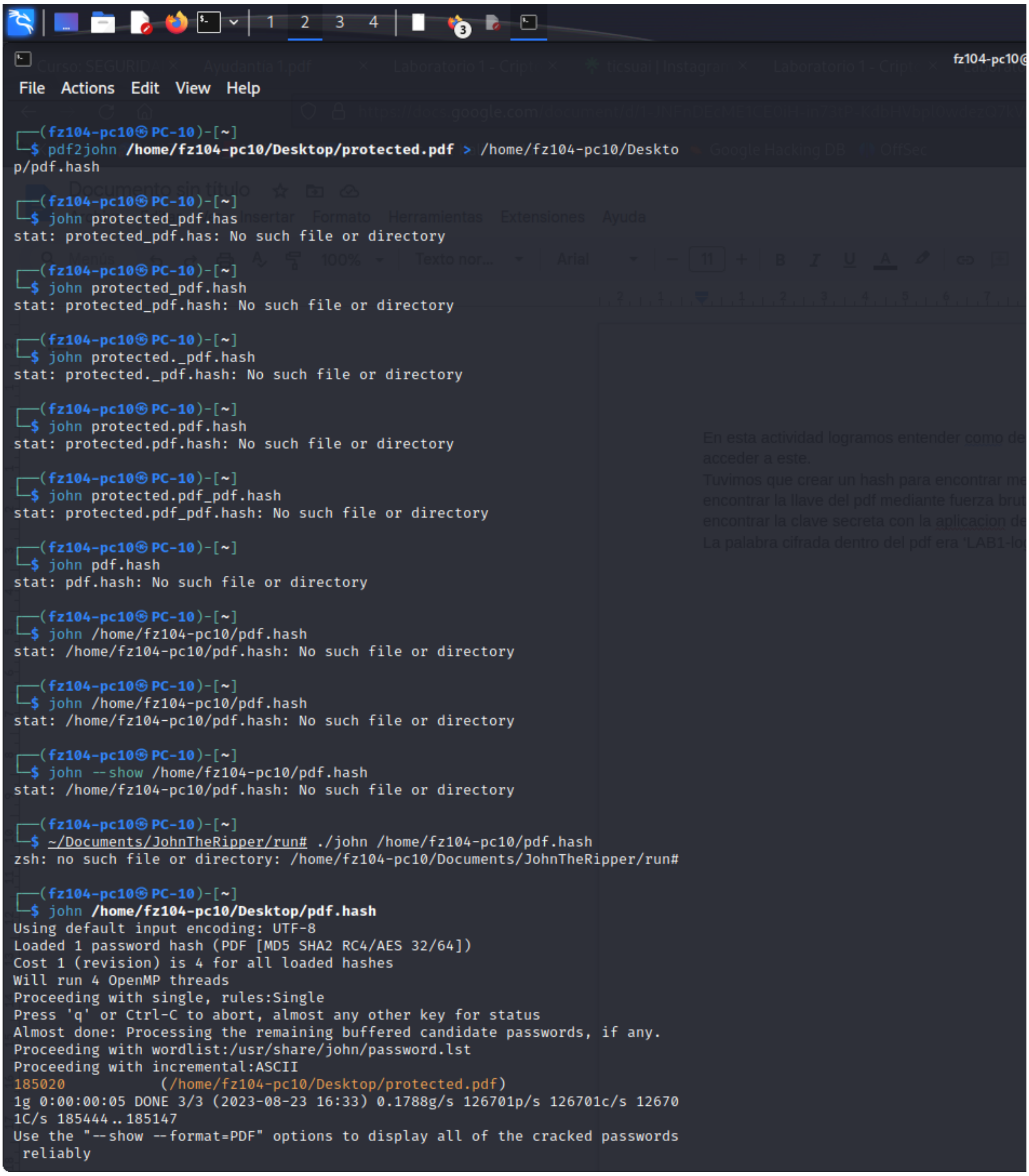
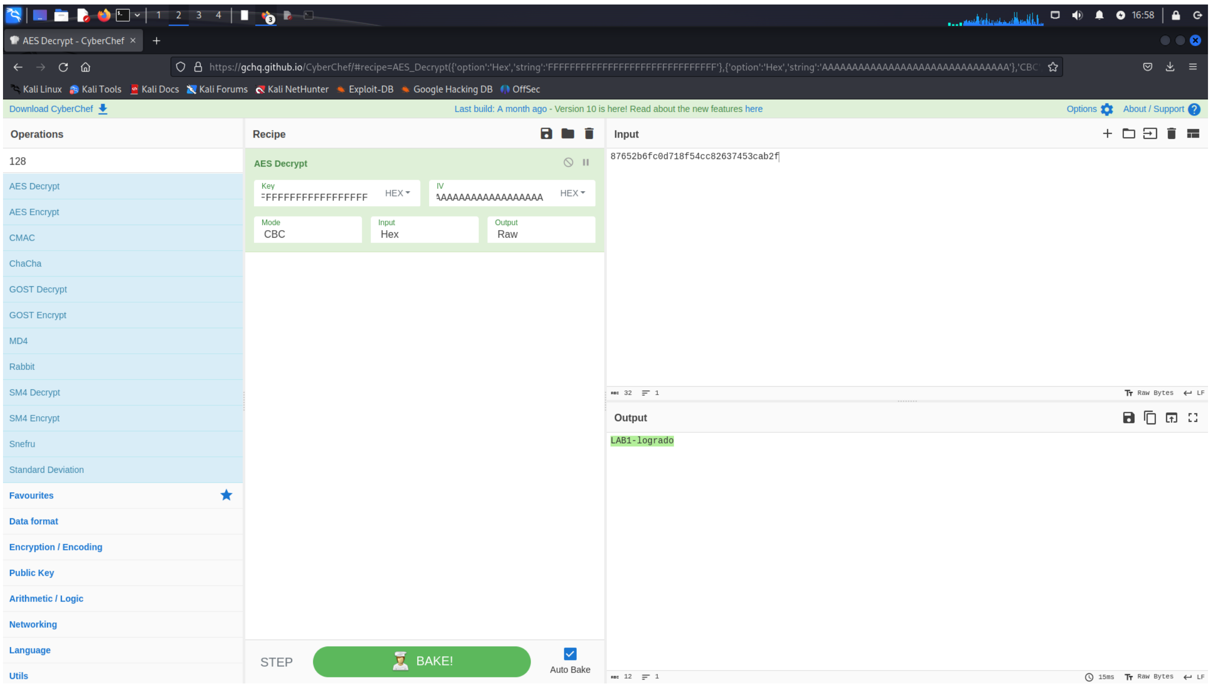
José Hevia Felipe Olivares Grupo 2
En esta actividad logramos entender como descifrar una clave escondida de un pdf para acceder a este.
Tuvimos que crear un hash para encontrar mediante la aplicacion john the ripper para encontrar la llave del pdf mediante fuerza bruta, la clave encontrada se ve en naranjo en la imagen y es 185020. Luego decodificamos lo que el pdf contenía para encontrar la clave secreta con la aplicacion de internet CyberChef.
La palabra cifrada dentro del pdf era ‘LAB1-logrado’



```
┌──(fz104-pc10㉿PC-10)-[~]
└─$ pdf2john /home/fz104-pc10/Desktop/protected.pdf > /home/fz104-pc10/Deskto
p/pdf.hash

┌──(fz104-pc10㉿PC-10)-[~]
└─$ john protected_pdf.has
stat: protected_pdf.has: No such file or directory

┌──(fz104-pc10㉿PC-10)-[~]
└─$ john protected_pdf.hash
stat: protected_pdf.hash: No such file or directory

┌──(fz104-pc10㉿PC-10)-[~]
└─$ john protected._pdf.hash
stat: protected._pdf.hash: No such file or directory

┌──(fz104-pc10㉿PC-10)-[~]
└─$ john protected.pdf.hash
stat: protected.pdf.hash: No such file or directory

┌──(fz104-pc10㉿PC-10)-[~]
└─$ john protected.pdf_pdf.hash
stat: protected.pdf_pdf.hash: No such file or directory

┌──(fz104-pc10㉿PC-10)-[~]
└─$ john pdf.hash
stat: pdf.hash: No such file or directory

┌──(fz104-pc10㉿PC-10)-[~]
└─$ john /home/fz104-pc10/pdf.hash
