**•Cryptography**  
Cryptography : ให้คนอื่นอ่านไม่ออก  
Cryptanalysis: อ่านที่คนอื่นเขียนให้ออก (break) มีอยู่สองแบบคือ Cryptanalysis คือใช้ความรู้เกี่ยวกับอัลกอริทึมในการเข้ารหัสมาถอดรหัส  
Cryptosystem: คือระบบเข้า-ถอดรหัส 5 ส่วน (E, D, M, K, C) ดังนี้ M คือข้อความธรรมดา (plaintext) K คือชุดกุญแจ/คีย์ ที่ใช้เข้ารหัส, C คือชุดของข้อมูลที่เข้ารหัสแล้ว (ciphertext),E คือฟังก์ชันในการเข้ารหัส C = MxK, D คือฟังก์ชันในการถอดรหัส M = CxK  
**• Cryptanalysis type**  
**•Transposition Ciphers**  
**•Substitution Ciphers**  
**•Caesar cipher**   
**• Kasiski algoritm**  
**•One-Time Pad**  
**•Playfair Cipher**  
**•DES  
•Double DES  
•Tripple DES**  
**•Simplified DES or S-DES**  
**• AES**  
**•Other Symmetric Cryptography  
•Public Key Cryptography**  
**•RSA algorithm**  
**•Diffie Hellman**  
**• ECC  
• Combining Symmetric key and Asymmetric Key**  
**• MD5**  
**•SHA (Secure Hash Algorithm)  
•HMAC** Hash-based Message Authentication Code  
**•PGP** **pretty good privacy**

**•S/MIME Secure Multipurpose Internet Mail Extensions**   
**•Certificate Authority and Public Key Infrastructure**

**•PKCS Public Key Cryptography Standards**

ตัวอย่าง

**•Transposition Ciphers**  
HELLO WORLD HLOOL   
 ELWRD → HLOOLELWRD