

# EJERCICIO 11. CIFRADO EN LAS CONTRASEÑAS

antonio nuñez

IES PUNTA DEL VERDE LUNES, 27 DE ENERO DE 2025

John the Ripper es una herramienta orientada al descifrado de contraseñas.

Instalar el programa en Linux y realizar pruebas de funcionamiento.

Enviar capturas de pantalla y un texto explicando el funcionamiento del mismo.

Para esta práctica voy a usar el hash que viene en el tutorial y voy a intentar romperlo con la herramienta John the Ripper

El hash en cuestión es: `user:AZl.zWwxIh15Q`

```
GNU nano 8.1 hash *
user:AZl.zWwxIh15Q
```

Primero voy a probar con el método de diccionario

```
/home/antonio/Desktop/ejercicio > ll
-rw-rw-r-- root root 33 B Mon Jan 27 17:24:20 2025 hash
-rw-r--r-- root root 133 MB Mon Jan 27 17:33:35 2025 rockyou.txt
```

Descargamos el diccionario rockyou.txt

```
/home/antonio/Desktop/ejercicio > john -wordlist=rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (descrypt, traditional crypt(3) [DES 256/256 AVX2])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
example (user)
1g 0:00:00:00 DONE (2025-01-27 17:51) 100.0g/s 6144Kp/s 6144Kc/s 6144KC/s robzombi..papaku
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Al ejecutar el comando podemos ver que la contraseña en texto claro es “example”

```
/home/antonio/Desktop/ejercicio > john --show hash
user:example

1 password hash cracked, 0 left
```

## Ahora voy a hacerlo con fuerza bruta

El hash en cuestión es: *user:AZl.zWwxIh15Q*

```
🔍 ~/Desktop/ejercicio > john --show hash2
0 password hashes cracked, 1 left

🔍 ~/Desktop/ejercicio > john hash2
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 8 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 13 candidates buffered for the current salt, minimum 32 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
|
```

Y ya está el hash descifrado.

```
🔍 /home/antonio/Desktop/ejercicio 🔥 > john --show hash
user:example

1 password hash cracked, 0 left
```