古典密碼學 補充1

計網中心 網路與資訊安全組

李南逸

資料保護另一種分類方式

- 資料保護：

1. 密碼學(Cryptography)： Cryptography means secret writing. In cryptography, sender does not send message directly to the receiver, before sending information to the receiver information or plain text is converted into cipher text by using some encryption algorithm then send to the receiver and receiver decrypt the cipher text into plain text to read the original information.

2. 隱藏學(Steganography)：Steganography is a method in which secret message is hidden in a cover media. Steganography means covered writing (hidden writing).
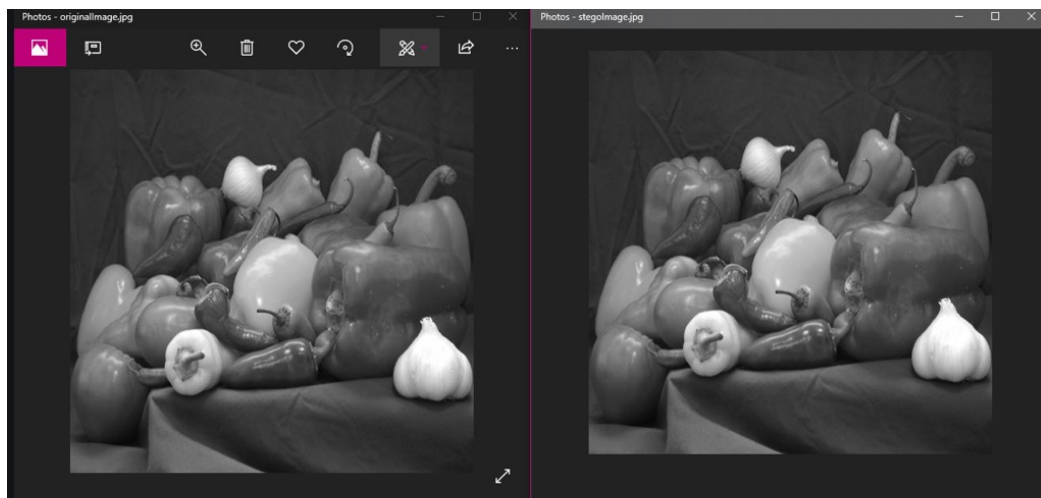
成功大學 NCKU
網路安全實驗室
Network Security LAB

Text and Image Steganography Samples

- Text Steganography

This book is mostly about cryptography, not steganography.

☐ ☐☐☐   ☐   ☐   ☐ ☐☐

0   1   0   0   0   0   1

- Image Steganography

ORIGINAL IMAGE   STEGO IMAGE

0101001**1**   1011110**0**   0101010**1**
0101111**0**   1011110**0**   0110010**1**
0111111**0**   0100101**0**   0001010**1**

Difference : Steganography and Cryptography

	Steganography	Cryptography
1.	Steganography means **covered writing.**	Cryptography means **secret writing.**
2.	Steganography is less popular than Cryptography.	While cryptography is more popular than Steganography.
3.	Attack's name in Steganography is **Steganalysis.**	While in cryptography, Attack's name is **Cryptanalysis.**
4.	In steganography, structure of data is not usually altered.	While in cryptography, structure of data is altered.
5.	Steganography supports **Confidentiality** and **Authentication** security principles.	While cryptography supports **Confidentiality** and **Authentication** security principles as well as **Data integrity** and **Non-repudiation**.
6.	In steganography, the fact that a secret communication is taking place is hidden.	While in cryptography only secret message is hidden.
7.	In steganography, not much mathematical transformations are involved.	Cryptography involves the use of number theory, mathematics etc. to modify data

作業1

- **請設計一套資訊隱藏技術**
  - **須包含藏入、取出機密訊息之過程或方式，以及範例**
  - **繳交**
    1. **Pdf檔案（可用手寫方式）**
    2. **兩週內繳交**
    3. **一人一組**