HW1

2021年3月20日　　上午 10:44

1.CIA

Confidentiality：確保傳輸的機密資訊不被未授權者讀取或揭露

例： CD Project 開發的遊戲 Cyberpunk 2077 原始碼被竊取違反了 Confidentiality

integrity ：確保機密資訊不備未授權者竄改

例：美國淨水廠系統遭駭客入侵，差點將強鹼濃度提升100倍，違反了 Integrity

Availability：確保機密資訊隨使可以被讀取或被使用

例： DDoS 攻擊可以讓特定服務被阻斷，違反了 Availability

2.Hash Function

One-wayness：給定 y，很難找到 x 使得 y = H(x)

例：Password Hashing

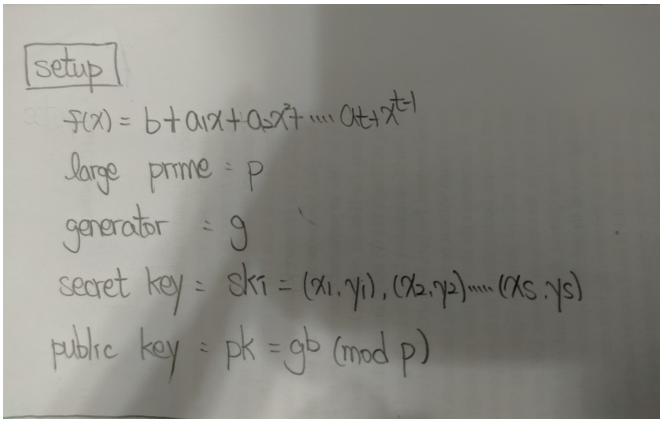
Weak collision resistance： 給定 x ，很難找到另外一個值 y 使得 H(x) = H(y)

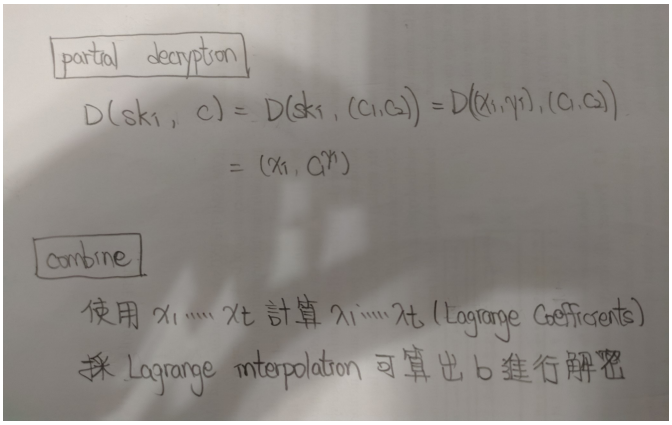
例：透過 MD5 驗證下載的資料是否損壞

Strong collision resistance：沒有任何一對輸入具有相同的 Hash 值

例：數位簽章

3.Elgamal Scheme

1. Bob 透過 Authenticated channel 將公鑰(g^b)傳送給 Alice ， 此時 Alice 可用 Bob 的公鑰對任意訊息進行加密，加密任意訊息後回傳(c1 = g^a)給 Bob ，在一來一往之中雙方有了 Shared Secret (g^ab) 可以做為 Symmetric Key
2. 



4.Simple Crypto

執行 Problem4/code4.py, Round 1 凱薩密碼的部分需要手動挑選解答，若挑選無誤可以順利推進 ， 在測試的時候 Round 2 的 Padding 有機會會出現 key 與 cipher Byte 數不相同情況，不過機率很低，大多數還是能夠獲得 Flag

```
Congratulations!
Here is the flag:
CNS{ClA331CAl_CRYPT0_1S_3ASY_XDD}
```

