บทที่ 4 : Cryptography & Steganography Part1

สธ412 ความมั่นคงของระบบสารสนเทศ

อาจารย์อภิพงศ์ ปิงยศ

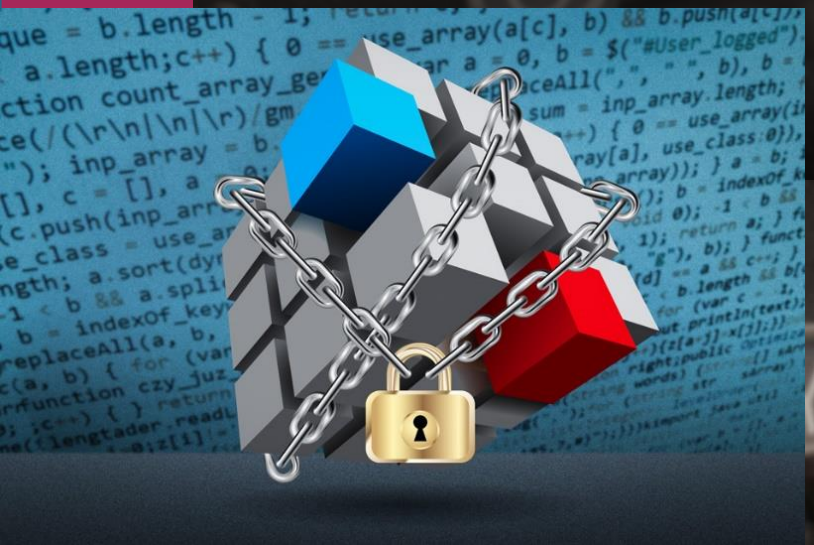
apipong.ping@gmail.com

Cryptography & Steganography

- Cryptography & Steganography
- Secret Key Cryptography

Cryptography & Steganography

- **Cryptography** คือการเข้าและถอดรหัสข้อมูล เป็นขั้นตอนหนึ่งสำหรับการรักษาข้อมูลให้มีความลับ
- **Steganography** คือการอำพรางข้อมูล โดยอำพรางไปกับไฟล์อื่นๆ เช่น รูปภาพ เสียง วีดีโอ ซึ่งเป็นการปกปิดทั้งวิธีการเข้ารหัสข้อมูลและคีย์ที่ใช้เข้ารหัส

