Cryptography

MS1 Thanin Muangpool

What is a Cryptography ?

การเข้ารหัสข้อมูล (Cryptography) มาจากคำ 2 คำ คือ

Crypto ที่แปลว่า **"การซ่อน"**

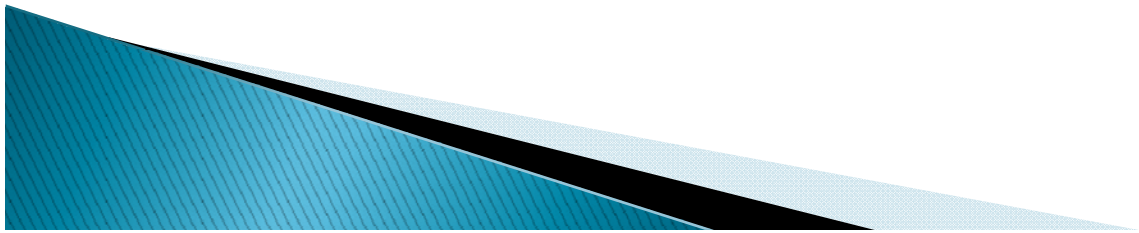
Graph ที่แปลว่า **"การเขียน"**

Cryptography จึงมีความหมายว่า **“การเขียนเพื่อซ่อนข้อมูล”** โดยมีจุดประสงค์เพื่อป้องกันไม่ให้ผู้อื่นสามารถอ่านข้อมูลได้ ยกเว้นผู้ที่เราต้องการให้อ่านได้เท่านั้น มีศัพท์ที่เกี่ยวข้องดังนี้ [Mark Stamp, 2006]

1. Cryptology : ศาสตร์และศิลป์ในการสร้างและแก้ไข รหัสลับ
2. Cryptography : การสร้างรหัสลับ
3. Crypanalysis : การแก้ไขรหัสลับ
4. Crypto : คำย่อที่ใช้เรียกแทนทุกคำ

ศัพท์ต่างๆ ที่ควรทราบเกี่ยวกับการเข้าและถอดรหัส

- **Plain Text** หมายถึง ข้อความหรือข้อมูลต่างๆ ที่ยังไม่ผ่านกรรมวิธีการเข้ารหัส
- **Cipher Text** หมายถึง ข้อความ หรือข้อมูลต่างๆที่ผ่านการเข้ารหัสแล้ว และทำให้รูปแบบของข้อมูลเปลี่ยนแปลงไป
- **Algorithm** หมายถึง แนวความคิดหรือลำดับความคิดที่มี รูปแบบที่สามารถนำไปประมวลผลทางคอมพิวเตอร์ได้โดยง่าย
- **Encryption** หมายถึง กระบวนการหรือขั้นตอนในการเข้ารหัสข้อมูล ที่เปลี่ยนแปลงไปจากเดิม



ศัพท์ต่างๆ ที่ควรทราบเกี่ยวกับการเข้าและถอดรหัส

- **Decryption** หมายถึง กระบวนการหรือขั้นตอนในการถอดรหัสข้อมูล เพื่อให้ข้อมูลที่เข้ารหัสไว้คืนสู่สภาพเดิมก่อนเข้ารหัส
  - **Key** หมายถึง กุญแจที่ใช้ร่วมกับ อัลกอริทึมในการเข้ารหัส และถอดรหัส
- **Cryptography** หมายถึง ระบบการรักษาความปลอดภัยที่ประกอบ ด้วย Encryption และ Decryption
- **Cryptanalysis** หมายถึง การพยายามวิเคราะห์เพื่อศึกษาประเด็นต่างๆ ที่เกี่ยวข้องกับ Cryptography
- **Sensitive Data** หมายถึง ข้อมูลสำคัญที่ถือว่าเป็นความลับไม่สามารถ แพร่งพรายออกสู่ภายนอกได้

Cryptography

กระบวนการของ **Cryptography** มี 2 อย่างคือ

- **Data Encryption** : การเข้ารหัสข้อมูล
- **Data Decryption** : การถอดรหัสข้อมูล

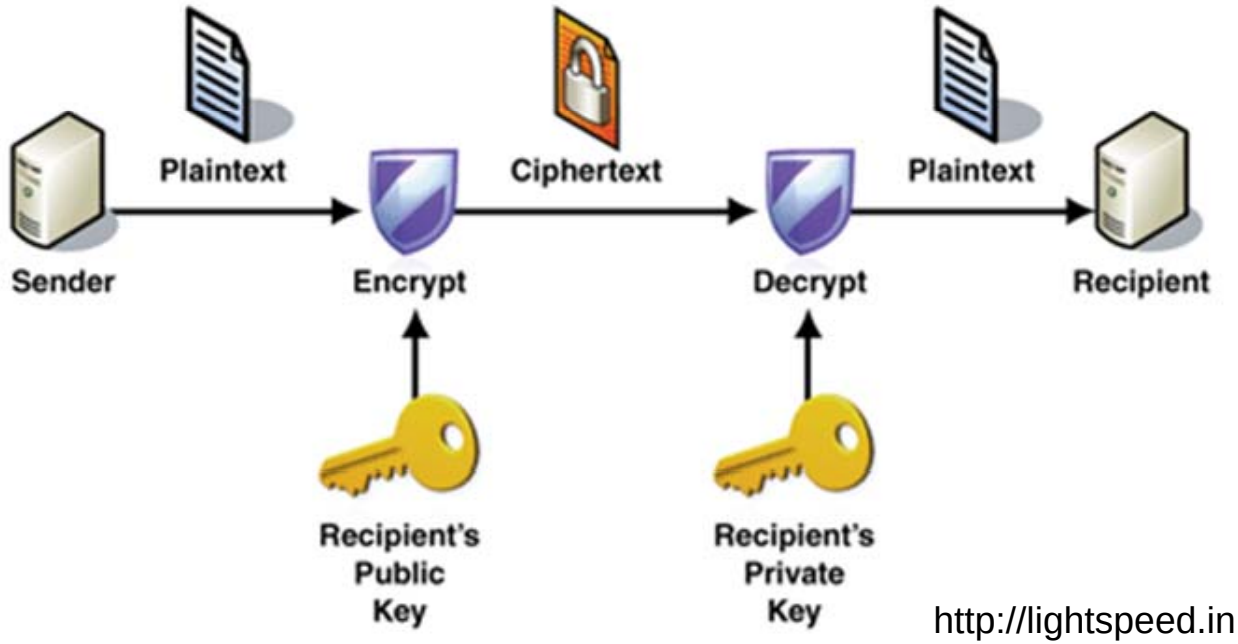
เพราะฉะนั้นประโยชน์ของ Cryptography คือการรักษาความลับของข้อมูล

Cryptography

Encryption + Decryption

Cryptography

- ข้อมูลที่สามารถอ่านได้ เรียกว่า Plain Text หรือ Clear Text
- ข้อมูลที่เข้ารหัสแล้วเราเรียกว่า Cipher Text
- ข้อมูลเมื่อเสร็จสิ้นการเข้ารหัสแล้ว ผลที่ได้ก็คือ Cipher Text ในการอ่านข้อความ Cipher Text นั้น



http://lightspeed.in.th/

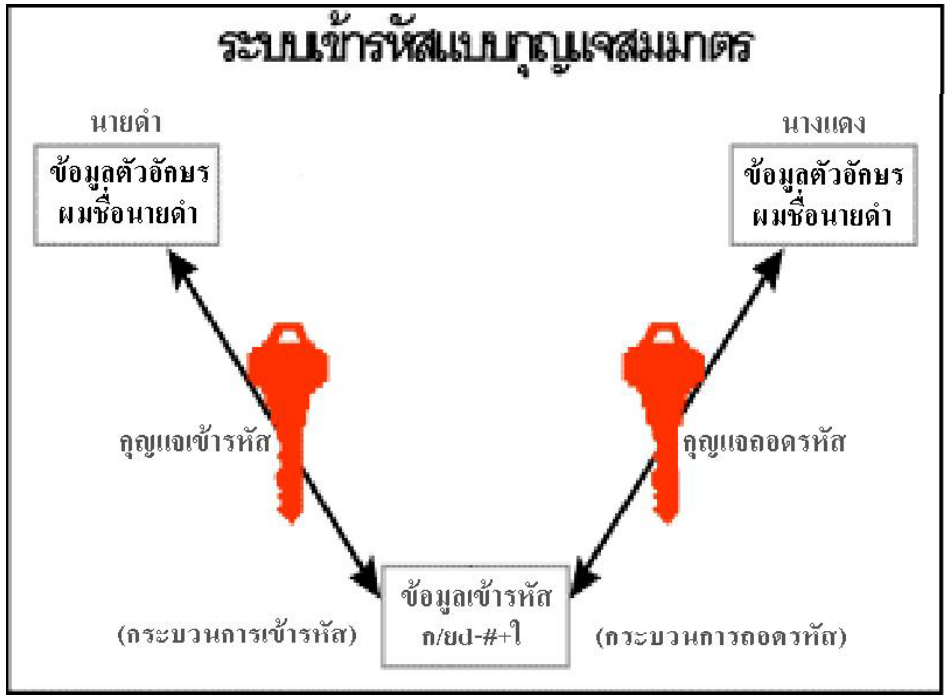
องค์ประกอบของรหัสลับ

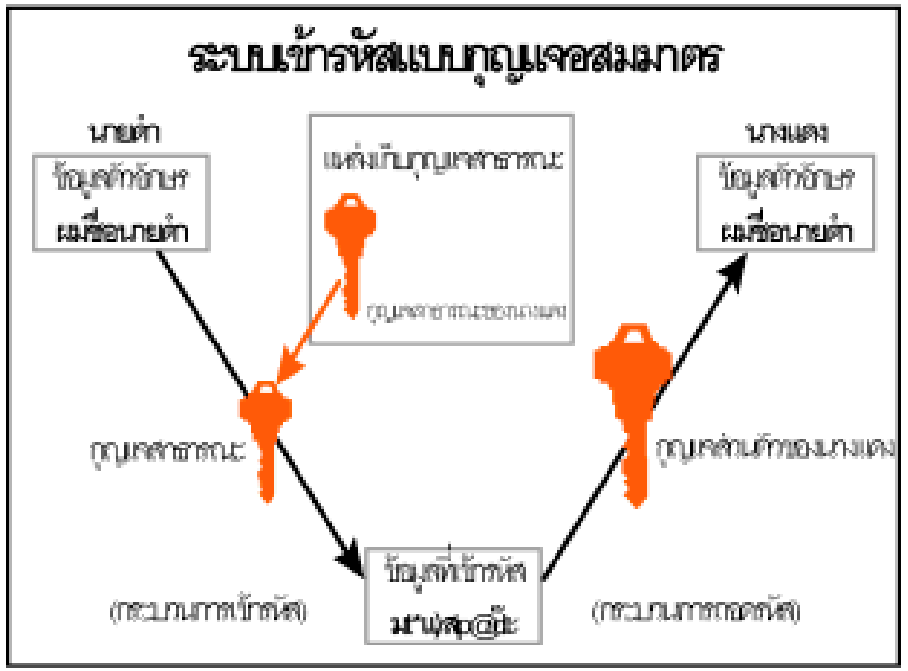
- **ข้อความต้นฉบับ (Plain Text)** คือ ข้อมูลต้นฉบับซึ่งเป็นข้อความที่สามารถอ่านแล้วเข้าใจ
- **อัลกอริทึมการเข้ารหัสลับ (Encryption Algorithm)** คือ กระบวนการหรือขั้นตอนที่ใช้ในการแปลงข้อมูลต้นฉบับเป็นข้อมูลที่ได้รับการเข้ารหัส
- **กุญแจลับ (Key)** คือ เป็นกุญแจที่ใช้ร่วมกับ อัลกอริทึมในการเข้ารหัส และถอดรหัส
- **ข้อความไซเฟอร์ (Cipher Text)** คือ ข้อมูลหรือข่าวสารที่ได้รับการเข้ารหัสทำให้อ่านไม่รู้เรื่อง
- **อัลกอริทึมการถอดรหัสลับ (Decryption Algorithm)** คือ กระบวนการหรือขั้นตอนในการแปลงข้อความไซเฟอร์ให้กลับเป็นข้อความต้นฉบับ โดยอาศัยกุญแจลับดอกเดียวกัน