5.RSA

執行 Problem5/code5.py

Flag 1 直接開三次根可得

Flag 2 取多組記錄下來跑中國餘數定理可得

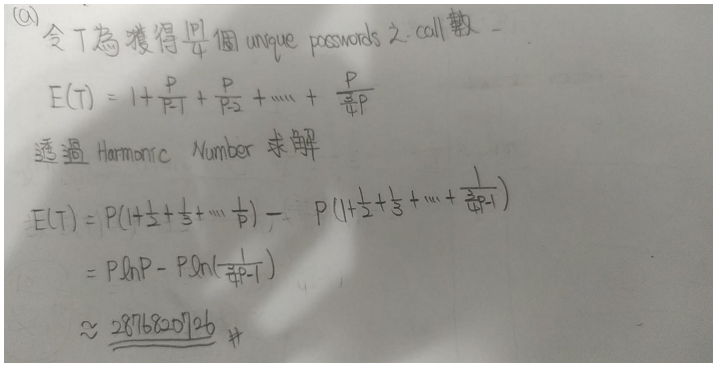
Flag 3 透過第一個 Input 把 N Try 出來，紀錄多組後跑中國餘數定理

FLAG 4 放棄

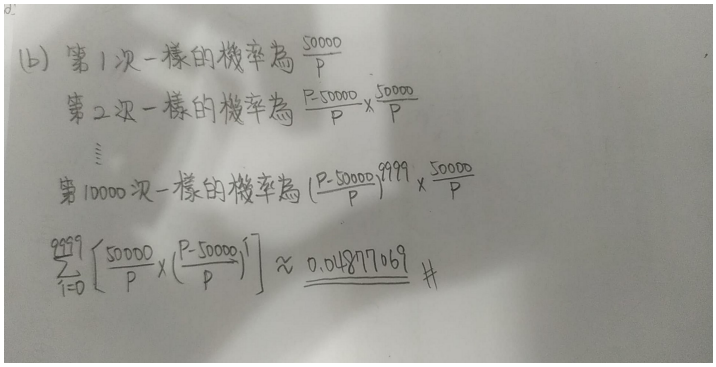
```
CNS{d1rect_cu6e_r00t}
CNS{Ch1nese_remaind3r_Theorem_1s_helpfu11111!!!!!}
CNS{NOw_y0u_kNOw_Never_use_sma11_YEEEEEEEEE_again}
```

6.Rainbow Table

1.



2.



3.放棄

7.Padding Oracle

執行 Problem 7/code7.py 即可，由於 padding attack 比較耗時，程式裡面直接將我跑完的中間值記錄下來，若要測試的話可以呼叫 padding_attack(cipher_3,cipher_1) 取得 IV

取得IV

將 id = i_am_the_??|| 輸入到 Server 的加密 Function 中，取得密文串 C1，並分割為五段 C1_1,C1_2,C1_3,C1_4,C1_5，接著將 C1_1 + C1_2 + C1_3 + C1_1 串接輸入到解密 Function 中，並進行 Padding Oracle Attack 將解密後的中間值 X 取出，最後將中間值 X xor C1_1 xor P1(id=i_am_the_??||) 可得 IV

