

## Informe de lab 01 seguridad TI

Nombres: Hans Barnert  
Benjamín Ulloa

En la primera tarea, leímos el instructivo, y verificamos si johntheripper estaba en el computador instalado.

Luego utilizamos el código que nos proporcionaba la página web, pero usando la ruta correspondiente a la nuestra que era /home/fz104/"pdfcifrado"

una vez resuelto esto, se creó un archivo .hash el cual nos ayudará a poder descifrar la contraseña a fuerza bruta.

```
(fz104@vmwin10-MGodoy)-[~/Downloads]  
$ pdf2john /home/fz104/Downloads/'CIFRADO PDF - password protected.pdf' > /home/fz104/Downloads/pdf.hash
```

A continuación, utilizamos la siguiente parte del código, la cual tenemos que poner "john pdf.hash" donde hacemos funcionar el johntheripper, lo cual finalmente nos da la clave: 185020

```
(fz104@vmwin10-MGodoy)-[~/Downloads]  
$ john pdf.hash  
Using default input encoding: UTF-8  
Loaded 1 password hash (PDF [MD5 SHA2 RC4/AES 32/64])  
Cost 1 (revision) is 4 for all loaded hashes  
Will run 6 OpenMP threads  
Proceeding with single, rules:Single  
Press 'q' or Ctrl-C to abort, almost any other key for status  
Almost done: Processing the remaining buffered candidate passwords, if any.  
Proceeding with wordlist:/usr/share/john/password.lst  
Proceeding with incremental:ASCII  
185020 (/home/fz104/Downloads/CIFRADO PDF - password protected.pdf)  
1g 0:00:00:04 DONE 3/3 (2023-08-23 18:55) 0.2079g/s 148001p/s 148001c/s 148001C/s 185682..185040  
Use the "--show --format=PDF" options to display all of the cracked passwords reliably  
Session completed.
```

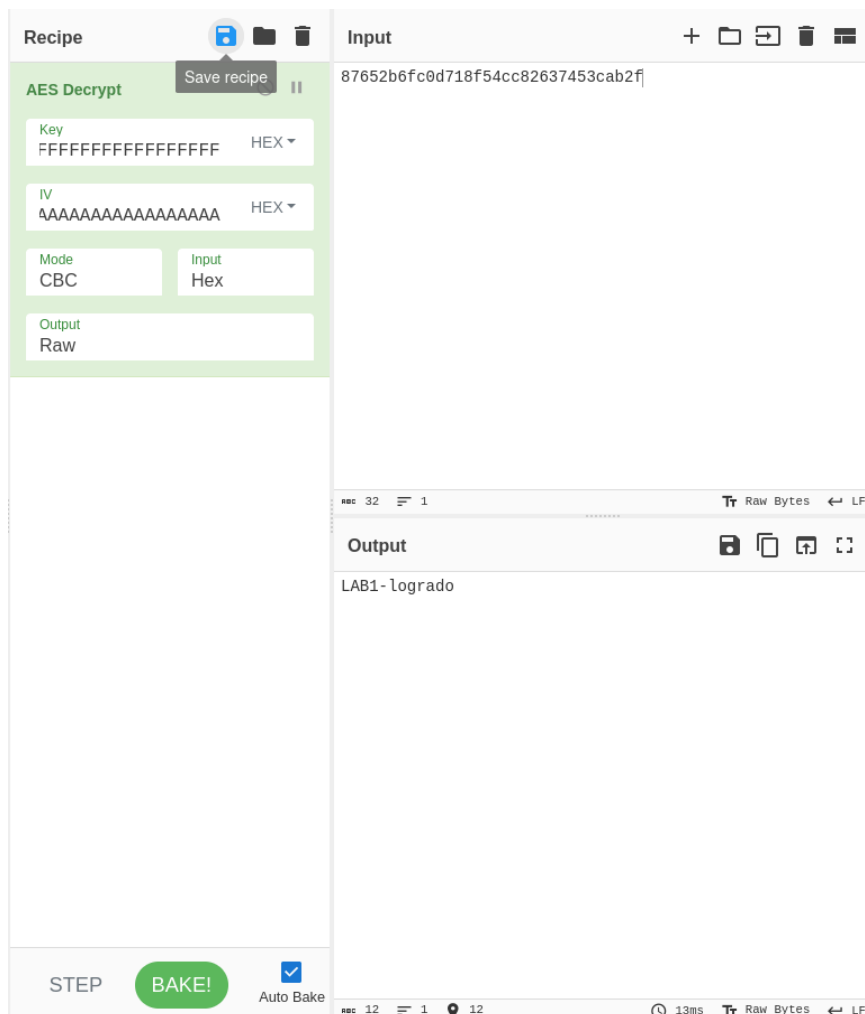
En la segunda parte

Tomamos el texto para descifrar y lo ponemos como input en la página de CYBERCHIEF, vamos a la sección de descifrado, en modo AES-128, y ahora introduciendo la clave, accedemos al pdf que contiene la siguiente información:

La llave es: Fs

- I. Ds
- II. Cs
- III. Bs
- IV. As
- V. 9s
- VI. 8s
- VII. 7s

Nos damos cuenta que necesita un input de 16 bytes, y la clave son Fs, por tanto, llegamos a la conclusión que son 16 Fs, y en IV, Ponemos las 16 As correspondientes, una vez, realizado esto, ponemos, “Bake” y nos desencripta el mensaje final el cual es: LAB1-logrado



The screenshot shows a web-based AES decryption tool interface. On the left, under the 'Recipe' tab, the 'AES Decrypt' recipe is selected. The 'Key' is set to 'FFFFFFFFFFFFFFFF' in 'HEX' mode. The 'IV' is set to 'AAAAAAAAAAAAAAAA' in 'HEX' mode. The 'Mode' is 'CBC' and the 'Input' is 'Hex'. The 'Output' is set to 'Raw'. A 'Save recipe' button is visible. On the right, under the 'Input' tab, the hex string '87652b6fc0d718f54cc82637453cab2f' is entered. Below the input, the 'Output' tab shows the result 'LAB1-logrado'. At the bottom, there is a 'STEP' button, a green 'BAKE!' button, and an 'Auto Bake' checkbox. The bottom status bar shows '13ms' and 'Raw Bytes'.

