Praktikum 2

https://courses.cs.ut.ee/2024/turve/spring/Main/Praktikum2

ÜL 1

aaYnY9JY1skVY - **ut**
abpNtJ15XGZyU - **ati**
XZkMWgaNMr552 - **hack**

1SoolSalt$6kodg6UCOHV2owr1QxUX60 - **hd**
5Andmeturve$aRN3yaCA0QP4tgVRUF6u8NxZS7o.OD2gAoSzj66wyS1 - **led**
6SomethingHere$L5zuxicIHC90jGVZ9xgoOjUw36DjduwH1nPGJ.uwcgLqCvhlGe6wWp55eojE9jAIXxDbcsmbAKLXuXg2AbKZo0 - **asdf**

Kood:

```
import string, crypt

paroolidA = ["aaYnY9JY1skVY", "abpNtJ15XGZyU", "XZkMWgaNMr552"]

paroolidB = ["$1$SoolSalt$6kodg6UCOHV2owr1QxUX60",
"$5$Andmeturve$aRN3yaCA0QP4tgVRUF6u8NxZS7o.OD2gAoSzj66wyS1",
"$6$SomethingHere$L5zuxicIHC90jGVZ9xgoOjUw36DjduwH1nPGJ.uwcgLqCvhlGe6wWp55eojE9jAIXxDbcsmbAKLXuXg2AbKZo0"]

def neljaTahelineA(parool):
    salt = parool[:2]
    for c1 in string.ascii_lowercase:
        for c2 in string.ascii_lowercase:
            for c3 in string.ascii_lowercase:
                for c4 in string.ascii_lowercase:
                        passwd = c1 + c2 + c3 + c4
                        if parool == crypt.crypt(passwd, salt):
                                return passwd

def neljaTahelineB(parool):
    index = parool.rfind("$")
    salt = parool[:(index)]
    for c1 in string.ascii_lowercase:
        for c2 in string.ascii_lowercase:
            for c3 in string.ascii_lowercase:
                for c4 in string.ascii_lowercase:
                        passwd = c1 + c2 + c3 + c4
                        if parool == crypt.crypt(passwd, salt):
                                return passwd
```

print(f"Räsi: {paroolidA[2]}, parool: {neljaTahelineA(paroolidA[2])}")
print(f"Räsi: {paroolidB[2]}, parool: {neljaTahelineB(paroolidB[2])}")

ÜL 2

DES.TXT failist leitud paroolid:

PAROOL	***KASUTAJA***
anekdoot	(test1)
kasutaja	(mustikas)
praktiku	(polt)
valimise	(kaposta)

MD5.txt failist leitud paroolid:

email	(treff)
foorum	(riva)

ÜL 3

Matrikli nr **CI551**, parool: **1950**