stat: /home/fz104-pc10/pdf.hash: No such file or directory

┌──(fz104-pc10㉿PC-10)-[~]
└─$ john /home/fz104-pc10/pdf.hash
stat: /home/fz104-pc10/pdf.hash: No such file or directory

┌──(fz104-pc10㉿PC-10)-[~]
└─$ john --show /home/fz104-pc10/pdf.hash
stat: /home/fz104-pc10/pdf.hash: No such file or directory

┌──(fz104-pc10㉿PC-10)-[~]
└─$ ~/Documents/JohnTheRipper/run# ./john /home/fz104-pc10/pdf.hash
zsh: no such file or directory: /home/fz104-pc10/Documents/JohnTheRipper/run#

┌──(fz104-pc10㉿PC-10)-[~]
└─$ john /home/fz104-pc10/Desktop/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 4 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-pc10/Desktop/protected.pdf)
1g 0:00:00:05 DONE 3/3 (2023-08-23 16:33) 0.1788g/s 126701p/s 126701c/s 12670
1C/s 185444..185147
Use the "--show --format=PDF" options to display all of the cracked passwords
 reliably
```



AES Decrypt - CyberChef

https://gchq.github.io/CyberChef/#recipe=AES_Decrypt({'option':'Hex','string':'FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF'},{'option':'Hex','string':'AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA'},'CBC

Last build: A month ago - Version 10 is here! Read about the new features here

Operations: 128

Recipe: AES Decrypt

Key: FFFFFFFFFFFFFFFFF HEX

IV: AAAAAAAAAAAAAAAAAA HEX

Mode: CBC

Input: Hex

Output: Raw

Input

```
87652b6fc0d718f54cc82637453cab2f
```

Output

```
LAB1-logrado
```