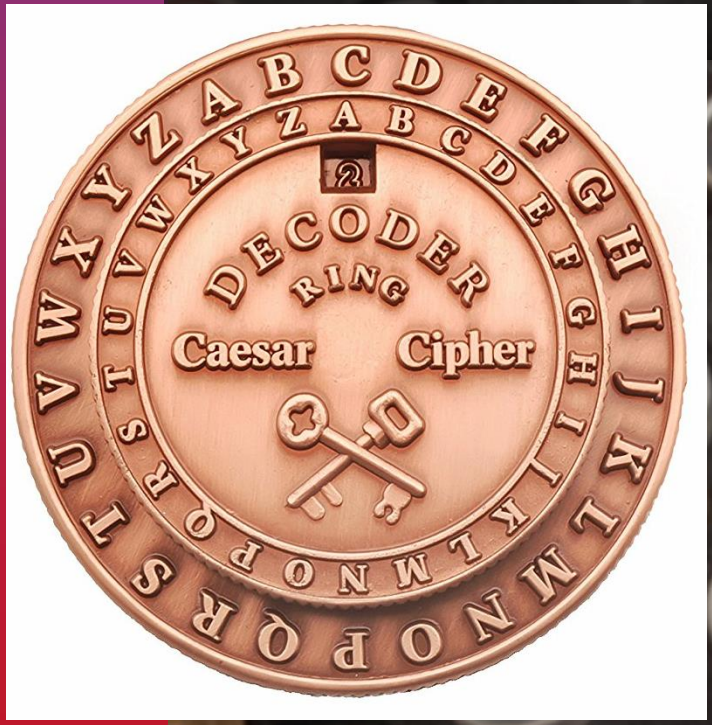


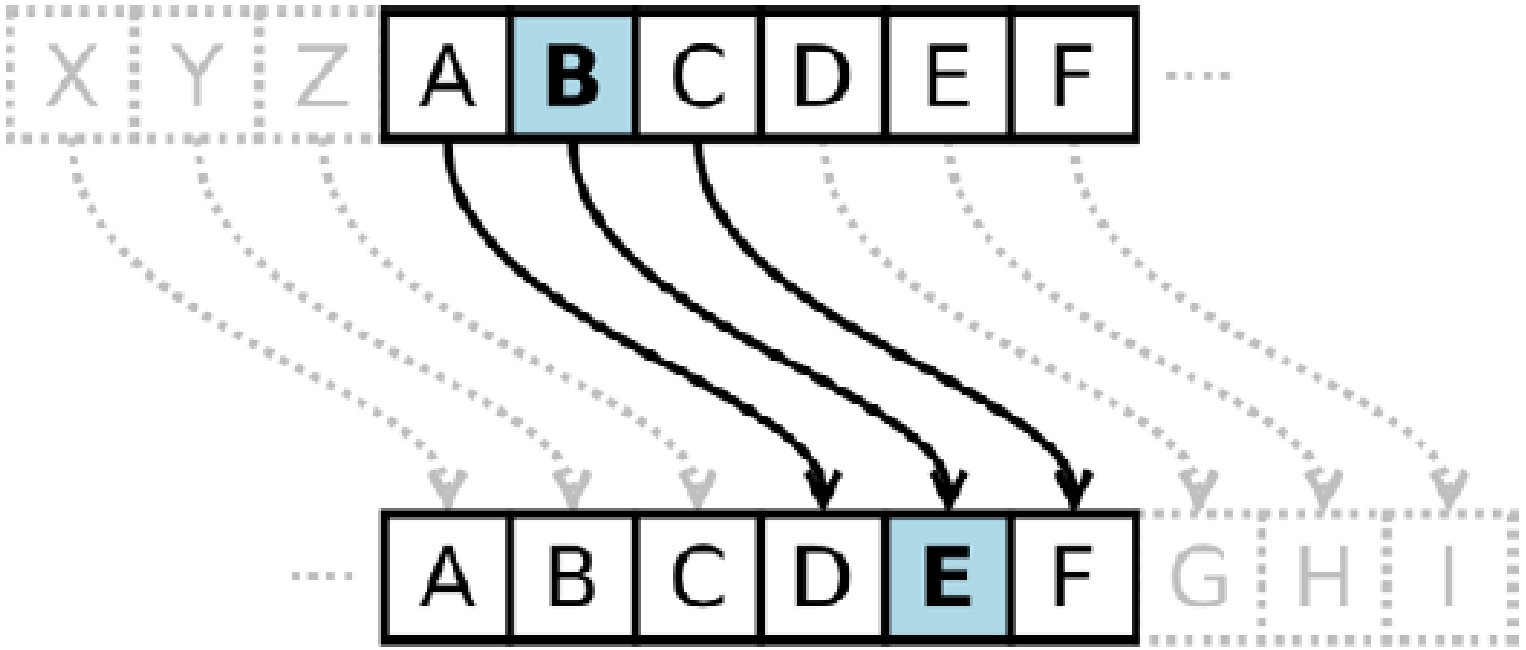
Cryptography & Steganography

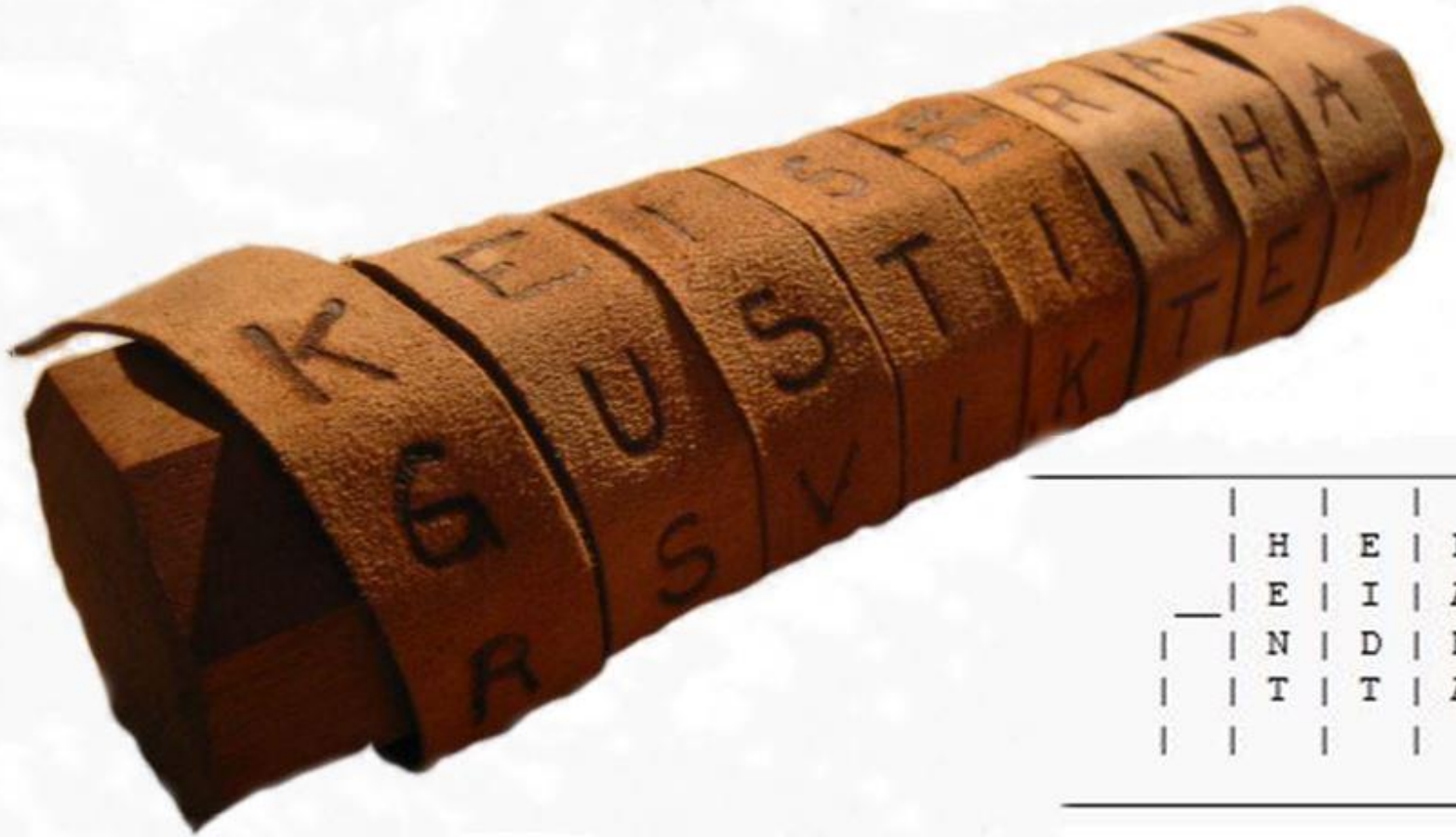
- เอกสารทางประวัติศาสตร์ระบุว่ามีการใช้การเข้ารหัสข้อมูลครั้งแรก 1900 ปีก่อนคริสตศักราช โดยชาวอียิปต์
- การเข้ารหัสข้อมูลถูกพัฒนาขึ้นมาเรื่อยๆตามระบบการสื่อสาร
- ความจำเป็นมีมากขึ้นโดยเฉพาะอย่างยิ่งบนเครือข่ายอินเทอร์เน็ต

ตัวอย่างการเข้ารหัสซีซาร์ไซเฟอร์ (Caesar Cipher)

เป็นเทคนิคการแทนตัวอักษรหนึ่งด้วยอักษรอีกตัวหนึ่ง (Substitution Cipher)