Cryptography

- การเข้ารหัสแบ่งออกเป็น 2 ประเภทใหญ่ๆ คือ
  - ***Symmetric Cryptography (Secret key)*** เรียกอีกอย่างว่า Single-key algorithm หรือ one-key algorithm คือ การเข้ารหัสและถอดรหัสโดยใช้กุญแจรหัสตัวเดียวกัน คือ ผู้ส่งและผู้รับจะต้องมีกุญแจรหัสที่เหมือนกันเพื่อใช้ในการเข้ารหัสและถอดรหัส
  - ***ASymmetric Cryptography (Public key)*** คือ การเข้ารหัสและถอดรหัสโดยใช้กุญแจรหัสคนละตัวกัน การส่งจะมีกุญแจรหัสตัวหนึ่งในการเข้ารหัส และผู้รับก็จะมีกุญแจรหัสอีกตัวหนึ่งเพื่อใช้ในการถอดรหัส ผู้ใช้รายหนึ่งๆ จึงมีกุญแจรหัส 2 ค่าเสมอ คือ กุญแจสาธารณะ (public key) และ กุญแจส่วนตัว (private key) ผู้ใช้จะประกาศให้ผู้อื่นทราบถึงกุญแจสาธารณะของตนเองเพื่อให้นำไปใช้ในการเข้ารหัสและส่งข้อมูลที่เข้ารหัสแล้วมาให้ ข้อมูลที่เข้ารหัสดังกล่าวจะถูกถอดออกได้โดยกุญแจส่วนตัวเท่านั้น

Cryptography

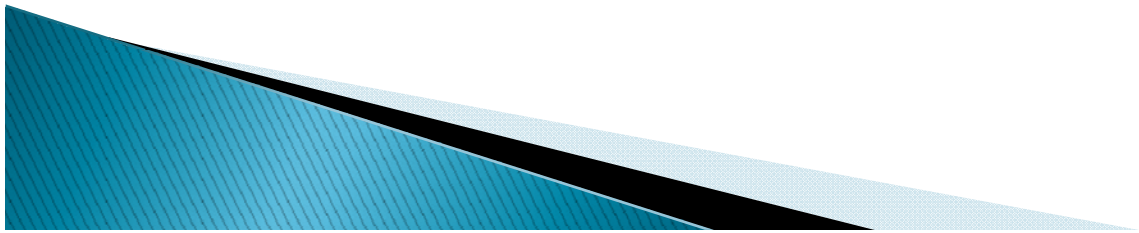




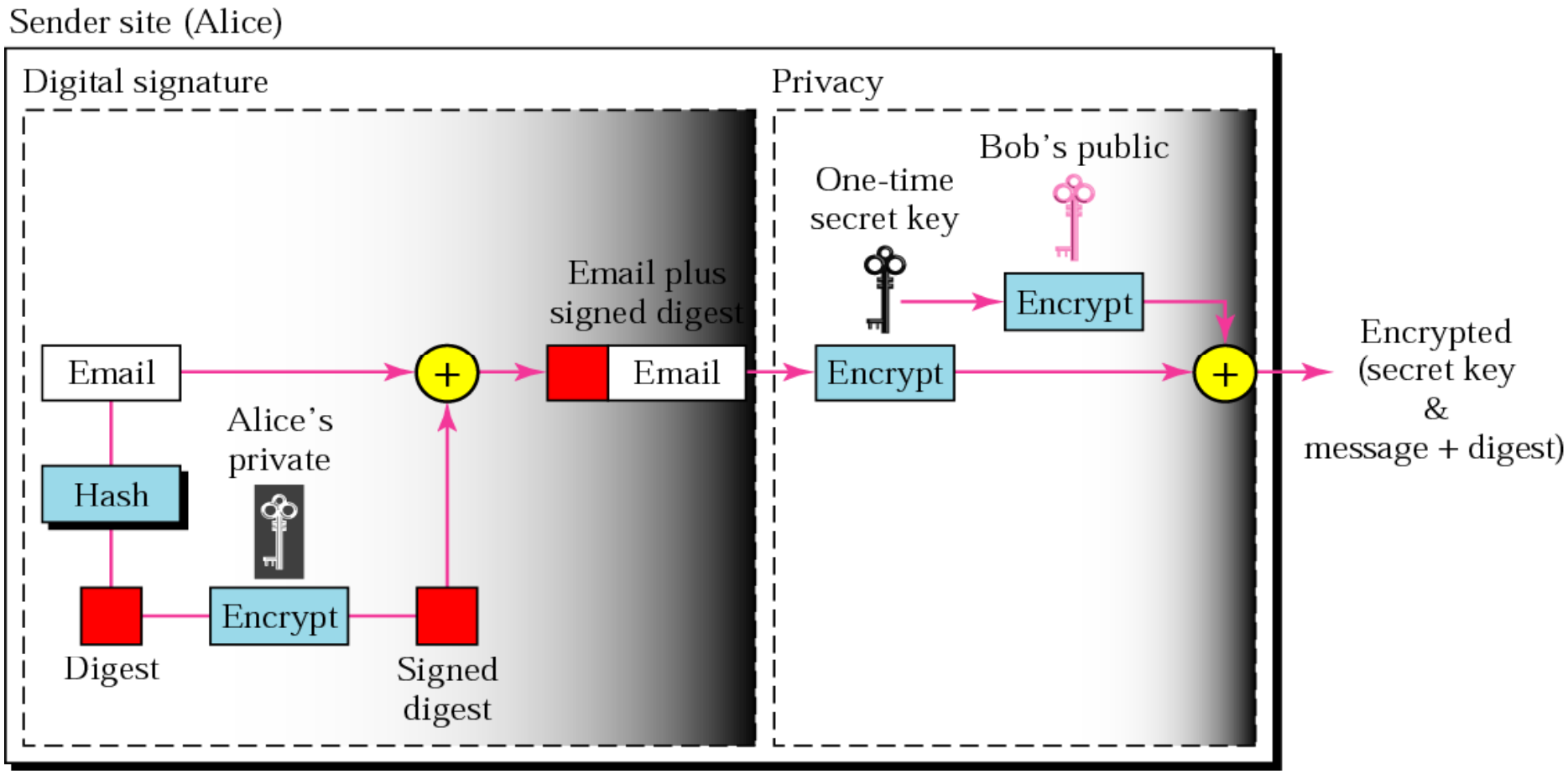
http://www.ku.ac.th/emagazine/august44/it/encryp.html

Cryptography

- ในทางปฏิบัติแล้วมักมีการใช้การเข้ารหัสทั้งสองระบบร่วมกัน เช่น ในระบบ PGP (Pretty Good Privacy) ซึ่งใช้ในการเข้ารหัส E-mail จะใช้วิธีสร้าง Session Key ซึ่งเป็นรหัสลับตามแบบ secret key เมื่อข้อมูลถูกเข้ารหัสด้วย Session Key แล้ว Session Key จะถูกเข้ารหัสโดยใช้กุญแจสาธารณะของผู้รับ และถูกส่งไปกับข้อมูลที่เข้ารหัสแล้ว

