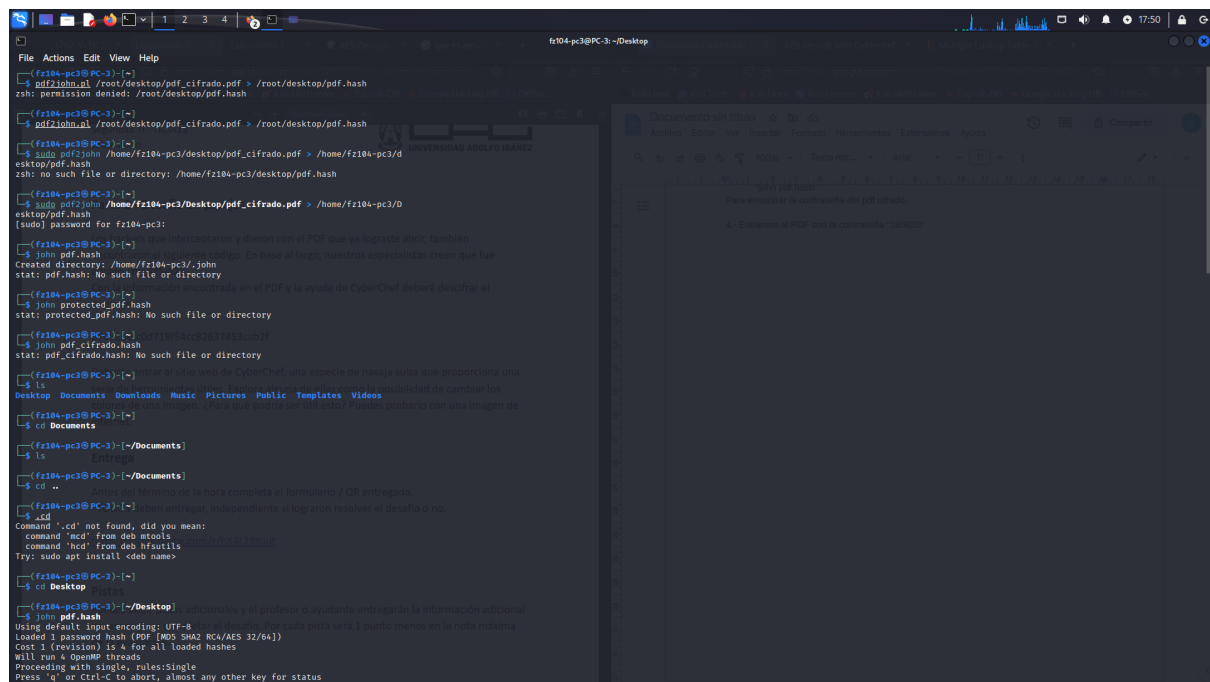


Laboratorio 1 - Seguridad TI

Cristobal Huilcaman
Marcos Valenzuela

- 1.- Descargamos el archivo pdf cifrado desde la web y lo guardamos en el escritorio
- 2.- Abrimos el terminal y creamos el archivo .hash con el comando.
“pdf2john.pl /root/desktop/pdf_cifrado.pdf > /root/desktop/pdf.hash”
- 3.- En el terminal, una vez situados en la carpeta Desktop, utilizamos el comando
“john pdf.hash”
Para encontrar la contraseña del pdf cifrado.
- 4.- Entramos al PDF con la contraseña “185020”



```
fr104-pc3@PC-3: ~/Desktop
$ pdf2john.pl /root/desktop/pdf_cifrado.pdf > /root/desktop/pdf.hash
zsh: permission denied: /root/desktop/pdf.hash

(fr104-pc3@PC-3)~$ pdf2john.pl /root/desktop/pdf_cifrado.pdf > /root/desktop/pdf.hash

(fr104-pc3@PC-3)~$ sudo pdf2john /home/fr104-pc3/desktop/pdf_cifrado.pdf > /home/fr104-pc3/desktop/pdf.hash
zsh: no such file or directory: /home/fr104-pc3/desktop/pdf.hash

(fr104-pc3@PC-3)~$ sudo pdf2john /home/fr104-pc3/Desktop/pdf_cifrado.pdf > /home/fr104-pc3/Desktop/pdf.hash
[sudo] password for fr104-pc3:
(fr104-pc3@PC-3)~$ john pdf.hash
Created directory: /home/fr104-pc3/.john
stat: pdf.hash: no such file or directory

(fr104-pc3@PC-3)~$ john protected_pdf.hash
