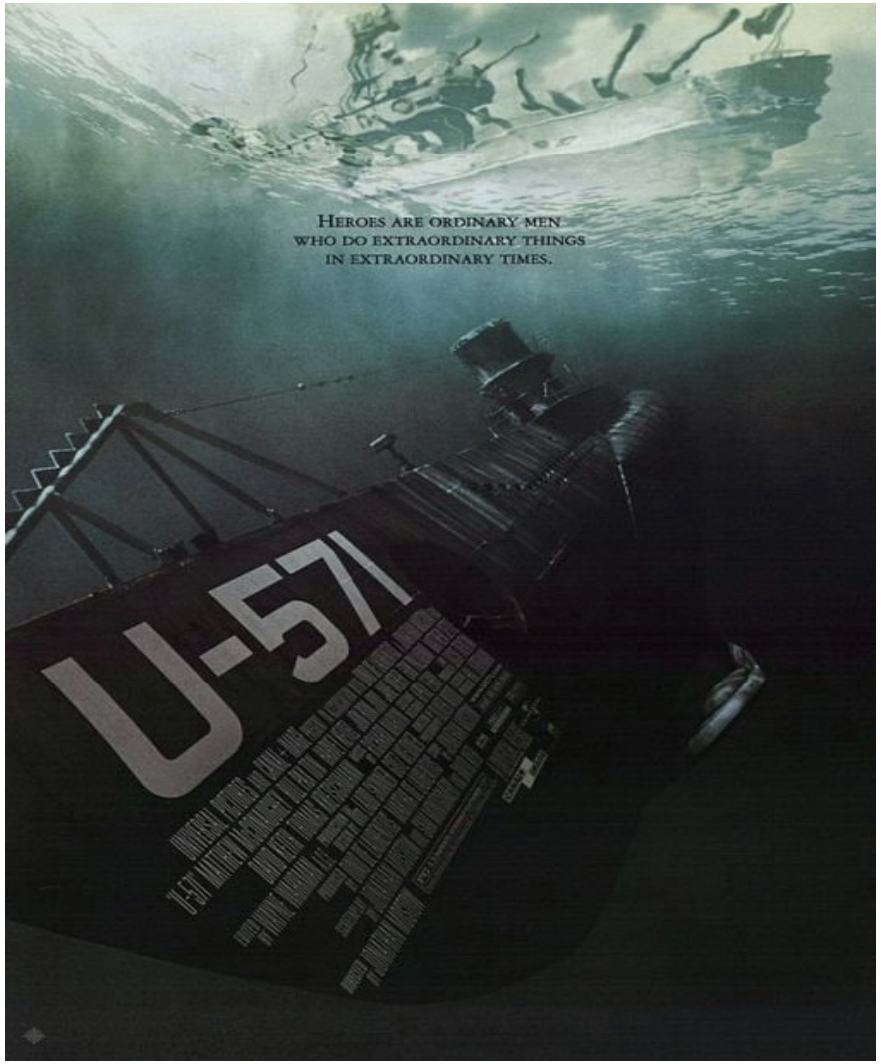
Introduction

- 第二次世界大戰的密碼戰爭
  - U-571
    - 1942年，美國與格陵蘭島海域
    - 德軍潛艦受創
    - 美軍S-33軍艦偽裝救援
    - 目的：取得德軍密碼機
    - 結果：扭轉二次大戰戰局



Introduction (Cont.)

- 攔截密碼戰 (Enigma [I'nIgmə])
  - 1943年，歐洲
  - 德軍密碼機 Enigma (謎)：利用轉輪及電流變化出數以兆計的鎖碼方式
  - 無預警重設定密碼，嚴重影響聯軍貨運隊的安危
  - 英國徵召數學家發明出類似大型電腦的計算機將可能性減少到只剩百萬種後，演算出解碼方程式，順利解得機密資訊

Introduction (Cont.)

- 德軍失敗的原因
  - 部份同盟國的Enigma密碼機解密人員被擄
  - 未對使用密碼人員作徹底調查
  - 對自己的密碼系統過於自信
- 你覺得自己的資料安全嗎?
- 你確定你上網購物的資訊不會被別人知道嗎?

Introduction (Cont.)