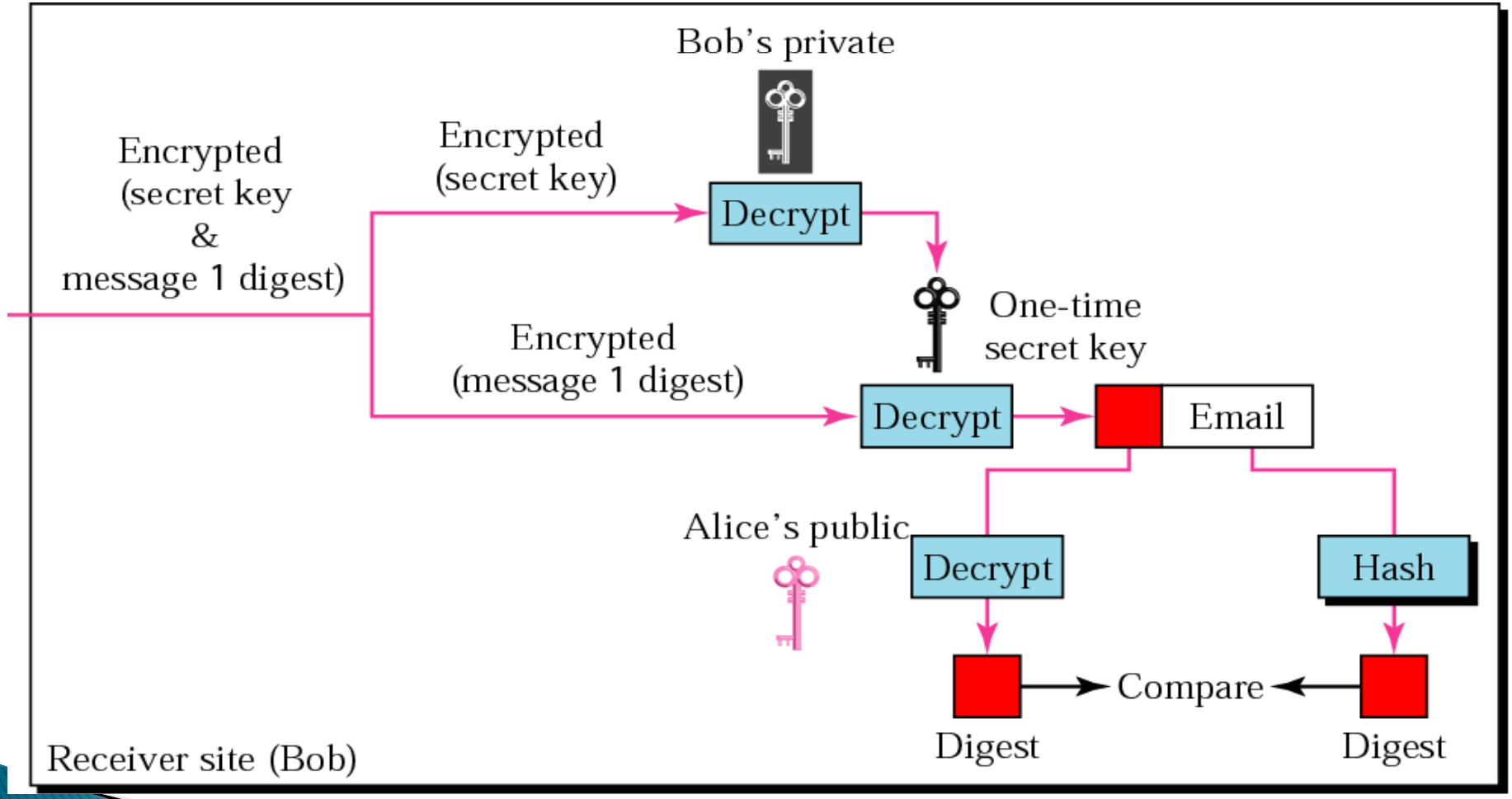


การเข้ารหัส



http://www.ku.ac.th/emagazine/august44/it/encryp.html

การถอดรหัส



http://www.ku.ac.th/emagazine/august44/it/encryp.html

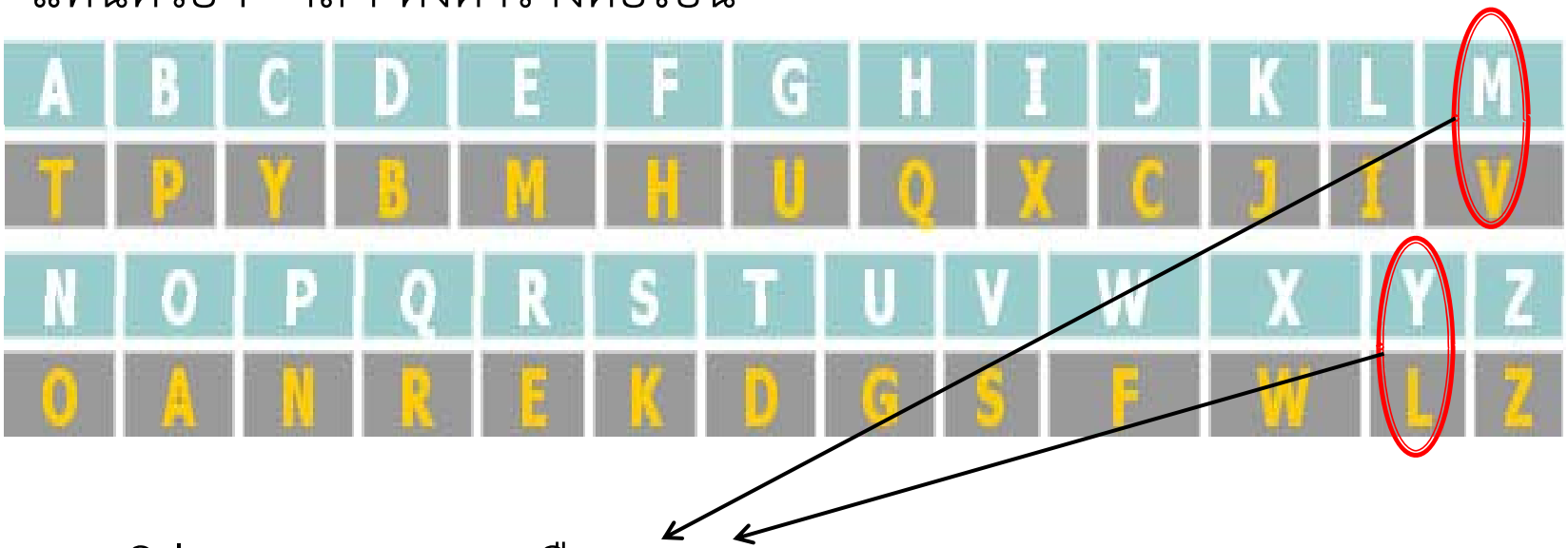
Cryptosystems

- **ระบบรหัสลับ Cryptosystems หรือเรียกว่า Cipher** มีองค์ประกอบหลายส่วน เพื่อการเข้ารหัสลับข้อมูล ประกอบด้วย อัลกอริทึ่ม เทคนิคการจัดการข้อมูล กระบวนการ และขั้นตอนการทำงาน จะถูกผสมผสานเข้าด้วยกันเพื่อเข้ารหัสข้อมูล
- มีวัตถุประสงค์เพื่อรักษาข้อมูลไว้เป็นความลับ Confidentiality และจัดเตรียม กลไกการพิสูจน์ตัวตน Authentication และการให้สิทธิ์ Authorization ในการดำเนินงานแต่ละขั้นตอนทางธุรกิจ
- สามารถแบ่งตามยุคสมัยได้เป็น 2 ยุคคือ
  1. ยุคประวัติศาสตร์ (หรือที่เรียกว่ายุค Classic)
  2. ยุคปัจจุบัน (Modern)

Cryptosystems → Substitution Cipher

- **ระบบรหัสลับแบบสับเปลี่ยน (Substitution Cipher)** หลักการคือต้องสับเปลี่ยนแต่ละตัวอักษรใน Plain Text ด้วยตัวอักษรอื่น แต่ก่อนอื่นต้องเลือกก่อนว่าจะแทนแต่ละตัวอักษรด้วยอะไร อย่างเช่น A แทนด้วย T, B แทนด้วย P ฯลฯ ดังตารางต่อไปนี้

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



- สมมุติว่า Plain Text คือ MY NAME IS THANIN.

  Cipher Text คือ VL OTVM XK DQTOXO

Cryptosystems → Substitution Cipher

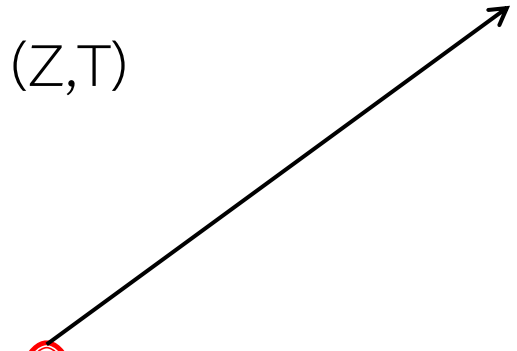
- ระบบรหัสลับแบบสับเปลี่ยนนี้มีหลายหลากแบบ เพราะมีการนำไปดัดแปลงกัน เพื่อให้ Key ดูง่ายจำง่ายขึ้น
- เช่น อาจจะใช้ตารางต่อไปนี้เป็น key

- ดังนั้นข้อความ Plain Text คือ T H A N I N

Cipher Text คือ 

Cryptosystems → Substitution Cipher

- การสุ่มจับคู่ตัวอักษร แล้วสับเปลี่ยนตัวอักษรแต่ละตัวใน Plain Text ด้วยตัวอักษรที่เป็นคู่กัน ถ้าเราใช้วิธีนี้กับตัวอักษรของภาษาอังกฤษ เราก็อาจจะจับคู่ได้ดังนี้ (A,V), (D,X), (H,B), (I, G), (K,J), (M,C), (O,Q), (R,L), (S,N), (U,E), (W,F), (Y,P), (Z,T)



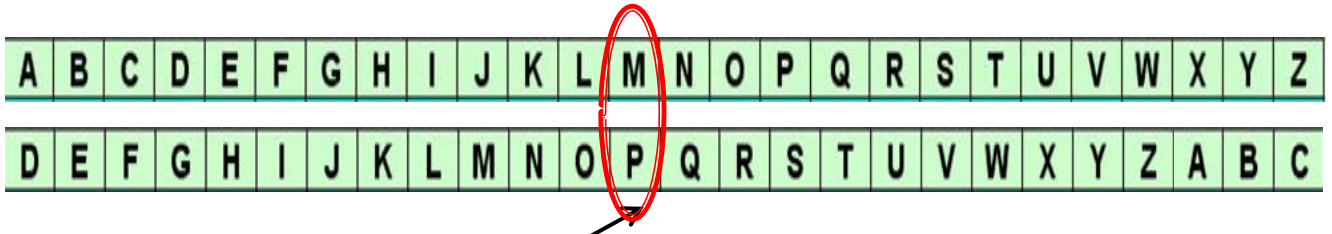
- ดังนั้นข้อความ Plain Text คือ M Y NAME IS THANIN.

  Cipher Text คือ C P SVCU GN ZBVSGS

Cryptosystems → Substitution Cipher

- บางครั้งอาจจะเป็นการกำหนด Key แทนตัวอักษรในภาษาอังกฤษตำแหน่งใด ๆ ด้วยลำดับตัวอักษรถัดไปอีกตาม Key ที่กำหนด เช่น กำหนด Key = 3 ตัวอักษรภาษาอังกฤษลำดับถัดไปอีก 3 ตำแหน่ง ก็คือตัวอักษรตัวที่ 4 ในภาษาอังกฤษนั่นเอง

- **Plain Text**
- **Cipher Text**

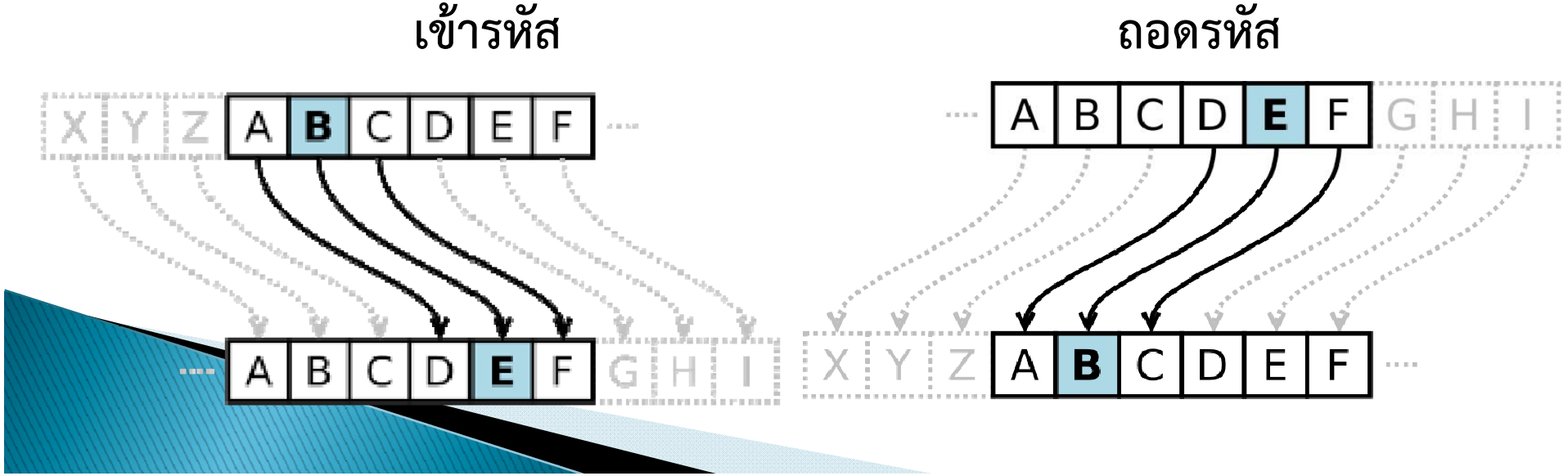


- ดังนั้นข้อความ Plain Text คือ M Y NAME IS THANIN.

  Cipher Text คือ P B QDPH LV WKDQLQ

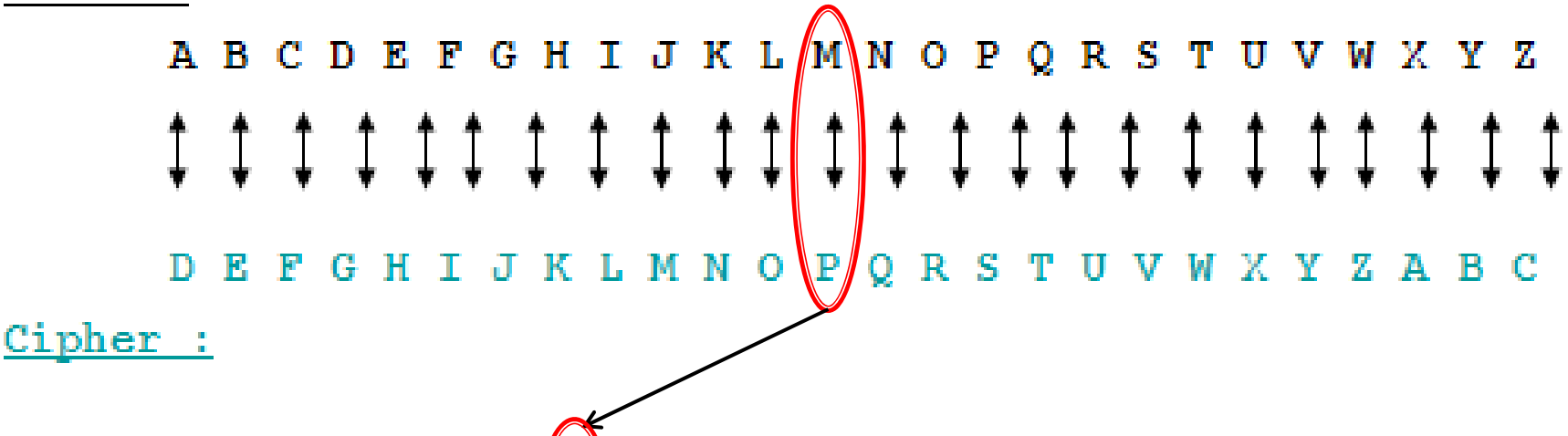
Cryptosystems → Caesar cipher

- Caesar cipher เป็นการเข้ารหัสแบบ Secret Key หรือ Symmetric Key Cryptography คิดค้นโดยกษัตริย์ Julius Caesar เพื่อสื่อสารกับทหารในกองทัพ และป้องกันไม่ให้ข่าวสารรั่วไหลไปถึงศัตรู
- <u>หลักการของ Caesar Cipher คือ จะ Shift หรือ เลื่อนตัวอักษรไป 3 ตำแหน่ง จากตำแหน่งเดิม</u>



