B04902103 資工四 蔡昀達

HW1

1. CIA
   - Condentiality: 機密性，是指個人或團體的訊息不為其他不應獲得者獲得。
     例如: 避免訊息被竊聽或偷窺。
   - Integrity: 真實性、完整性，確保信息或不被未授權的篡改。
     例如: 保護訊息在傳輸時被竄改。
   - Availability: 可用性，保證合法使用者對資訊和資源的使用不會被不正當地拒絕。
     例如: DDOS 是癱瘓 availability 的方式。

2. Hash Function
   - one-wayness: 無法以 hash value 找回原本的 x
     例如: password hashing 需要 one-wayness 避免被攻擊者還原明碼。
   - weak collision resistance: 給定 x，無法找到 hash value 一樣的 x'
     例如: checksum 可以利用 hash 確保下載檔案完整性。
   - strong collision resistance: 找到任一兩個(x, x') ，有同樣的 hash value
     例如: 不可否認性需要 strong collision resistance 讓承諾方不可更改承諾。

3. Threshold Signature
   Assume a single sinature S is enough to verify k given signatures S_i :
   $e(S, g) = e(\prod^k S_i, g) = e(\prod^k h^{ski}, g) = \prod^k e(h, g)^{ski} = \prod^k e(h, g^{ski}) = \prod^k e(h, PK_i)$
   Each individuals instead if publish $PK_i = g^{ski}$, publish $pk_i = g^r * pk_i^{-1}$
   Now thay can claim both signed the messages by $S = h^r$

4. Babe crypto :
   Flag : BALSN{CRYPT0_1S_3ASY_XDD}
   R1: caesar cipher
   R2: 字元相減發現規律
   R3: rail fence cipher
   R4: base64

5. OTP
   1. Flag : BALSN{7ime_Se3d_Cr4ck!n9}
      random seed 由 time.time() 轉成 int，在 local 同步計算將會得到同樣的結果，因此可以計算 key 並解密。
   2. 略

6. MD5 Collision :

Flag : BALSN{MD5_Ch3cK5Um_!5_Br0k3N}

利用 identical prefix attack 製造 md5 collision，使兩個不同的檔案 md5 相同。

Hidden : BALSN{Ex3cUTe_uNtrU5t3d_C0d3_15_V3rY_d4nG3R0uS}

利用沙盒執行程式碼並輸出結果的方式，讀取執行環境的檔案目錄，找到/home/md5 底下的檔案，可以找到 hidden flag。

Code1 =

'IyEvdXNyL2Jpbi9lbnYgcHl0aG9uMgojIC0qLSBjb2Rpbmc6IHV0Zi04IC0qLQojICAgICAKZGlmZiA9ICcnJ93
ULqypo+Pxng3Vf2HbiE3BxmRabVkIoDT2OZ7oJRHN98Pu57xM15RnBtj0MzCWbIQhrX4OQFXaAWyKYE
rBwoN3FoLvZuZzLSVDPpVCzCPAEZQ/UzzfwsiLxTD/h1+I5tOrQgSnxBEWegJOfIXY/NlJsNTczsycRX7gF7rY
lT6zJycnCnNhbWUgPSAnJyfd1C6sqaPj8Z4N1X9h24hNwcZkWm1ZCKA09jme6CURzffD7ue8TNeUZwbY
9DMwlmyEIa1+DkBV2gFsimBKwcKDdxaC72bmcy0lQz6VQswjwBGUP1M838LIi8Uw/4dfiObTq0IEp8QR
FnoCTnyF2PzZSbDU3M7MnEV+4Be62JU+sycnJwoKaWYgKHNhbWUgPT0gZGlmZik6CiAgICBwcmludCA
iTUQ1IGlzIHNlY3VyZSEiCgplbHNlOgogICAgcHJpbnQgIkp1c3Qga2lkZGluZyEiCgo='

Code2 =

'IyEvdXNyL2Jpbi9lbnYgcHl0aG9uMgojIC0qLSBjb2Rpbmc6IHV0Zi04IC0qLQojICAgICAKZGlmZiA9ICcnJ93
ULqypo+Pxng3Vf2HbiE3BxmTabVkIoDT2OZ7oJRHN98Pu57xM15RnBtj0M7CWbIQhrX4OQFXaAWyK4E
rBwoN3FoLvZuZzLSVDPpVCzCPAEZQ/0zzfwsiLxTD/h1+I5tOrQgSnxBEWegJOfIVY/NlJsNTczsycRX7gFzrY
lT6zJycnCnNhbWUgPSAnJyfd1C6sqaPj8Z4N1X9h24hNwcZkWm1ZCKA09jme6CURzffD7ue8TNeUZwbY
9DMwlmyEIa1+DkBV2gFsimBKwcKDdxaC72bmcy0lQz6VQswjwBGUP1M838LIi8Uw/4dfiObTq0IEp8QR
FnoCTnyF2PzZSbDU3M7MnEV+4Be62JU+sycnJwoKaWYgKHNhbWUgPT0gZGlmZik6CiAgICBwcmludCA
iTUQ1IGlzIHNlY3VyZSEiCgplbHNlOgogICAgcHJpbnQgIkp1c3Qga2lkZGluZyEiCgo='

7. Flag Market :

Flag : BALSN{L3ngTh_3xeT3n5i0N_4tTacK_i5_34sY_w1tH_H4shPump}

利用 length extension attack 偽造合法 sha256 的 token，添加重複的&BLASN_coin 可以成功注入錯誤的錢幣數量。

Hidden : BALSN{PyTh0n_F0rM4t_5trInG_C4n_B3_daNG3rOuS}

利用 python string format 的漏洞，可以呼叫 str.attributes，並藉此呼叫__doc__，從中拼湊符合的字串。

8. RSA :

Flag : BALSN{Therefore_We_5hould_Not_Choose_4_5mall_Public_Key...}

因為是很小的 exponent 因此利用 Håstad's Broadcast Attack，就可以反解得到密文。

9. Backdoor of Diffie Hellman：

Flag : BALSN{black magic number}

根據費馬小定理和提示，$g_{old}^{p-1} \bmod p \equiv g_{backdoor}^{691829} \bmod p \equiv 1$，由此可知 $g_{backdoor}$ 是比較小的 group，可以暴力搜尋 $a, b \in [0, 691829)$ 使得 $A = g_{backdoor}^{a} \bmod p$ 且 $B = g_{backdoor}^{b} \bmod p$。