

entramos con la clave 185020 encontrada con el pdf.hash probando con una combinación forzada de 4 dígitos

```
(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 (pdf.pdf)
1g 0:00:00:44 DONE 3/3 (2023-08-23 17:44) 0.02235g/s 14824p/s 14824c/s 14824C/s
185682..185040
Use the "--show --format=PDF" options to display all of the cracked passwords reliably
Session completed.

(fz104@vmwin10-MGodoy)-[~/Downloads]
$

(fz104@vmwin10-MGodoy)-[~/Downloads]
$
```

Al lograr abrir el pdf tuvimos que descifrar el comando gracias al pdf encontrado, con el mensaje a descifrar y las pistas, se descifró por las siguientes pistas uno s es la letra 16 del abecedario por lo cual escribimos 16 la f que era la llave y ademas por el numero 4 romano se nos dio a entender que la otra letra a trabajar era la A. también tuvimos varios errores los cuales consistieron en usar repetidamente Fs para llegar a los 16 bytes, ya que Fs era solo uno y teníamos que llegar a los 16, también usamos todas las letras dadas y nos daban 8 bytes, tambien usamos en manera de fila los datos entregados. y luego de pensar y que s es la letra número 16 pensamos que era una indicación de repetir la letra la letra 16 veces

Laboratorio 1 - Criptografía

seguridadtics413.file.core.windows.net

Seguridad TI - TICS413  
Laboratorio

La llave es: Fs

I. Ds

II. Cs

III. Bs

IV. As

V. 9s

VI. 8s

VII. 7s

3767-V-TICS413

How to crack a | Laboratorio 1 - Criptografía | AES Decrypt - C | Documento sin | jhon the ripper - |

https://github.com/CyberChef/CyberChef#recipe=AES\_Decrypt(option:"Hex",string:"FFFFFFFFFFFFFFFF")

Download CyberChef

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

Options About / Support

Operations

Recipe

Input

aes

AES Decrypt

AES Encrypt

AES Key Wrap

AES Key Unwrap

Parse ASN.1 hex string

Group IP addresses

Parse IPv6 address

Defang IP Addresses

Generate all hashes

Extract IP addresses

Format MAC addresses

Extract MAC addresses

Caesar Box Cipher

Extract email addresses

Parse SSH Host Key

Swap endianness

JPath expression

AES Decrypt

Key

FFFFFFFFFFFFFFFFFFFFFFFF

HEX

IV

AAAAAAAAAA

HEX

Mode

CBC

Input

Hex

Output

Raw

87652b6fc0d718f54cc82637453cab2f

Output

LAB1 - logrado

Parses a SSH host key and extracts fields from it. The key type can be:

- ssh-rsa
- ssh-dss
- ecdsa-sha2
- ssh-ed25519

The key format can be either Hex or Base64.

[Secure Shell on Wikipedia](#)

Auto Bake

32 1

Raw Bytes