Raziskovalne naloge za dijake

Varnost gesel

Nahajamo se na pragu vsesplošnega komuniciranja in e-trgovanja na Internetu, preko katerega so dostopne številne podatkovne baze. Vlade, industrija ter posamezniki, vsi hranijo informacije v digitalni obliki. Z razvojem telekomunikacij, računalniških omrežij in obdelovanja informacij pa je precej lažje prestreči in spremeniti digitalno informacijo kot pa njenega papirnega predhodnika. Zato so se povečale zahteve po varnosti. Želimo preprečiti nepooblaščeno uporabo digitalnih podatkov ali sistemov. Med preventivnimi ukrepi, ki so na voljo danes, nudi pravilno implementirana in uporabljana kriptografija največjo stopnjo varnosti glede na svojo prilagodljivost digitalnim medijem. To je veda, ki nam ponuja konkretne rešitve za varnost in zaščito na pravkar omenjenih področjih, ter s tem predstavlja osnovo informacijske družbe (cilji: zasebnost, celovitost podatkov, overjanje/podpisovanje, digitalni denar, e-volitve in drugi kriptografski protokoli).

Dijak naj sestavi program, ki nam pove, kako varno je naše geslo, pri tem pa morda niti ni nujno, da geslo izdamo. Za to nalogo bi se bilo dobro spoznati z zgoščevalnimi funkcijami in njihovimi lastnostmi. Pripomoček bomo vgradili v *Kriptogram*, kriptoportal za popularizacijo kriptografije (http://lkrv.fri.uni-lj.si/crypto-portal) in bo tako dostopen vsem.

Delo bo potekalo v jeziku Python in JavaScript. Osnove področja vam bomo predstavili in vas uvedli v delo sodelavci Laboratorija za kriptografijo in računalniško varnost, Fakultete za računalništvo in informatiko Univerze v Ljubljani. V laboratoriju so voljo strežniki ter tablice za poskuse in testiranje doma.

Mentorji: prof. dr. Aleksandar Jurišić, dr. Aljaž Zalar, dr. Janoš Vidali Univerza v Ljubljani, Fakulteta za računalništvo in informatiko,
E-Pošta: aj@fri.uni-lj.si, ajurisic@valjhun.fmf.uni-lj.si, aljaz.zalar@@fri.uni-lj.si

Klasične šifre

Nahajamo se na pragu vsesplošnega komuniciranja in e-trgovanja na Internetu, preko katerega so dostopne številne podatkovne baze. Vlade, industrija ter posamezniki, vsi hranijo informacije v digitalni obliki. Z razvojem telekomunikacij, računalniških omrežij in obdelovanja informacij pa je precej lažje prestreči in spremeniti digitalno informacijo kot pa njenega papirnega predhodnika. Zato so se povečale zahteve po varnosti. Želimo preprečiti nepooblaščeno uporabo digitalnih podatkov ali sistemov. Med preventivnimi ukrepi, ki so na voljo danes, nudi pravilno implementirana in uporabljana kriptografija največjo stopnjo varnosti glede na svojo prilagodljivost digitalnim medijem. To je veda, ki nam ponuja konkretne rešitve za varnost in zaščito na pravkar omenjenih področjih, ter s tem predstavlja osnovo informacijske družbe (cilji: zasebnost, celovitost podatkov, overjanje/podpisovanje, digitalni denar, e-volitve in drugi kriptografski protokoli).

Raziskovalne naloge za dijake

Med najbolj osnovne šifre spadajo:

- premešalka (oz. transpozicijska šifra),
- zamenjalna šifra (oz. substitucijska šifra),
- Viegenerjeva šifra in
- metoda s kodnimi knjigami.

Dijak naj se spozna z eno od zgornjih šifer in sestavi program za njeno sestavljanje oz. razbijanje z računalnikom. Pripomoček bomo vgradili v Kriptogram, kriptoportal za popularizacijo kriptografije (http://lkrv.fri.uni-lj.si/crypto-portal) in bo tako dostopen vsem.

Delo bo potekalo v jeziku Python in JavaScript. Osnove področja vam bomo predstavili in vas uvedli v delo sodelavci Laboratorija za kriptografijo in računalniško varnost, Fakultete za računalništvo in informatiko Univerze v Ljubljani. V laboratoriju so voljo strežniki ter tablice za poskuse in testiranje doma.

Mentorji: prof. dr. Aleksandar Jurišić, dr. Aljaž Zalar, dr. Janoš Vidali Univerza v Ljubljani, Fakulteta za računalništvo in informatiko,
E-Pošta: aj@fri.uni-lj.si, ajurisic@valjhun.fmf.uni-lj.si, aljaz.zalar@@fri.uni-lj.si

Srednji napadalec v kriptografiji

Nahajamo se na pragu vsesplošnega komuniciranja in e-trgovanja na Internetu, preko katerega so dostopne številne podatkovne baze. Vlade, industrija ter posamezniki, vsi hranijo informacije v digitalni obliki. Z razvojem telekomunikacij, računalniških omrežij in obdelovanja informacij pa je precej lažje prestreči in spremeniti digitalno informacijo kot pa njenega papirnega predhodnika. Zato so se povečale zahteve po varnosti. Želimo preprečiti nepooblaščeno uporabo digitalnih podatkov ali sistemov. Med preventivnimi ukrepi, ki so na voljo danes, nudi pravilno implementirana in uporabljana kriptografija največjo stopnjo varnosti glede na svojo prilagodljivost digitalnim medijem. To je veda, ki nam ponuja konkretne rešitve za varnost in zaščito na pravkar omenjenih področjih, ter s tem predstavlja osnovo informacijske družbe (cilji: zasebnost, celovitost podatkov, overjanje/podpisovanje, digitalni denar, e-volitve in drugi kriptografski protokoli).