Cryptosystems → Caesar cipher

- ดังนั้น ตัวอักษรปกติจะถูกแทนที่ด้วยตัวอักษรที่อยู่ถัดไปอีก 3 ตัว โดย ตัวอักษรปกติจะเรียกว่า Plain ตัวอักษรที่มาแทนที่จะเรียกว่า Cipher

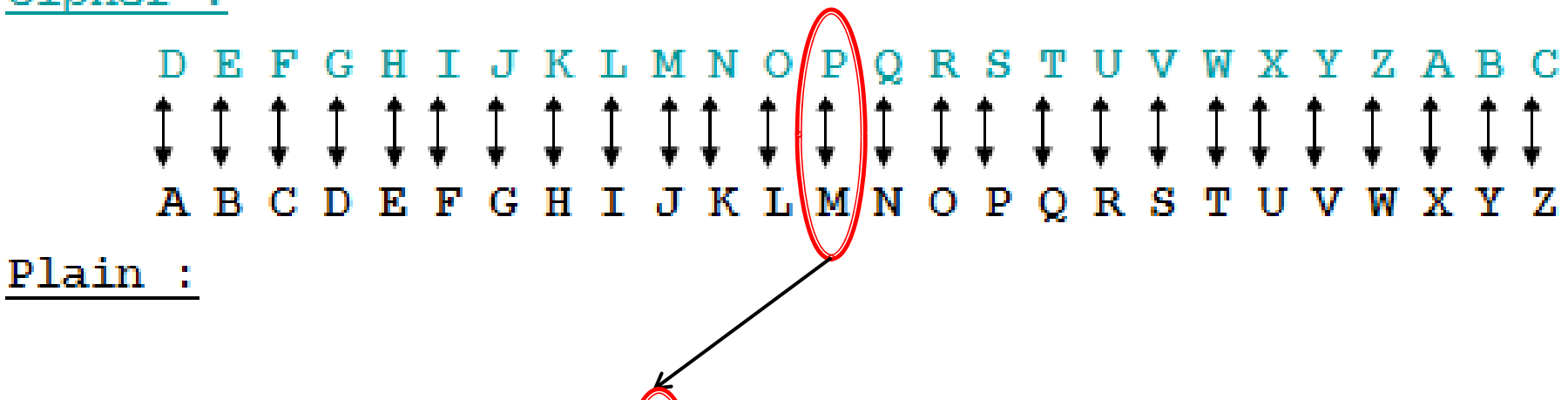


- สมมุติว่า Plain คือ M Y NAME IS THANIN

  Cipher คือ P B QDPH LV WKDQLQ

Cryptosystems → Caesar cipher

- และการถอดรหัสก็จะใช้การเทียบย้อนกลับระหว่าง Cipher กับ Plain

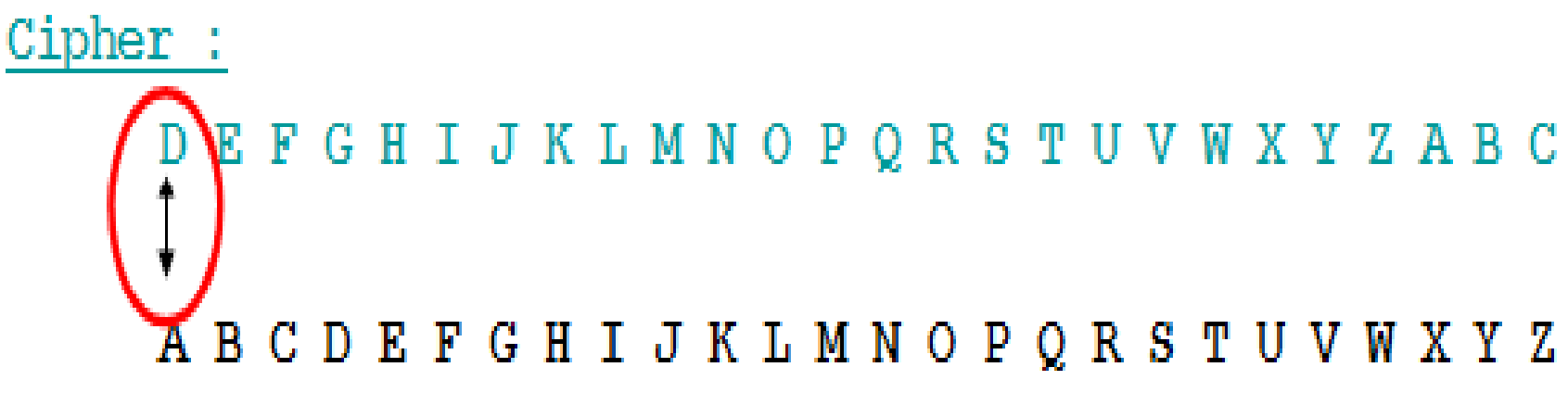


- สมมุติว่า Cipher คือ P B QDPH LV WKDQLQ

  Plain คือ M Y NAME IS THANIN

Cryptosystems → Caesar cipher

- จุดสังเกตของ Caesar Cipher คือ Key ที่ใช้จะเป็น Key D เนื่องจากตัวอักษรตัวแรกของภาษาอังกฤษคือตัว A เมื่อผ่านการเข้ารหัสจะถูกแทนที่ด้วยตัว D จะเห็นว่า Cipher ของ Caesar จะขึ้นต้นด้วยตัว D



ข้อดีของการเข้ารหัสแบบซีซาร์ (Caesar)

- คือ ความง่ายในการเข้ารหัส แต่ก็มีข้อเสียคือการที่สามารถจะทำการวิเคราะห์หาข้อความเดิมจาก Cipher Text ได้ง่าย ซึ่งการเข้ารหัสที่ดีนั้นจะต้องหลีกเลี่ยงการถูกวิเคราะห์โดยง่ายนี้ให้ได้ วิธีการที่นำมาวิเคราะห์ดังกล่าวนี้ก็คือ การหาสิ่งซ้ำ ๆ กันจากวิธีการเข้ารหัสที่เราเรียกว่าการหา Pattern ของตัวอักษร ซึ่งหากทำการวิเคราะห์ให้ดีจากตัวอักษรของ Cipher Text จำนวนมากพอ ก็จะเห็นได้ง่ายว่ามีการเลื่อนลำดับของตัวอักษร 3 ตัว ดังนั้นจึงไม่เป็นการยากนักที่ผู้ไม่ประสงค์ดีจะทำการ Cryptanalysis ของวิธีการเข้ารหัสแบบซีซาร์นี้

การแกะรหัส Caesar Cipher

- เราสามารถที่จะถอดรหัสของ Caesar ได้โดยง่ายแม้ไม่รู้ Key โดยการกระทำที่เรียกว่า Brute Force Attack ซึ่งสามารถแกะรหัสได้โดยไล่สุ่ม Key เพียงไม่เกิน 25 ครั้งเท่านั้น

Decryption shift		Candidate plaintext
0	(Ciphertext)	exxegoexsrgi
1	(Key B)	fyyfhpfytshj
2	(Key C)	gzzgiqgzutik
...		
24	(Key Y)	cvvcemcvqpeg
25	(Key Z)	dwwdfndwrqfh

Cryptosystems → Monoalphabetic Ciphers

การเข้ารหัสข้อมูลแบบ Monoalphabetic Cipher หรือเรียกว่า Monoalphabetic Substitution Ciphers คิดค้นโดยชาวอาหรับ โดยใช้วิธีการแทนที่ตัวอักษรแบบ 1 ต่อ 1 ไม่ใช่การเลื่อน ตัวอย่างของ Monoalphabetic Ciphers ในยุคแรก ๆ คือการเข้ารหัสข้อมูลแบบ Atbash ใช้การแทนที่ตัว A ด้วยตัว Z แทนที่ตัว B ด้วยตัว Y และแทนที่ตัว C ด้วยตัว X เป็นต้น

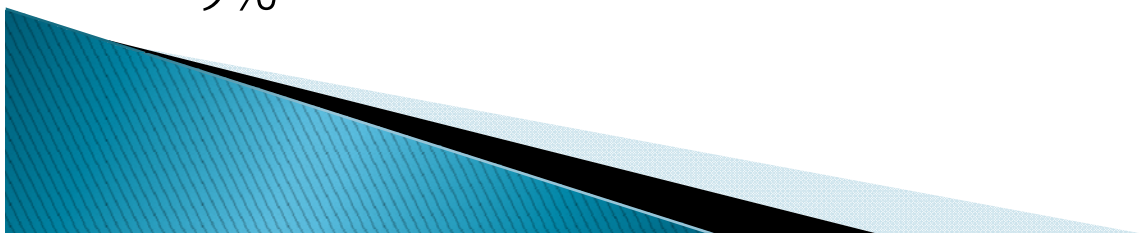
Plain Text : ABCDEFGHIJKLMNOPQRSTUVWXYZ

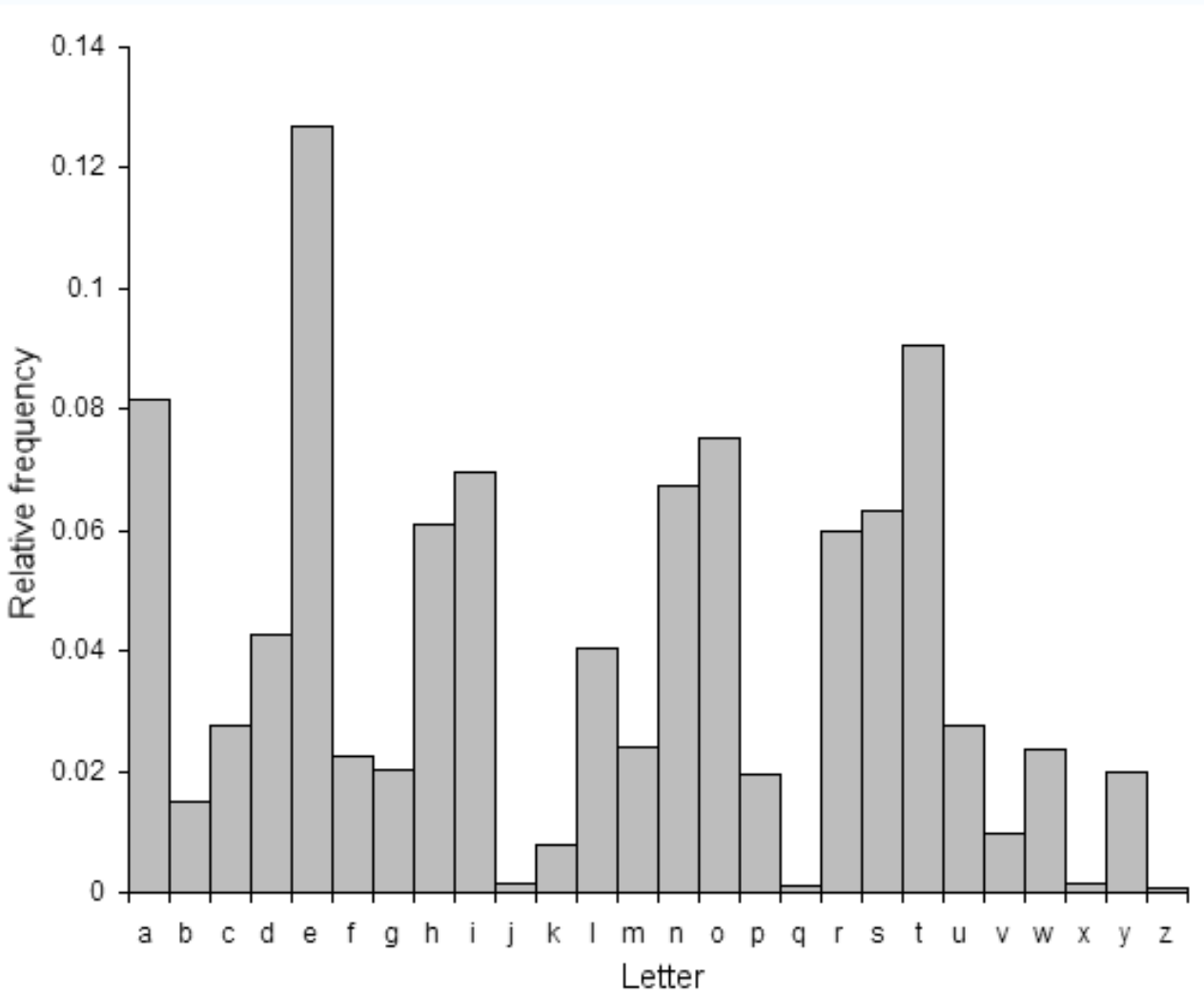
Cipher Text : ZYXWVUTSRQPONMLKJIHGFEDCBA

