資安入門?

CTF?

Capture The Flag

- Jeopardy
- King of The Hill
- Attack & Defense

類型

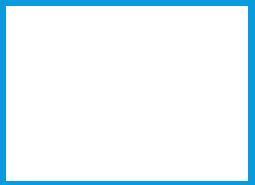
- Web 網頁
- Forensic 鑑識
- Crypto 密碼學
- Pwn 胖
- Reverse 逆向

基本能力

- Linux
- 打扣看扣(python,組合語言)
- Google!!!

CRYPTO 加密囉!!

- 古典 v.s. 現代
- 對稱 v.s. 不對稱
- 明文+(金鑰 or 操作)=密文
- 密文+(金鑰 or 操作)=明文
- cryptii.com



古典加密

- 替換式密碼
  - 凱薩加密
  - 維吉尼亞加密
  - Rot 13,47
- 圖案
  - 摩斯密碼
  - 點字
  - 奇怪代號

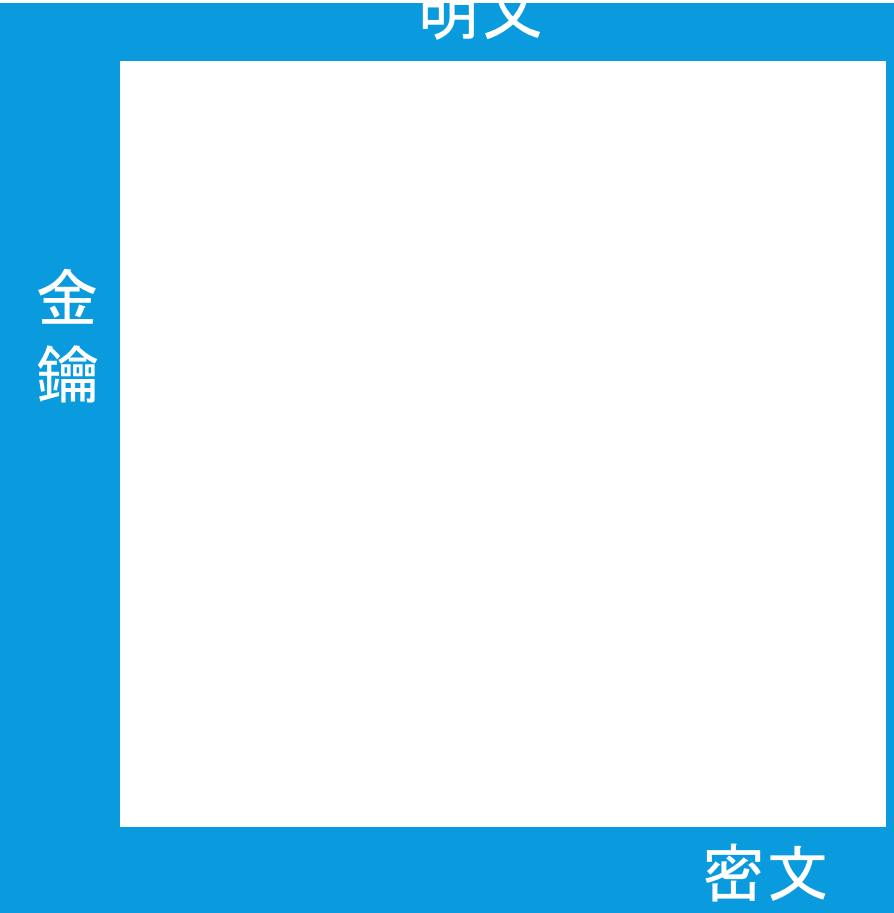
古典加密

- 其他的
  - 頻率分析 https://quipqiup.com/
  - 換位子
  - 找規律

凱薩加密

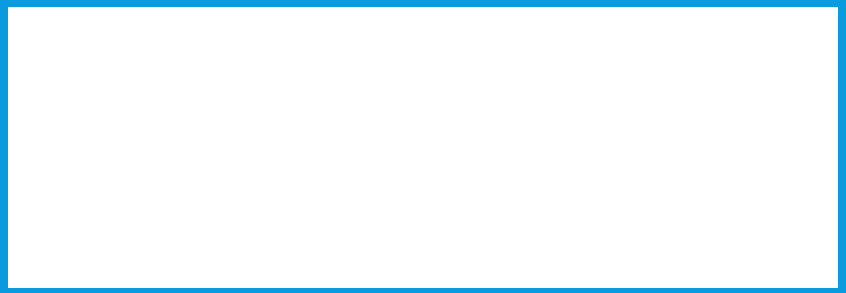
- 平移
- 範例　first +10 > psbcd
- 練習　olssvd dvysk

- 延伸版的凱薩加密
- 範例
  - 明文hate
  - 金鑰nope
  - 密文uoii
- 練習
  - 密文Kiywjsihrihzaf
  - 金鑰password



ROT 13

- Rot 13 : 26個英文字母 =13位的凱薩
- Rot 47 ?



圖案

- 摩斯密碼
- 點字
- 奇怪代號

頻率分析

- 可解決圖案、凱薩等
- https://quipqiup.com/
- 範例

eky tkyyufo wyuettkwqonef vnol cemrnuh qfi zqmwnyuh nh uqhg oe upwbqnf. olug'yu ove hniuh es olu hqmu tenf, qiiyuhhnfd eky sqhtnfqonef vnol hup, iuqol qfi seei. olug'yu reol kfiuqi, olug reol suui ef kh, olug reol wqhh ef hemu xnfi es wbqdku qfi olug tqf reol ru xnbbui vnol hwutnqbnho outlfnjkuh – q hoqxu olyekdl olu luqyo ey q inhumryqnfnfd. rko olug huum oe lqzu rutemu webqynhui. zqmwnyuh qyu olu kfiuqi es tlentu sey dnybh, qfi cemrnuh sey regh. zqmwnyuh qyu teeb, qbees, ruqkonskb, ryeeinfd tyuqokyuh es olu fndlo. ogwntqb meeig ouufqdu regh, rqhntqbbg. cemrnuh qyu ikmr, rykoqb, kdbg qfi mnfibuhhbg znebufo. vlntl mqxuh olum qbhe bnxu ogwntqb ouufqdu regh, n hkwwehu.

換位子

- 寫著倒子句把
- 亂全把部用
- 或格方你出

  是子式看來

  用的讓不喔

找規律

- 字面上的意思
- 範例
  - 1 : duhrw
  - 2 : esl ov
  - 3 : f qpl u
  - 4 : ? ? ?