เพลย์แฟร์ไซเฟอร์

Playfair Cipher

นายเก่ง จันทร์นวล

บทคัดย่อ

การรักษาความลับข้อความหรือไฟล์ที่สำคัญสามารถทำได้หลายวิธี วิธีการที่ง่ายและประหยัดที่สุดวิธีหนึ่งคือการใช้วิทยาการเข้ารหัสลับ ข้อมูลที่เข้ารหัสลับจะมีความปลอดภัยมากน้อยขึ้นอยู่กับการเลือกอัลกอริทึมที่ดี และการกำหนดคีย์ว่ามีความยาวหรือมีความซับซ้อนมากน้อยแค่ไหน ง่ายต่อการคาดเดาหรือไม่ อัลกอริทึมหรือขั้นตอน วิธีการเข้ารหัสลับมีหลายวิธี ความยากง่ายขึ้นอยู่กับวิธีการ ซึ่งเอกสารฉบับนี้เป็นการนำเสนอกระบวนการพื้นฐาน การกำหนดคีย์ และวิธีการเข้ารหัสลับของอัลกอริทึม Playfair เพื่อใช้เป็นเอกสารประกอบการเรียนวิชาความมั่นคงของสารสนเทศ ตลอดจนผู้ที่สนในเกี่ยวกับการเข้ารหัสลับข้อมูล

1. บทนำ

Playfair Cipher ถูกพัฒนาโดย Charles Wheatstone ในปี ค.ศ. 1854 แต่ใช้ชื่อตาม Lord Playfair เพราะว่า Playfair เป็นผู้ส่งเสริมให้ใช้อัลกอริทึมนี้ [1]

Playfair Cipher เป็นวิธีเข้ารหัสข้อมูลแบบบ็อกซ์ไซเฟอร์ (box cipher) โดยใช้เทคนิคการแทนที่ตัวอักษรของข้อความธรรมดา (plaintext) ด้วยตัวอักษรอื่นในข้อความที่เข้ารหัส (cipher text) การแทนที่ตัวอักษรตัวเดียวกันในแต่ละตำแหน่งเป็นแบบไม่คงที่ หมายความว่าตัวอักษรตัวเดียวกันไม่จำเป็นต้องแทนที่ด้วยตัวอักษรเหมือนกัน การแทนที่แบบไม่คงที่นี้เรียกว่า Polyalphabetic Substitution การเลือกตัวอักษรที่จะใช้แทนที่ขึ้นอยู่กับตัวอักษรของข้อความธรรมดา และคีย์ที่ใช้ การแทนที่แต่ละครั้งจะกระทำเป็นคู่ๆ

2. แนวคิดของ Playfair Cipher

กำหนดคีย์ที่จะใช้ในการเข้ารหัส นำคีย์ที่ถูกเลือกมาสร้างตารางขนาด 5 x 5 และเพิ่มตัวอักษรที่ยังไม่ปรากฏในคีย์ให้ครบทุกช่องของตารางตามลำดับ เนื่องจากตารางสามารถเก็บได้ 25 ตัวอักษรแต่ตัวอักษรภาษาอังกฤษมีทั้งหมด 26 ตัวอักษร โดยทั่วไปส่วนใหญ่เลือกใช้สองแนวทางดังนี้ 1) ตัดตัว J ออกใช้ตัว I (ไอ) แทนเพราะสามารถใช้แทนกันได้ หรือ 2) ตัดตัว Q ออกไม่นำมาเขียนในตารางโดยคงตัว J ไว้ในตาราง ซึ่งทั้งสองวิธีเพื่อต้องการตัวอักษร 25 ตัว ในเอกสารฉบับนี้จะเลือกวิธีการสร้างตารางในแบบแรก ดังตัวอย่าง สมมติให้คีย์คือ “keyword” เมื่อนำมาสร้างตารางขนาด 5 x 5 จะได้ดังนี้

K	E	Y	W	O
R	D			

รูปที่ 1 การนำคีย์มาสร้างเมทริกต์ 5 x 5

เมื่อใส่คีย์ในแต่ละช่องครบแล้ว ให้เพิ่มตัวอักษรภาษาอังกฤษที่ยังไม่มีในคีย์ลงในช่องว่างให้เต็มโดยให้เขียนเพิ่มแต่ละช่องตามลำดับ เนื่องจากมี 26 ตัวอักษรและมีทั้งหมด 25 ช่อง ดังนั้นให้กำหนด I และ J ไว้ในช่องเดียวกัน ดังรูปที่ 2