Cryptosystems → Monoalphabetic Ciphers

การเบรค Monoalphabetic Ciphers จะทำได้ยากกว่าการเบรค Caesar cipher เนื่องจากมีคู่ที่เป็นไปได้อยู่ 26 ยกกำลัง 26 คู่ การเบรคจะต้องใช้การสุ่มไปเรื่อย ๆ จนกว่าจะสำเร็จ ซึ่งจะต้องใช้จำนวนครั้งในการคำนวณการคำนวณถึง 26! ครั้ง (26! = 26 x 25 x 24 x 23 x ... x 1)

การเบรค Monoalphabetic ciphers สามารถทำได้อีกวิธีหนึ่งคือ การวิเคราะห์ความถี่ของตัวอักษรที่ปรากฏ (Frequency Analysis) ตัวอย่างเช่นตัวอักษร e กับ t จะเกิดบ่อยที่สุดในข้อความภาษาอังกฤษ โดยอักษร e มีอัตราการเกิดบ่อยถึง 13% ส่วนอักษร t มีอัตราการเกิดบ่อยถึง 9%



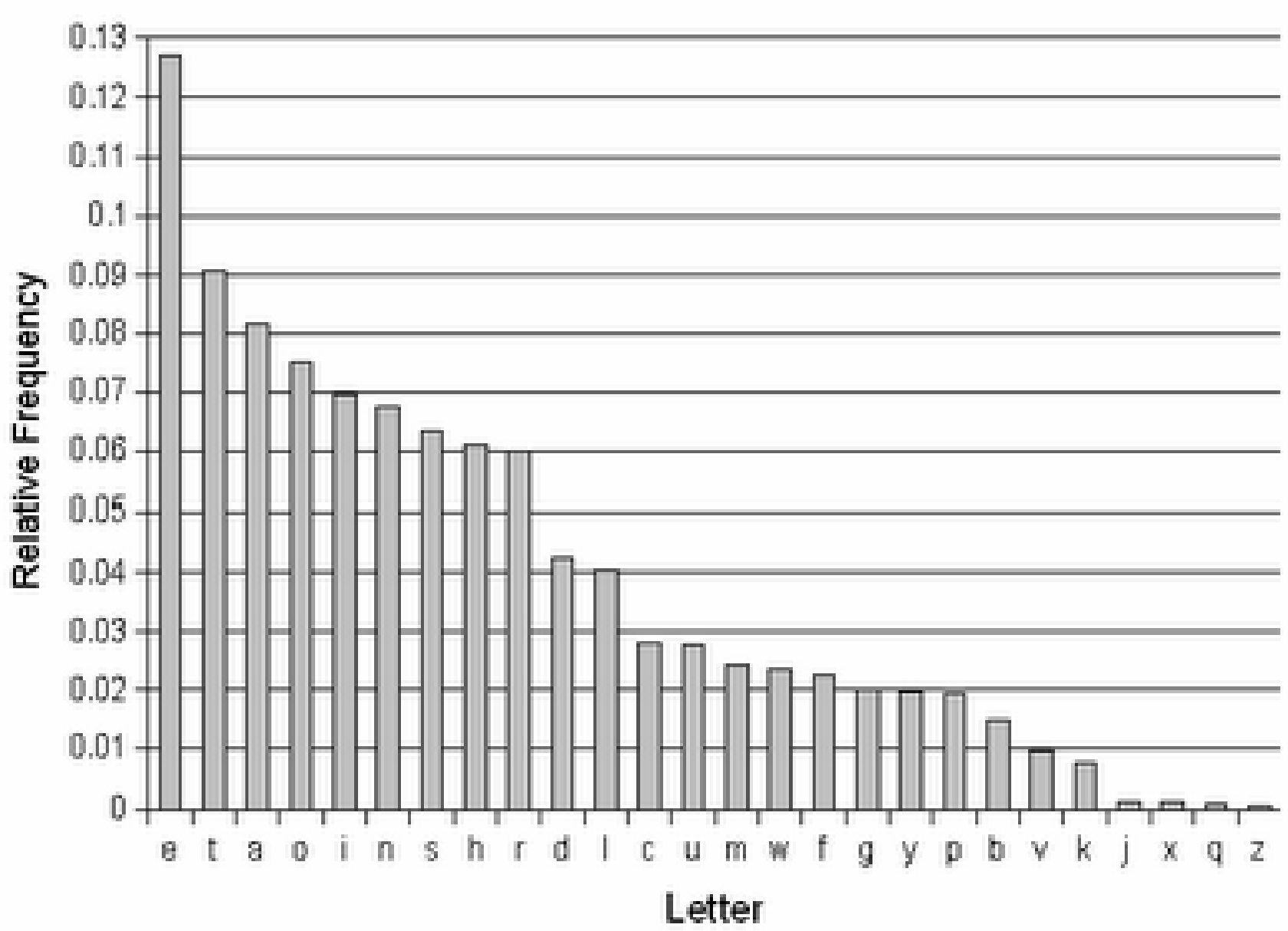


ความถี่ของตัวอักษรที่ปรากฏ

Cryptosystems → Monoalphabetic Ciphers

- การทำ Brute Force Attack ยังถือว่าเป็นการเสียเวลา เพราะต้องไล่สุ่ม Key ไปเรื่อยๆ จนกว่าจะเจอ
- ต่อมาจึงมีการคิดค้นวิธีต่างๆ ที่จะช่วยให้เราสามารถคาดเดารหัสได้ง่ายและเร็วขึ้น โดยใช้กระบวนการทางสถิติต่างๆ เช่น Frequency Analysis
- วิธีการเดาจะเริ่มจากการค้นหาตัวอักษรที่ซ้ำๆ กันก่อน
- พิจารณาอักษร 3 ตัวแรกของประโยค ตัวที่ 2 หรือ 3 มักจะเป็นสระเสมอ
- ความน่าจะเป็นของตัวอักษรที่ซ้ำๆ กันได้แก่
  - ตัวอักษรที่เป็นสระในภาษาอังกฤษ A E I O U
  - ตัวอักษรที่มีความถี่ปรากฏในคำภาษาอังกฤษบ่อยที่สุด

    C D H L N R S T



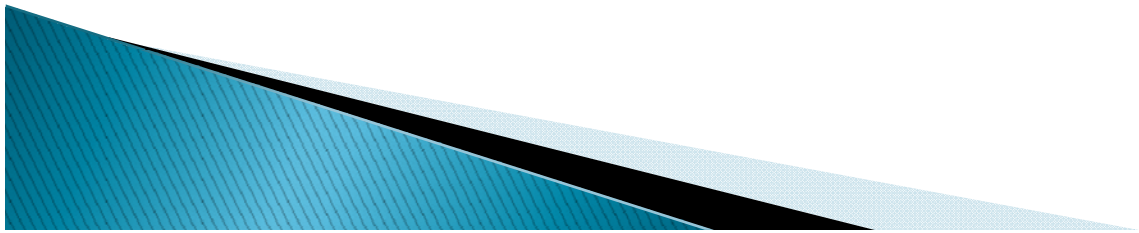
ความถี่ของตัวอักษรที่ปรากฏ (เรียงตามความถี่มากไปน้อย)

การเพิ่มระดับความปลอดภัยให้กับการเข้ารหัส

- วิธีหนึ่งที่สามารถนำมาใช้ในการเพิ่มระดับความปลอดภัยให้กับการเข้ารหัสแบบที่ใช้สัญลักษณ์เพียงหนึ่งตัวมาแทนค่าตัวอักษร ก็คือการใช้กุญแจเข้ารหัสมาช่วย (Encryption Key) อย่างไรก็ตามการใช้วิธีที่เรียกว่า Frequency Distribution ซึ่งเป็นการวัดเปรียบเทียบระหว่างความซ้ำกันของตัวอักษรทั้งหมดที่มีอยู่ในข้อความที่เป็น Cipher Text แล้วเอาไปเปรียบเทียบกับความซ้ำกันของตัวอักษรทั้งหมดที่มีอยู่ของคำในภาษาอังกฤษ ผลที่ได้ก็คือผู้ที่ทำการเจาะรหัสนั้นสามารถรู้ได้ว่าตัวอักษรที่ใช้ใน Cipher Text นั้นเป็นตัวอักษรตัวใดกันแน่ในภาษาอังกฤษ

Poly-alphabetics Substitutions Ciphers

- เป็นวิธีที่ได้รับการปรับปรุงจากวิธีแรกโดยมีจุดประสงค์คือไม่ให้สามารถทำการวิเคราะห์ได้โดยใช้วิธี Frequency Distributions
- หลักการที่ใช้ก็คือการใช้สัญลักษณ์หลายตัวเพื่อแทนค่าตัวอักษรภาษาอังกฤษตัวเดียววิธีการนี้สามารถลดความซ้ำกันของตัวอักษรในข้อความ Cipher Text ได้ ดังนั้นผู้ที่ทำการเจาะรหัสได้สามารถทำการเปรียบเทียบได้ว่าตัวอักษรในข้อความ Cipher text นั้นใช้แทนตัวอักษรใดกันแน่ในภาษาอังกฤษ

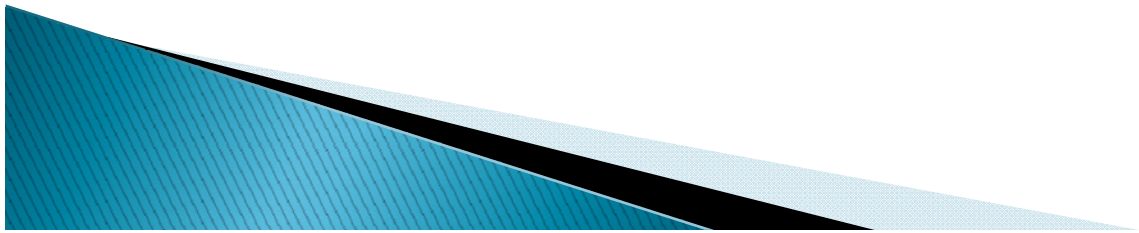


Poly-alphabetics Substitutions Ciphers

- วิธีการแทนค่าที่นิยมนำมาใช้กับการเข้ารหัสแบบนั้นก็คือ การใช้ตารางแทนค่าที่เรียกว่า Vigenere Tableaux ซึ่งสามารถทำให้การวิเคราะห์โดยใช้ Frequency Distributions ยากขึ้นมาก แต่อย่างไรก็ตามยังมีวิธีการที่ใช้ได้ผลสามารถนำมาทำการเจาะรหัสแบบนี้ นั่นคือวิธีการที่เรียกว่า The Kasiski Method for Repeated Patterns โดยอาศัยหลักที่ว่าคำในภาษาอังกฤษนั้นมีคำที่ใช้ทั่วไปและซ้ำกันมากเช่น คำว่า the, is, are, and, then, but, im-, in-, un-, -tion, -ion.....etc... เป็นต้น และคำพวกนี้สามารถทำให้เกิด Pattern ได้ใน Cipher Text ดังนั้นหากใช้วิธีการทางคณิตศาสตร์ที่เกี่ยวกับความน่าจะเป็น (Probability) มาทำการวิเคราะห์ pattern เหล่านี้โดยละเอียดแล้วก็จะสามารถเจาะรหัสหาข้อความเดิม (Clear Text)ได้

