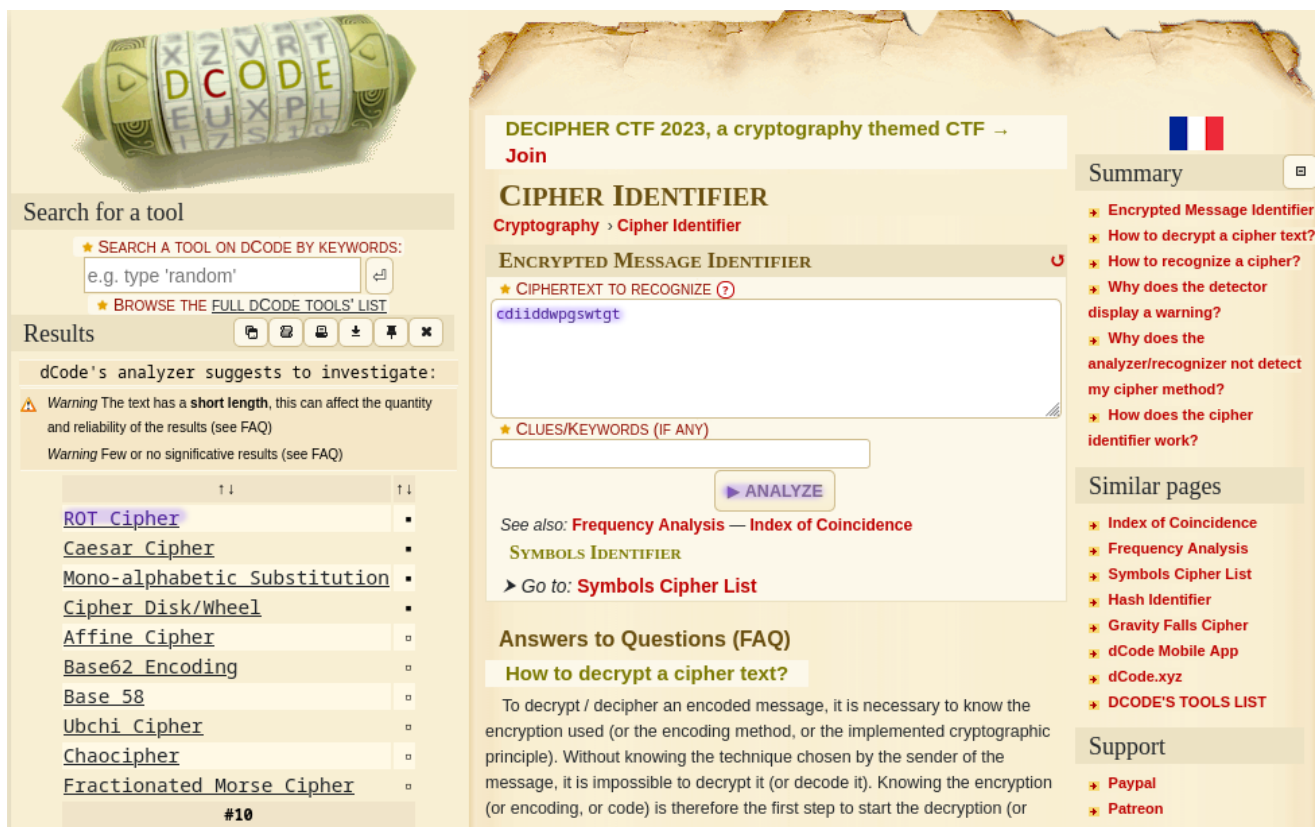# Level00

Using the `find` command, is it possible to enumerate two files owned by `flag00`. These files are identical, owned by `flag00` user and read only.

```
level00@SnowCrash:~$ find / -user flag00 -exec ls -l {} \; 2>/dev/null
----r--r-- 1 flag00 flag00 15 Mar 5 2016 /usr/sbin/john
----r--r-- 1 flag00 flag00 15 Mar 5 2016 /rofs/usr/sbin/john
```

By inspecting the file contents with the `cat` command, we can see a short word that looks like a token. Our attempt to login as user `flag00` with this token fails so it is possibly cyphered.

```
level00@SnowCrash:~$ cat /usr/sbin/john
cdiiddwpgswtgt
level00@SnowCrash:~$ su flag00
Password:
su: Authentication failure
```

Online tools exist such as [Dcode](#) to help **cypher identification** and decryption. The tool suggests looking at several cyphers, so we try the first suggestion, the **ROT** cypher tool.

ROT cypher is a simple method of cyphering that consists of rotating letters of the alphabet by **N** places. For example with **N = 13**, the letter **A** becomes **N**, **B** becomes **O** and so on.

Results of the **ROT** bruteforcer of [Dcode](#) gives us an interesting result where **N = 15**. By applying this cypher to the token `cdiiddwpgswtgt`, it gives us out the token `nottoohardhere` wich is the only human readable result.

We can now attempt to log in as user `flag00`, wich works, and use the `getflag` command to obtain the flag.

```
level00@SnowCrash:~$ su flag00
Password:
Don't forget to launch getflag !
flag00@SnowCrash:~$ getflag
Check flag.Here is your token : x24ti5gi3x0ol2eh4esiuxias
```