K	E	Y	W	O
R	D	A	B	C

F	G	H	I/J	L
M	N	P	Q	S
T	U	V	X	Z

รูปที่ 2 การสร้างเมทริกต์ 5 x 5 เพื่อกำหนดตัวอักษรแทนที่

3. ก่อนการเข้ารหัสข้อมูล

การเข้ารหัสข้อความของ Playfiar Cipher ต้องทำการแยกตัวอักษรของข้อความออกเป็นคู่ๆ และเปลี่ยนเป็นตัวอักษรพิมพ์ใหญ่ทั้งหมด โดยไม่สนใจเครื่องหมายวรรคตอน หรือช่องว่างระหว่างคำ ยกตัวอย่างเช่น

ข้อความ “Why, don’t you?”
แยกออกเป็นคู่ WH YD ON TY OU

ในการแยกตัวอักษรอออกเป็นคู่อาจเกิด 2 เหตุการณ์ ดังข้อ 3.1 และ 3.2

3.1 จำนวนตัวอักษรของข้อความธรรมดาเป็นจำนวนคี่ ดังตัวอย่าง

ข้อความ “Come to the windows”
แยกออกเป็นคู่ CO ME TO TH EW IN DO W

แนวทางแก้ปัญหานี้คือ ให้ใส่ตัวอักษรพิเศษให้กับตัวอักษรที่เหลือเศษ เพื่อให้ครบคู่ ซึ่งโดยทั่วไปตัวอักษรพิเศษที่ใช้คือตัวคิว (Q) หรือตัว เอ็กซ์ (X) (ในเอกสารฉบับนี้ขอเลือกใช้ตัว Q) ดังนั้นจากข้อความข้างบนจะเป็นดังนี้

แยกออกเป็นคู่ CO ME TO TH EW IN DO WQ

3.2 ตัวอักษรที่แยกออกเป็นคู่ ถ้ามีคู่ที่มีตัวอักษรซ้ำกัน ให้ดำเนินการดังนี้

ข้อความ “the big wheel”
แยกออกเป็นคู่ TH EB IG WH EE LQ

แนวทางแก้ปัญหานี้คือ ให้แยกคู่ของตัวอักษรที่ซ้ำกันออกโดยใช้ตัวอักษรพิเศษ(Q) มาจับคู่แทน ดังนี้

แยกออกเป็นคู่ TH EB IG WH EQ EL

4. การเข้ารหัสข้อมูล

การเข้ารหัสข้อมูลของ Playfair Cipher เป็นการเลือกเอาตัวอักษรที่อยู่ในตารางที่สร้างขึ้นมาแทนตัวอักษรของข้อความธรรมดาที่ถูกแยกออกเป็นคู่ การเลือกตัวอักษรที่นำมาแทนที่ให้ดูตัวอักษรภายในตารางโดยให้มองเป็นสี่เหลี่ยม(ให้เลือกเอาตัวอักษรที่อยู่มุมสี่เหลี่ยมสองตัว) ซึ่งการแทนที่ตัวอักษรสามารถแทนได้ดังนี้

4.1 มุมมองสี่เหลี่ยมจาก ขวา – ซ้าย

ข้อความ “Why, don’t you?” แยกออกเป็นคู่ WH YD ON TY OU

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

รูปที่ 3 พื้นที่สี่เหลี่ยมเพื่อเลือกตัวอักษรแทน WH

การแทนคู่ตัวอักษร WH ให้มองตัวอักษร W ไปยังตัวอักษร H ในตาราง (ขวา – ซ้าย) จะเกิดสี่เหลี่ยมภายในตาราง (ช่องตารางที่มีสีพื้น) ตัวอักษรที่จะนำมาแทนตัวอักษรคู่นี้คือตัวอักษรที่อยู่มุมสี่เหลี่ยมที่เกิดขึ้นภายในตารางนั่นก็คือ YI

ในทำนองเดียวกันตัวอักษรคู่ต่อไปนี้ YD ON และ OU จะเป็นแบบ ขวา – ซ้าย ซึ่งจะแทนด้วยคู่ตัวอักษร EA ES EZ ตามลำดับ