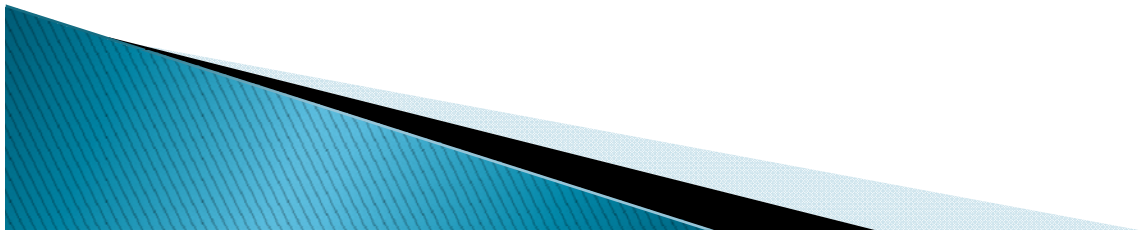
Poly-alphabetics Substitutions Ciphers

เทคนิคนี้จะใช้ในช่วงสงครามโลกครั้งที่ 1 และยากที่จะถอดรหัสด้วยมือเปล่า แต่ถ้าใช้คอมพิวเตอร์จะสามารถถอดรหัสได้ง่าย นอกจากนั้นหากต้องการจะเบรคโดยใช้คอมพิวเตอร์ก็จะทำการเบรคได้ง่ายเช่นกัน ผู้ที่เบรค Polyalphabetic Encryption ได้เป็นชาวรัสเซียชื่อ Friedrich Kasiski เบรคได้ในปี 1863 โดยให้ข้อสังเกตว่าถ้าได้ Cipher Text ที่มีความยาวมากพอ Pattern จะเริ่มซ้ำ และสามารถที่จะเห็นความเหมือนของ Cipher text โดยดูที่ Frequency Analysis ตัวอักษรแต่ละตัวปรากฏบ่อยแค่ไหน



Cryptosystems → Vigenere Cipher

- Vigenere Cipher เป็นการเข้ารหัสแบบซีเคร็ทคีย์ (Secret Key) หรือ Symmetric Key Cryptography ที่อาศัยพื้นฐานเดียวกันกับ Caesar
- หลักการของ Vigenere Cipher คือ จะใช้ Key ที่เป็นคำมาเรียงต่อๆ กัน แล้วเข้ารหัสโดยสร้าง Caesar Cipher จากตัวอักษรที่ปรากฏอยู่ใน Key
- Vigenere Cipher เป็นอีกชนิดหนึ่งที่อาศัยตารางตัวอักษรเป็นรหัสลับ เรียกว่า Vegenere Squre ในลักษณะ 26 X 26 ตัวอักษร



Cryptosystems → Vigenere Cipher

	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	D
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	C
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	B
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

Cryptosystems → Vigenere Cipher

- **ตัวอย่างเช่น**

  Plaintext : ATTACK AT DAWN และเลือกใช้ **Keyword :** LEMON

  นำ Plaintext มาเรียงคู่กับ Keyword ให้ได้ความยาวเท่ากันดังนี้

Plain Text	**:**	ATTACK	AT	DAWN
Key	**:**	LEMONL	EM	ONLE
Cipher Text	**:**	LXFOPV	EF	RNHR

  - ตัวอักษรตัวแรก - A จะถูกเข้ารหัสด้วย Caesar Cipher Key L
  - ตัวอักษรตัวที่ 2 - T จะถูกเข้ารหัสด้วย Caesar Cipher Key E
  - ตัวอักษรตัวที่ 3 - T จะถูกเข้ารหัสด้วย Caesar Cipher Key M
  - ตัวอักษรตัวที่ 4 - A จะถูกเข้ารหัสด้วย Caesar Cipher Key O
  - ตัวอักษรตัวที่ 5 - C จะถูกเข้ารหัสด้วย Caesar Cipher Key N

    และเรียงต่อไปเรื่อยๆ จนกว่าจะครบประโยค

Cryptosystems → Vigenere Cipher

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- ตัวอย่างเช่น

Plain Text : ATTACK AT DAWN

Key : LEMONL EM ONLE

Cipher Text : LXFOPV EF RNHR

P	0	19
K	11	12
C	11	31

: C = P + K ถ้า C มีค่ามากกว่าหรือ 26 ให้นำ 26 ไปลบออก ค่าที่ได้นำไปเทียบค่าน้ำหนักตัวอักษร

http://makcoder.sourceforge.net/demo/vigenere.php

Cryptosystems → Vigenere Cipher

- **การถอดรหัสก็ให้ทำกระบวนการย้อนกลับเหมือนกับของ Caesar แต่ต้องรู้ Keyword**
  - **Cipher Text : LXFOPV EF RNHR และ Keyword : LEMON**

    นำ Cipher Text มาเรียงคู่กับ Keyword ให้ได้ความยาวเท่ากันดังนี้

    Cipher Text : LXFOPV EF RNHR

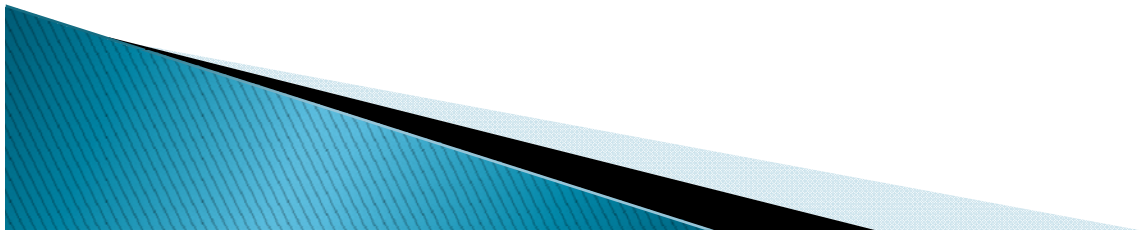
    Key : LEMONL EM ONLE

    Plain Text : ATTACK AT DAWN
  - ตัวอักษรตัวแรก - L จะถูกถอดรหัสด้วย Caesar Cipher Key L
  - ตัวอักษรตัวที่ 2 - X จะถูกถอดรหัสด้วย Caesar Cipher Key E
  - ตัวอักษรตัวที่ 3 - F จะถูกถอดรหัสด้วย Caesar Cipher Key M
  - ตัวอักษรตัวที่ 4 - O จะถูกถอดรหัสด้วย Caesar Cipher Key O
  - ตัวอักษรตัวที่ 5 - P จะถูกถอดรหัสด้วย Caesar Cipher Key N

    และเรียงต[illegible]ๆ จนกว่าจะครบประโยค

Cryptosystems → Vigenere Cipher

- ใช้ Keyword ที่เป็นคำมาเรียงต่อๆ กัน แล้วเข้ารหัสโดยสร้าง Caesar Cipher จากตัวอักษรที่ปรากฏอยู่ใน Key ทำให้โครงสร้างของ Cipher ที่ใช้ในการเข้ารหัสซับซ้อนยิ่งขึ้น
- แต่ถ้า Keyword ถูกขโมยไปใช้ ข้อมูลก็จะถูกถอดรหัสได้
- ถึงไม่รู้ Keyword ก็ยังสามารถคาดเดา Keyword ได้จากการทดสอบตัวอักษรที่เรียงซ้ำๆ กันควบคู่กับการพิจารณาระยะห่าง โดยวิธีการที่เรียกว่า Kasiski examination และ Friedman



Cryptosystems → Vernam Cipher

พัฒนาขึ้นครั้งแรกที่ AT&T โดยใช้ร่วมกับอุปกรณ์ที่ชื่อว่า เครื่องเวอร์-แนม (Vernam Machine) One-time Pad

ขั้นตอนวิธี

- กำหนดให้ค่าให้กับอักขระแต่ละตัวโดยเริ่มต้นค่าจากน้อยไปมาก เช่น A = 0, B = 1, ..., Z = 25
- แทนค่าข้อความต้นฉบับที่ต้องการเข้ารหัสและข้อความนำเข้าไซเฟอร์จากค่าของอักขระแต่ละตัวที่กำหนดในข้อ 1
- บวกค่าอักขระแต่ละตัวในข้อความต้นฉบับกับค่าของอักขระแต่ละตัวในข้อความนำเข้าไซเฟอร์
- ถ้าผลลัพธ์ที่ได้มากกว่า 25, ให้ลบออกด้วย 26
- แปลงค่าจำนวนที่ได้กลับเป็นตัวอักขระที่เกี่ยวข้อง ซึ่งจะได้เป็นข้อความไซเฟอร์

Cryptosystems → Vernam Cipher

- การเข้ารหัสและการถอดรหัสเพื่อให้ได้ข้อความที่อ่านได้ (Plain Text) กลับมานั้นจำเป็นต้องใช้ตัวเลขสุ่ม (Random Number) โดยมากแล้ววิธีการที่ใช้ในการกำเนิดตัวเลขสุ่มที่นิยมใช้กันมากก็คือ วิธี Linear Congruential Random Number Generator ซึ่งจะให้กำเนิดตัวเลขสุ่มที่เริ่มด้วยตัวเลขเริ่มต้นตามที่กำหนดให้ เราเรียกตัวเลขนี้ว่า Seed อย่างไรก็ตามวิธีการนี้ก็สามารถจะให้ตัวเลขสุ่มได้จำนวนหนึ่งก่อนที่จะเริ่มให้ตัวเลขที่ซ้ำกันอีก ดังนั้นการใช้วิธีให้กำหนดตัวเลขสุ่มนี้ก็ต้องใช้ความระมัดระวังด้วยมิฉะนั้นอาจทำให้ตัวอักษรใน Cipher Text มีลักษณะที่ซ้ำกันได้และจะง่ายต่อการวิเคราะห์ Cryptanalysis

Cryptosystems → Vernam Cipher

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

plain text =	V	E	R	N	A	M	C	I	P	H	E	R
number =	21	4	17	13	0	12	2	8	15	7	4	17
andom number =	76	48	16	82	44	3	58	11	60	5	48	88
sum =	97	52	33	95	44	15	60	19	75	12	52	105
mod 26 =	19	0	7	17	18	15	8	19	23	12	0	1
cipher text =	T	A	H	R	S	P	I	T	X	M	A	B

