CNS Homework1

姓名: 徐有慶
學號: r05922162

Handwriting:

1. CIA

Confidentiality:

是在防止沒有經過授權的披露，除了交談的雙方外，沒有第三人能知道交談的內容。如: Alice 寄一封郵件給 Bob，除了這兩個人之外，沒有第三者能夠知道郵件內容。

Integrity:

保證傳遞的訊息是完整的，除了交談的雙方外，沒有第三人能夠改動訊息的內容。如: Alice 約 Bob 今晚六點吃飯，要確保訊息到 Bob 手中時是 Alice 約他今晚六點吃飯，而不會變今晚五點吃飯之類的。

Availability:

確保預期的用戶能夠使用服務。如: 我今天要連上一個網站，若有人惡意攻擊那個網站，讓我連不上他，這樣就違反了 Availability。

2. Hash Function

假設 hash function 為 H

One-wayness:

Given y, hard to find x s.t. y = H(x)。如: 假設有個廚師，給他一樣的食譜，他都可以做出味道一模一樣的菜，今天他為你炒好一盤菜，你很難知道他的食譜是甚麼，加了多少鹽、多少醬油之類的。

Weak collision resistance:

Given x, hard to find x' ≠ x s.t. H(x) = H(x')。如: 給你一個食譜，你很難找到另一個食譜，可以讓這廚師炒出一樣的味道。

String collision resistance:

Hard to find x and x' s.t. x' ≠ x and H(x) = H(x')。如: 你很難找到不同的食譜，炒出來的菜味道卻一樣。

3. Symmetric Cryptography with KDC

(a) (5%) What's the purpose of *NA* and *NB* in this protocol? (Imagine if the protocol doesn't use nonce, what kind of the attack would become possible?)

Nonce 的目的在於防止 replay attack。同老師在課堂上所提到的，如果攻擊者有幸可能獲得 A 跟 B 之間的 shared secret key S，就可以扮演 KDC，發給 A 之前發送過的 $E_{K_{SA}}(K_S||ID_B||N_1||E_{K_{SB}}(K_S||ID_A))$，而 A 就和 B 就會使用攻擊者知道的 shared secret key S 來做通訊。

(b) (5%) How can an attacker break the goal of the protocol?

KDC 會為兩個 legal users A、B 建立一個 shared secret key S，若今天 B 畢業了，但 A 不知道，因為在 B 畢業前，他們就有一個 shared secret key S，所以 A 和 B 之間還是可以做通訊，且 A 始終認為 B 是 legal user。這就打破了 Eric 想達到的第二點 A can be assured that B is legal。

(c) (5%) Try to fix the protocol to prevent the attacker you described above. Please explain clearly.

Shared secret key 要有一個時效性，通訊的雙方，每過一段時間就要請 KDC 重新產生一組 shared secret key。

Capture The Flag

4. Classical Cipher

Flag:

BALSN{C14$5ic41_c!ph3r_1$_r34lly_cl455ic41}

Round1:

Caesar Cipher，計算 offset 後即可解碼。

Round2:

暴力破解，計算 offset 1-25 解碼後得到的明文，找出最像英文句子的明文。

Round3:

找出 offset 的規律，發現每個位置的 offset 會遞增，假設第 1 個位置的 offset 為 3，則第 2 個位置的 offset 即為 4，以此類推。

Round4:

找出 offset 的規律，發現 offset 為一串會循環的值，假設 offset 每兩次會一循環，若第 1 個位置的 offset 為 5，第 2 個位置的 offset 為 15，則第 3 個位置 offset 也為 5，第 4 個位置 offset 為 15，以此類推。

Round5:

和 offset 無關，和字的位置有關，m1 = [a-z][A-Z]，若 a = m1[0] = c1[13]，則 x = c2[13] = m2[0]，以此類推。

Round6:

類似 Columnar Cipher，只是都是由 column1 開始轉換成 cipher，由 key length = 2 開始解碼 c1，若解不回 m1，則 key length 加 1，直到解回 m1，並記錄 key length，便可解碼 c2。

Round7:

Base64 編碼，解碼回去即可。

5. Google can beat this

Flag: BALSN{D0NT_7RU57_SHA1_N0W}

參考: https://shattered.io/static/shattered.pdf

可以得知

$$\text{SHA-1}\left(P\|M_1^{(1)}\|M_2^{(1)}\|S\right) = \text{SHA-1}\left(P\|M_1^{(2)}\|M_2^{(2)}\|S\right).$$

利用裡面提供的 P，$M_1^{(1)}$，$M_1^{(1)}$，$M_2^{(1)}$，$M_1^{(2)}$，$M_1^{(2)}$，暴力去試出 S 找出 x 符合最右邊 24bits 與題目要求的相同，同時也可以得到 y 使得 Sha1(x) == Sha1(y)。S 的找法從 0x0，0x1，0x2…開始以此類推，直到找到一個數值符合題目要求，因為並不是每次都能在 2 分鐘內找到，所以會記錄這次所試過的值及做完 Sha1 後產生的數值，存成”hex.txt”，下一次先從”hex.txt”中搜尋，若沒有找到才繼續暴力搜尋 S。

6. Many-time pad

Flag: BALSN{using a key one time is not enough, have you tried using it twice?}

參考: http://crypto.stackexchange.com/questions/6020/many-time-pad-attack/6095#6095

message ⊕ key = cipher text

c1 ⊕ c2 = m1 ⊕ key ⊕ m2 ⊕ key = m1 ⊕ m2

由參考網頁得知，" " ⊕ [a-zA-z] = [A-Za-z]。

Step1.
c1 和其他 c2 ~ c10 做 xor 得到 xi，i = 0…8，c2 對應到 x0，以此類推。若 xi 第 3 個位置皆為字母，則假設 m1 第 3 個位置為 space，並將其餘 m2 ~ m10 第 3 個位置的字母設為 xi 第 3 個位置的字母的大小寫相反字母；假設 x0[2] = a 則 m2[2] = A。

Step2.
接著換 c2 重複做 Step1，直到 c10

Step3.
做完 step1 及 step2 後可以得到 10 個有缺陷的 message，根據英文文法及單字，盡可能地猜出 message 是甚麼。

Step4.
利用還原最多的 message 和其 cipher text 做 xor 可以得到一個可能的 key K，利用 K 和其他 cipher text 做 xor 可以得到更完整的 message。重複 step3，直到還原出 64bytes 正確的 key。

觀察可知 key 的值會循環，即 key[64] = key[0]，由此可解碼全部 cipher text，得到 flag。

7. Backdoor of Diffie Hellman

未做

8. Man in the Middle

Flag: BALSN{Wow_you_are_really_in_the_middle}

參考: http://mslc.ctf.su/wp/hitcon-ctf-quals-2016-pake-pake-crypto-250-150/

Method1.

對 Server 分別做兩次連線，connection A(cA)及 connection B(cB)，藉此達到 man in the middle attack。Password 長度為 3，且皆為 1-20 的值。例: 要猜第 i 個 password p 的值(i= 1,2,3)，在 Round i 分別從 cA 和 cB 收到 messages，mA 和 mB，且傳送 g_p 給 cA 和 cB，其餘的 Round 則直接將 cA、cB 的值對傳，將最後由 cA、cB 傳來的 flag fA、fB 對 mA、mB 分別做 xor，若得到的結果相同，則猜對 password。由第 1 個 password，value = 1 開始猜，直到將 3 個 password 的值皆找出。找到 password 後便可利用老師上課提到的 Example: MitM attack against DH key agreement 找到 flag。

Metho2.

只需和 Serve 建一次連線，直接利用上課提到的 Example: MitM attack against DH key agreement 試可能的 password 組合，共 20*20*20 = 8000 種，可以產生 8000 種 generator，將每種 generator 和 server 溝通產生的 key 都和 server 最後傳來的 flag 做 xor，已知 flag 皆為 BALSN{…}，搜尋 BALSN 即可找到 flag。

備註:

code8.py 實作 method1。

9. Only admin can print flag

未做