- 獵風行動 (Wind talkers)
  - 1944年，太平洋，賽班島
  - 美軍密電碼始終被日本破解
  - 美軍徵召印地安少數民族納瓦荷(Navajo Indians)人擔任通訊兵
  - 據查當時全球非納瓦荷族人且懂該民族語的僅28人，且均不在德國或日本等軸心國

Introduction (Cont.)

- 日本攻擊中途島失敗
  - 美軍破解機密資訊得知日軍攻擊計畫，但不知地點，僅知地點是“AF”
  - 美軍自中途島發出一段電文「***島上的海水過濾設備故障***」
  - 日軍截得後傳出電報「AF水源不足」
  - 美軍截得電報後得知 AF = 中途島
- ★小心★你的個人資訊不要被人套走了!!

Introduction (Cont.)

- 資訊隱藏技術 (Information hiding)
  - 王小明為了追求隔壁班阿花，於是出了個選擇題給阿花，題目是

    □愛情　□友情
  - 阿花只回送了一首詩

    願君多諒知識淺，選題未答繳白卷，

    愛莫能助實有愧，情願送詩供君覽。

Introduction (Cont.)

- 聖經真有密碼?
- 從聖經第一字母開始，找尋一種可能跳躍序列，從1、2、3個字母，依序到跳過數千個字母，看能拼出什麼字，然後再從第2個字母開始，周而復始。
- Rips ExplAineD thaT eacH codE is a Case Of adDing Every fourth or twelth or fiftieth to form a word
- READ THE CODE

Introduction (Cont.)

- 藏頭詩

七月初七情意綿，　七月秋涼情兩望，
夕風殘月人仰天。　夕燈早上人初妝。
佳期郎女快思訴，　佳成飛鵲快牽引，
節過今夕樂明年。　節慶年年樂四方。

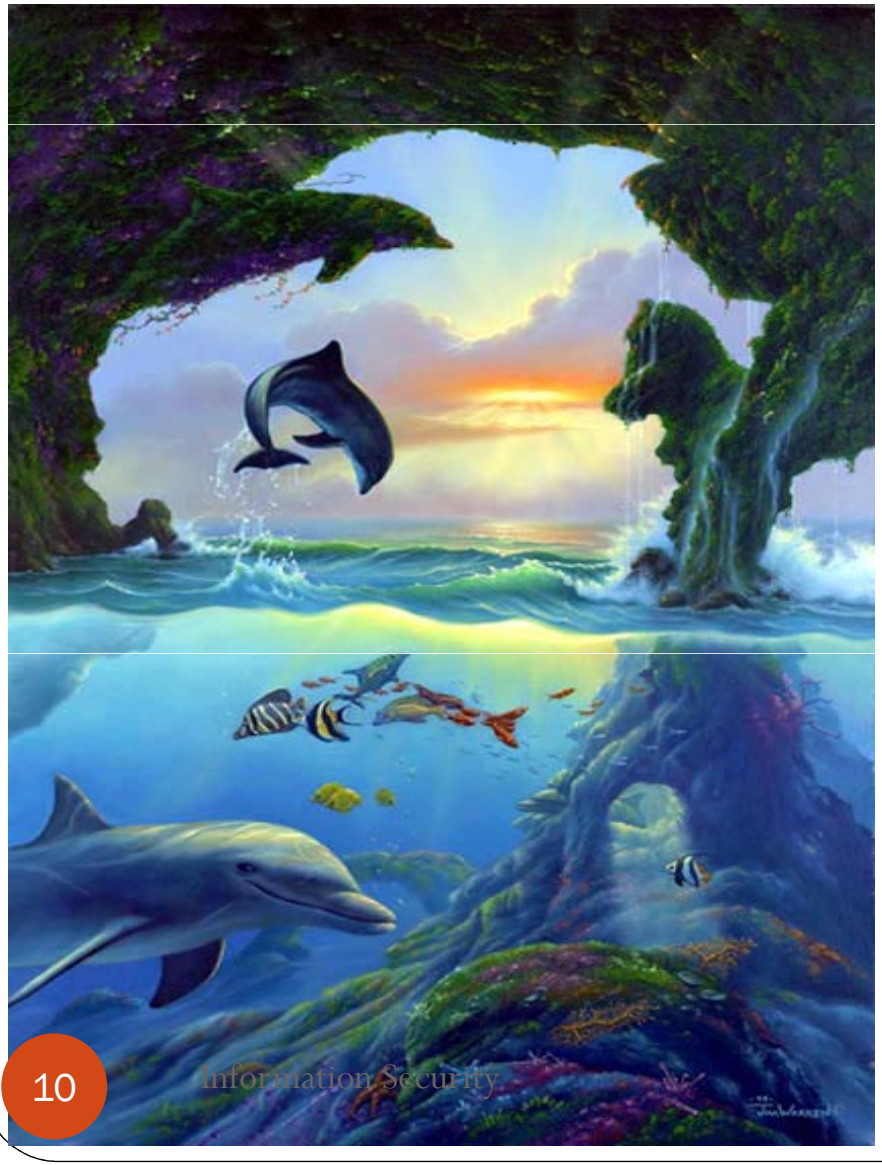
- 你知道下列數字要表達什麼嗎?
  - 345
    - *相思苦*
  - 1573
    - *一往情深*
  - 53406
    - *我想死妳了*
  - 0800-956-956
    - *恁別贏贏-救摸聊-救摸聊*

