิ์สกุล.
วิทยาการเข้ารหัสลับและเทคโนโลยีบล็อกเชน.-- อุบลราชธานี : คณะวิทยาการคอมพิวเตอร์ มหาวิทยาลัยราชภัฏอุบลราชธานี, 2566.
300 หน้า.

1. บล็อกเชน. 2. รหัสต้นฉบับ (วิทยาการคอมพิวเตอร์). I. ชื่อเรื่อง.

005.74
ISBN (e-book) 978-616-608-304-0

จัดทำโดย:
ผู้ช่วยศาสตราจารย์ ดร. ชาญศักดิ์ ศรีสวัสดิ์สกุล
คณะวิทยาการคอมพิวเตอร์ มหาวิทยาลัยราชภัฏอุบลราชธานี
เลขที่ 2 ถ.ราชธานี ต.ในเมือง อ.เมือง จ.อุบลราชธานี 34000
Email: charnsak@charnsak.com

คำนำ

ท่ามกลางความเปลี่ยนแปลงอย่างรวดเร็วในยุคปัจจุบัน วิทยาการเข้ารหัสลับและเทคโนโลยีบล็อกเชนได้กลายเป็นเครื่องมือสำคัญในการปกป้องข้อมูล การสื่อสาร และการสร้างความเชื่อมั่นในระบบดิจิทัล โดยเฉพาะการนำมาประยุกต์ใช้ในด้านต่าง ๆ เช่น เงินตราเข้ารหัสลับที่กำลังปฏิวัติวงการเทคโนโลยีและสังคมดิจิทัลในปัจจุบัน จึงนับเป็นวิชาที่สำคัญมากต่อการเรียนทางด้านวิทยาการคอมพิวเตอร์ เทคโนโลยีสารสนสนเทศ และสาขาอื่น ๆ ที่เกี่ยวข้อง

ตำราเล่มนี้ได้ถูกจัดทำขึ้นมาเพื่อใช้ในการเรียนการสอนรายวิชา วิทยาการเข้ารหัสลับและเทคโนโลยีบล็อกเชน รหัสรายวิชา 4123142 ของหลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชานวัตกรรมดิจิทัล พ.ศ. 2563 คณะวิทยาการคอมพิวเตอร์ มหาวิทยาลัยราชภัฏอุบลราชธานี ซึ่งเป็นสาขาที่เน้นผสมผสานนวัตกรรมกับโลกธุรกิจ หนังสือเล่มนี้ได้ออกแบบให้ครอบคลุมกับคำอธิบายรายวิชา ดังนี้

“พื้นฐานวิทยาการเข้ารหัสลับ วิทยาการเข้ารหัสแบบบล็อก วิทยาการเข้ารหัสแบบกระแสข้อมูล วิทยาการเข้ารหัสลับแบบสมมาตรและอสมมาตร รหัสพิสูจน์ตัวจริงข้อความ การพิสูจน์ตัวจริง การควบคุมการเข้าถึง การอนุญาตให้เข้าใช้ ระบบลายมือชื่อดิจิทัล แอปพลิเคชันของวิทยาการเข้ารหัสลับ การทำงานของบล็อกเชน การนำบล็อกเชนไปใช้ การสร้างบล็อกเชน”

ข้าพเจ้ามีความพยายามเป็นอย่างยิ่งที่จะเขียนตำราเล่มให้สามารถทำความเข้าใจได้โดยง่ายและรวดเร็วที่สุดด้วยตัวเอง โดยที่ไม่ต้องเรียนในชั้นเรียน โครงสร้างของตำราถูกออกแบบให้ครอบคลุมคำอธิบายรายวิชาดังกล่าว โดยมีเนื้อหาทั้งหมด 9 บท ได้แก่ พื้นฐานวิทยาการเข้ารหัสลับ วิทยาการเข้ารหัสลับแบบสมมาตร วิทยาการเข้ารหัสลับแบบอสมมาตร การควบคุมการเข้าถึง แอปพลิเคชันของการเข้ารหัสลับ หลักการทำงานของบล็อกเชน บิตคอยน์และเงินตราเข้ารหัสลับ การประยุกต์ใช้บล็อกเชน และ การสร้างบล็อกเชน

ในบทต่าง ๆ ได้มีการสอดแทรกและสังเคราะห์ผลการศึกษาจากงานวิจัยและจากประสบการณ์ของผู้เขียนในรูปแบบกรณีศึกษา ประกอบไปด้วยหัวข้อวิจัย 3 หัวข้อ คือ 1) Lectrading : เว็บไซต์จำลองการเทรดเหรียญคริปโตเคอร์เรนซี่ โดยอิงราคา เหรียญตามจริง 2) การพัฒนาต้นแบบระบบรายงานผลการเรียนด้วยเทคโนโลยีบล็อกเชน กรณีศึกษานักศึกษาในจังหวัดอุบลราชธานี และ 3) VaccChain วัคซีนพาสปอร์ตบนเทคโนโลยีบล็อกเชน โดยทั้ง 3 งานวิจัยนี้ถูกจัดเป็นกรณีศึกษาในหัวข้อที่ 7.7 8.12 และ 8.13 ตามลำดับ

คำศัพท์ภาษาอังกฤษและศัพท์เทคนิคในตำรานี้นำมาจาก ระบบศัพท์บัญญัติของสำนักงานราชบัณฑิตยสภา และ ระบบฐานข้อมูลคำทับศัพท์ของสำนักงานราชบัณฑิตยสภา ส่วนคำศัพท์ที่ไม่สามารถหาได้จากระบบดังกล่าว จะใช้วิธีการเขียนทับศัพท์ตามประกาศสำนักนายกรัฐมนตรี เรื่อง หลักเกณฑ์การทับศัพท์ภาษาอังกฤษ พ.ศ. 2532 การอ้างอิงใช้ระบบ American Psychological Association 7th edition

ตำราเล่มนี้ไม่อาจสำเร็จขึ้นมาได้หากขาดการช่วยเหลือ การสนับสนุน กำลังใจ และแรงบันดาลใจจากผู้คนสำคัญในชีวิตของข้าพเจ้าตลอดมา ข้าพเจ้าขอกราบขอบพระคุณอาจารย์ผู้ที่มอบความรู้และเปิดโลกทัศน์ ข้าพเจ้าขอบคุณอย่างสุดหัวใจไปยังทุก ๆ คนในครอบครัวของข้าพเจ้า โดยเฉพาะภรรยาและลูก ๆ ที่เป็นดั่งแรงบันดาลใจและความสุขที่ไม่มีวันจางหายในทุก ๆ วันของชีวิต รวมไปถึง นายโตมร คำทอง นักศึกษาปริญญาตรี คณะวิทยาการคอมพิวเตอร์ มหาวิทยาลัยราชภัฏอุบลราชธานี ที่ร่วมดำเนินงานวิจัยที่เกี่ยวข้องอย่างตั้งใจจนประสบความสำเร็จ และสุดท้ายขอขอบพระคุณผู้ทรงคุณวุฒิทั้ง 2 ท่านที่ได้ช่วยประเมินเนื้อหาในตำราเล่มนี้และได้ให้ความเห็นข้อเสนอแนะ ที่เป็นประโยชน์ก่อนที่จะเผยแพร่สู่สาธารณชน

ผู้เขียนหวังเป็นอย่างยิ่งว่าตำราเล่มนี้จะเป็นประโยชน์ต่อ นักศึกษา อาจารย์ ร่วมถึงผู้อ่านที่สนใจทั่วไป ผู้เขียนยินดีน้อมรับคำติชมและข้อเสนอแนะใด ๆ ที่จะช่วยให้ตำรานี้สมบูรณ์ยิ่งขึ้น เพื่อนำไปพัฒนาปรับปรุงตำราต่อไป โดยสามารถติดต่อข้าพเจ้าได้ที่ charnsak@charnsak.com

ผู้ช่วยศาสตราจารย์ ดร. ชาญศักดิ์ ศรีสวัสดิ์สกุล
มหาวิทยาลัยราชภัฏอุบลราชธานี

สารบัญ

หน้า

คำนำ ..... **ก**

สารบัญ ..... **ค**

สารบัญตาราง ..... **ช**

สารบัญภาพ ..... **ฌ**

บทที่ 1 พื้นฐานวิทยาการเข้ารหัสลับ **1**

1.1 บทนำ 1

1.2 ความรู้เบื้องต้นเกี่ยวกับวิทยาการเข้ารหัสลับ 1

1.3 หลักการพื้นฐานของการเข้ารหัสลับ 2

1.4 ระบบการเข้ารหัสลับดั้งเดิม 6

1.5 ระบบการเข้ารหัสลับสมัยใหม่ 13

1.6 สรุป 17

แบบฝึกหัดท้ายบทที่ 1 19

บทที่ 2 วิทยาการเข้ารหัสลับแบบสมมาตร **21**

2.1 บทนำ 21

2.2 การเข้ารหัสลับแบบสมมาตร 21

2.3 เอกซ์คลูซีฟออร์ 23

2.4 วิทยาการเข้ารหัสแบบกระแสข้อมูล 24

2.5 วิทยาการเข้ารหัสแบบบล็อก 26

2.6 รหัสพิสูจน์ตัวจริงข้อความ 30

2.7 มาตรฐานการเข้ารหัสข้อมูล 33

2.8 มาตรฐานการเข้ารหัสขั้นสูง 35

2.9 สรุป 38

แบบฝึกหัดท้ายบทที่ 2 39

บทที่ 3 วิทยาการเข้ารหัสลับแบบอสมมาตร **41**

3.1 บทนำ 41

3.2 แนะนำวิธีการเข้ารหัสแบบอสมมาตร....41
3.3 ริเวสต์-ชาร์เมียร์-เอเดิลแมน....45
3.4 การเข้ารหัสลับด้วยเส้นโค้งอิลลิปติก....56
3.5 ลายมือชื่ออิเล็กทรอนิกส์....57
3.6 สรุป....62
แบบฝึกหัดท้ายบทที่ 3....63
บทที่ 4 การควบคุมการเข้าถึง....65
4.1 บทนำ....65
4.2 การควบคุมการเข้าถึง....65
4.3 การระบุตัวตน....69
4.4 การพิสูจน์ตัวจริง....69
4.5 การอนุญาตให้เข้าใช้....74
4.6 การตรวจสอบได้....75
4.7 ระบบบริหารจัดการตัวตนและการเข้าถึงทรัพยากร....77
4.8 สรุป....78
แบบฝึกหัดท้ายบทที่ 4....81
บทที่ 5 แอปพลิเคชันของวิทยาการเข้ารหัสลับ....83
5.1 บทนำ....83
5.2 แอปพลิเคชันของวิทยาการเข้ารหัสลับในด้านต่าง ๆ....83
5.3 บล็อกเชน: แอปพลิเคชันของวิทยาการเข้ารหัสลับแห่งยุค....88
5.4 แอปพลิเคชันของวิทยาการเข้ารหัสลับในเทคโนโลยีบล็อกเชน....91
5.5 ประวัติของเทคโนโลยีบล็อกเชน....92
5.6 ประเภทของเทคโนโลยีบล็อกเชน....94
5.7 บล็อกเชนกับระบบจัดการฐานข้อมูลแบบดั้งเดิม....96
5.8 เงินตราเข้ารหัสลับ และ เศรษฐศาสตร์คริปโท....98
5.9 สรุป....98
แบบฝึกหัดท้ายบทที่ 5....101
บทที่ 6 หลักการทำงานของบล็อกเชน....103
6.1 บทนำ....103
6.2 องค์ประกอบของบล็อกเชน....103
6.3 ฟังก์ชันแฮช....105

6.4 ต้นไม้เมอร์เคิล 108
6.5 โครงสร้างของบล็อกเชน 110
6.6 ระบบฉันทมติ ในบล็อกเชน 117
6.7 สัญญาอัจฉริยะและแอปพลิเคชันกระจายศูนย์ 120
6.8 สรุป 124
แบบฝึกหัดท้ายบทที่ 6 125
บทที่ 7 บิตคอยน์และเงินตราเข้ารหัสลับ 127
7.1 บทนำ 127
7.2 เงินคืออะไร 127
7.3 บิตคอยน์ 133
7.4 เหรียญทางเลือก 144
7.5 กระเป๋าเงินตราเข้ารหัสลับ 157
7.6 การซื้อขายแลกเปลี่ยนเงินตราเข้ารหัสลับ 166
7.7 กรณีศึกษา: Lectrading เว็บไซต์จำลองการเทรดเหรียญคริปโตเคอร์เรนซี่ โดยอิงราคาเหรียญตามจริง 171
7.8 สรุป 174
แบบฝึกหัดท้ายบทที่ 7 175
บทที่ 8 การประยุกต์ใช้บล็อกเชน 177
8.1 บทนำ 177
8.2 การเปลี่ยนให้เป็นโทเค็น 178
8.3 อุตสาหกรรมการเงิน 186
8.4 อุตสาหกรรมการตลาดและการโฆษณา 189
8.5 อุตสาหกรรมประกันชีวิตและประกันภัย 190
8.6 อุตสาหกรรมสุขภาพ 191
8.7 อุตสาหกรรมการศึกษา 193
8.8 อุตสาหกรรมอสังหาริมทรัพย์ 195
8.9 การระดมทุนจากบุคคลทั่วไป 199
8.10 อุตสาหกรรมพลังงาน 204
8.11 อุตสาหกรรมการเกษตร 207
8.12 กรณีศึกษาจากงานวิจัยของผู้เขียน 1 “การพัฒนาต้นแบบระบบรายงานผลการเรียนด้วยเทคโนโลยีบล็อกเชนของนักศึกษาในจังหวัดอุบลราชธานี” 208

