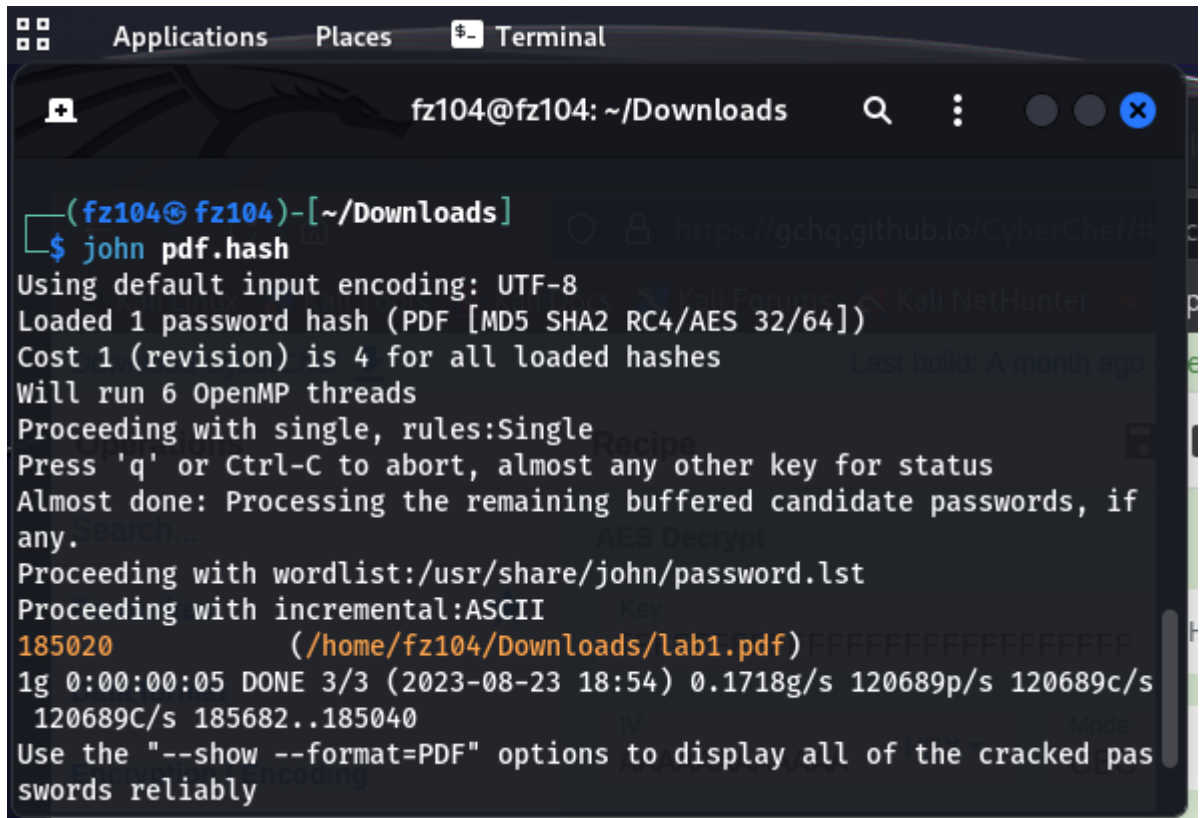


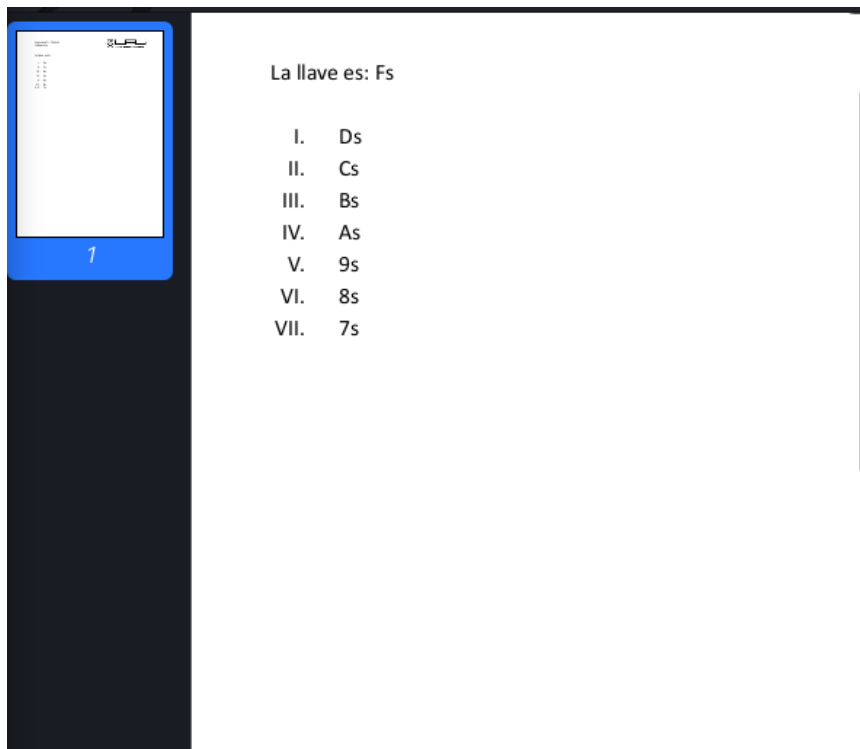
## Informe laboratorio 1 Seguridad en T.I

Integrantes Cristian Sepulveda - Nicolas Quilhot

1. Actividad 1: En primer lugar, luego de leer las instrucciones, abrimos la herramienta John The Ripper que nos sirvió para poder descifrar con fuerza bruta la clave del pdf encriptado. El código de acceso obtenido fue 185020, con el cual accedimos al pdf para luego obtener las pistas para la parte 2.



```
(fz104@fz104)-[~/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/lab1.pdf) FFFFFFFFFFFFFFFFFF
1g 0:00:00:05 DONE 3/3 (2023-08-23 18:54) 0.1718g/s 120689p/s 120689c/s
120689C/s 185682..185040
Use the "--show --format=PDF" options to display all of the cracked pas
swords reliably
```



La llave es: Fs

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

2. Actividad 2: El documento pdf desbloqueado, nos sirvió para tener la clave a utilizar en CyberChef con la cual al utilizar la herramienta AES- decrypt pudimos descifrar el código cifrado en AES-128. Luego ingresando la Key entregada en el pdf junto con IV pudimos descifrar el código y terminar el ejercicio.