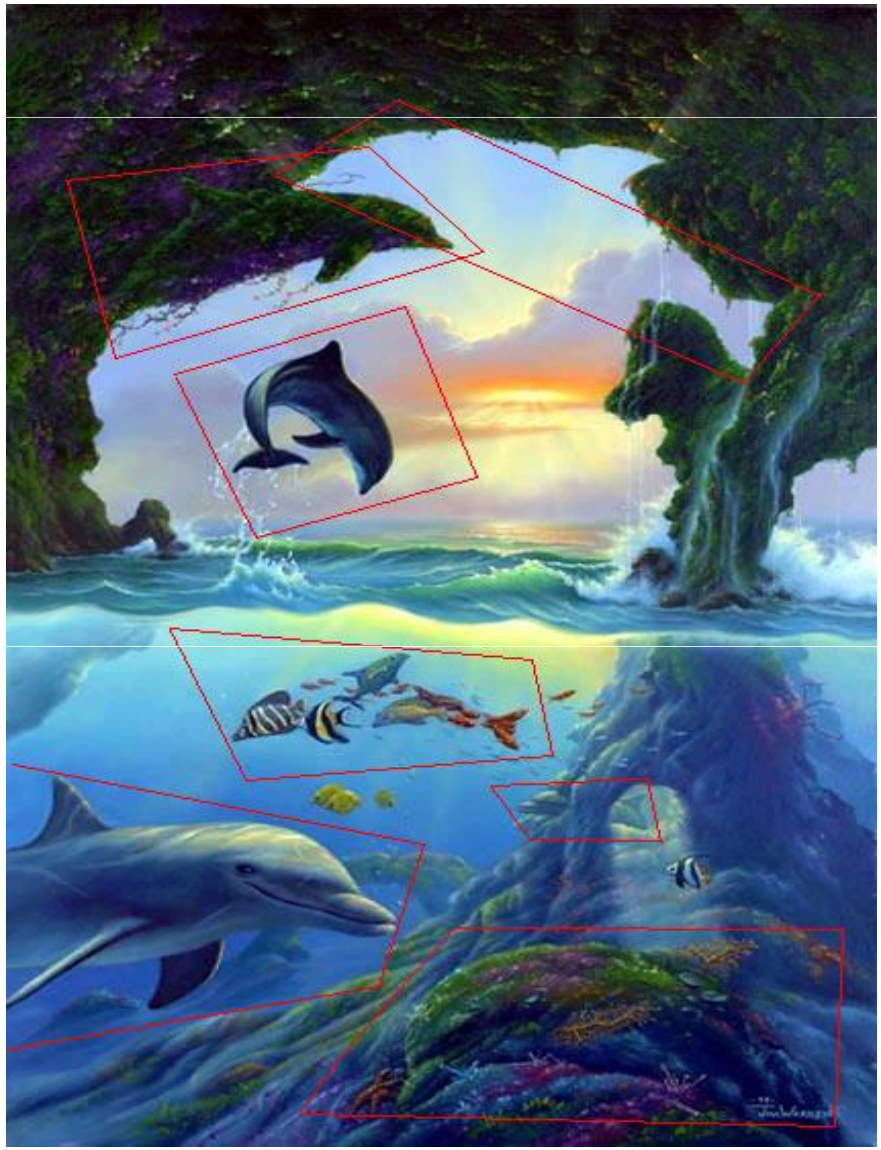
Introduction (Cont.)