8.13 กรณีศึกษาจากงานวิจัยของผู้เขียน 2 “VaccChain วัคซีนพาสปอร์ตบนเทคโนโลยีบล็อกเชน” 211
8.14 พระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561 213
8.15 สรุป 214
แบบฝึกหัดท้ายบทที่ 8 215
บทที่ 9 การสร้างบล็อกเชน 217
9.1 บทนำ 217
9.2 สร้างบล็อกเชนอย่างง่ายด้วยไพทอน 217
9.3 การสร้างบล็อกเชนส่วนตัวด้วยเครือข่ายอีเธอเรียม 233
9.4 สร้างสัญญาอัจฉริยะด้วยทรัฟเฟิลสวีต 241
9.5 บล็อกเชนในรูปแบบการบริการ 259
9.6 สรุป 262
แบบฝึกหัดท้ายบทที่ 9 263
บรรณานุกรม 265
ประวัติผู้เขียน 273
ดัชนี 274

สารบัญตาราง

หน้า

ตารางที่ 1.1 ความแตกต่างระหว่างระบบการเข้ารหัสลับแบบดั้งเดิมและสมัยใหม่ 14
ตารางที่ 2.1 ตารางความจริงเมื่อทำการเอกซ์คลูซีฟออร์ 23
ตารางที่ 2.2 ขนาดกุญแจและจำนวนรอบที่ต้องการในการเข้ารหัส 36
ตารางที่ 3.1 เปรียบเทียบคุณสมบัติระหว่าง อีซีซี และ อาร์เอสเอ..... 56
ตารางที่ 3.2 เปรียบเทียบขนาดกุญแจระหว่าง อีซีซี และ อาร์เอสเอ ที่มีความปลอดภัยเทียบเท่า... 59
ตารางที่ 5.1 ความหมายของคำที่เกี่ยวข้องกับบล็อกเชนโดยองค์กรระดับนานาชาติ 89
ตารางที่ 5.2 เปรียบเทียบความแตกต่างระหว่างบล็อกเชนและระบบฐานข้อมูลแบบดั้งเดิม 97
ตารางที่ 6.1 โครงสร้างข้อมูลของบล็อกเชนที่บิตคอยน์ใช้ 111
ตารางที่ 6.2 เขตข้อมูลที่เก็บไว้ในบล็อกส่วนหัวของบิตคอยน์..... 111
ตารางที่ 7.1 เปรียบเทียบคุณลักษณะของเงินระหว่าง ทองคำ เงินเฟียต และบิตคอยน์..... 133
ตารางที่ 8.1 เปรียบเทียบคุณสมบัติของการเงินดั้งเดิม และฟินเทค 188
ตารางที่ 8.2 เปรียบเทียบคุณลักษณะอสังหาริมทรัพย์แบบดั้งเดิมและ แพลตฟอร์มอสังหาริมทรัพย์บนบล็อกเชน..... 198

สารบัญภาพ

หน้า

ภาพที่ 1.1 ขั้นตอนการเข้ารหัสลับ 4
ภาพที่ 1.2 ขั้นตอนการถอดรหัส 4
ภาพที่ 1.3 โมเดลซีไอเอ 5
ภาพที่ 1.4 การเข้ารหัสซีซาร์ไซเฟอร์ 7
ภาพที่ 1.5 การเข้ารหัสด้วยการแทนที่ตัวอักษรแบบเดี่ยว 8
ภาพที่ 1.6 การเข้ารหัสข้อความ “gotobangkok” ด้วยการแทนที่ตัวอักษรแบบเดี่ยว 9
ภาพที่ 1.7 การแทนค่าเข้ารหัสของวีฌแนร์ 10
ภาพที่ 1.8 เครื่อง Enigma ขณะที่กำลังถูกใช้งาน 12
ภาพที่ 1.9 เว็บแอปพลิเคชัน CrypTool ขณะใช้เข้ารหัสซีซาร์ 14
ภาพที่ 1.10 พื้นฐานระบบการเข้ารหัสลับสมัยใหม่ 16
ภาพที่ 2.1 วิธีการเข้ารหัสลับและถอดรหัสลับแบบสมมาตร 22
ภาพที่ 2.2 การเข้ารหัสลับแบบกระแสข้อมูล 25
ภาพที่ 2.3 เข้ารหัสลับกระแสข้อมูลแบบประสานเวลา (ขวา) การเข้ารหัสลับกระแสข้อมูลแบบไม่ประสานเวลา (ซ้าย) 25
ภาพที่ 2.4 ขั้นตอนในการเข้ารหัสแบบบล็อก 27
ภาพที่ 2.5 ขั้นตอนในการถอดรหัสแบบบล็อก 28
ภาพที่ 2.6 การทำงานของวิทยาการเข้ารหัสแบบบล็อกในโหมด ECB 28
ภาพที่ 2.7 การทำงานของวิทยาการเข้ารหัสแบบบล็อกในโหมด ไซเฟอร์บล็อกเชนนิ่ง 29
ภาพที่ 2.8 การทำงานรหัสพิสูจน์ตัวจริงข้อความ 32
ภาพที่ 2.9 ทดลองการสร้าง HMAC 33
ภาพที่ 2.10 ค่า HMAC ที่ได้จากการคำนวณ 33
ภาพที่ 2.11 เครื่องมือ EFF DES cracker สำหรับโจมตีมาตรฐานการเข้ารหัสข้อมูล 35
ภาพที่ 2.12 ขั้นตอนการทำงานของมาตรฐานการเข้ารหัสขั้นสูง 37
ภาพที่ 3.1 การเข้ารหัสแบบอสมมาตรทั่วไป 42
ภาพที่ 3.2 การสร้างกุญแจของ RSA 46

หน้า

ภาพที่ 3.3 การทำงานของ ริเวสต์-ชาร์เมียร์-เอเดิลแมน ระหว่างผู้รับและผู้ส่ง....48
ภาพที่ 3.4 การทำงานของ OpenSSL ที่สามารถเข้ารหัสและถอดรหัส....50
ภาพที่ 3.5 คำสั่งเพื่อสร้างกุญแจส่วนตัวโดยใช้ขนาดกุญแจ 1024 บิตด้วยอัลกอริทึม ริเวสต์-ชาร์เมียร์-เอเดิลแมน....50
ภาพที่ 3.6 ไฟล์ private.pem ที่เก็บค่ากุญแจส่วนตัวไว้....51
ภาพที่ 3.7 คำสั่งเพื่อสร้างกุญแจสาธารณะด้วยกุญแจส่วนตัวของ ริเวสต์-ชาร์เมียร์-เอเดิลแมน....52
ภาพที่ 3.8 ตัวอย่างกุญแจสาธารณะของ ริเวสต์-ชาร์เมียร์-เอเดิลแมน....52
ภาพที่ 3.9 การสร้างกุญแจส่วนตัวของ ริเวสต์-ชาร์เมียร์-เอเดิลแมน....53
ภาพที่ 3.10 การสร้างกุญแจสาธารณะของ ริเวสต์-ชาร์เมียร์-เอเดิลแมน....54
ภาพที่ 3.11 สร้างข้อความต้นฉบับเพื่อทดลองเข้ารหัส....54
ภาพที่ 3.12 ใช้คำสั่งเพื่อเข้ารหัสไฟล์ข้อความ....55
ภาพที่ 3.13 ใช้คำสั่งเพื่อถอดรหัสไฟล์ข้อความ....55
ภาพที่ 3.14 การทำงานของลายมือชื่อดิจิทัล....61
ภาพที่ 4.1 ตัวอย่างกระบวนการควบคุมการเข้าถึง....67
ภาพที่ 4.2 การทำงานของอุปกรณ์พิสูจน์ตัวจริง....73
ภาพที่ 4.3 โปรแกรมผู้รับชมเหตุการณ์ ใน วินโดวส์ 10 และ วินโดวส์ 11....77
ภาพที่ 5.1 การเข้ารหัสด้วยกุญแจสาธารณะของ เอชทีทีพีเอส....84
ภาพที่ 5.2 การเข้ารหัสแบบต้นทางถึงปลายทางในโปรแกรมสนทนา....85
ภาพที่ 5.3 การใช้งานบิตล็อกเกอร์ เพื่อเข้ารหัสไฟล์ในระบบปฏิบัติการวินโดวส์....87
ภาพที่ 5.4 เส้นเวลาการพัฒนาของบิตคอยน์....93
ภาพที่ 5.5 ประเภทของเทคโนโลยีบล็อกเชน....95
ภาพที่ 6.1 องค์ประกอบของบล็อกเชน....104
ภาพที่ 6.2 การทำงานทางเดียวของฟังก์ชันแฮช....105
ภาพที่ 6.3 คุณสมบัติที่ต้องเหมือนเดิมเสมอของค่าแฮชไม่ว่าจะใช้กี่ครั้งก็ตาม....106
ภาพที่ 6.4 ตัวอย่างการทำงานของฟังก์ชันแฮช....106
ภาพที่ 6.5 ความต้านทานการชนกันของฟังก์ชันแฮช....107
ภาพที่ 6.6 ตัวอย่างการใช้ฟังก์ชันแฮชในการตรวจสอบความถูกต้อง....108
ภาพที่ 6.7 การทำงานของฟังก์ชันแฮชในบริบทของบล็อกเชน....108
ภาพที่ 6.8 ตัวอย่างการใช้ฟังก์ชันแฮชในต้นไม้เมอร์เคิล....109

หน้า

ภาพที่ 6.9 รูปแบบโครงสร้างข้อมูลแบบรายการโยง 110
ภาพที่ 6.10 รูปแบบโครงสร้างข้อมูลของบล็อกเชนแบบง่าย 110
ภาพที่ 6.11 โครงสร้างการทำงานของบล็อกเชนสำหรับบิตคอยน์ 112
ภาพที่ 6.12 แสดงขั้นตอนการเพิ่มธุรกรรมเข้าสู่บล็อกเชน 115
ภาพที่ 7.1 สรุปคุณลักษณะที่ดีของเงิน 129
ภาพที่ 7.2 บัตรเครดิตที่ใช้กันในปัจจุบัน 131
ภาพที่ 7.3 ตัวอย่างการใช้รหัสคิวอาร์เพื่อชำระเงิน 131
ภาพที่ 7.4 วิวัฒนาการของเงิน 133
ภาพที่ 7.5 แผนที่แสดงโหนดที่กำลังทำงานของบิตคอยน์ 136
ภาพที่ 7.6 บล็อกหมายเลข 170 ของบิตคอยน์ 140
ภาพที่ 7.7 รายการธุรกรรมที่เกิดขึ้นในบล็อกหมายเลข 170 ของบิตคอยน์ 140
ภาพที่ 7.8 หมายเลขกระเป๋าของนากาโมโต้ที่ปัจจุบันยังมี BTC เหลืออยู่ 141
ภาพที่ 7.9 บล็อกล่าสุดในบล็อกเชนของบิตคอยน์ในขณะที่เขียนตำรา 142
ภาพที่ 7.10 ปริมาณ BTC ที่มีอยู่ในระบบ 142
ภาพที่ 7.11 การโดนโจมตีของ Bitcoin Gold 144
ภาพที่ 7.12 เว็บไซต์ CoinGecko ที่ให้บริการข้อมูลเหรียญทั่วโลก 145
ภาพที่ 7.13 ค่าของเหรียญ USDT ที่จะมีค่าใกล้เคียง 1 USD ตลอดเวลา 146
ภาพที่ 7.14 อีลอน มัสก์ โพสต์รูปสุนัขทำให้ราคา โดชคอยน์ ราคาสูงขึ้น 300% 148
ภาพที่ 7.15 เหรียญสควิดเกมถูกเทขายจาก ราคา 523 เหลือกเพียง 0.003 ดอลลาร์สหรัฐ 148
ภาพที่ 7.16 ระบบดูข้อมูลธุรกรรมในไลท์คอยน์ 149
ภาพที่ 7.17 ระบบดูข้อมูลธุรกรรมใน อีเธอเรียม 151
ภาพที่ 7.18 ระบบดูข้อมูลธุรกรรมของเหรียญริปเปิ้ล 152
ภาพที่ 7.19 ระบบดูข้อมูลธุรกรรม เครือข่ายคอร์นาโด 153
ภาพที่ 7.20 เว็บขาย เอ็นเอฟที Degenerate Ape Academy 154
ภาพที่ 7.21 ระบบดูข้อมูลธุรกรรม โซลาน่า 155
ภาพที่ 7.22 ระบบดูข้อมูลธุรกรรม โพลีกอน 157
ภาพที่ 7.23 รายงานธุรกรรมของที่อยู่กระเป๋าของ ซาโตชิ 161
ภาพที่ 7.24 Billfodl ตัวอย่างกระเป๋าเงินตราเข้ารหัสลับโลหะ 163
ภาพที่ 7.25 BitBox ตัวอย่างกระเป๋าเงินตราเข้ารหัสลับแบบฮาร์ดแวร์ 164

