

ZIP cracking

Known plaintext (file)

- <https://github.com/keyunluo/pkcrack>

Need one exact file in plaintext from the encrypted archive. The ZIP archive encrypts each file individually but using same key, so one can list contents and file sizes before and after compression.

```
pkcrack -C web_labyrinth_linguist.zip -c
challenge/src/main/resources/static/font/Ancient_G_Written.ttf -P web_labyrinth_linguist-
plain.zip -p challenge/src/main/resources/static/font/Ancient_G_Written.ttf -d
web_labyrinth_linguist-decrypt.zip -a
```

Make sure that encrypted and plaintext ZIP archive file size after compression is the same (same compression settings).

```
zip -9 -r web_labyrinth_linguist-plain.zip challenge
unzip -lvv web_labyrinth_linguist-plain.zip | grep Ancient
unzip -lv web_labyrinth_linguist.zip | grep Ancient
```

Revision #2

Created 2026-02-21 20:56:50 GMT by HexaHack

Updated 2026-02-26 21:10:13 GMT by HexaHack