Domača naloga 3 iz Teorije kodiranja in kriptografije

Domačo nalogo rešujte samostojno. Tokrat je cilj naloge objaviti blok teksta na spletni učilnici. Kljub temu je potrebno oddati dokument s kodo preko spletne učilnice. Poročilo lahko podate kot komentarje v kodi ali pa kot ločen dokument. Priporočeno in zaželeno je, da za programski jezik uporabite Python. V kolikor želite uporabiti kak drug jezik, najprej pišite asistentu za potrditev. Rok za oddajo je 19.5.2020. Datoteke pred oddajo združite v eno datoteko (zip, rar,...) z vašim imenom in vpisno v imenu, recimo *tilen_marc_23424123745.zip*. Ni potrebno implementirati vse iz nič, uporabite obstoječe knjižnice.

Iskanje trkov, podpisovanje in blockchain
Osnovna ideja blockchaina je decentralizirano ustvarjanje zaporedja blokov, ki vsebujejo informacije (transakcije, pogodbe, itd.), o katerih se sodelujoči strinjajo. V tej nalogi bomo ustvarili tako zaporedje blokov, ki bodo vsebovali vaše rešitve naloge.

- **Iskanje kvazi-trkov SHA-1:** Najdite dve (ne predolgi) besedi, ki ju SHA-1 funkcija preslika v niza, ki se ujemata v prvih 44 bitih (ekvivalentno v prvih 11 znakih v šestnajstiškem sistemu). Opomba: v Pythonu najdete SHA-1 v knjižnici *hashlib*.

- **Podpis vaše rešitve:** Vaše besedilo naj bosta besedi iz prejšnje naloge ločeni s presledkom. Uporabite SHA-1 funkcijo na besedilu in dobljeni rezultat spremenite v število. Generirajte svoj javni (p, q, α, β) in zasebni ključ (a) za DSA podpis. Za parametre DSA poglejte prosojnice na učilnici. Podpišite rezultat prejšnje naloge.

- **Blockchain:** Objavite svoje rezultate na spletni učilnici v blockchain obliki. Na učilnici najdete Blockchain povezavo, ki vas privede na dokument, ki ga lahko urejate. Na začetku dokumenta objavite svoj javni ključ skupaj s svojo vpisno številko (lahko tudi z imenom, če menite, da to ne posega v vašo zasebnost). Nato dodajte nov blok s svojo rešitvijo na konec dokumenta. To storite tako, da dodate 5 novih vrstic:

  - Prva vrstica vsebuje rezultat prve naloge (torej dve besedi ločeni s presledkom) in njihov hash kot število (to lahko v Pythonu storite tako, da pokličete *int(x, 16)*, kjer je x hash v heksagonalni obliki).
  - Druga vrsica vsebuje vašo identiteto in podpis prejšnje rešitve (γ, δ).
  - Tretja vrstica vsebuje hash (peto vrstico) prejšnjega bloka (zato ime blockchain – vaše rešitve bodo povezane v verigo blokov, ki se je ne da popravljati sredi verige).
  - Četrta vrstica vsebuje poljuben tekst.
  - Peta vrstica vsebuje hash vrednost (funkcije SHA-1, v heksagonalni obliki) prvih štirih vrstic (vrstice sestavite v en niz, v katerem so vrstice ločene s znakom $\backslash n$).

  Nov blok je veljaven, če se njegova hash vrednost (v heksagonalnem zapisu) začne s 7 ničlami (ekvivalentno je prvih 28 bitov enakih nič). Da lahko to dosežete spreminjajte četrto vrstico, dokler hash vrednost ni take oblike. Iskanje slednjega bi moralo v Python3 trajati nekaj minut, torej za tvorjenje novega bloka potrebujete nekaj računanja. Seveda je blok veljaven, samo če je v predpisani obliki.

  Ko ustvarite nov blok, morajo biti vsi predhodni bloki veljavni. Če niso, se skličite (tretja vrstica) na zadnji veljaven blok. Če bloki na katere se sklicujete niso veljavni, tudi vaš blok ni veljaven. V spletnem dokumentu ne brišite neveljavnih blokov, prva dva bloka sta že ustvarjena. Vsak blok naj vsebuje drugačen kvazi-trk. Če ne najdete trka iz prve naloge in bi vseeno dodali blok, v prvo vrstico napišite *brez trka*. Če nimate podpisa v drugo vrstico napišite svojo identiteto in *brez podpisa*.

Ideja naloge je, da ustvarimo blockchain verigo, ki omogoči dve stvari:

- Vi oddate svoje rešitve, in je za nazaj ne morete spreminjati.

- Decentralizirano preverimo rešitve drugih: vi se odločite, da boste verigo nadaljevali iz prejšnjega bloka, torej se strinjate, da so prejšnji bloki v redu. Blockchain nima zunanje avtoritete; če se tvorci blokov strinjajo, da je vse v redu, potem nihče ne more tega spremeniti.

Ko imate napisan algoritem za tvorjenje blokov, lahko (ob različnih časih) dodate več blokov, da bomo imeli daljši blockchain in bo bolj zanimivo.