หน้า

ภาพที่ 7.26 ตัวอย่างกระเป๋าเงินเว็บในกระดานซื้อขาย Bitkub 165
ภาพที่ 7.27 ตัวอย่างกระเป๋าเงินซอฟต์แวร์ที่ได้รับความนิยม Atomic Wallet 166
ภาพที่ 7.28 การแลกเปลี่ยนเงินตราเข้ารหัสลับและเงินบาทในเว็บ Bitkub 168
ภาพที่ 7.29 ตัวอย่างการจับคู่เหรียญของ Binance 169
ภาพที่ 7.30 การใช้งานแลกเปลี่ยนใน Uniswap 170
ภาพที่ 7.31 lectrading.online เว็บไซต์สำหรับจำลองการซื้อขายเงินตราเข้ารหัสลับ 172
ภาพที่ 7.32 ตัวอย่างหน้าจอการซื้อขายแบบ Spot 173
ภาพที่ 7.33 ตัวอย่างหน้าจอจำลองกระเป๋าเงินตราเข้ารหัสลับ 173
ภาพที่ 8.1 หน้าที่มีการประมูลทวีตแรกในระบบ OpenSea 182
ภาพที่ 8.2 บิทคับเอ็นเอฟที สำหรับซื้อขาย เอ็นเอฟที ของไทย 182
ภาพที่ 8.3 รายการโทเค็นที่ใช้มาตรฐาน ERC-20 ในการพัฒนา 184
ภาพที่ 8.4 หน้าเว็บ AAVE สำหรับการกู้ยืมเหรียญเงินตราเข้ารหัสลับ 187
ภาพที่ 8.5 หน้าเว็บ Compound.finance สำหรับการกู้ยืมเหรียญเงินตราเข้ารหัสลับ 187
ภาพที่ 8.6 บริษัท NYIAX แพลตฟอร์มที่ทำหน้าที่ซื้อขายสัญญาโฆษณาล่วงหน้า 190
ภาพที่ 8.7 บริษัท Lemonade ที่ให้บริการกรมธรรม์บนสัญญาอัจฉริยะ 191
ภาพที่ 8.8 บริษัท BurstIQ ให้บริการโซลูชันด้านการแพทย์ด้วยบล็อกเชน 192
ภาพที่ 8.9 บริษัท Chronicled ที่เชี่ยวชาญด้านห้วงโซ่อุปทาน 193
ภาพที่ 8.10 บริษัท Blockcerts บริการรายงานผลการเรียน 195
ภาพที่ 8.11 บริษัท SMARTRealty เพื่อนำสัญญาอัจฉริยะมาใช้ในการทำสัญญาต่าง ๆ 197
ภาพที่ 8.12 บริษัท เรียลท์ ที่เปิดให้ลงทุนในอสังหาริมทรัพย์ด้วยบล็อกเชน 198
ภาพที่ 8.13 บริษัท indiegogo ที่ให้บริการการระดมทุนจากบุคคลทั่วไป 200
ภาพที่ 8.14 ข้อมูลการทำไอซีโอของ อีเธอเรียม 201
ภาพที่ 8.15 Binance Launchpad เว็บไซต์เพื่อทำ ไออีโอ ของไบแน๊นซ์ 202
ภาพที่ 8.16 บริษัท โพลิแมท ที่ให้บริการทำเอสทีโอแบบครบวงจร 204
ภาพที่ 8.17 บริษัท พาวเวอร์ เล็ดเจอร์ ที่เปิดให้ขายไฟฟ้าจากพลังงานแสงอาทิตย์ได้โดยตรง 205
ภาพที่ 8.18 บริษัท โซลาร์คอยน์ เปลี่ยนการผลิตไฟฟ้าเป็นเงินตราเข้ารหัสลับ 206
ภาพที่ 8.19 Wholechain ให้บริการระบบติดตามห่วงโซ่อุปทานบนบล็อกเชน 207
ภาพที่ 8.20 ตัวอย่างปัญหาการรับทำคุณวุฒิปลอมของประเทศไทย 208
ภาพที่ 8.21 กรอบแนวคิดงานวิจัยและผลการทดลอง 210

หน้า

ภาพที่ 8.22 ตัวอย่างเอกสารรับรองการฉีดวัคซีนแบบดั้งเดิม 212
ภาพที่ 8.23 กรอบแนวคิดการพัฒนา VaccChain 213
ภาพที่ 9.1 เว็บไซต์เพื่อความโหลดโปรแกรมติดตั้ง ไพชาร์ม 218
ภาพที่ 9.2 ไฟล์ติดตั้งโปรแกรม ไพชาร์ม สำหรับ วินโดวส์ 219
ภาพที่ 9.3 หน้าจอต้อนรับเข้าสู่โปรแกรมติดตั้ง 219
ภาพที่ 9.4 หน้าจอสำหรับกำหนดโฟลเดอร์เพื่อติดตั้งโปรแกรม ไพชาร์ม 220
ภาพที่ 9.5 ตัวเลือกการตั้งค่าสำหรับติดตั้งโปรแกรม 220
ภาพที่ 9.6 กำหนดชอร์ตคัทสำหรับเรียกใช้โปรแกรม 221
ภาพที่ 9.7 โปรแกรม ไพชาร์ม ขณะที่กำลังติดตั้ง 221
ภาพที่ 9.8 เมื่อติดตั้งเสร็จแล้วให้ทำการรีสตาร์ทคอมพิวเตอร์ 1 ครั้ง 222
ภาพที่ 9.9 นโยบายในการแบ่งปันข้อมูลแบบนิรนาม ส่วนนี้จะเลือกเป็น Send หรือ Don’t Send ก็ได้ 222
ภาพที่ 9.10 เมื่อเปิดโปรแกรม ไพชาร์ม ขึ้นมาครั้งแรก 223
ภาพที่ 9.11 การตั้งค่าเพื่อสร้างโปรเจกต์ใหม่ 223
ภาพที่ 9.12 ไฟล์โปรเจกต์ใหม่เพิ่งสร้างขึ้น 224
ภาพที่ 9.13 การติดตั้ง Flask และ jsonify 225
ภาพที่ 9.14 การสั่งให้แอปพลิเคชันทำงานและดู URL ที่เข้าใช้ 231
ภาพที่ 9.15 คำสั่งเรียกฟังก์ชัน mine_block() 232
ภาพที่ 9.16 การแสดงบล็อกทั้งหมดในเชน 232
ภาพที่ 9.17 เว็บสำหรับดาวน์โหลดเก็ท 234
ภาพที่ 9.18 เว็บไซต์หลักของกานาช 235
ภาพที่ 9.19 ไฟล์สำหรับ ติดตั้ง Ganache ใน วินโดวส์ 236
ภาพที่ 9.20 เริ่มการติดตั้งให้คลิกที่ Install 236
ภาพที่ 9.21 ภาพขณะกำลังติดตั้งโปรแกรม 237
ภาพที่ 9.22 หน้าจอแสดงขอความร่วมมือในการติดตามการใช้งาน 237
ภาพที่ 9.23 เริ่มสร้างพื้นที่การทำงานใหม่ให้กับบล็อกเชน 238
ภาพที่ 9.24 รายการกระเป๋าเงินตราเข้ารหัสลับ 239
ภาพที่ 9.25 คลิกปุ่ม Save เพื่อบันทึกพื้นที่การทำงาน 240
ภาพที่ 9.26 พื้นที่ทำงานที่ได้ถูกบันทึกเอาไว้ 240

หน้า

ภาพที่ 9.27 เว็บสำหรับดาวน์โหลดและติดตั้ง Node.js สำหรับระบบปฏิบัติการต่าง ๆ 242
ภาพที่ 9.28 ไฟล์สำหรับติดตั้ง Node.js บน วินโดวส์ 242
ภาพที่ 9.29 เริ่มติดตั้งโปรแกรม Node.js ให้คลิกที่ Next 243
ภาพที่ 9.30 ทำการคลิกปุ่มยอมรับเงื่อนไขในการใช้งานและคลิก Next..... 243
ภาพที่ 9.31 เลือกโฟลเดอร์ที่ต้องการติดตั้ง ไม่จำเป็นต้องเปลี่ยนค่า คลิก Next 244
ภาพที่ 9.32 เลือกติดตั้งตามมาตรฐานของ Node.js คลิก Next 244
ภาพที่ 9.33 ระบบติดตั้งเครื่องมือเพิ่มเติม ในกรณีนี้ไม่ต้องใช้ คลิก Next..... 245
ภาพที่ 9.34 โปรแกรม Node.js กำลังติดตั้ง 245
ภาพที่ 9.35 ติดตั้งโปรแกรม Node.js สำเร็จแล้ว 246
ภาพที่ 9.36 ตั้งค่า PowerShell ให้สามารถติดตั้งโปรแกรมได้ 246
ภาพที่ 9.37 เริ่มติดตั้งโปรแกรม Truffle Suite 247
ภาพที่ 9.38 สร้างโครงการสำหรับทรัฟเฟิล..... 248
ภาพที่ 9.39 โครงสร้างโฟลเดอร์สำหรับทรัฟเฟิล..... 248
ภาพที่ 9.40 การสั่งให้โปรแกรมสร้างเมต้าคอยน์บ็อกซ์..... 249
ภาพที่ 9.41 โครงสร้างโฟลเดอร์ของเมต้าคอยน์บ็อกซ์ที่โปรแกรมสร้างให้ 250
ภาพที่ 9.42 ผลของการสั่งให้โปรแกรมทดสอบเมต้าคอยน์ บ็อกซ์ 253
ภาพที่ 9.43 ผลของการสั่งคอมไพล์สัญญาอัจฉริยะ..... 253
ภาพที่ 9.44 การติดตั้งสัญญาอัจฉริยะไปยังบล็อกเชนสำเร็จ 254
ภาพที่ 9.45 การติดตั้งสัญญาอัจฉริยะไปยังบล็อกเชนสำเร็จ 255
ภาพที่ 9.46 แสดงรายการธุรกรรมที่เกิดจากการสร้างสัญญาอัจฉริยะ..... 255
ภาพที่ 9.47 รายละเอียดของธุรกรรม 255
ภาพที่ 9.48 คำสั่งเมื่อเข้า Truffle Console 256
ภาพที่ 9.49 คำสั่งเมื่อเข้า Truffle Console (ต่อ)..... 256
ภาพที่ 9.50 คำสั่งเรียกดูยอดเงินคงเหลือ..... 257
ภาพที่ 9.51 บล็อกที่ถูกสร้างขึ้นใหม่เมื่อมีการโอนเหรียญ 258
ภาพที่ 9.52 ธุรกรรมของการโอนเหรียญที่บันทึกอยู่ในบล็อก..... 258
ภาพที่ 9.53 เว็บไซต์หลักของอเมซอนแมนเนจบล็อกเชน 260
ภาพที่ 9.54 เว็บไซต์หลักของ Coinbase Cloud 261
ภาพที่ 9.55 เว็บไซต์หลักของ IBM Blockchain Platform 262

บทที่ 1
พื้นฐานวิทยาการเข้ารหัสลับ

1.1 บทนำ

ในยุคปัจจุบันที่เทคโนโลยีดิจิทัลและการสื่อสารผ่านเครือข่ายอินเทอร์เน็ตได้รับการพัฒนาอย่างรวดเร็ว ข้อมูลและธุรกรรมมากมายทั้งเรื่องส่วนตัวและการทำงานต่างถูกส่งและใช้งานผ่านทางช่องทางนี้ทั้งสิ้น ดังนั้นเพื่อให้ข้อมูลที่ส่งผ่านเครือข่ายอินเทอร์เน็ตมีความปลอดภัย มีความเป็นส่วนตัว มีความสมบูรณ์ และคุณสมบัติอื่น ๆ การประยุกต์ใช้วิทยาการเข้ารหัสลับกลายเป็นสิ่งที่ขาดไม่ได้เนื่องจากเป็นปัจจัยหลักที่สนับสนุนให้การสื่อสารและการจัดเก็บข้อมูลสามารถดำเนินการได้อย่างปลอดภัยและมีประสิทธิภาพ ดังนั้นในบทที่ 1 นี้จะเป็นการแนะนำท่านผู้อ่านเข้าสู่โลกของวิทยาการเข้ารหัสลับ โดยมีหัวข้อที่จะถูกนำเสนอตามลำดับดังนี้

