



Jesenji semestar, 2022/23

PREDMET: IT381 Zaštita i bezbednost informacija

Domaći zadatak: 1

Ime i prezime: **Aleksa Cekić**

Broj indeksa: **4173**

Datum izrade: **27.11.2022**

Dajte odgovore na sledeća pitanja:

P: Koliko vremena je trebalo alatu da “razbije” neke lozinke?

O: Nekoliko sekundi do ~1h 30min.

P: Koliko dodatnih lozinki je razbio?

O: 4/6.

P: Koje su najjednostavnije lozinke?

O: Lozinke koje su iste kao korisničko ime, mejl.

P: Koliko se razbijenih lozinki može naći u rečniku?

O: 4/11.

P: Koliko razbijenih lozinki sadrže promenljive kombinacije slova, simbola i brojeva?

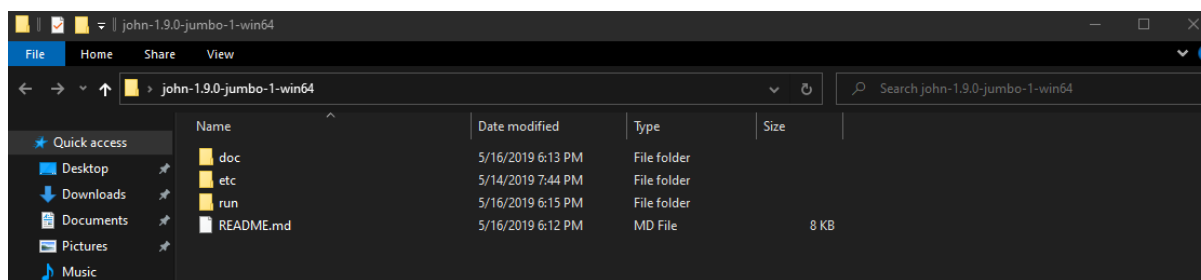
O: 3.

P: Da li su razbijene lozinke duže ili kraće?

O: Uglavnom su razbijene sve lozinke sem najduže.

P: Koliko lozinki nikada nije bilo razbijeno?

O: 2



Preuzet John the Ripper software sa [linka](#).

MD5 Hash Generator

Use this generator to create an MD5 hash of a string:

iloveyou

Generate →

Your String	iloveyou
MD5 Hash	f25a2fc72690b780b2a14e140ef6a9e0 <button>Copy</button>
SHA1 Hash	ee8d8728f435fd550f83852aabab5234ce1da528 <button>Copy</button>

This MD5 hash generator is useful for encoding passwords, credit cards numbers and other sensitive data into MySQL, Postgress or other databases. PHP programmers, ASP programmers and anyone developing on MySQL, SQL, Postgress or similar should find this online tool an especially handy resource.

Preko ovog sajta hesiramo neke sifre koje će se nalaziti unutar crack-these-please.txt fajlu.



crack-these-please.txt - Notepad

File Edit Format View Help

```
5f4dcc3b5aa765d61d8327deb882cf99
4d5257e5acc7fcac2f5dcd66c4e78f9a
d16d377af76c99d27093abc22244b342
f25a2fc72690b780b2a14e140ef6a9e0|
```

```
C:\Users\Aleksa\Desktop\john-1.9.0-jumbo-1-win64\run>john -w:password.lst --format=raw-MD5 crack-these-please.txt.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
password      (?)
mickey         (?)
jordan         (?)
iloveyou       (?)
4g 0:00:00:00 DONE (2022-11-28 00:26) 102.5g/s 9846p/s 9846c/s 39384C/s 123456..larry
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed
```

```
C:\Users\Aleksa\Desktop\john-1.9.0-jumbo-1-win64\run>type john.pot
$dynamic_0$5f4dcc3b5aa765d61d8327deb882cf99:password
$dynamic_0$4d5257e5acc7fcac2f5dcd66c4e78f9a:mickey
$dynamic_0$d16d377af76c99d27093abc22244b342:jordan
$dynamic_0$f25a2fc72690b780b2a14e140ef6a9e0:iloveyou
```

```
C:\Users\Aleksa\Desktop\john-1.9.0-jumbo-1-win64\run>john -w:password.lst --format=raw-MD5 -rules crack-these-please.txt.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
No password hashes left to crack (see FAQ)
```