CNS Homework 1

資工三 b05902058 陳竣宇

1. CIA

- Confidentiality
  - 保密性: 機密資訊不可暴露在未經授權的主體之下，主體可以是一個人、一個團體或一套系統
  - 破解password從而讀取或使用機密資料
- Integrity
  - 完整性: 對於機密資訊的改動都必須是經過授權且無竄改情事的，主要目的就是維持資料的真實、一致性
  - 竄改他人的對話內容或是刪除機密檔案等
- Availability
  - 已授權主體可以及時、不受中斷的存取或使用資訊
  - DDoS attack: 用大量的zombie向攻擊目標發送大量網路請求使目標伺服器癱瘓

2. Hash Function

- One-wayness
  - 在給定hash值 y 的情況下很難找到原訊息 x 使得 $y = H(x)$
  - Password hashing: 將password以經過hash的方式儲存，當資料洩漏時，攻擊者很難以現有的hash推回原本的password
- Weak collision resistance
  - 在給定原訊息 x 的情況下很難找到另一個訊息 x' 使得 $H(x) = H(x')$
  - Password hashing: 因為database方是以hash的方式儲存，因此當given x(先前提供之原始密碼)的條件下攻擊者若能有效率地解出 x' 使得 $H(x') = H(x)$，就能夠用 x' 通過系統認證
- Strong collision resistance
  - 很難找到兩個不同的訊息 $x \ and \ x'$ 使得 $H(x) = H(x')$
  - 在一個很大的database查詢資料時，可以以計算query之hash值的方式來避免資料量太大導致拖慢速度。而這個機制需要確保對於任意兩個不同的dataset他們的hash值不相同

4. Babe crypto

```
BALSN{CRYPT0_1S_3ASY_XDD}
```

- Round1
  - Caesar cipher
- Round2
  - Vigenère cipher
- Round3
  - Rail fence cipher
- Round4
  - Base64 encoding

5. OTP

5-1

```
BALSN{7ime_Se3d_Cr4ck!n9}
```

- 因為使用time.time()當作random seed，所以暴搜random seed，用密文和其產生的random number做xor就能得到flag

5-2

```
BALSN{Tria1_4nd_3rr0r_And_Tri@l_AnD_Get_Fla9<3!}
```

- keys是使用 secret.seed當作random seed，所以可以知道產生的64把key都相同
- 找65組不同的cipher並同時call random.seed(time.time()) 取得其key_index
- 找出一組奇數dependent(key_indices 互相 xor = 0)的組合並在同一時間xor對應的cipher就能取得flag

6. MD5 Collision

```
BALSN{MD5_Ch3cK5Um_!5_Br0k3N}
```

- https://github.com/thereal1024/python-md5-collision (https://github.com/thereal1024/python-md5-collision)
- 把連結中的repository clone下來之後將gen_coll_python.py這個檔案的部分內容更改並執行後取得2個base64-encoded code。
- nc後把他們複製貼上就可取得flag。

1. **code1**:
   IyEvdXNyL2Jpbi9lbnYgcHl0aG9uMgojIC0qLSBjb2Rpbmc6IHV0Zi04IC0qLQojICAgICAKZGlmZiA9ICcnJzCvUHMoDbq43WODgw2hkBaw1gLMvZKeBmUiOcb1TcKz4AsN4stC975r2tABJQguk9esaXqkJdVkPb/ZX+OWCK6pWhAJEOSvoeEHTJQa9t39jlDVNjPqwDsIqd2FzKjd7RVvP8JOFc/HYlIBsopcrlwF/aIZerazz7NXeXIh8xF+JycnCnNhbWUgPSAnJycwr1BzKA26uN1jg4MNoZAWsNYCzL2SngZlIjnG9U3Cs+ALDeLLQve+a9rQASUILpPXrGl6pCXVZD2/2V/jlgiuqV

oQCRDkr6HhB0yUGvbd/Y5Q1TYz6sA7CKndhcyo3e0Vbz/CThXPx2JSAbKKXK5cBf2iGXq2s8+zV3lyIfMRficnJwoKaWYgKHNhbWUgPT0gZGlmZik6CiAgICBwcmludCAnTUQ1IGlzIHNlY3VyZSEnCgplbHNlOgogICAgcHJpbnQgJ0p1c3Qga2lkZGluZyEnCgo=