1) ความรู้เบื้องต้นของวิทยาการเข้ารหัสลับ
2) หลักการพื้นฐานของวิทยาการเข้ารหัสลับ
3) การเข้ารหัสลับดั้งเดิม
4) การเข้ารหัสลับแบบสมัยใหม่

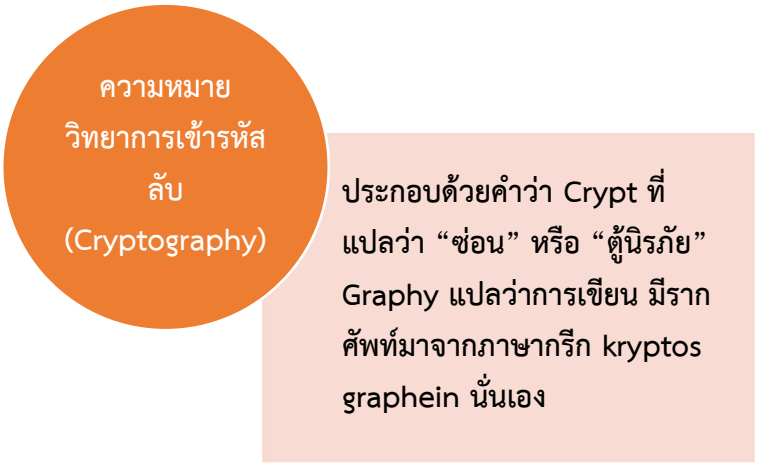
เนื้อหาในบทนี้จะช่วยเตรียมความพร้อมให้ผู้อ่านสามารถนำความรู้ไปใช้ประโยชน์ในอนาคตและเป็นพื้นฐานที่สำคัญสำหรับการศึกษาและทำความเข้าใจในบทต่อ ๆ ไป

1.2 ความรู้เบื้องต้นเกี่ยวกับวิทยาการเข้ารหัสลับ

เมื่อเกิดการสื่อสารแลกเปลี่ยนข้อมูลขึ้นสิ่งที่สำคัญที่สุดคือการรักษาความลับของสารหรือข้อมูลที่จะทำการแลกเปลี่ยน เป้าหมายของการรักษาความลับคือ ทำอย่างไรให้ข้อมูลนั้นสามารถถูกเปิดอ่านได้เฉพาะผู้รับสารเท่านั้นที่ หรือกล่าวในอีกนัยหนึ่งคือการที่ไม่อนุญาตให้บุคคลที่สามสามารถเข้าถึงข้อมูลดังกล่าวได้ นักวิชาการตั้งแต่อดีตจนถึงปัจจุบันจึงได้คิดค้นวิธีการทำให้ข้อมูลที่เราส่งอยู่ในรูปแบบที่ถูกซ่อน และไม่สามารถอ่านได้ด้วยบุคคลอื่น วิธีการเหล่านี้เรียกว่า **“วิทยาการเข้ารหัสลับ (Cryptography)”**

ในปัจจุบันนี้วิทยาการเข้ารหัสลับเป็นสาขาที่รวมเอาศาสตร์ทางคณิตศาสตร์และวิทยาการคอมพิวเตอร์ที่มุ่งเน้นเพื่อการรักษาความลับของข้อมูลในยุคดิจิทัล ทั้งในการสื่อสารและการจัดเก็บข้อมูลในเครื่องคอมพิวเตอร์ สาระสำคัญของวิทยาการเข้ารหัสลับอยู่ที่การแปลงข้อมูลจากรูปแบบที่

อ่านแล้วเข้าใจได้ (Plaintext) เป็นข้อมูลที่เข้าใจไม่ได้ (Ciphertext) โดยใช้วิธีที่เรียกว่า **“การเข้ารหัสลับ (Encryption)”** และการย้อนกลับข้อมูลเหล่านั้นเป็นรูปแบบที่อ่านแล้วเข้าใจได้โดยใช้วิธี **“การถอดรหัสลับ (Decryption)”** (Singh, 1999)



ตัวอย่างเช่นหากคุณผู้อ่านมีข้อความ “HELLO” และต้องการส่งข้อความเหล่าไปยังปลายทางอย่างเป็นความลับ โดยใช้วิธีการเข้ารหัสแบบดั้งเดิมอย่าง การเข้ารหัสแบบ ซีซาร์ ไซเฟอร์ ที่เป็นวิธีการเข้ารหัสลับที่เรียบง่ายเพียงแค่เลื่อนแต่ละอักษรออกไป 3 ตำแหน่งในอักษรภาษาอังกฤษ ดังนั้นการเข้ารหัส “HELLO” จะได้ผลลัพธ์คือ “KHOOR” สิ่งที่คุณผู้อ่านต้องทำคือส่งข้อความ “KHOOR” ไปยังปลายทาง และแจ้งปลายทางว่า นี่เป็นการเข้ารหัสด้วยซีซาร์ ไซเฟอร์ ปลายทางจะทำการถอดรหัสด้วยวิธีย้อนกลับ ก็จะได้เป็นข้อความ “HELLO” ตามเดิม

อย่างไรก็ดีวิทยาการเข้ารหัสลับเป็นมากกว่าการเข้ารหัสและการถอดรหัสลับข้อความเท่านั้น ปัจจุบันสามารถนำไปใช้งานได้หลากหลาย เช่น การรับรองความถูกต้องของข้อมูล การทำให้ข้อมูลแปลงกลับไปเป็นต้นฉบับเดิมไม่ได้ การพิสูจน์ตัวจริงของบุคคล เป็นต้น ทำให้วิทยาการเข้ารหัสลับเป็นหัวใจสำคัญในโลกดิจิทัลและอินเทอร์เน็ต การนำเอาวิทยาการเข้ารหัสลับไปประยุกต์ใช้ก่อให้เกิดบริการต่าง ๆ มากมาย เช่น การทำธุรกรรมทางการเงินออนไลน์ การส่งอีเมลที่เข้ารหัส และการสร้างและตรวจสอบลายมือชื่อดิจิทัล เป็นต้น

1.3 หลักการพื้นฐานของการเข้ารหัสลับ

ดังที่ได้กล่าวไปแล้วว่าหัวใจพื้นฐานของการเข้ารหัสลับคือการรักษาความลับของข้อมูล เพื่อปกป้องข้อมูลเหล่านั้น และการจะปกป้องข้อมูลได้นั้นวิธีที่เป็นมาตรฐานที่สุดคือทำให้ข้อมูลที่ถูกส่งไปมานั้นไม่สามารถถูกอ่านได้โดยผู้ที่ไม่มีสิทธิ์ ซึ่งมีหลักการดังนี้

1.3.1 ทำไมถึงต้องมีการเข้ารหัสลับ

ทำไมเราถึงต้องมีการเข้ารหัสลับ ประโยชน์หลัก ๆ ของการเข้ารหัสลับมีดังนี้

1) ความปลอดภัยและความเป็นส่วนตัวของข้อมูล

การเข้ารหัสลับช่วยให้ข้อมูลที่ส่งผ่านการสื่อสารปลอดภัยและมีความเป็นส่วนตัว เนื่องจาก พื้นฐานของวิทยาการเข้ารหัสลับเป็นกระบวนการที่จะทำให้ข้อมูลไม่สามารถอ่านหรือเข้าใจได้ ทำให้เมื่อถูกส่งผ่านไปทางเครือข่ายสาธารณะ ถึงแม้จะมีคนเห็นข้อมูลเข้ารหัสก็ไม่สามารถที่จะอ่านเข้าใจได้ นอกจากผู้ที่ได้รับอนุญาตที่มีกุญแจที่ถูกต้องสำหรับการถอดรหัสเท่านั้น (Stallings, 2017) เช่น การเข้ารหัสอีเมลส่วนตัว การเข้ารหัสการสื่อสารออนไลน์ หรือการเข้ารหัสข้อมูลบนฮาร์ดไดรฟ์ ทำให้ผู้ไม่ประสงค์ดีไม่สามารถเข้าถึงข้อมูลที่สำคัญของคุณได้

2) การเข้ารหัสลับและการสื่อสารออนไลน์

อินเทอร์เน็ตเป็นสถานที่ที่ผู้คนสื่อสารและแบ่งปันข้อมูลกันอย่างมหาศาลและรวดเร็ว ทำให้มีความเสี่ยงที่ข้อมูลจะถูกดักจับข้อมูลหรือถูกโจมตีสูงมากขึ้นตามไปด้วย ดังนั้น ในปัจจุบันข้อมูลที่ใช้ในบริการต่าง ๆ ที่อยู่ในโลกอินเทอร์เน็ตจะมีการเข้ารหัสลับอยู่เกือบตลอดเวลา การเข้ารหัสลับช่วยให้ผู้ใช้สามารถสื่อสารอย่างปลอดภัยผ่านอินเทอร์เน็ต โดยไม่ต้องกังวลว่าข้อมูลของคุณจะถูกผู้อื่นดักฟังหรือถูกโจมตี ยกตัวอย่างบริการในอินเทอร์เน็ตที่ต้องใช้การเข้ารหัสลับได้แก่ การทำธุรกรรมทางการเงิน การรับส่งอีเมล การซื้อขายสินค้าออนไลน์ การเข้าสู่เว็บไซต์ เป็นต้น

1.3.2 คำจำกัดความที่สำคัญของการเข้ารหัสลับ

การเข้ารหัสลับเป็นวิทยาการที่มีความซับซ้อนและมีคำศัพท์เฉพาะทางที่หลากหลาย การทำความเข้าใจในคำศัพท์เหล่านี้จึงจำเป็นสำหรับผู้ที่ต้องการศึกษาศาสตร์การเข้ารหัสลับ ในหัวข้อนี้ช่วยให้ผู้อ่านทำความเข้าใจเกี่ยวกับคำศัพท์และนิยามที่เกี่ยวข้องกับการเข้ารหัสลับ เพื่อให้ผู้อ่านมีความเข้าใจที่ถูกต้องในการศึกษาบทต่อ ๆ ไป โดยมีคำศัพท์พื้นฐานที่ต้องเข้าใจดังนี้

1) ข้อความต้นฉบับ หรือ ข้อความดั้งเดิม หรือ ข้อความธรรมดา (Plaintext) คือข้อความหรือข้อมูลที่สามารถเข้าใจได้ตามปกติโดยผู้ใช้ ข้อความเหล่านี้ไม่มีการเข้ารหัสใด ๆ หากเปรียบกับข้อมูลในคอมพิวเตอร์ก็คือข้อมูลที่สามารถเปิดอ่านได้เลยนั่นเอง เช่นไฟล์ .txt เป็นต้น

2) ข้อความเข้ารหัส (Ciphertext) คือ ข้อความหรือข้อมูลที่ถูกเข้ารหัสแล้ว ทำให้ไม่สามารถอ่านหรือเข้าใจได้โดยที่ยังไม่ได้ทำการถอดรหัสได้ ในโลกคอมพิวเตอร์เปรียบเสมือนไฟล์ PDF ที่เข้ารหัสไว้ หรือการเข้ารหัสไฟล์ให้ไม่สามารถอ่านได้ เป็นต้น

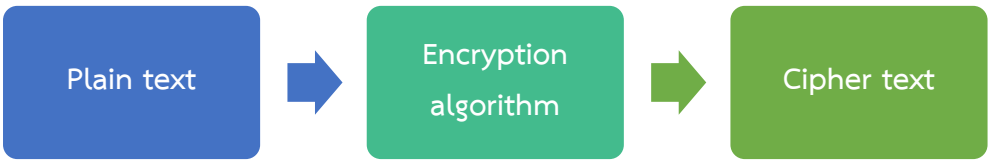
3) อัลกอริทึมการเข้ารหัสหรือวิธีการเข้ารหัสลับ (Encryption algorithm) เป็นกระบวนการ เทคนิค หรือ ขั้นตอนที่ใช้ในการแปลงข้อความต้นฉบับเป็นข้อความเข้ารหัส

4) อัลกอริทึมการถอดรหัสหรือวิธีการถอดรหัสลับ (Decryption algorithm) เป็นกระบวนการ เทคนิค หรือ ขั้นตอนที่ใช้ในการแปลงข้อความเข้ารหัสเป็นข้อความต้นฉบับ

5) กุญแจ (Key) คือรหัส (Code) หรือข้อมูลที่ใช้ร่วมกับอัลกอริทึมการเข้ารหัสหรือถอดรหัสเพื่อให้สามารถทำงานในการเข้ารหัส หรือถอดรหัสได้โดยสมบูรณ์