4.2 มุมมองสี่เหลี่ยมจาก ซ้าย – ขวา

ในที่นี้ขอแสดงตัวอย่างการแทนที่ของข้อความในข้อ 3.1 ซึ่งเหลืออยู่หนึ่งคู่คือ TY

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

รูปที่ 4 พื้นที่สี่เหลี่ยมเพื่อเลือกตัวอักษรแทน TY

ในกรณีนี้คู่ตัวอักษรจะถูกมองจากซ้าย(T) ไปมุมทางขวา (Y) จะเกิดสี่เหลี่ยมขึ้นภายในตาราง(ช่องที่มีสีพื้น) ดังนี้ตัวอักษรที่อยู่มุมสองตัวจะถูกเลือกเป็นตัวอักษรที่ใช้ในการแทนค่าคือ VK

4.3 มุมมองอยู่แถวเดียวกัน

ในกรณีที่คู่ตัวอักษรที่ต้องการแทนที่อยู่ในแถวเดียวกันของตาราง ซึ่งอาจเกิดขึ้นได้ 4 กรณี

- กรณีที่ 1 คู่ตัวอักษรที่ต้องการแทนที่อยู่ไม่ติดกัน

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

รูปที่ 5 พื้นที่สี่เหลี่ยมเพื่อเลือกตัวอักษรแทน DB

ถ้าต้องการแทน DB ให้เลือกเอาตัวอักษรที่นำมาแทนที่หนึ่งในสองให้เอาตัวอักษรที่อยู่ภายในระหว่าง DB คือตัวอักษร A และตัวที่สองคือ C ดังนั้นตัวอักษรที่นำมาแทนที่ DB คือ AC

ในทางกลับกันถ้าต้องการแทนที่คู่ LG ตัวอักษรที่ถูกเลือกจะเป็น IF แทน (ให้พิจารณาตามลำดับการเลือก)

- กรณีที่ 2 คู่ตัวอักษรที่ต้องการแทนที่อยู่ติดกัน

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

รูปที่ 6 พื้นที่สี่เหลี่ยมเพื่อเลือกตัวอักษรแทน AB

ถ้าต้องการแทน AB เนื่องระหว่าง AB ไม่มีตัวอักษรอื่นดังนั้นตัวแรกที่ถูกเลือกก็คือตัวอักษร B และตัวที่สองคือ C ดังนั้นสามารถแทนค่า AB ด้วยตัวอักษร BC

- กรณีที่ 3 คู่ตัวอักษรที่ต้องการแทนที่อยู่ตำแหน่งตัวแรกและตัวสุดท้ายของแถวนั้น

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

รูปที่ 7 พื้นที่สี่เหลี่ยมเพื่อเลือกตัวอักษรแทน RC

ถ้าต้องการแทน RC ถ้าเกิดกรณีนี้ขึ้นให้ใช้หลักการเดียวกันคือตัวแรกที่ถูกเลือกคือตัวอักษรที่อยู่ภายในระหว่าง RC คือตัว D ส่วนตัวที่สองจะเป็นตัวที่อยู่ทางขวาของตัว C แต่ตำแหน่งตัว C อยู่ที่ตำแหน่งสุดท้ายของแถว การแก้ปัญหานี้คือให้เลื่อนไปยังตัวอักษรที่อยู่ถัดไปในแถวเดิมซึ่งจะเป็น

ตำแหน่งแรกสุด ดังนั้นคู่ตัวอักษร RC ตัวอักษรที่ถูกเลือกมาแทนที่คือ DR

- กรณีที่ 4 ถ้าคู่ตัวอักษรตัวแรกอยู่ตำแหน่งทางขวา และตัวที่สองอยู่ตำแหน่งทางซ้ายของแถว

ในกรณีนี้การเลือกตัวอักษรมาแทนที่ให้มองตำแหน่งลำดับทางขวาอย่างเดียว

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

รูปที่ 8 พื้นที่สี่เหลี่ยมเพื่อเลือกตัวอักษรแทน QN

สมมติต้องการแทนที่คู่ตัวอักษร QN ให้เลือกตัวอักษรตำแหน่งที่อยู่ทางขวาของ Q และ N ดังนั้นตัวอักษรที่นำมาแทนที่คือ SP

