NA

第一題

和 b03902130 討論

NASA{Ev3n_s3cure_PRF_1S_bre4kble_1f_u5ed_unc0rr3ctly}

server 的 SecureEncryption 加密四次、解密四次，我們發現如果 unpad 長度不是 16 倍數就無法再 aes 解密 所以我們可以確定四把鑰匙中的後三把最後一定是\x10，所以在找第四把 key 時就固定前六個字，只讓兩個變換，考慮所有 printable 的字元，暴力解是可行的 另外兩把鑰匙也是用這個方式來解。而最後一把鑰匙因為不用再 aes decrypt 所以長度不保證是 16 的倍數 我們就要找尾端由 1 到 16 來暴力搜尋 最後搜到尾端是\t\t\t\t\t\t\t\t 是我們的鑰匙

鑰匙是 jizz7722 由這個鑰匙，我們可以得到 flag

第二題

和 b03902130 b06902075 討論

NASA{Tw0_3qual5_to_0ne_Whyyyyyy}'

我們可以把雙層 aes 一層用 plaintext 與第一把 key 向前加密，另一層用 cipher 與第二把 key 向後解密 因為 key 的長度保證小於 2**23 所以我們用 for 迴圈暴力搜尋。再加密解密時，我設一個 inside 存值，如果加解密出來的結果相同，我們就找出兩把 key 了，得到兩把 key 後我們就可以解開 flag

第三題

和 b03902130 b06902075 TA 討論

NASA{Ahhhh…I_g0t_Mitm_4g41n…}

密碼:15,7,18,12,3,17,1,13,9,10

我們一次只猜一個數字，一次開兩個連線連上 server，在前面九次我把兩台 server 給的 a 互相傳給對方，這樣他們就會產生相同的 key，到第十次時我開始猜密碼，猜一個密碼然後用 password 的規則製造然後傳給兩台。如果 password 猜對了，那兩台的 a1^a2^a3…^my_guess^flag 會等於 b1^b2^b3…^my_guess^flag 最後 xor 出來的東西就會是 0 就代表我們猜對了，這樣最多 20*10 次就可以得到正確密碼