1.3.3 ขั้นตอนพื้นฐานของการเข้ารหัสลับ

ขั้นตอนพื้นฐานในการเข้ารหัสลับประกอบด้วยการเลือกข้อความที่ต้องการเข้ารหัส การเลือกอัลกอริทึมการเข้ารหัส ซึ่งจะมีอยู่มากมายหลายวิธี อาจจะใช้หรือไม่ใช้คู่กับกุญแจประเภทต่าง ๆ ก็ได้ จากนั้นทำการส่งข้อความต้นฉบับเข้าไปให้กับอัลกอริทึมการเข้ารหัส ผลลัพธ์ที่ได้จะได้เป็นข้อความเข้ารหัสออกมา ผู้ส่งสามารถนำเอาข้อความเข้ารหัสนี้ส่งไปยังผู้รับได้ทันที สำหรับขั้นตอนการถอดรหัสเป็นกระบวนการย้อนกลับ กล่าวคือ ผู้จะใช้จะต้องส่งข้อความเข้ารหัสให้กับอัลกอริทึมถอดรหัส จากนั้นอัลกอริทึมจะส่งเป็นข้อความต้นฉบับออกมา จะเห็นว่าแม้ข้อความเข้ารหัสจะถูกเปิดโดยผู้อื่นที่ไม่ทราบอัลกอริทึมในการถอดรหัสจะไม่สามารถอ่านข้อความนั้นได้ (นอกจากการเบรกการเข้ารหัส) ขั้นตอนเหล่านี้แสดงอยู่ในภาพที่ 1.1 และ 1.2

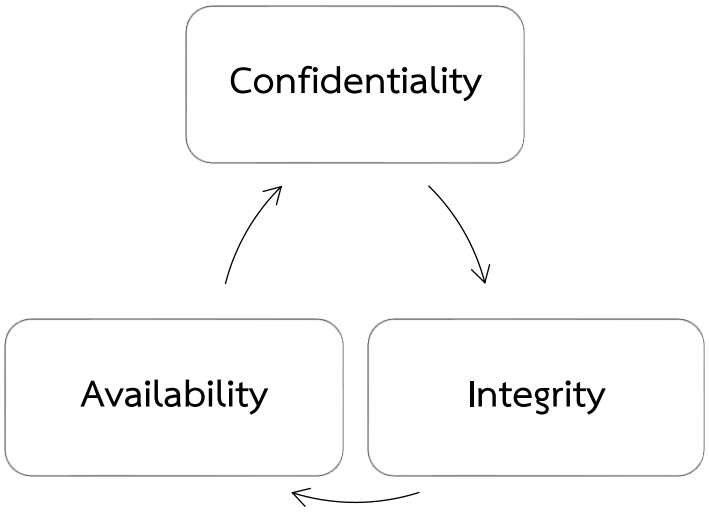


ภาพที่ 1.1 ขั้นตอนการเข้ารหัสลับ

ภาพที่ 1.2 ขั้นตอนการถอดรหัส

1.3.4 ส่วนประกอบด้านความปลอดภัยของระบบสารสนเทศ

กรอบแนวคิด ความลับ ความสมบูรณ์ ความพร้อมใช้งาน เรียกอีกชื่อว่า **“โมเดลซีไอเอ (Confidentiality Integrity Availability; CIA)”** คือองค์ประกอบและรูปแบบพื้นฐานที่ใช้ในการนิยามเกี่ยวกับขั้นตอนและองค์ประกอบของการปกป้องและรักษาความปลอดภัยของข้อมูล (Anderson, 1972) โดยโมเดลนี้แสดงอยู่ในภาพที่ 1.3 แต่ละองค์ประกอบมีความหมายดังนี้



ภาพที่ 1.3 โมเดลซีไอเอ

ที่มา: Anderson, 1972

1) ความลับ (Confidentiality) หมายถึงการรักษาความลับของข้อมูล คือ ข้อมูลนั้นถูกเก็บรักษาและปกป้องจากการเข้าถึงโดยบุคคลหรือระบบที่ไม่ได้รับอนุญาต ตัวอย่างเช่น ข้อมูลทางการเงินของลูกค้าในธนาคารจะต้องถูกรักษาความลับจากผู้ที่ไม่มีสิทธิ์ในการเข้าถึงนอกจากเจ้าของบัญชีและเจ้าหน้าที่ที่มีความเกี่ยวข้องเท่านั้น

2) ความสมบูรณ์ (Integrity) หมายถึงการรักษาสภาพของข้อมูลให้คงความสมบูรณ์อยู่เสมอ คือ ข้อมูลนั้นต้องมีความถูกต้อง ไม่ถูกปรับเปลี่ยน แก้ไข ทำลายบางส่วน หรือทำให้สูญหายโดยไม่ได้รับอนุญาต ตัวอย่างเช่น ระบบการจัดการฐานข้อมูลของโรงพยาบาลจะต้องรักษาความสมบูรณ์ของข้อมูลทางการแพทย์ของผู้ป่วยให้มีความถูกต้องเสมอ

3) ความพร้อมใช้งาน (Availability) หมายถึงการที่ข้อมูลนั้นจะต้องสามารถเข้าถึงได้และพร้อมใช้งานได้ทุกเมื่อที่ต้องการ ตัวอย่างเช่น ระบบจองตั๋วออนไลน์ของสายการบินจะต้องมีความพร้อมใช้สูงเพื่อให้ผู้ใช้สามารถจองตั๋วได้ในเวลาที่ต้องการไม่ว่าจะเป็นเวลาใด

โมเดลซีไอเอเป็นโมเดลที่ถูกใช้กันอย่างแพร่หลายตั้งแต่ในยุคอดีตมาจนถึงยุคปัจจุบันสำหรับการประเมินและปรับปรุงความปลอดภัยของข้อมูลในองค์กรและบริษัทต่างๆ แต่ปัจจุบันนี้นอกจากแค่โมเดลซีไอเอยังได้มีการเพิ่มตัวแปรเข้ามาเพื่อให้ทันกับการพัฒนาของเทคโนโลยี นั่นคือ

4) การไม่สามารถปฏิเสธความรับผิดชอบ (Non-Repudiation) หมายถึง คือการป้องกันไม่ให้ผู้ใช้ปฏิเสธความรับผิดชอบต่อการดำเนินการหรือธุรกรรมที่เกิดขึ้น หรือก็คือการรับรองว่าผู้ใช้ได้ทำธุรกรรมบางอย่างที่เกิดขึ้นแล้วจริง ไม่สามารถปฏิเสธได้ ไม่ว่าจะเป็นการส่งข้อมูล การรับข้อมูล หรือการแก้ไขข้อมูล ตัวอย่างเช่น หากผู้ใช้ได้ทำการส่งอีเมลไปยังบุคคลอื่น ผู้ใช้คนนั้นจะไม่สามารถปฏิเสธได้ว่าไม่ได้ส่งอีเมลนั้น หรือหากมีการลงชื่อดิจิทัลในเอกสาร ผู้ที่ลงชื่อจะไม่สามารถปฏิเสธได้ว่าพวกเขาไม่ได้ลงชื่อ เป็นต้น ทั้งหมดนี้ต้องพิสูจน์ได้ด้วยวิธีการบางอย่าง

1.3.5 ความแข็งแกร่งในการเข้ารหัสลับ

ความแข็งแกร่งในการเข้ารหัสลับเป็นหนึ่งในปัจจัยสำคัญที่กำหนดว่าข้อมูลหรือการสื่อสารของเรานั้นมีความปลอดภัยมากน้อยเพียงใด ความแข็งแกร่งในที่นี้ไม่ได้หมายถึงความซับซ้อนของวิธีการเข้ารหัสเท่านั้น แต่ยังรวมถึงความยากของการโจมตีในรูปแบบต่าง ๆ เพื่อถอดรหัส เรียกว่าการทำลาย หรือเบรกรหัส (Codebreaking) ซึ่งขึ้นอยู่กับหลายปัจจัย เช่น ความยาวของกุญแจ อัลกอริทึมการเข้ารหัส และความเร็วในการประมวลผลของเทคโนโลยีปัจจุบัน หรืออีกนัยหนึ่งคือความแข็งแกร่งของการเข้ารหัสลับสามารถวัดได้ด้วย**เวลาและทรัพยากร**ที่ใช้ในการถอดรหัสลับจากข้อมูลเข้ารหัสเป็นข้อความธรรมดาโดยที่ไม่มีวิธีการถอดรหัส

ดังนั้นการเลือกใช้วิธีการเข้ารหัสที่มีความแข็งแกร่งสูงจะช่วยป้องกันไม่ให้ข้อมูลถูกบุกรุกหรือถูกเข้าถึงโดยไม่ได้รับอนุญาตได้โดยง่าย แต่ในขณะเดียวกันยังต้องพิจารณาถึงประสิทธิภาพในการใช้งานเพื่อให้การสื่อสารหรือการจัดเก็บข้อมูลสามารถดำเนินการได้อย่างรวดเร็วและมีประสิทธิภาพ หากการเข้ารหัสหรือถอดรหัสใช้เวลานานเกินไป หรือทำให้สิ้นเปลืองทรัพยากรมากเกินไป ก็จะทำให้ไม่สะดวกในการใช้งานจริง เป็นต้น

1.4 ระบบการเข้ารหัสลับดั้งเดิม

การเข้ารหัสลับนั้นมีประวัติยาวนาน ระบบการเข้ารหัสลับดั้งเดิมหรือ Classic Cryptosystem นั้นใช้วิธีการที่ผู้คนทั่วไปสามารถทำความเข้าใจเพื่อทำการเข้ารหัสและถอดรหัสได้โดยไม่ต้องใช้ความรู้เฉพาะทาง หรือเครื่องมือ อุปกรณ์พิเศษใด ๆ การเข้ารหัสลับแบบนี้มักจะใช้การแปลงข้อความต้นฉบับให้เป็นข้อความที่ยากต่อการอ่านหรือเข้าใจ โดยมีเทคนิคการเข้ารหัสดังนี้

1.4.1 การเข้ารหัสลับด้วยวิธีสับเปลี่ยน

การเข้ารหัสด้วยวิธีสับเปลี่ยน (Substitution Cipher) คือ ระบบการเข้ารหัสที่สลับตัวอักษรเป็นตัวอื่น เพื่อให้ไม่มีความหมาย ตัวอย่างการเข้ารหัสด้วยวิธีสับเปลี่ยนที่มีประวัติมายาวนานได้แก่วิธีที่เรียกว่า **“ซีซาร์ ไซเฟอร์ (Caesar cipher)”** ที่ถูกตั้งชื่อตามจูเลียสซีซาร์ (Julius Caesar) ซีซาร์แบบดั้งเดิมจะใช้วิธีการเลื่อนตัวอักษรไปทางขวา 3 ตำแหน่ง (เรียกว่า Shift key) เช่น a ถูกเปลี่ยนเป็น d b ถูกเปลี่ยนเป็น e c ถูกเปลี่ยนเป็น f และเป็นแบบนี้ต่อไปเรื่อย ๆ ตำแหน่งการเลื่อนสามารถเปลี่ยนได้ เพื่อไม่ให้ผู้โจมตีสามารถถอดรหัสได้โดยง่าย เช่น เลื่อนไปข้างหลัง 8 ตำแหน่ง (Shift key=-8) หรือ ข้างหน้า 7 ตำแหน่ง (Shift key=7) เป็นต้น ตัวอย่างเช่น หากเราต้องการใช้ซีซาร์ ไซเฟอร์ กับข้อความธรรมดาคำว่า “happy” เราก็จะได้ข้อความเข้ารหัสเป็น “kdssB” วิธีการนี้จะมีชื่อเรียกทางเทคนิคว่า “การเข้ารหัสแบบเลื่อนที่ใช้พื้นที่กุญแจแบบเพียงพอ **(Shift cipher and the sufficient key-space principle)**” (Katz & Lindell, 2020) เพื่อให้ผู้อ่านสามารถเห็นภาพได้ง่ายขึ้น ภาพที่ 1.4 แสดงตารางการสับเปลี่ยนตัวอักษรของการเข้ารหัสแบบ ซีซาร์ ไซเฟอร์แบบดั้งเดิม (Shift key=3) ในกรณีนี้จะเปรียบเทียบ Shift key ว่าเป็นกุญแจก็ได้

Text	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
Key	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

ภาพที่ 1.4 การเข้ารหัสซีซาร์ไซเฟอร์

1) วิธีการถอดรหัสซีซาร์ไซเฟอร์

การถอดรหัสซีซาร์ไซเฟอร์ ทำได้ง่ายมาก หากผู้ถอดรู้กุญแจที่ถูกใช้ในการเข้ารหัส วิธีการถอดรหัสเพียงแค่ทำการเลื่อนตัวอักษรไปทางซ้าย หรือ ขวาตามค่าของกุญแจ ตัวอย่างจากข้อความเข้ารหัส **KHOOR** ที่ได้กล่าวถึงไปก่อนหน้านี้ ถ้ากุญแจคือ 3 ผู้อ่านจะต้องเลื่อน **“K”** กลับไปเป็น **“H”**, **“H”** เป็น **“E”**, และ **“O”** เป็น **“L”**, และต่อไปเรื่อย ๆ และสุดท้ายจะได้ข้อความต้นฉบับเป็น **“HELLO”**