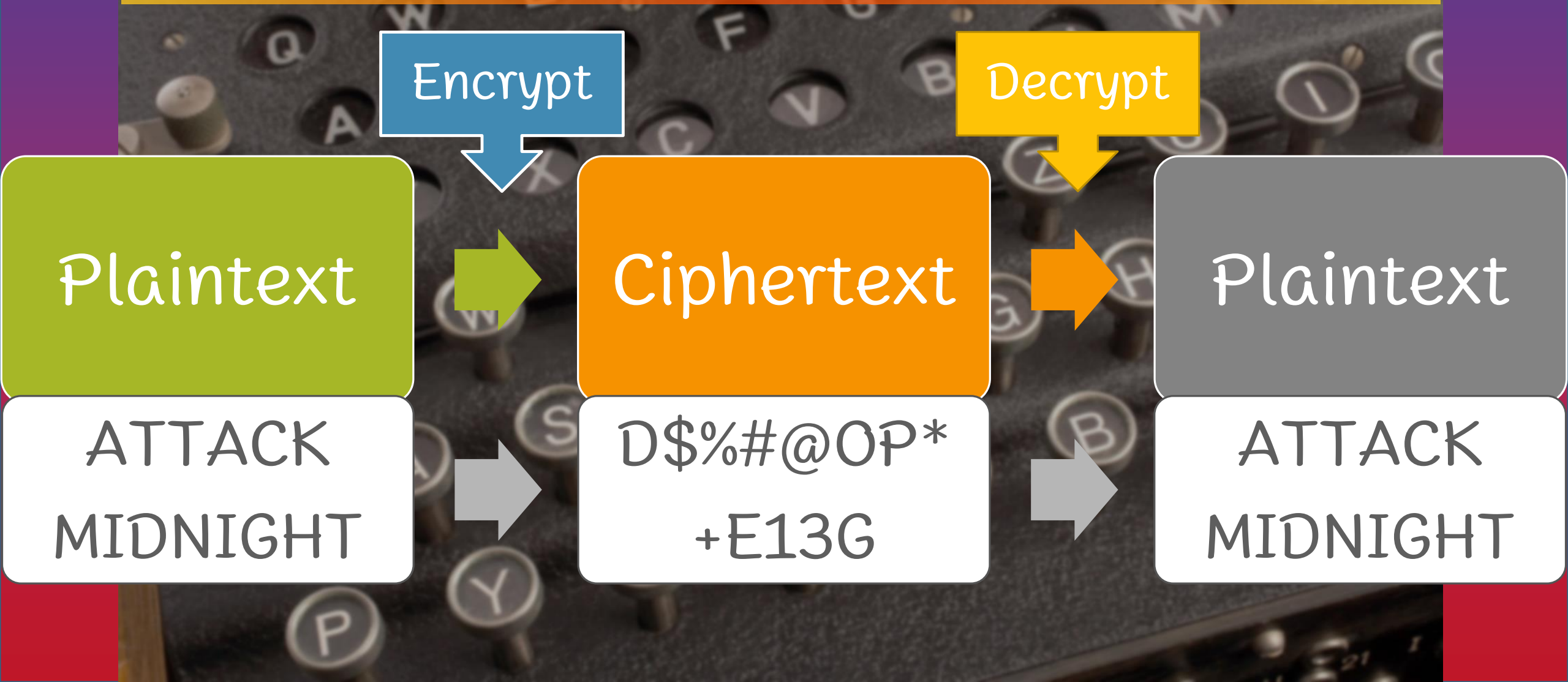





```
 _____________________________________________
|     |     |     |     |     |     |     |
|     | H   | E   | L   | P   | M   |     |
|  __ | E   | I   | A   | M   | U   | __  |
| |   | N   | D   | E   | R   | A   |     |
| |   | T   | T   | A   | C   | K   |     |
| |   |     |     |     |     |     |     |
 ---------------------------------------------
```

"Help me I am under attack".