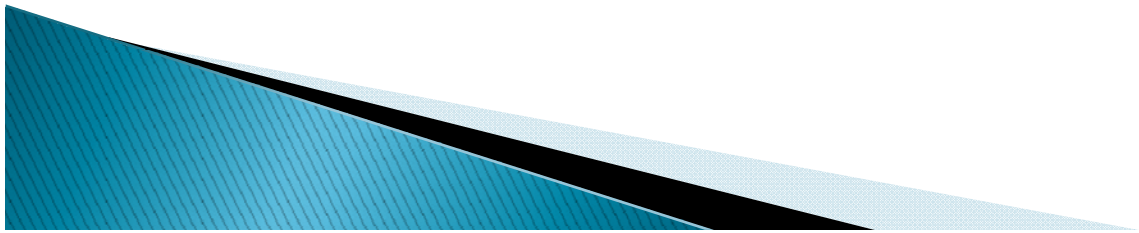
วิธีการ mod	97 mod 26 = 19	--> 96/26 = 3.69	26 x 3 = 78	97 - 78 = 19	หมายถึงตัว T
	52 mod 26 = 0	--> 52/26 = 2.0	26 x 2 = 52	52 - 52 = 0	หมายถึงตัว A
	33 mod 26 = 7	--> 33/26 = 1.26	26 x 1 = 26	33 - 26 = 7	หมายถึงตัว H

Cryptosystems → Vernam Cipher

ตัวอย่างที่ 3.7 กำหนดให้ข้อความต้นฉบับ คือ

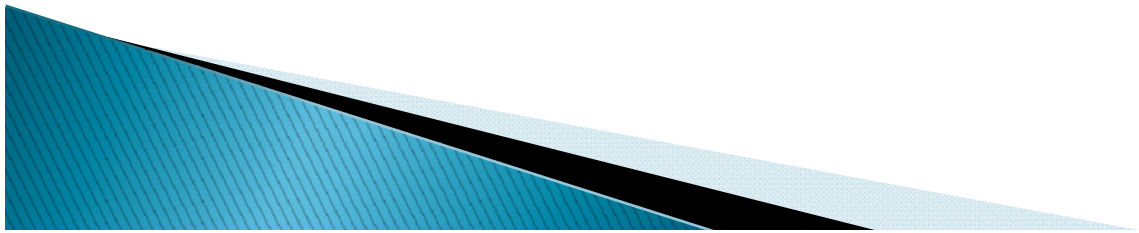
- Plain Text : HELLO
- Key One-Time Pad คือ *X M C K L*
- Cipher Text : E Q N V Z

- **ข้อดี:** มีความปลอดภัยของข้อความสูงและเหมาะสมกับข้อความต้นฉบับที่มีขนาดสั้น
- **ข้อเสีย:** ไม่เหมาะสำหรับข้อความต้นฉบับขนาดใหญ่



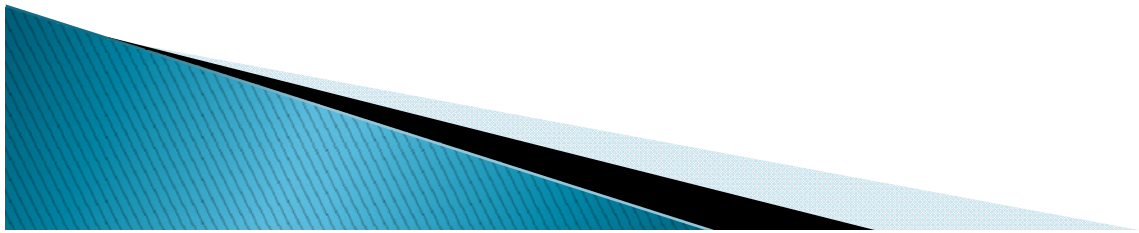
Cryptosystems → Vernam Cipher

แต่อย่างไรก็ตาม One-Time Pad ก็ยังมีปัญหาอยู่เช่น Key ที่ใหญ่เท่ากับ Plain Text จะต้องใช้พื้นที่มากสำหรับเก็บ Key นอกจากนั้น Key ที่ใหญ่ก็ทำให้ใช้งานได้อย่างลำบาก หากเทียบกับการใช้ Key ที่มีขนาดเล็ก นอกจากนั้นผู้ส่งข้อความจะต้องมีการส่ง Key ไปยังปลายทางเพื่อใช้ในการถอดรหัส ซึ่งอาจจะทำให้ Key ถูกขโมยได้ในระหว่างขั้นตอนการส่งคีย์



Cryptosystems → Playfair Cipher

Playfair cipher เป็น Block Cipher ตัวแรกเกิดขึ้นในปี ค.ศ. 1854 โดย Sir Charles Wheatstone ซึ่งเล่าให้ Baron Playfair ฟัง แล้วจากนั้นก็ถูกเล่าต่อให้ Albert และ Load Palmerston ฟังบนโต๊ะอาหารเย็น Playfair cipher ถูกใช้ในกองกำลังทางประเทศสหราชอาณาจักรในสงครามโลกครั้งที่ 1 มีขบวนการทำงานของอัลกอริทึมดังนี้

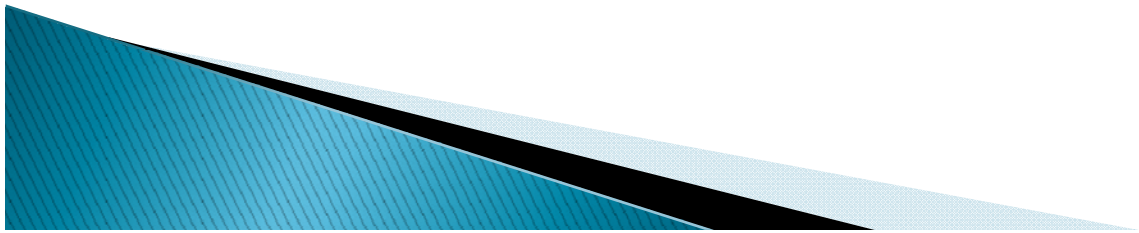


Cryptosystems → Playfair Cipher

(1) สร้างตาราง Key ขนาด 5 x 5 = 25 แบบสุ่มโดยตัดตัว Q ออก

ตัวย่าง Key ขนาด 5x5

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



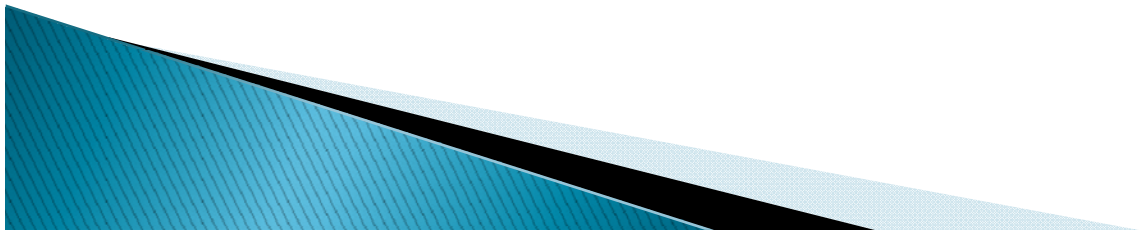
Cryptosystems → Playfair Cipher

(2) แบ่งตัวอักษร Plain Text ต้นฉบับออกมาเป็นคู่ ๆ หากมีตัวอักษรที่ติดกันให้เอา X คั่นกลาง และหากตัวสุดท้ายไม่ครบคู่ให้ใส่ Z เข้าไปแทน เช่น ต้องการเข้ารหัสข้อความว่า "Hide the gold in the tree stump" ก็สามารถจัดตัวอักษรเป็นคู่ ๆ ได้ดังนี้

HI DE TH EG OL DI NT HE TR EX ES TU MP

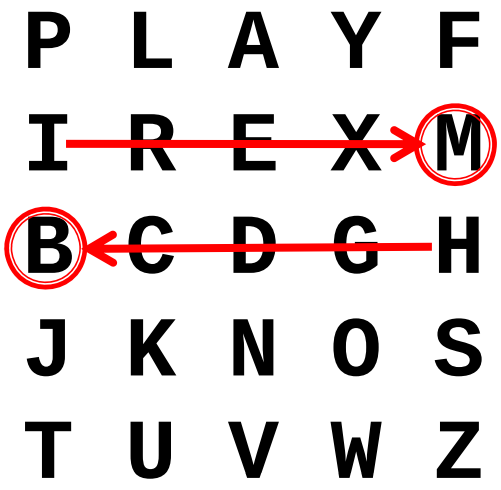
^

ใส่ X เข้าไปเนื่องจากมีตัว E สองตัวติดกัน



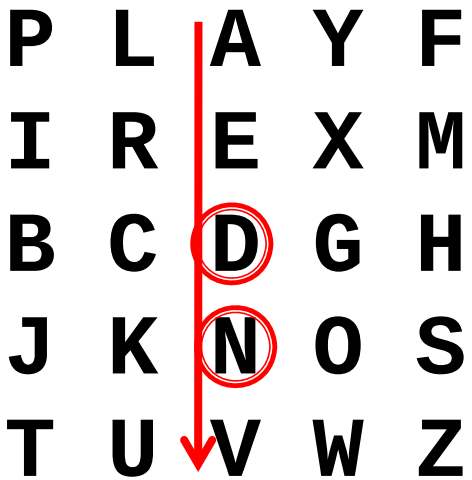
Cryptosystems → Playfair Cipher

(3) นำตัวอักษรแต่ละคู่มาเปรียบเทียบกับตาราง Key ถ้าไม่อยู่ในแถวและ Column เดียวกัน ให้แทนที่ตัวอักษรแบบไขว้กัน เช่น HI ในข้อความต้นฉบับ (H ไม่ได้อยู่แถวเดียวกันกับ I และ H ก็ไม่ได้อยู่ใน Column เดียวกันกับ I) จะกลายเป็น BM (H กลายเป็น I และ B กลายเป็น M)



Cryptosystems → Playfair Cipher

(4) ถ้า 2 ตัวอักษรอยู่ Column เดียวกัน ให้เอาตัวอักษรที่อยู่ข้างล่างติดกันมาแทนที่ โดยทำทีละตัว (หากตัวอักษรนั้นอยู่ล่างสุดให้เอาตัวบนสุดมาแทนที่) เช่น DE ในข้อความต้นฉบับ จะกลายเป็น ND เนื่องจาก D ถูกแทนที่ด้วย N ส่วน E ถูกแทนที่ด้วย D



Cryptosystems → Playfair Cipher

(5) ถ้า 2 ตัวอักษรอยู่แถวเดียวกัน ให้เอาตัวอักษรที่อยู่ขวามือมาแทนที่ โดยทำทีละตัว (หากตัวอักษรนั้นอยู่ขวาสุดให้เอาตัวซ้ายสุดมาแทนที่) เช่น TU ในข้อความต้นฉบับ จะกลายเป็น UV เนื่องจาก T ถูกแทนที่ด้วย U ส่วน U ถูกแทนที่ด้วย V

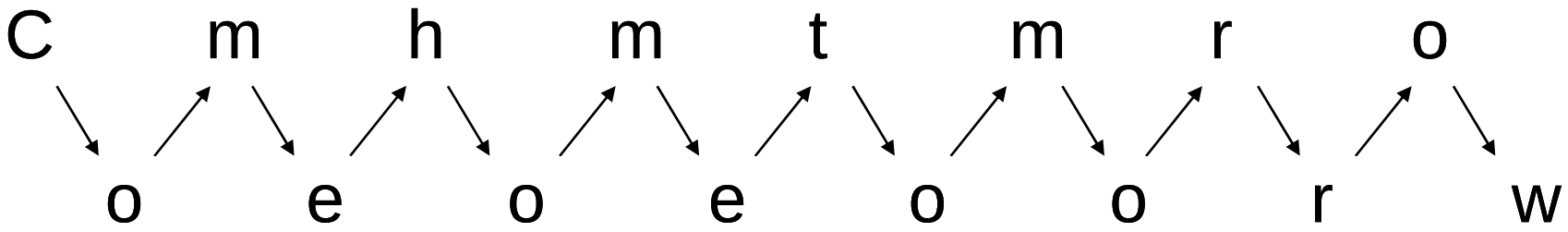
P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
J	K	N	O	S
T	U	V	W	Z

หากทำการเข้ารหัสแล้วจะได้ดังนี้

Plain Text: HI DE TH EG OL DI NT HE TR EX ES TU MP
Cipher Text: BM ND ZB XD KY BE JV DM UI XM MN UV IF