2) จุดแข็งของ ซีซาร์ไซเฟอร์

- ง่ายต่อการทำความเข้าใจและการใช้งาน
- สามารถใช้ได้กับทั้งข้อความและข้อมูลที่ไม่ใช่ข้อความ
- มีประโยชน์ในสภาวะที่มีการสื่อสารที่จำกัดมาก

➢ การเข้ารหัสและถอดรหัสทำได้โดยการคำนวณของมนุษย์

3) จุดอ่อนของ ซีซาร์ไซเฟอร์

ซีซาร์ ไซเฟอร์ มีข้อจำกัดอย่างร้ายแรงคือมีจำนวนกุญแจที่จำกัดเนื่องจากเป็น การเข้ารหัสแทนที่มีข้อจำกัดในการสับเปลี่ยน กล่าวคือถ้าเราพิจารณาเฉพาะในภาษาอังกฤษ จะมีเพียง 26 กุญแจที่เป็นไปได้หรือประมาณ 4 x 10^26 กุญแจ การเข้ารหัสนี้อาจถูกถอดออกได้เพียงแค่ใช้ทดลองอย่างรวดเร็วด้วยการทดสอบทั้งหมด 25 กุญแจไปเรื่อย ๆ หรือ เทคนิคที่เรียกว่า **“การใช้กำลังทำทั้งหมด” (Brute force)** แค่ใช้มนุษย์ร่วมกันคำนวณไม่นานก็จะสามารถถอดออกได้ทั้งหมด ยิ่งกว่านั้นในปัจจุบันที่คอมพิวเตอร์สามารถคำนวณได้อย่างรวดเร็วใช้เวลาเพียงเสี้ยววินาที

นอกจากนี้ยังไม่มีการป้องกันเมื่อใช้การวิเคราะห์ความถี่ สำหรับข้อความที่มีความยาวเพียงพอ ผู้โจมตีสามารถสังเกตการณ์ความถี่ของตัวอักษรที่ปรากฏในข้อความเข้ารหัส และเดาโดยใช้สถิติความถี่ของตัวอักษรที่เกิดในประโยคต่าง ๆ ได้ เช่น ในภาษาอังกฤษสระ เป็นตัวอักษรที่มีการใช้งานบ่อยมาก (A E I O U) ทำให้เดาได้อย่างง่ายดายจากในข้อความเข้ารหัส ต่อมากจากสถิติตัวอักษรที่ถูกใช้มากที่สุดในภาษาอังกฤษคือ e, t ซึ่งหากมีตัวอักษรใดซ้ำ ๆ คำเหล่านี้ก็สามารถคาดเดาได้ ไปจนถึงการใช้งานคำที่ใช้บ่อย ๆ เช่น “the”, “ing”, “and”, “ion” ข้อความที่ถูกเข้ารหัสแทนที่ด้วยกุญแจเดียวจึงสามารถถูกถอดรหัสได้ด้วยการสังเกตความถี่ของตัวอักษร

1.4.2 การเข้ารหัสแบบแทนที่ตัวอักษรแบบเดี่ยว

ในระบบการเข้ารหัสด้วยวิธีสับเปลี่ยนนั้น ตัวกุญแจก็คือจำนวนของตัวอักษรจะถูกกำหนดให้เปลี่ยนค่าแบบเรียงต่อกันไปเรื่อย ๆ การสับเปลี่ยนแบบนี้เกิดขึ้นแบบคงที่ขึ้นอยู่กับค่าของกุญแจดังที่ได้กล่าวไปแล้วในหัวข้อที่แล้ว แต่สำหรับ **“การเข้ารหัสแบบแทนที่ตัวอักษรแบบเดี่ยว (**Mono-alphabetic substitution cipher)” ตัวกุญแจจะถูกกำหนดโดยเฉพาะแบบไม่คงที่ ผ่านการสร้างแผนที่สำหรับจับคู่การแทนที่ตัวอักษรแบบสุ่ม ไม่มีกำหนดการเลื่อนค่าตัวอักษรแบบตายตัว โดยมีเงื่อนไขเดียวคือตัวอักษร 1 ตัวจะสามารถแทนที่ได้ด้วยกุญแจ 1 ตัวดังนั้น พื้นที่ของกุญแจประกอบด้วยการเชื่อมต่อหนึ่งต่อหนึ่งทั้งหมด ตัวอย่างของกุญแจที่ใช้กำหนดการแทนที่เป็นดังนี้

Text	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
Key	X	E	U	A	D	N	B	K	V	M	R	O	C	Q	F	S	Y	H	W	G	L	Z	I	J	P	T

ภาพที่ 1.5 การเข้ารหัสด้วยการแทนที่ตัวอักษรแบบเดี่ยว

จากภาพที่ 1.5 เข้าใจได้ง่าย ๆ หากต้องการเข้ารหัส เมื่อพบตัวอักษร a ก็แค่เปลี่ยนเป็น X b เปลี่ยนเป็น E t เปลี่ยนเป็น G (ตัวพิมพ์ใหญ่หรือพิมพ์เล็กตามแผนที่) ดังนั้นหากเราต้องการเข้ารหัสคำว่า “gotobangkok” ก็จะได้เป็น BFGFEXQBRFR ด้วยวิธีการจำคู่แบบ 1 ต่อ 1 โปรดดูภาพที่ 1.6 เพื่อความเข้าใจมากยิ่งขึ้น

ข้อความต้นฉบับ	g	o	t	o	b	a	n	g	k	o	k
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
ข้อความเข้ารหัส	B	F	G	F	E	X	Q	B	R	F	R

ภาพที่ 1.6 การเข้ารหัสข้อความ “gotobangkok” ด้วยการแทนที่ตัวอักษรแบบเดี่ยว

สมมุติว่าเราใช้ภาษาอังกฤษที่มีจำนวนตัวอักษรทั้งหมด 26 ตัวอักษร (A-Z) จำนวนความน่าจะเป็นทั้งหมดที่สามารถใช้ได้ของกุญแจจะมีขนาดเท่ากับ $26! = 26 \cdot 25 \cdot 24 \cdots 2 \cdot 1$ (เช่นเดียวกับซีซาร์) หรือประมาณ 2^{88} ซึ่งมีขนาดใหญ่มาก ทำให้เพิ่มความยากสำหรับการโจมตีด้วยการใช้กำลังทำทั้งหมดได้ แต่การเข้ารหัสนี้ก็ไม่ได้ปลอดภัยที่สุดซะทีเดียว ตรงกันข้ามแม้ว่าจะโจมตีแบบใช้กำลังทำทั้งหมดยาก แต่ในความเป็นจริงมีจุดอ่อนที่ง่ายต่อการทำลายระบบการเข้ารหัสนี้ ตัวอย่างเช่น เราสมมุติว่าข้อความที่ถูกเข้ารหัสเป็นข้อความภาษาอังกฤษ โดยข้อความที่จะถอดรหัสเป็นการเขียนภาษาอังกฤษที่ถูกต้องทางไวยากรณ์ ไม่ใช่แค่ข้อความที่เขียนโดยใช้ตัวอักษรของภาษาอังกฤษแบบสุ่มเท่านั้น ผู้โจมตีทำการวิเคราะห์สถิติของตัวอักษรต่าง ๆ ที่ปรากฏได้โดยเทคนิคดังนี้

1) เนื่องจากแผนที่การเข้ารหัสแต่ละอักษรจะเป็นค่าคงที่ ดังนั้นถ้าอักษร e ถูกจำคู่กับ D จะทำให้การปรากฏของ e ในข้อความต้นฉบับแสดงผลเป็น D ในข้อความเข้ารหัสลับทุกครั้ง ทำให้สามารถคาดเดาได้เช่น คำว่า Teen อาจจะเป็น ADDI ซึ่งเมื่อมีการใช้คำที่มีตัว e มาก ๆ เข้าก็จะสามารถเดาได้โดยง่ายว่า D คือ e นั่นเอง

2) การกระจายความถี่ของอักษรแต่ละตัวในข้อความภาษาอังกฤษ เป็นสิ่งที่สามารถเรียนรู้ได้และเป็นสิ่งที่มีข้อมูลกันมายาวนาน ทำให้ข้อความภาษาอังกฤษเพียงไม่กี่ประโยคที่ส่งออกไปก็จะสามารถจับคู่หรือ คาดเดาต่อไปได้ว่าน่าจะเป็นตัวอักษรใดมากกว่ากัน วิธีการนี้จะใช้งานได้ดีสำหรับข้อความที่มีความยาวระดับหนึ่ง

1.4.3 การเข้ารหัสแบบการแทนที่ด้วยหลายตัวอักษร หรือ การเข้ารหัสวีฌแนร์

การเข้ารหัสแบบการแทนที่ด้วยหลายตัวอักษร (Polyalphabetic substitution cipher) มีอีกชื่อเรียกว่า **“การเข้ารหัสวีฌแนร์ (Vigenère)”** ตั้งตามชื่อผู้คิดค้น Blaise de Vigenère นักคณิตศาสตร์ฝรั่งเศสในศตวรรษที่ 16 วีฌแนร์ ถูกออกแบบมาเพื่อป้องกันการโจมตีด้วยสถิติตัวอักษร ซึ่งเป็นจุดอ่อนของการเข้ารหัสแบบการแทนที่ตัวอักษรแบบเดี่ยว โดยใช้วิธีการสับเปลี่ยนโดยใช้ตัวอักษรหลาย ๆ ตัว ตัวอย่างเช่น กุญแจอาจจะจับคู่บล็อก 2 ตัวอักษร ab ไปยัง DZ แต่จับคู่ ac ไปยัง TY ซึ่งจะเห็นว่า ตัว a ที่อยู่ในคำนั้นเมื่อทำการเข้ารหัสแล้วไม่มีสิ่งใดที่เกี่ยวข้องกันเลย ทำให้การวิเคราะห์ทางสถิติของกระจายความถี่ของตัวอักษรไม่สามารถนำมาใช้ได้ การแทนที่จะกระทำไปครั้งละตัวอักษรในข้อความด้วยตัวอักษรที่ถูกเลื่อนไปตามกุญแจ ถ้ากุญแจมีความยาวน้อยกว่าข้อความกุญแจจะถูกทำซ้ำจนถึงความยาวของข้อความ ตารางแสดงการแทนค่าเข้ารหัสของวีฌแนร์ ถูกแสดงไว้ในภาพที่ 1.7 การเข้ารหัสแบบนี้ถูกเบรกรหัสได้ในปี พ.ศ. 2406 (ค.ศ. 1863) โดย Friedrich Kasiski ซึ่งเป็นชาวรัสเซีย

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

ภาพที่ 1.7 การแทนค่าเข้ารหัสของวีฌแนร์

1.4.4 การเข้ารหัสลับโดยการจัดเรียง

การเข้ารหัสลับโดยการจัดเรียง (Transposition Cipher) เป็นการเข้ารหัสข้อมูลที่ใช้การเปลี่ยนตำแหน่งอักษรในข้อความ แตกต่างจากการเข้ารหัสด้วยวิธีสับเปลี่ยนตรงที่เป็นการจัดเรียงเฉพาะตัวอักษรที่อยู่ในข้อความต้นฉบับเองเท่านั้น ตัวอย่างการเข้ารหัสลับแบบนี้คือ การเข้ารหัสแบบรั้วรางรถไฟ (Rail Fence Cipher) มีอีกชื่อเรียกว่าเป็น การเข้ารหัสแบบซิกแซก (Zigzag cipher) ซึ่งจะจัดเรียงตัวอักษรแบบรั้วและรางที่เชื่อมต่อกัน วิธีการคือทำการกำหนดจำนวนแถวที่ต้องการเอาไว้ จากนั้นทำการเขียนข้อความตามแนวทแยงให้ครบตามจำนวนแถว จากบนลงล่าง และล่างขึ้นบน โดยเว้นวรรคทุก ๆ ตัวอักษรที่มี โดยเอาช่องว่างและอักขระต่าง ๆ ออก ตัวอย่างเช่น การเข้ารหัสคำว่า **ATTACK AT NOON** ด้วยจำนวนแถวทั้งหมด 3 แถวจะได้ดังนี้

A				C				N			
	T		A		K		T		O		N
		T				A				O	

เมื่อได้ตำแหน่งแต่ละแถวแล้วให้ทำการรวมตัวอักษรทุกตัวในแต่ละแถวขึ้นมาเป็นแถวเดียว ก็จะได้เป็น **“ACNTAKTONTAO”** ซึ่งก็เป็นการเข้ารหัสที่ช่วยแก้ปัญหาเรื่องกุญแจ และความถี่และสถิติของตัวอักษรภาษาอังกฤษได้ ดังนั้นการเข้ารหัสแบบนี้จึงเหมาะสมกับข้อความที่มีความยาวไม่มากนัก และมีหลายคำในประโยค