stat: protected_pdf.hash: No such file or directory

(fr104-pc3@PC-3)~$ john pdf_cifrado.hash
stat: pdf_cifrado.hash: No such file or directory

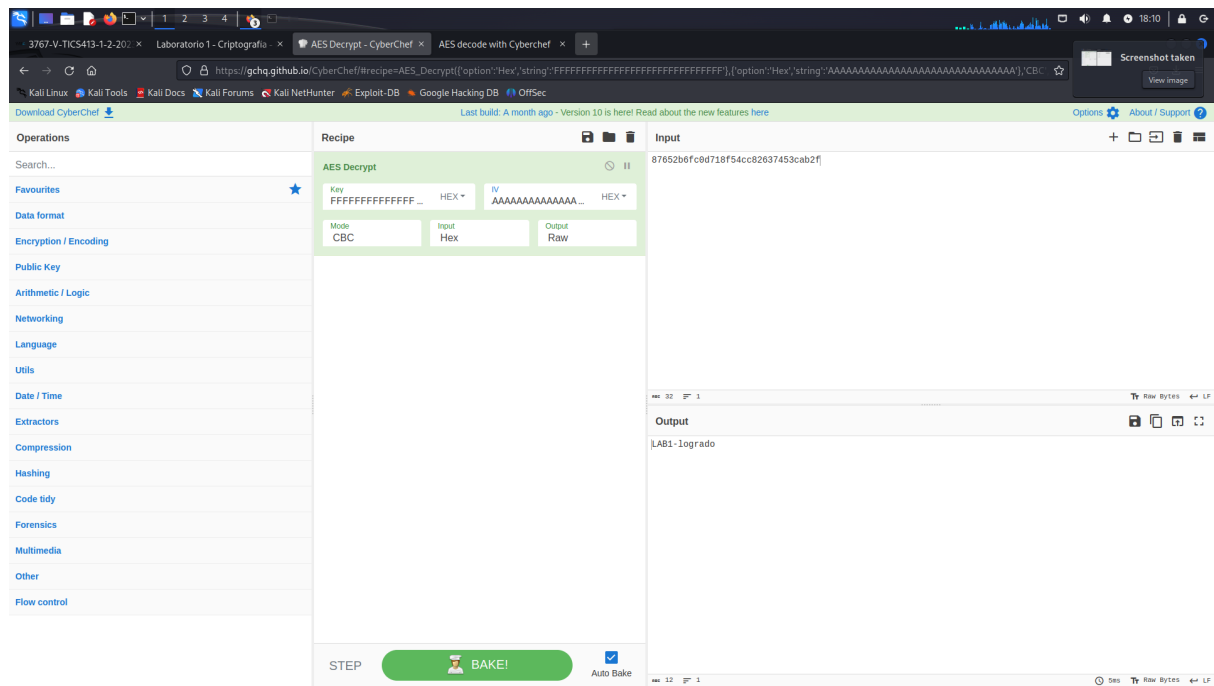
(fr104-pc3@PC-3)~$ john pdf_cifrado.hash
stat: pdf_cifrado.hash: No such file or directory

(fr104-pc3@PC-3)~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
(fr104-pc3@PC-3)~$ cd Documents
(fr104-pc3@PC-3)~/Documents$ ls
Entrada
(fr104-pc3@PC-3)~/Documents$ cd ..
Antes del termino de la hora completa el formulario / QR entregado.
(fr104-pc3@PC-3)~$ cd
Command 'cd' not found, did you mean:
  command 'ncd' from deb ncdutils
  command 'hcd' from deb hfsutils
Try: sudo apt install <deb name>

(fr104-pc3@PC-3)~$ cd Desktop
(fr104-pc3@PC-3)~/Desktop$ john pdf.hash
Using default input encoding: UTF-8
Loaded 1 password hash (PDF [MD5 SHA256/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
```

Parte 2

Luego de descifrar el pdf nos dimos cuenta de las pistas que había en su contenido, y logramos concluir el mensaje cifrado.



La llave era Fs y necesitábamos 16 bytes por lo tanto repetimos hasta dar con la clave. posterior a eso identificamos el IV y nos demos cuenta de que era As por lo que repetimos el proceso anterior y pudimos descifrar el mensaje.