## **Mobile Challenges**

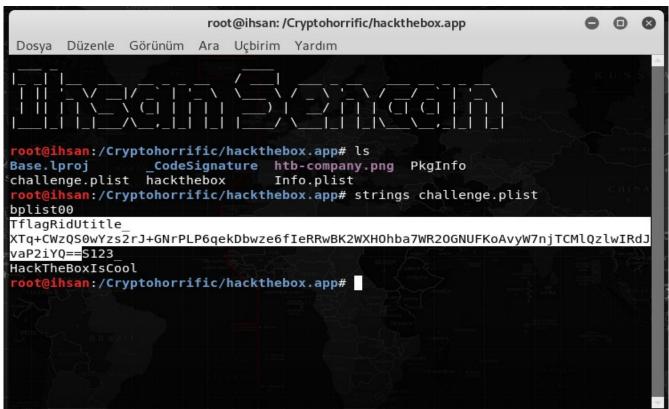
## Cryptohorrific

## **IhSanSencan**

www.ihsan.net

https://www.hackthebox.eu/profile/100992





```
📳 IDA View-A 🔲 🔘 Hex View-1 🗵 🛕
                                                   × E
                                        Structures
                                                            Enums
                                                                        Imports
          objc methname:00000001000024B8
                                                                               objc_const:
          objc methname:00000001000024C3 aWindow 0
                                                     db ' window',θ
                                                                            ; DATA XREF:
          objc_methname:00000001000024C3 __objc_methname ends
          objc methname:00000001000024C3
          cstring:00000001000024CB
          cstring:00000001000024CB ; Segment type: Pure data
          cstring:00000001000024CB __cstring
                                                segment byte public 'DATA' use64
          cstring:00000001000024CB
                                                assume cs: cstring
          cstring:00000001000024CB
                                                ;org 1000024CBh
          cstring:00000001000024CB aADGKapdsgvky
                                                db '!A%D*G-KaPdSgVkY',0 ; DATA XREF: __cfstri
          cstring:0000001000024DC aQftjwnzq4t7wZC db 'QfTjWnZq4t7w!z%C',0 ; DATA XREF: __cfstri
                                                db 'challenge',θ
          cstring:00000001000024ED aChallenge
                                                                      ; DATA XREF: __cfstri
          cstring:00000001000024F7 aPlist
                                                db 'plist',0
                                                                      ; DATA XREF: __cfstri
                                                db 'flag',0
          cstring:00000001000024FD aFlag
                                                                      ; DATA XREF: __cfstri
                                                                      ; DATA XREF: __objc_c
          cstring:0000000100002502 aHash 0
                                                db 'hash',θ
          cstring:0000000100002502
                                                                      ; objc const:000000
                                                                      ; DATA XREF: __objc_c
                                                db 'TQ,R',θ
          cstring:0000000100002507 aTqR
          cstring:0000000100002507
                                                                      ; objc const:000000
          cstring:000000010000250C aSuperclass 0
                                                db 'superclass',0
                                                                      ; DATA XREF: objc c
                                                                        _objc_const:000000
          cstring:000000010000250C
                                                db 'T#,R',θ
                                                                      ; DATA XREF: objc c
          cstring:0000000100002517 aTR
          cstring:0000000100002517
                                                                      ; objc const:000000
          cstring:000000010000251C aDescription 0 db 'description',0
                                                                      ; DATA XREF: objc c
        00000400 000000100000400
                                                001 1 417 70 70
```

```
//Ihsan Sencan
   //Mobile Challenges / Cryptohorrific
                   = 128; // 192, 256
AES($imputText, $imputKey, $blockSize);
 9
                     →decrypt();
           setData(
10
                 )ata(pen.

→decrypt();

→ion: ".$enc."<br/>";
13
14
15
16
17
18
    lass AES {
         const M_CBC const M_CFB
                              'cbc'
                 M_ECB
M_NOFB
19
                            = 'nofb';
= 'ofb';
20
21
22
23
24
                  M_OFB
                  M_STREAM = 'stream';
25
```



Decryption: HTB{%SoC00l\_H4ckTh3b0xbyBs3cur31stCh4ll3ng3!!Cı