1.4.5 การพัฒนาของการเข้ารหัสแบบดั้งเดิม

การเข้ารหัสลับแบบดั้งเดิมมีการพัฒนาอย่างต่อเนื่อง เกิดการพัฒนาแบบก้าวกระโดดในช่วงสงครามโลกครั้งที่ 2 ที่การเข้ารหัสลับถือเป็นสิ่งที่สำคัญอย่างมากในการทหาร ตัวอย่างเครื่องมือเข้ารหัสทางทหารที่มีชื่อเสียงได้แก่เครื่อง เอ็นนิกมา (Enigma) ซึ่งเป็นเครื่องมือเข้ารหัสที่ใช้ในระหว่างสงครามโลกครั้งที่สอง พัฒนาขึ้นโดยช่างกลชาวเยอรมันชื่อว่า อาเธอร์ เชอร์เบียส (Arthur Scherbius) ในปี พ.ศ. 2461 (ค.ศ. 1918) ซึ่งเครื่องมือนี้มีอัลกอริทึมที่สามารถเข้ารหัสข้อความโดยใช้วิธีการหมุนถอยหลัง (Rotor) และการสลับ (Substitution) ความท้าทายของเอ็นนิกมาอยู่ที่การกำหนดระดับความซับซ้อนของกุญแจ ซึ่งมีการเปลี่ยนแปลงตามประกาศของฝ่ายเยอรมันในการต่อสู้แต่ละวัน โดยการใช้เครื่องเอ็นนิกมากับคู่ของตัวอักษร 26 ตัว จะสามารถเกิดความน่าจะเป็นของกุญแจได้สูงถึง 150 ล้าน ล้าน รูปแบบเลยทีเดียว

ภาพที่ 1.8 เครื่อง Enigma ขณะที่กำลังถูกใช้งาน

ที่มา: Bundesarchiv, 1943

ในช่วงสงครามโลกครั้งที่สอง มีการใช้เอ็นนิกมาอย่างกว้างขวางในกองทัพเยอรมัน ซึ่งทางกองทัพเยอรมันมีความมั่นใจในเรื่องความปลอดภัยเป็นอย่างมาก โดยเฉพาะในการสื่อสารทางทะเล ขั้นตอน รูปแบบการสร้างเครื่องเอ็นนิกมาของเยอรมันนั้นเป็นความลับสูงสุด ทำให้ไม่มีใครสามารถถอดรหัสได้ จนกระทั่งในช่วงปี พ.ศ 2482 – 2483 (ค.ศ. 1939-1940) หน่วยงานความมั่นคงที่มีรหัสเรียกขานว่า อัลตร้า (Ultra) ของสหราชอาณาจักร ได้ทำการเรียนรู้ถึงขั้นตอนการเข้ารหัสของเครื่องเอ็นนิกมาและพัฒนาเครื่องเข้ารหัสของตนเองที่สามารถถอดรหัสข้อความจากเอ็นนิกมาได้ การรู้ความลับนี้ส่งผลให้ฝ่ายสัมพันธมิตรได้เปรียบทางการรบเป็นอย่างมาก ทำให้สหราชอาณาจักรสามารถเคลื่อนทัพเรือที่อยู่ในทะเลแอตแลนติก เพื่อเข้าโจมตีได้โดยที่เยอรมันไม่ทันตั้งตัว ช่วยให้สหราชอาณาจักรทราบแผนการโจมตีของเยอรมันและสามารถป้องกันได้ล่วงหน้า แม้จะผ่านไปหลายปีแล้ว เอ็นนิกมาส่งผลกระทบให้เกิดการพัฒนาเทคโนโลยีการเข้ารหัสลับอย่างต่อเนื่องมาจนถึงปัจจุบัน ปัจจุบันนี้เครื่องเอ็นนิกมาที่ยังหลงเหลืออยู่ ถูกเก็บรักษาไว้เป็นโบราณวัตถุที่มีคุณค่า เป็นสัญลักษณ์ของการถอดรหัสทางทหารและสามารถพบเห็นได้ในพิพิธภัณฑ์ทั่วโลก

หลังจากสงครามโลกครั้งที่สองสิ้นสุดลง ทั้งโลกยังคงต้องมีการดำเนินการทางทหารเพื่อพลิกฟื้นตนเองจากความบอบช้ำของสงคราม และก็เริ่มเข้าสู่ยุคสงครามเย็น ทำให้วิทยาการเข้ารหัสลับยังคงมีบทบาทสำคัญอย่างต่อเนื่อง ตัวอย่างเช่น สหภาพโซเวียตใช้วันไทม์แพ็ด (One-Time Pad) ใน

การรับส่งข้อมูลกับสายลับ วันไทม์แพ็ดใช้ปึกกระดาษที่มีตัวเลขสุ่มเป็นคีย์ในการเข้ารหัสข้อความ และแต่ละหน้ากระดาษจะใช้คีย์เพียงครั้งเดียวในการเข้ารหัสข้อความเดียว แต่ในช่วงนั้นสหภาพโซเวียตละเมิดกฎการใช้วันไทม์แพ็ดโดยใช้คีย์มากกว่าหนึ่งครั้ง ซึ่งทำให้ง่ายต่อการถอดรหัสข้อความ

ผู้อ่านจะเห็นได้ว่าระบบการเข้ารหัสลับนั้นมีประวัติการใช้งานและพัฒนาต่อเนื่องมาอย่างยาวนาน ทั้งในเรื่องของความปลอดภัย วิธีการสื่อสารทั่วไป และ การใช้ชีวิตประจำวัน เริ่มตั้งแต่ส่งกันด้วย คนส่งสาร กระดาษ คลื่นวิทยุ จนกระทั่งในปัจจุบันนี้ ข้อมูลที่ถูกส่งไม่ได้มีเพียงแค่ข้อความธรรมดาเหมือนเมื่อก่อนแล้ว แต่เป็นการพัฒนาให้อยู่ในรูปแบบข้อมูลที่ส่งผ่านการติดต่อสื่อสารด้วยระบบดิจิทัล ไม่ว่าจะเป็น รูปภาพ วิดีโอ เสียง และ อื่น ๆ ทำให้ระบบการเข้ารหัสจำเป็นที่จะต้องพัฒนาอย่างรวดเร็วและต่อเนื่อง กลายเป็นระบบการเข้ารหัสลับสมัยใหม่ที่จะไม่สามารถถูกถอดได้ด้วยบุคคลทั่วไปเหมือนก่อน ซึ่งจะต้องมีเครื่องมือ เทคนิค วิธีการขั้นสูงมากยิ่งขึ้นที่จะกล่าวในหัวข้อถัดไป

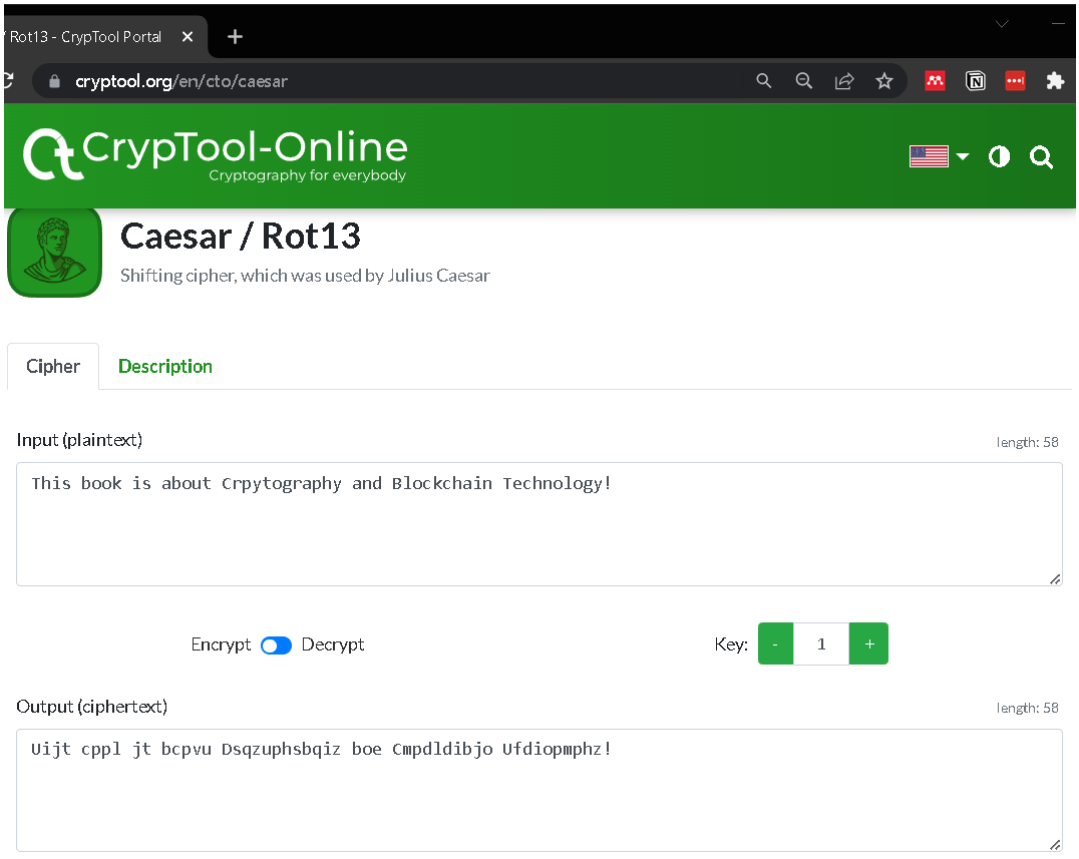
1.5 ระบบการเข้ารหัสลับสมัยใหม่

ปัจจุบันนี้ระบบคอมพิวเตอร์และเทคโนโลยีสารสนเทศและการสื่อสารได้มีการพัฒนาอย่างรวดเร็ว ทำให้การเข้ารหัสลับดั้งเดิมที่คนทั่วไปสามารถถอดได้ สามารถถูกถอดได้ด้วยคอมพิวเตอร์โดยใช้เวลาเพียงไม่กี่วินาที ที่สำคัญรูปแบบการติดต่อสื่อสารและการเก็บข้อมูลได้เปลี่ยนรูปแบบไปอยู่ในรูปแบบดิจิทัลเพื่อใช้งานในโลกคอมพิวเตอร์และอินเทอร์เน็ตเป็นส่วนใหญ่ ดังนั้น ระบบการเข้ารหัสลับแบบดั้งเดิมจึงไม่มีความปลอดภัยอีกต่อไปหากนำมาประยุกต์ใช้ในยุคนี้

เมื่อเทียบกับระบบเข้ารหัสแบบดั้งเดิมแล้ว ระบบการเข้ารหัสลับสมัยใหม่ จำเป็นต้องมีความซับซ้อนและความปลอดภัยที่มากกว่าอย่างมาก ระบบเข้ารหัสแบบดั้งเดิมเช่น ระบบเข้ารหัสซีซ่าร์ไซเฟอร์ หรือ เอ็นนิกมา ที่ใช้ในสงครามโลกครั้งที่สอง มักจะอาศัยการดำเนินการทางคณิตศาสตร์ที่เรียบง่าย อย่างการเปลี่ยนแปลงลำดับของตัวอักษรหรือคำ หรือการเปลี่ยนตำแหน่งของคำเท่านั้น เพื่อให้การเข้ารหัสและการถอดรหัสมีความปลอดภัยมากขึ้น ซึ่งวิธีดังกล่าวระบบคอมพิวเตอร์สามารถถอดได้ด้วยการโจมตีแบบใช้กำลังทำทั้งหมดได้อย่างรวดเร็ว ตารางที่ 1.1 เปรียบเทียบความแตกต่างระหว่างการเข้ารหัสลับแบบดั้งเดิมและสมัยใหม่

ตารางที่ 1.1 ความแตกต่างระหว่างระบบการเข้ารหัสลับแบบดั้งเดิมและสมัยใหม่

คุณลักษณะ	ระบบการเข้ารหัสลับแบบดั้งเดิม	ระบบการเข้ารหัสลับสมัยใหม่
ความซับซ้อน	การเข้ารหัสส่วนใหญ่ใช้หลักการทางคณิตศาสตร์ที่เรียบง่าย	การเข้ารหัสใช้หลักการทางคณิตศาสตร์ที่ซับซ้อน เช่น การคำนวณแบบ modular, การใช้จำนวนเฉพาะ
การกระจายกุญแจ	การกระจายกุญแจอย่างปลอดภัยเป็นสิ่งที่ยาก	ระบบเข้ารหัสแบบไม่สมมาตรสามารถกระจายกุญแจสาธารณะได้อย่างปลอดภัย
ความปลอดภัยต่อการโจมตี	มีความป้องกันที่น้อยต่อการโจมตีแบบบังคับบัญชา หรือการโจมตีโดยใช้คอมพิวเตอร์	อัลกอริทึมถูกออกแบบมาเพื่อความปลอดภัยต่อการโจมตีแบบบังคับบัญชาและการโจมตีด้วยคอมพิวเตอร์
ความทนทานต่อควอนตัม	ไม่มีการคำนึงถึงความทนทานต่อควอนตัม	อัลกอริทึมถูกพัฒนามาเพื่อทนทานต่อการโจมตีด้วยคอมพิวเตอร์ควอนตัม