Cryptosystems → Rail Fence Cipher

- Write the plaintext downwards on successive "rails" of an imaginary fence. When you get to the bottom start moving up. Write the message line by line.
- เป็นการเข้ารหัสอย่างง่าย ใช้ลักษณะของ Row-by-Row หรือ Zigzag
- Plain Text : Come home tomorrow Key = 2



- Cipher Text : Cmhmtmrooeoeoorw

Cryptosystems → Rail Fence Cipher

Example:

Plain Text : Come home tomorrow by my car Key = 3

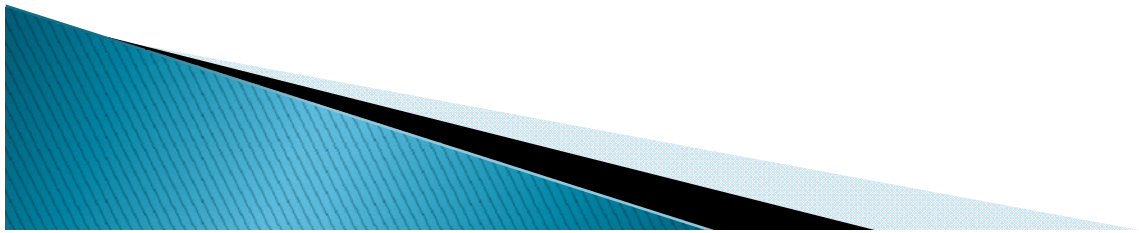
C				E				M				O				R				W			
	O				H				E				M				R				B		
		M				O				T				O				O				Y	

M				A				O				H				E				M			
	R				M				R				B				Y				R		
		O				T				O				O				Y				C	

Cipher Text : CEMORWMAOHEMRBYRMOTOOYC

Cryptosystems → Route Cipher

- The plaintext is first written out in a grid of given dimensions, then we read it off in a pattern given in the key.
- เขียนข้อความต้นฉบับที่ละแถวลงในเมทริกซ์ ที่มีจำนวนคอลัมน์ ตามกำหนด เช่น
- Plain Text : “I go to the conference tomorrow at NPRU”
- Matrix is **6 X 6**
- The key say : read message from top right corner down and to the left.



ตัวอย่าง Plain Text : I go to the conference tomorrow at NPRU

ลำดับแถว => I G O T O T

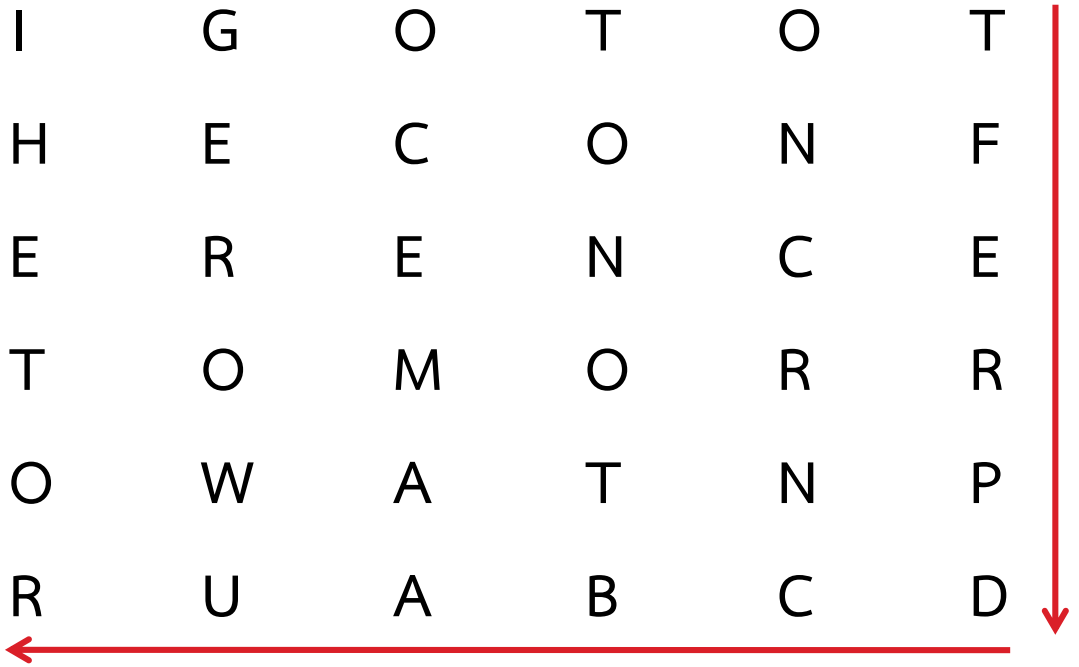
H E C O N F

E R E N C E

T O M O R R

O W A T N P

R U A B C D



- Key => read message from top right corner down and to the left.
- ข้อความ Cipher ที่ได้

TFERPDCBAURONCRNTAWOTONOMOTOCEREGEHI

Cryptosystems → Columnar Transposition Cipher

- ไซเฟอร์แบบคอลัมน์ (Columnar Transposition Cipher) เริ่มต้นด้วยการกำหนดขนาดคอลัมน์ ที่ใช้ในการเข้ารหัส
- เขียนข้อความต้นฉบับที่ละแถวลงในเมทริกซ์ ที่มีจำนวนคอลัมน์ ตามกำหนด เช่น
- Plain Text : “I go to the conference tomorrow at NPRU”
- Key : 412536

ตัวอย่าง Plain Text : I go to the conference tomorrow at NPRU

ลำดับแถว =>	1	2	3	4	5	6
	I	G	O	T	O	T
	H	E	C	O	N	F
	E	R	E	N	C	E
	T	O	M	O	R	R
	O	W	A	T	N	P
	R	U	A	B	C	D
key =>	4	1	2	5	3	6

- ข้อความ Cipher ที่ได้

GEROWU OCEMAA ONCRMC IHETOR TONOTB TFERBD

Cryptosystems → Columnar Transposition Cipher

- Write the message in rows of a fixed length, and then read out again column by column. The columns are chosen in some scrambled order. Both the length of the rows and the permutation of the columns are usually defined by a keyword.
- เขียนข้อความต้นฉบับที่ละแถวลงในเมทริกซ์ ที่มีจำนวนคอลัมน์ ตามกำหนด เช่น
- **Plant Text : “I go to the conference tomorrow at NPRU”**
- Key : THANIN

ตัวอย่าง Plain Text : I go to the conference tomorrow at NPRU

key	=>	T	H	A	N	I	N
ลำดับแถว	=>	I	G	O	T	O	T
		H	E	C	O	N	F
		E	R	E	N	C	E
		T	O	M	O	R	R
		O	W	A	T	N	P
		R	U	A	B	C	D

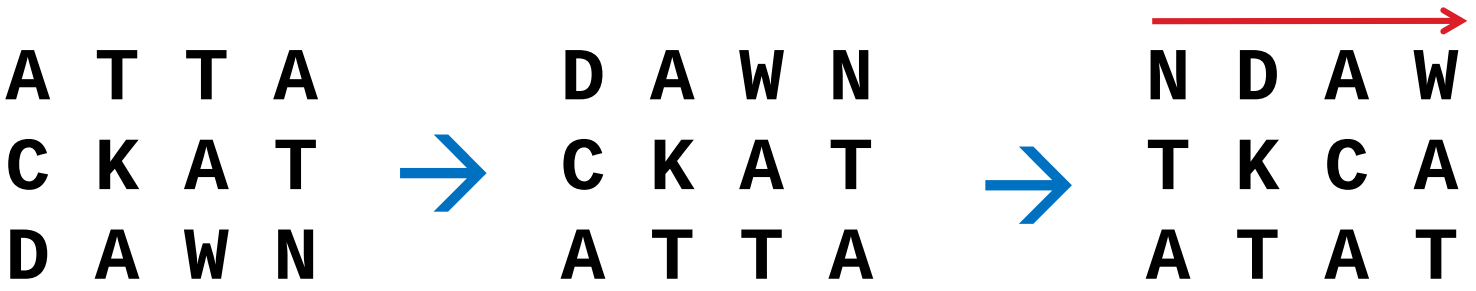
- ข้อความ Cipher ที่ได้

OCEMAAGEROWUONCRNCTONOTBTFERPDIHETOR

Cryptosystems → Double Transposition Cipher

- เป็นการสลับตำแหน่งข้อความ Plain Text แบบ Array 2 มิติ ตามที่กำหนด เช่น
- **Plain Text : “Attack at Dawn”**
- **Array 2 มิติ : 3 X 4**
- Key Pattern Column : (1, 2, 3) → (3, 2, 1)

  Row : (1, 2, 3, 4) → (4, 2, 1, 3)



ข้อความ Cipher ที่ได้ NDAW TKCA ATAT

Cryptosystems → eXclusive OR

- XOR เป็นการกระทำทางตรรกศาสตร์ โดยมีหลักการ คือ
  - มีอินพุตตั้งแต่สองอินพุตขึ้นไป เช่น A, B (ในตารางความจริงด้านล่าง)
  - จะให้เอาท์พุตเป็นลอจิก 0 เมื่อ อินพุตมี ลอจิกเหมือนกัน
  - จะให้เอาท์พุตเป็นลอจิก 1 เมื่อ อินพุตมี ลอจิกต่างกัน

A	B	XOR
0	0	0
0	1	1
1	0	1
1	1	0

หรือ

True Xor True = False

True Xor False = True

False Xor True = True

False Xor False = False

หรือ

1 Xor 1 = 0

1 Xor 0 = 1

0 Xor 1 = 1

0 Xor 0 = 0

Cryptosystems → eXclusive OR

- **การดำเนินการทางตรรกศาสตร์ของ XOR**
- จะหาคำตอบได้ ก็ต่อเมื่อต้องแปลงเลขฐาน 10 ให้กลายเป็นเลขฐาน 2 (Binary) ก่อน เช่น
  กำหนดตัวแปร A = 10 หรือ กระจายเป็นเลขฐาน 2 (Binary) = 1 0 1 0
  กำหนดตัวแปร B = 8 หรือ กระจายเป็นเลขฐาน 2 (Binary) = 1 0 0 0
  ดังนั้นเมื่อให้ A Xor B คือ

1 0 1 0
1 0 0 0
---
0 0 1 0 **(ฐาน 2) หรือ 2 (ฐาน 10)**
=====

การดำเนินการทางตรรกศาสตร์ของ XOR ภาษาระดับสูง

- เวลาที่เขียนคำสั่ง 65 Xor 20 จะได้คำตอบคือ 85 (ฐาน 10) ... นี่คือความสามารถของภาษาระดับสูง
  แต่แท้ที่จริงแล้ว **จะเกิดปฏิบัติการระดับบิตขึ้นมา** โดยที่มองไม่เห็น ...**แต่ต้องสนใจความเป็นมา**
  หมายความว่า ทั้งตัวตั้ง (65) และ ตัวกระทำ (20) จะต้องถูกแปลงให้เป็นเลขฐาน 2 ออกมาก่อน ดังนี้ คือ
  1 0 0 0 0 0 1 ... หรือ 65 (ฐาน 10)
  X X 1 0 1 0 0 ... หรือ 20 (ฐาน 10) ... ค่าใดที่มากระทำ XOR กับ X ก็จะได้ค่านั้นเสมอ
  ---
  1 0 1 0 1 0 1 ... หรือ 85 (ฐาน 10)
  ========

Cryptosystems → Running Key Cipher

- Running Key Cipher –ใช้ คีย์ยาวเท่ากับ Plaintext มาแปลงเป็น Ciphertext ดังรูป
- Key : “On a non interfering basis over …”
- Message : “This material is enciphered”

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Message : This

Key : Onan

33-26 = 7

Ciphertext

huif anbrkmrg mj

Questions and Answers

MS1 Thanin Muangpool

Thank you