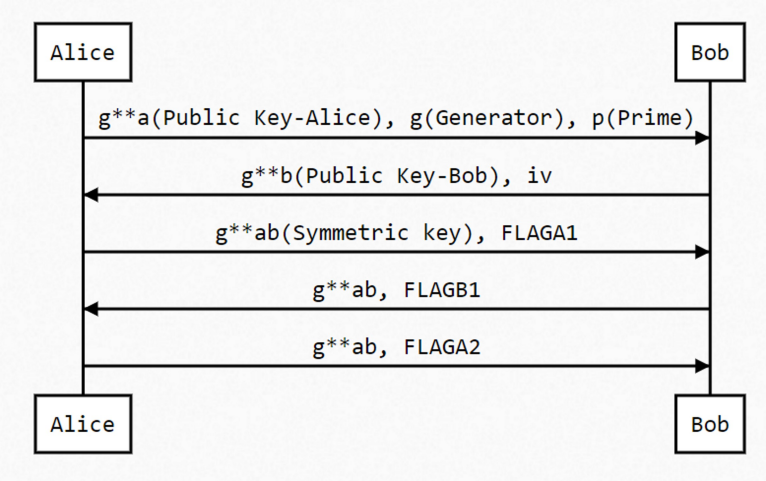
構造密文

將 C1_3 xor (id = i_am_the_ta||) xor IV 輸入至加密 Function 中，取輸出的前16個Bytes構造出的第一段構造密文 CC1，接著再將 C1_3 xor (act=printtheflag) xor CC1 輸入至加密 Function 中，取得第二段構造密文 CC2 ，即可更新權限取得 Flag

```
CNS{(=^.x.^=)W15H Y0U H4V3 FUN}
```

8.Secret Exchange

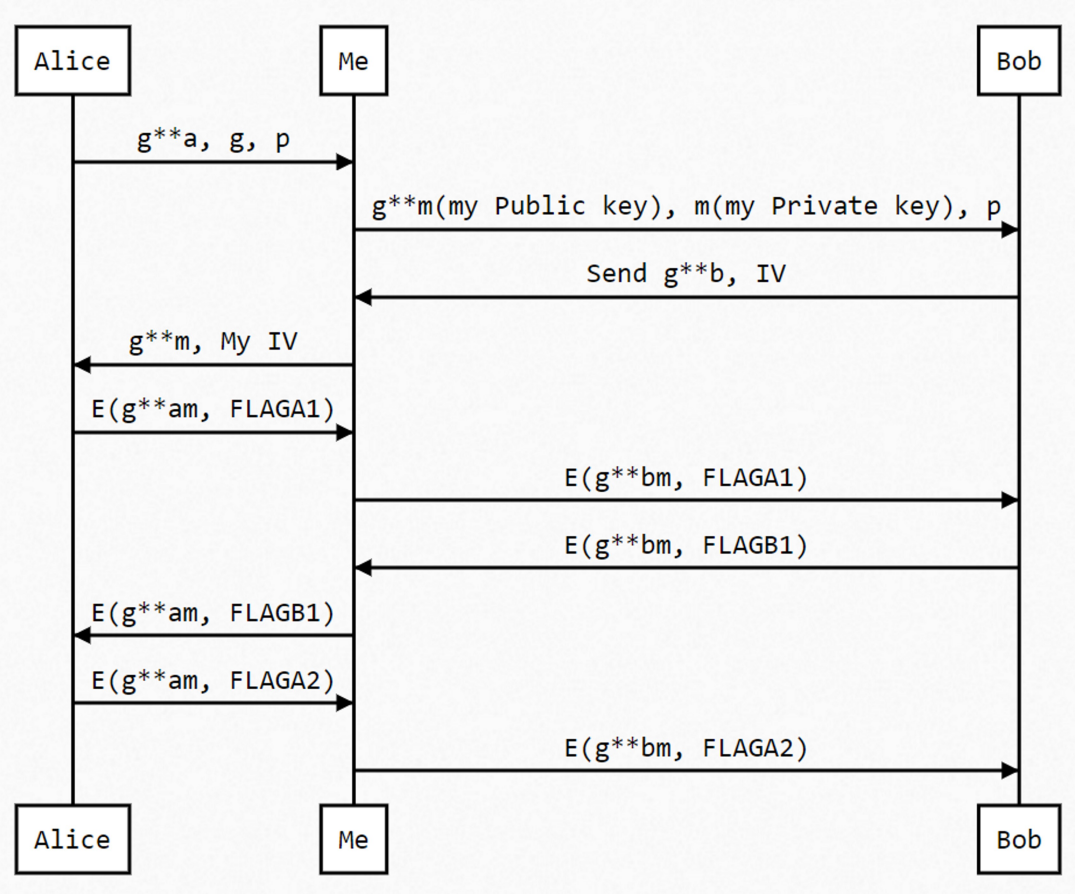
(A) 1.



2.

CNS{this_is_called_man_in_the_middle_attack.&_&}

3.



(b) 放棄