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

รูปที่ 9 พื้นที่สี่เหลี่ยมเพื่อเลือกตัวอักษรแทน IH

สมมติต้องการแทนที่คู่ตัวอักษร IH ให้เลือกตัวอักษรตำแหน่งที่อยู่ทางขวาของ I และ H ดังนั้นตัวอักษรที่นำมาแทนที่คือ LI

ดังนั้นในกรณีที่ตัวอักษรต้องการแทนที่อยู่ในคอลัมน์เดียวกัน ให้พิจารณาตามหลักการแทนที่ของตัวอักษรที่ต้องการแทนที่ที่อยู่ในแถวเดียวกัน(พิจารณาตามหลักการข้อ 4.3) แต่ให้มองลำดับตำแหน่งตัวอักษรที่อยู่ลำดับถัดไปที่อยู่ตำแหน่งด้านล่างของตัวอักษรที่กำลังพิจารณาแทน

5. การใช้คีย์

คีย์หรือกุญแจ คือส่วนนำมาร่วมกับอัลกอริทึมเพื่อใช้ในการเข้ารหัสข้อมูล การเข้ารหัสข้อมูลแบบ Playfair นำเอาคีย์มาสร้างตารางขนาด 5 x 5 ซึ่งสามารถเก็บตัวอักษรได้ 25 ตัวอักษร ในบทความฉบับนี้ใช้วิธีไม่ใช้ตัวอักษร J แต่ใช้ตัว I แทน ดังนั้นถ้าคีย์ที่เลือกมีตัวอักษร J ปรากฏอยู่จะต้องแทนด้วย I และถ้ามีตัวอักษรซ้ำให้ตัดตัวอักษรที่ซ้ำออก ดังตัวอย่าง

คีย์คือ JIM TRESSEL
แทนตัว J ด้วยตัว I ดังนั้นเขียนคีย์ใหม่คือ IIM TRESSEL
ตัดตัวอักษรที่ซ้ำออก ดังนั้นเขียนคีย์ใหม่คือ IM TRESL

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

รูปที่ 10 การกำหนดค่าคีย์ JIM TRESSEL ในตาราง

6. สรุป

อัลกอริทึม Playfair เป็นอัลกอริทึมที่ใช้เทคนิคการแทนที่ด้วยตัวอักษรแบบไม่คงที่ การดำเนินการจะกระทำเป็นคู่ โดยไม่สนใจเครื่องหมายวรรคตอน หรือช่องว่างระหว่างคำ ทำให้ผู้รับข้อความไม่ทราบรูปแบบข้อความเดิม ปัญหานี้สามารถแก้ได้โดยการนำเอาข้อความที่เข้ารหัสมาจัดรูปแบบให้เหมือนข้อความต้นฉบับทำให้ผู้รับข้อความทราบเครื่องหมายเหล่านั้นได้
อัลกอริทึม Playfair เป็นอัลกอริทึมที่มีความแข็งแรงระดับหนึ่งเท่านั้นแต่ก็ยังค่อนข้างง่ายต่อการโจมตีในรูปแบบต่างๆ แต่อย่างไรก็ดีเอกสารฉบับนี้เพียงแต่ต้องการนำเสนอความรู้เบื้องต้นเกี่ยวกับอัลกอริทึมนี้เท่านั้น

7. เอกสารอ้างอิง

[1] Muhammad Salam, Nasir Rashid, Shah Khalid, Muhammad Raees Khan, “A NXM Version of 5X5 Playfair Cipher for any Natural Language (Urdu as Special Case)”, [Online], http://www.waset.org/journals/waset/v73/v73-160.pdf.

[2] Dr. Nancy Childress. "Playfair Ciphers", [Online], http://math.la.asu.edu/~nc/playfair.pdf.

[3] Chris Brew, “The Playfair Cipher”, [Online], http://www.ling.ohio-state.edu/~cbrew/2008/spring/playfair.pdf.

[4] Wikipedia, "Playfair cipher", [Online], http://en.wikipedia.org/wiki/Playfair_cipher.

[5] Dr. Brian Harvey. "Example: Playfair Cipher", [Online], http://www.cs.berkeley.edu/~bh/pdf/v1ch12.pdf.