- 你知道下列數字要表達什麼嗎?
  - 345
    - *相思苦*
  - 1573
    - *一往情深*
  - 53406
    - *我想死妳了*
  - 0800-956-956
    - *恁別贏贏-救摸聊-救摸聊*

Introduction (Cont.)

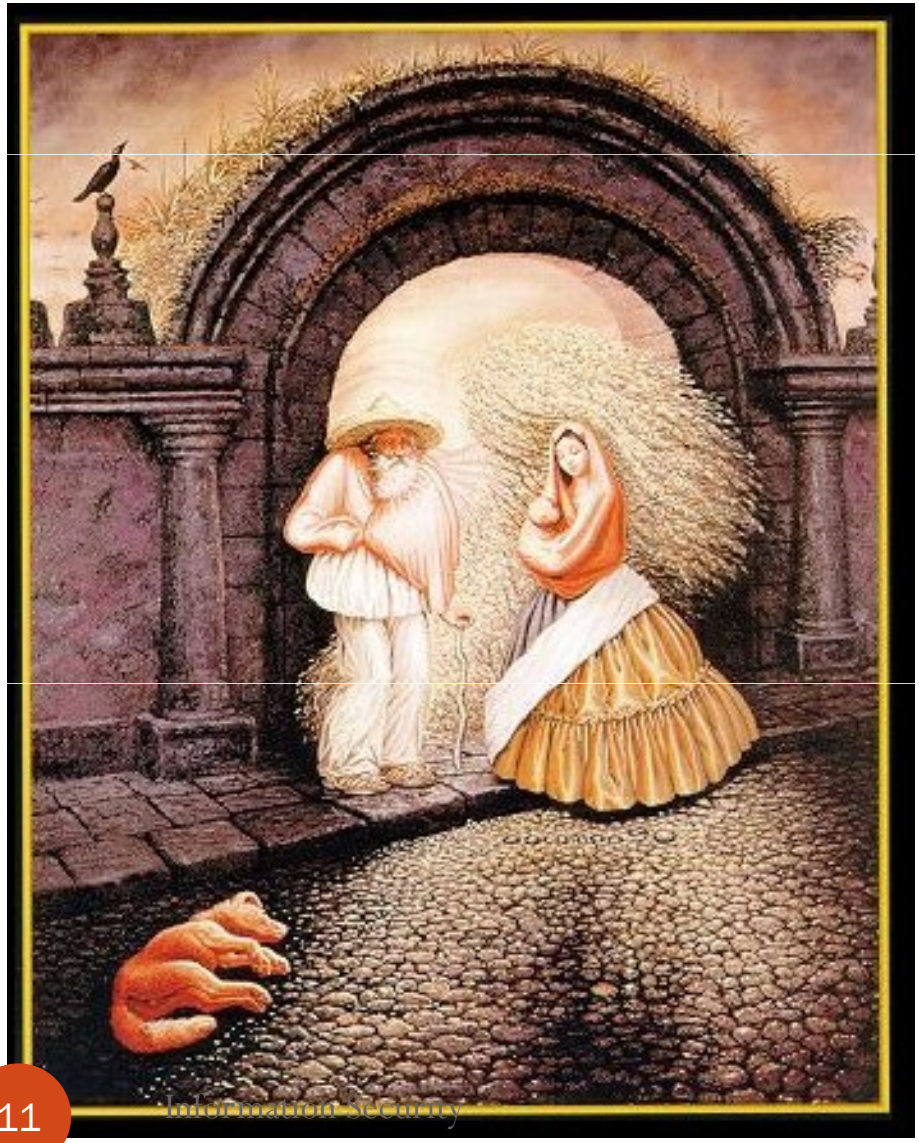
- 你的觀察力好不好?
  - ***海豚有幾隻?***

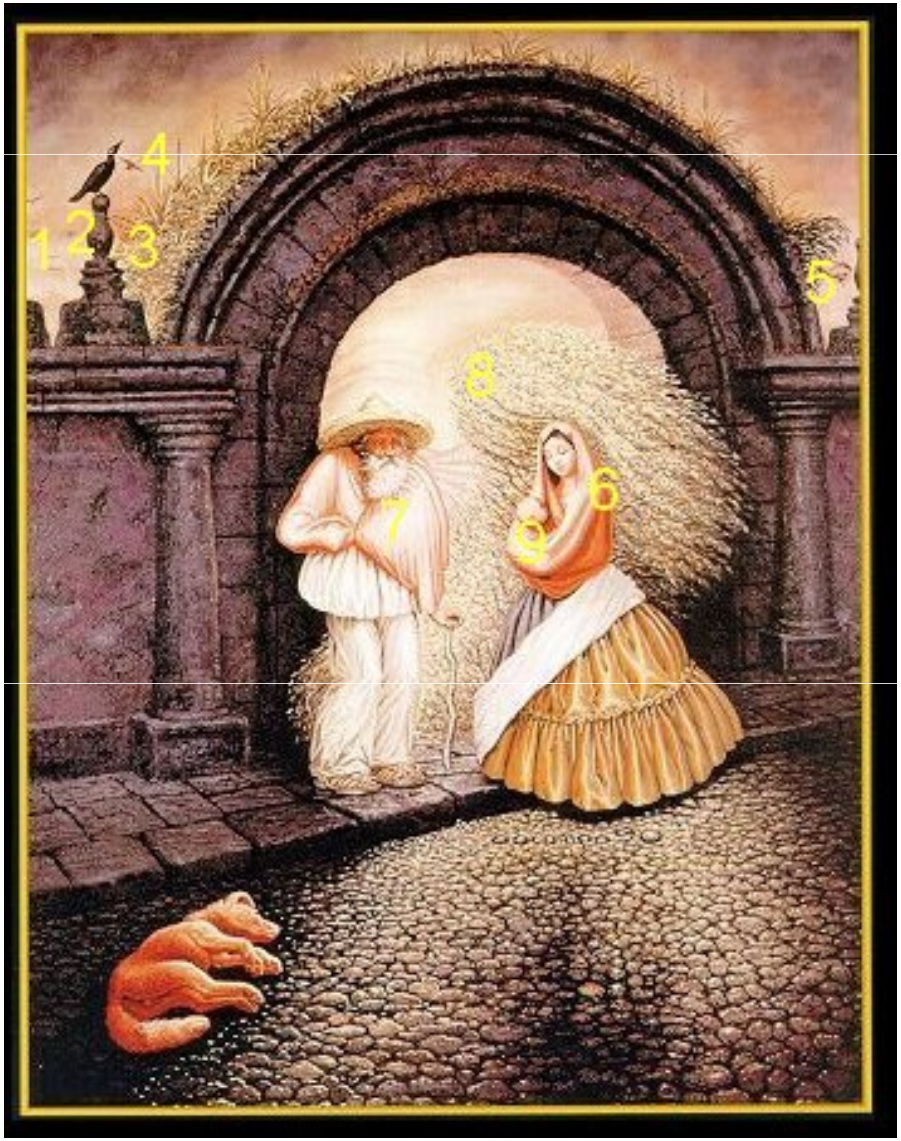




Introduction (Cont.)

- 圖中有幾個人?





Introduction (Cont.)

- 資訊安全說的就是密碼學嗎?
  - 資訊安全探討的範圍有
    - 機密資訊的傳遞
    - 電子商務安全
    - 網路安全
    - 多媒體安全
    - 系統安全
    - 資料加密
    - ...

Introduction (Cont.)

- 你的資料安全嗎?
  - 安全傳遞
    - 被動的unexpected user
      - 監看網路上傳遞的資訊
      - 嚐試非法讀取網路上傳遞的資訊
    - 主動的unexpected user
      - 試著去終止某使用者的資訊傳遞
      - 傳送假訊息

Introduction (Cont.)

- 如何反制Unexpected user
  - 將資料加密—Cryptography
  - 將資料藏起來傳送—Steganography
- Cryptography
  - 將資料以特殊方式予以打亂成無意思的內容，只有正確的接收者才能順利解出機密資訊
- Steganography
  - 將資料以藏入演算法嵌入到多媒體檔案中(e.g. 影像)，只有正確的使用者才能從該影像中取出機密資訊

Introduction (Cont.)

- Steganoraphy
  - 隱形墨水—鹽水
    - 用鹽水在紙上書寫
    - 乾了之後拿給接收方
    - 接收方用燭火烤出機密資訊

Introduction (Cont.)