ภาพที่ 1.9 เว็บแอปพลิเคชัน CrypTool ขณะใช้เข้ารหัสซีซาร์

ที่มา: CrypTool, 2022

ผู้อ่านสามารถเข้าไปลองใช้โปรแกรมเพื่อเข้าและถอดรหัสลับแบบดั้งเดิมตามที่ได้กล่าวถึงไปแล้วได้ที่เว็บไซต์ https://www.cryptool.org/ ซึ่งเป็นเว็บแอปพลิเคชัน ที่เปิดให้บริการมาอย่างยาวนาน ปัจจุบันมีในรูปแบบแอปพลิเคชันที่ทำงานบนพีซีให้ดาวน์โหลดมาใช้งานได้ฟรี ที่รวบรวมเอาการเข้ารหัสและถอดรหัสมากมายให้ลองทดสอบ ดังภาพที่ 1.9 แสดงให้เห็นถึงการเข้ารหัสแบบซีซาร์ในเว็บ การเข้ารหัสและถอดรหัสสามารถทำได้สำเร็จเพียงแค่ไม่กี่คลิก

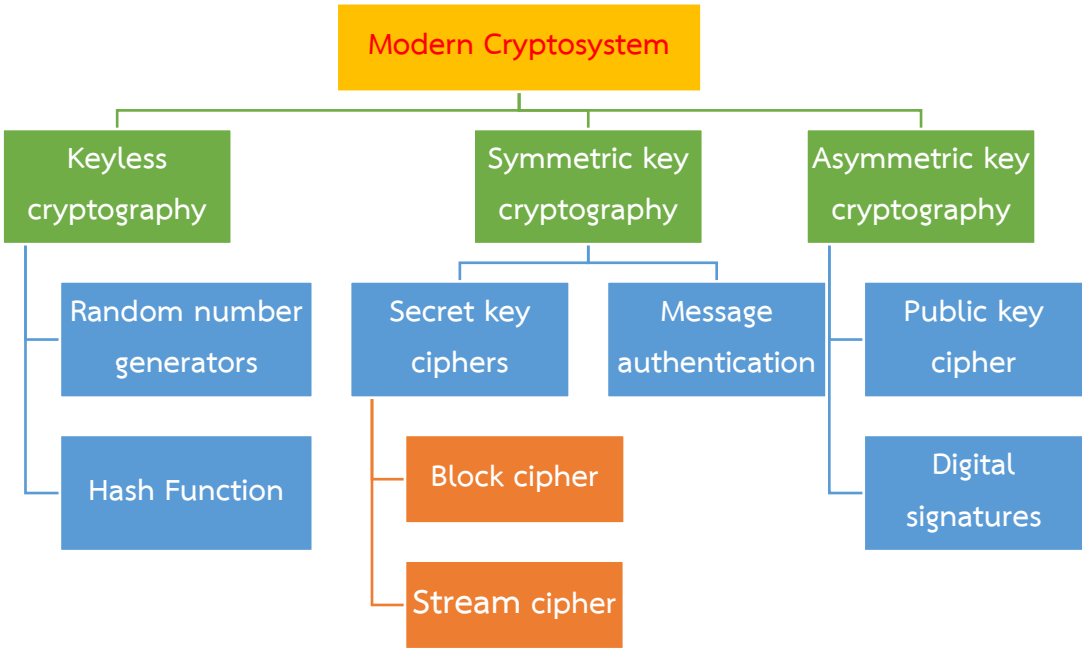
ดังนั้นระบบเข้ารหัสลับสมัยใหม่ (Modern Cryptosystem) จึงได้ถูกพัฒนาขึ้นมาแทนที่และกลายเป็นรากฐานของความปลอดภัยสำหรับโลกดิจิทัลในยุคปัจจุบันนี้ อย่างไรก็ดีในสถานการณ์ที่แตกต่างกันจำเป็นที่จะต้องใช้วิธีการเข้ารหัสลับที่ต่างกัน ทำให้ระบบการเข้ารหัสลับสมัยใหม่มีการแบ่งออกแบบหลายประเภทเพื่อให้เหมาะสมกับบริบทการทำงาน โดยสามารถแบ่งประเภทของการเข้ารหัสลับแบบสมัยใหม่ออกได้เป็น 3 ประเภทหลัก ๆ ได้แก่ แบบไม่ใช้กุญแจ (Keyless cryptography) แบบสมมาตร (Symmetric key cryptography) และ แบบอสมมาตร (Asymmetric key cryptography) ดังแสดงในภาพที่ 1.10 ซึ่งแต่ละประเภทจะมีประเภทย่อย ๆ ลงไปอีกสามารถอธิบายคร่าว ๆ ได้ดังนี้

1.5.1 ระบบเข้ารหัสที่ไม่ต้องการกุญแจ

เป็นไปตามชื่อของวิธีนี้ คือการเข้ารหัสแบบนี้จะไม่ต้องการกุญแจในการเข้ารหัส ซึ่งแบ่งออกได้เป็น 2 ประเภทย่อย

1) **การสุ่มตัวเลข (Random Numbers)** เป็นวิธีที่ขาดไม่ได้เลยในโลกของความปลอดภัยของข้อมูล การสุ่มช่วยให้ข้อมูลไม่สามารถถูกคาดเดาได้ด้วยผู้โจมตี ซึ่งการสุ่มตัวเลขออกมานี้จะถูกดำเนินการด้วยอัลกอริทึมบางอย่าง เป้าหมายคือการสุ่มตัวเลขออกมาให้ไม่สามารถคาดเดาได้ ซึ่งการสุ่มตัวเลขสามารถแบ่งได้เป็น 2 ประเภทคือ ตัวสร้างเลขสุ่มแบบธรรมดา (Random Number Generators; RNGs) และ ตัวสร้างเลขสุ่มแบบเทียม (Pseudorandom Number Generators; PRNGs)

2) **ฟังก์ชันแฮช (Hash Function)** มีบทบาทสำคัญในระบบเข้ารหัสสมัยใหม่และเทคโนโลยีบล็อกเชนเป็นอย่างมาก ฟังก์ชันนี้เป็นอัลกอริทึมทางคณิตศาสตร์ที่รับอินพุตและส่งคืนสายอักขระ (string) ของไบต์ที่มีขนาดคงที่ซึ่งเราจะเรียกว่าเป็นการทำ “การย่อยสลายข้อมูล” หรือไดเจส “(digest”” ฟังก์ชันแบบแฮชที่ดีจะมีแม้ข้อมูลจะเปลี่ยนไปแค่ 1 บิตของข้อมูลนำเข้าก็จะทำให้เกิดการเปลี่ยนแปลงที่สังเกตได้ในข้อมูลส่งออก จนค่า Hash ใหม่ไม่มีความเกี่ยวข้องกับค่าเก่าเลย คุณสมบัตินี้เป็นสิ่งที่สำคัญสำหรับการตรวจสอบความสมบูรณ์ของข้อมูล



ภาพที่ 1.10 พื้นฐานระบบการเข้ารหัสลับสมัยใหม่

ที่มา: Bashir, 2022

1.5.2 ระบบเข้ารหัสแบบสมมาตร

สามารถแบ่งได้ออกเป็น 2 วิธีย่อย ผู้เขียนจะกล่าวถึงวิธีการนี้ในบทที่ 2 อย่างละเอียด

1) **การเข้ารหัสลับด้วยกุญแจลับ (Secret key)** หรือ กุญแจส่วนตัว (Private key) จะใช้กุญแจชุดเดียวกันในการเข้ารหัสและถอดรหัส ซึ่งทำให้มีความยุ่งยากในการจัดการกุญแจ แต่มีความเร็วในการทำงานมากกว่าระบบเข้ารหัสแบบอสมมาตร ระบบการเข้ารหัสแบบนี้สามารถแบ่งออกได้เป็น 2 ประเภทย่อย คือ การเข้ารหัสแบบกระแสข้อมูล (Stream cipher) และ การเข้ารหัสแบบบล็อก (Block cipher)

2) **รหัสพิสูจน์ตัวจริงของข้อความ (Message Authentication Code)** บางครั้งจะเรียกว่า เป็นฟังก์ชันแฮชแบบมีกุญแจ (Keyed hash functions) เป็นการเข้ารหัสที่ออกแบบมาเพื่อการยืนยันตัวตนและความสมบูรณ์ของข้อมูล โดยสามารถทำงานได้ทั้งการเข้ารหัสแบบบล็อกและฟังก์ชันแฮช

1.5.3 ระบบเข้ารหัสแบบอสมมาตร

1) **การเข้ารหัสลับด้วยกุญแจสาธารณะ (Public key cipher)** วิธีนี้จะทำงานด้วยกุญแจ 2 ชนิดที่ทำงานด้วยกันเป็นคู่คือ กุญแจสาธารณะ (public key) และกุญแจส่วนตัว ใน

หลักการทำงานจะใช้กุญแจสาธารณะในการเข้ารหัสและใช้กุญแจส่วนตัวในการถอดรหัส เรื่องของกุญแจสาธารณะเป็นพื้นฐานของบล็อกเชน และจะพูดถึงอย่างละเอียด ในบทที่ 3

2) ลายมือชื่อดิจิทัล (Digital signature) จะคล้ายใช้กุญแจสาธารณะในการตรวจสอบลายมือชื่อดิจิทัล และใช้กุญแจส่วนตัวในการสร้างลายมือชื่อดิจิทัล (Stallings, 2006) ซึ่งจะถูกกล่าวถึงในบทต่อ ๆ ไปในตำราเล่มนี้

นอกจากนี้ระบบเข้ารหัสสมัยใหม่ยังรวมถึงโพรโทคอลสำหรับการสื่อสารที่ปลอดภัยที่ได้มีการรวมเอาวิธีการต่าง ๆ มาผสมผสานกัน เพื่อสร้างความปลอดภัยในสถานการณ์ต่าง ๆ อีกด้วย ตัวอย่างเช่น มาตรฐานการป้องกันระดับซ็อกเก็ต หรือ เอสเอสแอล (SSL; Secure Sockets Layer) ที่ใช้สำหรับบริการบนเว็บไซต์ ซึ่งต่อมาถูกพัฒนาเป็น โพรโทคอลความปลอดภัยสำหรับการสร้างช่องทางการเข้ารหัสผ่านเครือข่ายคอมพิวเตอร์ (TLS; Transport Layer Security) ทั้ง 2 เทคโนโลยีนี้เป็นโพรโทคอลทางคณิตศาสตร์ที่ออกแบบมาเพื่อให้การสื่อสารที่ปลอดภัยผ่านเครือข่ายคอมพิวเตอร์ โดยใช้การผสมผสานระหว่างการเข้ารหัสแบบสมมาตรและไม่สมมาตร รวมถึงฟังก์ชันแบบแฮช เพื่อให้ความลับ การตรวจสอบสิทธิ์ และการตรวจสอบความถูกต้อง

1.6 สรุป

ในบทนี้ได้กล่าวถึงพื้นฐานของวิทยาการเข้ารหัสลับที่ไม่ได้เป็นเพียงแค่เครื่องมือในการปกป้องข้อมูลและการสื่อสารเท่านั้น แต่ยังเป็นหัวใจสำคัญของระบบความปลอดภัยที่ใช้ในองค์กรธุรกิจ และระบบราชการ หัวข้อหลัก ๆ ที่ผู้อ่านได้ศึกษาไปแล้วในบทนี้ ได้แก่ พื้นฐานของวิทยาการเข้ารหัสลับ ระบบการเข้ารหัสลับแบบดั้งเดิม และระบบการเข้ารหัสลับแบบสมัยใหม่ โดยเนื้อหาทั้งหมดในบทนี้เป็นเพียงขั้นตอนแรกในการเข้าใจความซับซ้อนและความหลากหลายของวิทยาการเข้ารหัสลับที่สูงขึ้น ไปจนถึงเทคโนโลยีบล็อกเชน สำหรับการเข้ารหัสลับแบบต่าง ๆ จะถูกอธิบายโดยละเอียดในบทต่อ ๆ ไป

ความรู้และความเข้าใจที่ได้จากบทนี้จะเป็นพื้นฐานที่สำคัญสำหรับการศึกษาและทำความเข้าใจในบทต่อ ๆ ไป ซึ่งในบางหัวข้อของบทนี้จะถูกขยายความให้มีความละเอียดมากยิ่งขึ้น ไปจนถึงเทคนิคการเข้ารหัสลับที่ซับซ้อนยิ่งขึ้น การใช้งานในระบบที่หลากหลาย และความสัมพันธ์ระหว่างวิทยาการเข้ารหัสลับกับเทคโนโลยีอื่น ๆ ที่เกี่ยวข้อง