2. **code2**:
lyEvdXNyL2Jpbi9lbnYgcHl0aG9uMgojIC0qLSBjb2Rpbmc6IHV0Zi04IC0qLQojICAgICAKZGlmZiA9ICcnJzCvUHMoDbq43WODgw2hkBaw1gJMvZKeBmUiOcb1TcKz4AsN4stC975r2tABJYguk9esaXqkJdVkPb/Z3+OWCK6pWhAJEOSvoeEHTJQa9t39jlDVtjPqwDsIqd2FzKjd7RVvP8JOFc/HYlIBsorcrVwF/aIZerazz7NXeflh8xF+JycnCnNhbWUgPSAnJycwr1BzKA26uN1jg4MNoZAWsNYCzL2SngZlIjnG9U3Cs+ALDeLLQve+a9rQASUILpPXrGl6pCXVZD2/2V/jlgiuqVoQCRDkr6HhB0yUGvbd/Y5Q1TYz6sA7CKndhcyo3e0Vbz/CThXPx2JSAbKKXK5cBf2iGXq2s8+zV3lyIfMRficnJwoKaWYgKHNhbWUgPT0gZGlmZik6CiAgICBwcmludCAnTUQ1IGlzIHNlY3VyZSEnCgplbHNlOgogICAgcHJpbnQgJ0p1c3Qga2lkZGluZyEnCgo=

Bonus

```
BALSN{Ex3cUTe_uNtrU5t3d_C0d3_15_V3rY_d4nG3R0uS}
```

- 因為server會在程式中去執行我們所傳入的code，因此傳入glob.glob()即可印出當前目錄的所有檔案路徑列表
- 在 `home/md5/` 之中發現名為 `b0nU5_FL4g_Y0U_F0unD_m3` 的檔案，因此傳入開檔與讀檔的code之後取得flag

7. Flag Market

```
BALSN{L3ngTh_3xeT3n5i0N_4tTacK_i5_34sY_w1tH_H4shPump}
```

- 使用 `HashPump` 實作length extension attack
- extension data = “&BALSN_Coin=1000”
- 暴搜key length，讓extent之後的字串經過sha256之後和原本輸入規定範圍的coin數的hash值相同，通過條件判斷之後取得flag

Bonus

```
BALSN{PyTh0n_F0rM4t_5trInG_C4n_B3_daNG3rOuS}
```

- `.__doc__` 能夠取得module, method...開頭注釋內容
- `dir('')` 能夠取得當前範圍的所有module, method...
- 使用 `0.{attribute}.__doc__[i]` 經過 `.format('')` 會轉成文件裡的character
- 暴搜 `dir('')` 找出符合source code要求的character並且字數最少，把extension data改為"&BALSN_Coin=2147483648&hidden_flag="，後面加上之前找出的結果send後取得flag
- 因為python2和python3的 `.__doc__` 內容不同，因此我是在python2找出結果後放到原本的python3 code執行

8. RSA

```
BALSN{Therefore_We_5hould_Not_Choose_4_5mall_Public_Key...}
```

- Håstad's broadcast attack
- 使用 `gmpy2` 計算CRT、開方
- 因為 e 恆等於3，因此使用中國剩餘定理可以得知 $m^3\ mod\ (n1 * n2 * n3) = C$，因為 $m^3 < (n1 * n2 * n3)$，因此把 C 開3方就可以得到明文 $m(flag)$

9. The Backdoor of Diffie-Hellman

```
BALSN{black magic number}
```

- $g_{backdoor}^{691829} = g_{old}^{p-1} \equiv 1 \pmod{p}$
- 因為範圍確定，因此可以暴搜 a, b
- 使用 `pycrypto` 計算 $(g^{ab})^{-1}$，乘上cipher後便可轉換出flag