การเข้า-ถอด รหัสข้อมูล
Encryption - Decryption



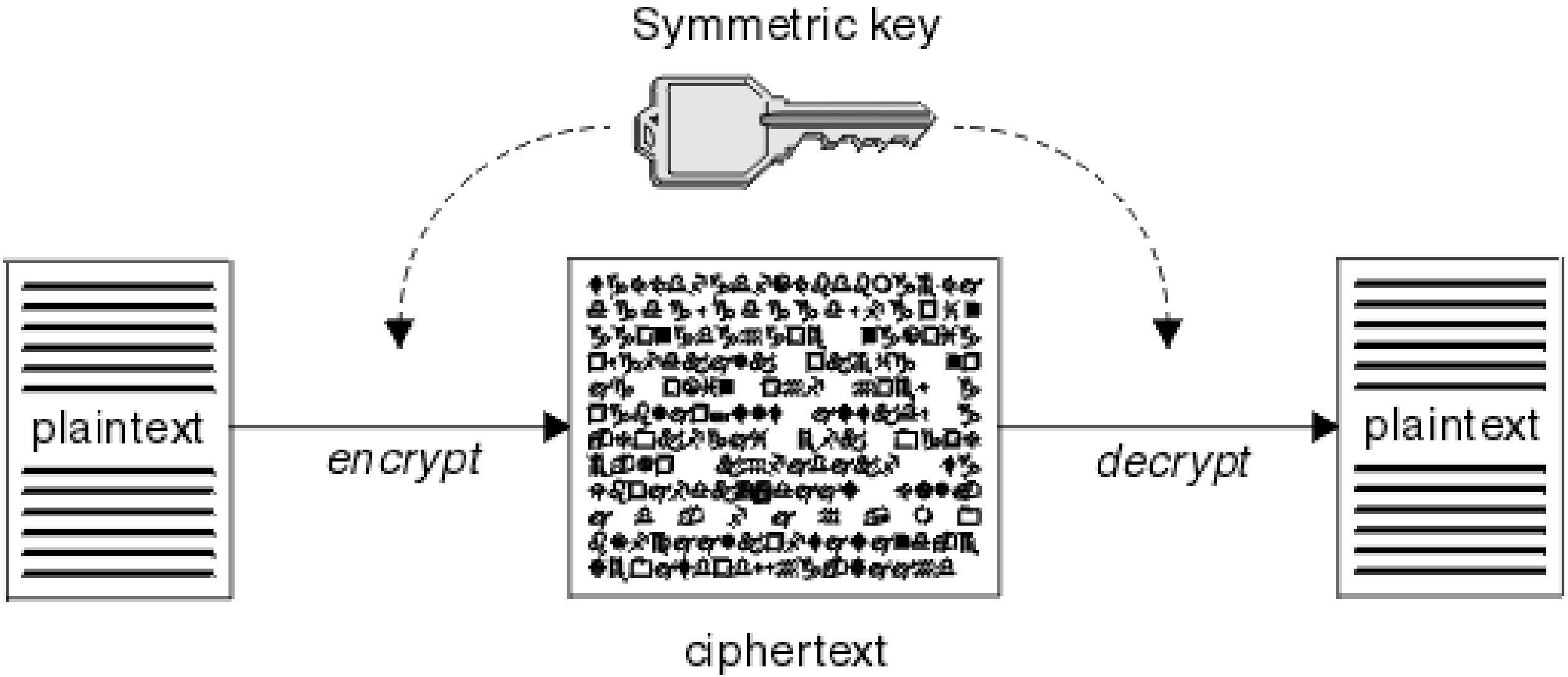
Cryptography & Steganography

- แบ่งประเภทการเข้าและถอดรหัสข้อมูล (Cryptography) เป็น 3 ประเภท คือ
  - Secret Key Cryptography
  - Public Key Cryptography (Next...)
  - Hash Function (Next...)

Secret Key Cryptography

- เป็นวิธีการเข้ารหัสและถอดรหัส โดยใช้ Key เดียวกัน
- เรียกอีกอย่างหนึ่งว่า *การเข้าและถอดรหัสแบบสมมาตร (Symmetric Key)*
- คีย์ที่ใช้จะมีความยาวคงที่

Secret Key Cryptosystem



Secret Key Cryptography

- การเข้ารหัสข้อมูลแบบนี้ คีย์ที่ใช้ในการเข้าและถอดรหัสจะต้องทราบเหมือนกันทั้งฝ่ายรับและฝ่ายส่ง ซึ่งจะต้องเก็บเป็นความลับ
- จุดอ่อนของวิธีนี้คือการแจกจ่ายคีย์ เพราะตอนเริ่มต้นจะต้องมีฝ่ายใดฝ่ายหนึ่งที่ยังไม่ได้รับคีย์
- ควรมีการยืนยันตัวตน (Authentication) ก่อนการแจกจ่ายคีย์

Secret Key Cryptography

- **ข้อดี**คือเป็นวิธีที่ค่อนข้างเร็วมาก
- **ข้อเสีย** คืออัลกอริทึมที่ใช้เข้าและถอดรหัสถูกตีพิมพ์เป็นสาธารณะ และคีย์ที่ใช้เข้าและถอดรหัสเป็นตัวเดียวกัน ทำให้ใครก็ตามที่ได้คีย์ไปก็สามารถถอดรหัสข้อมูลได้
- การแจกจ่ายคีย์อาจเป็นการส่งมอบผ่านช่องทางอื่นๆที่เป็นคนละช่องทางกับการส่งข้อมูล Ciphertext หรือต้องเข้ารหัสซีเคร็ทคีย์อีกชั้นหนึ่ง

Secret Key Algorithm ที่นิยมใช้

DES/3DES

AES

DES
(Data Encryption Standard)

- พัฒนาโดย IBM
- ถูกใช้เมื่อปี 1977 โดยรัฐบาล USA
- ปัจจุบันเป็นอัลกอริทึมที่ **ไม่ปลอดภัย** เนื่องจากถูกถอดรหัสได้ง่ายมากด้วยวิธี Brute Force Attack
- มีการปรับปรุงเป็น 3DES เพื่อเพิ่มความยาวคีย์ แต่ก็ไม่นิยมใช้แล้วเช่นกัน

AES
(Advanced Encryption Standard)

- เป็นมาตรฐานที่มาแทนที่ DES ในปี 2001 โดยใช้อัลกอริทึม Rijndael
- มีคีย์ขนาด 128, 192 และ 256 บิต
- เป็นมาตรฐานการเข้ารหัสแบบไม่มีลิขสิทธิ์ มีการใช้งานอย่างแพร่หลาย
- ยังไม่มีรายงานว่าสามารถถูกโจมตีได้