Čeprav gre pri srednjem napadalcu za kriptografski koncept, se ga da opisati na poljuden način. Premožna gospa želi najti pomoč pri pospravljanju hiše in v časopisu objavi oglas, da rabi pomoč. Ko se javi primerna oseba, jo gospa vpraša po priporočilih, da preveri njene izkušnje in zanesljivost. Kakšne so slabosti takšnega preverjanja?

Tatica najame lepo hišo ali pa počaka, da gredo kakšni sosedi na dopust, njej pa pustijo ključe zaradi zalivanja rož. Tik pred tem sama objavi podoben oglas in opravi nekaj pogovorov pri katerih se izdaja za lastnico hiše, čeprav gre v resnici za staro znanko policije. Tako pridobljena priporočila uporabi sama in si z njimi najde zaposlitev pomočnice v bogati hiši. Službo je dobila z dobrimi priporočili – pa saj so vendar prava, čeprav niso njena – in

nato odnese iz hiše vso zlatnino in ostale vrednosti.

Kaj se je zgodilo v zgornjem primeru? Navidezna gospa pomočnica se je postavila na sredino komunikacije med pravo pomočnico ter pravo gospo in se predstavila vsaki kot tista druga. Pomočnica pošlje priporočila nekomu, ki ni prava gospa. Prava gospa preveri priporočila, ne da bi preverila, da v resnici ne pripadajo lažni pomočnici.

Dijak naj sestavi igro, v kateri na različne načine pride do izraza zgoraj opisan napad. Vgradili jo bomo v Kriptogram, kriptoportal za popularizacijo kriptografije (http://lkrv.fri.uni-lj.si/crypto-portal) in bo tako dostopen vsem.

Delo bo potekalo v jeziku Python in JavaScript. Osnove področja vam bomo predstavili in vas uvedli v delo sodelavci Laboratorija za kriptografijo in računalniško varnost, Fakultete za računalništvo in informatiko Univerze v Ljubljani. V laboratoriju so voljo strežniki ter tablice za poskuse in testiranje doma.

Mentorji: prof. dr. Aleksandar Jurišić, dr. Aljaž Zalar, dr. Janoš Vidali Univerza v Ljubljani, Fakulteta za računalništvo in informatiko,
E-Pošta: aj@fri.uni-lj.si, ajurisic@valjhun.fmf.uni-lj.si, aljaz.zalar@@fri.uni-lj.si

Vizualna kriptografija

Nahajamo se na pragu vsesplošnega komuniciranja in e-trgovanja na Internetu, preko katerega so dostopne številne podatkovne baze. Vlade, industrija ter posamezniki, vsi hranijo informacije v digitalni obliki. Z razvojem telekomunikacij, računalniških omrežij in obdelovanja informacij pa je precej lažje prestreči in spremeniti digitalno informacijo kot pa njenega papirnega predhodnika. Zato so se povečale zahteve po varnosti. Želimo preprečiti nepooblaščeno uporabo digitalnih podatkov ali sistemov. Med preventivnimi ukrepi, ki so na voljo danes, nudi pravilno implementirana in uporabljana kriptografija največjo stopnjo varnosti glede na svojo prilagodljivost digitalnim medijem. To je veda, ki nam ponuja konkretne rešitve za varnost in zaščito na pravkar omenjenih področjih, ter s tem predstavlja osnovo informacijske družbe (cilji: zasebnost, celovitost podatkov, overjanje/podpisovanje, digitalni denar, e-volitve in drugi kriptografski protokoli).

Dijak naj preuči, kako razdeliti barvno sliko na dva dela, da na vsakem od njiju ne bo prav nič razvidno, ko pa ju postavimo skupaj (tako da se prekrivata), pa prakticno vse. Pripomoček bomo vgradili v Kriptogram, kriptoportal za popularizacijo kriptografije (http://lkrv.fri.uni-lj.si/crypto-portal) in bo tako dostopen vsem.

Delo bo potekalo v jeziku Python in JavaScript. Osnove področja vam bomo predstavili in vas uvedli v delo sodelavci Laboratorija za kriptografijo in računalniško varnost, Fakultete za računalništvo in informatiko Univerze v Ljubljani. V laboratoriju so voljo strežniki ter tablice za poskuse in testiranje doma.

Raziskovalne naloge za dijake

Mentorji: prof. dr. Aleksandar Jurišić, dr. Aljaž Zalar, dr. Janoš Vidali Univerza v Ljubljani, Fakulteta za računalništvo in informatiko,
E-Pošta: aj@fri.uni-lj.si, ajurisic@valjhun.fmf.uni-lj.si, aljaz.zalar@@fri.uni-lj.si

Umetna inteligenca in vejice

Področje umetne inteligence je v zadnjem času doseglo velik napredek pri reševanju prej nerešljivih problemov pri računalniškem vidu (npr. prepoznavanje obrazov je že na nivoju ljudi), igranju iger (nedavno je program premagal človeškega prvaka v igri Go) in razumevanju naravnega jezika (odlično strojno razpoznavanje govora in vse boljši rezultati strojnega prevajanja). Ti uspehi so večinoma rezultat napredka na področju globokih nevronskih mrež. Umetne nevronske mreže so sestavljene iz velike zbirke povezanih preprostih računskih enot, imenovanih umetni nevroni, ki ustrezajo nevronom v možganih. V zadnjem času lahko raziskovalci v nevronske mreže učinkovito dodajajo vse več plasti »nevronov«. Tako imenovana globoka omrežja s številnimi sloji nevronov zahtevajo za uspešno učenje velike zbirke rešenih primerov in hitre vzporedne računalnike. Danes imamo na razpolago oboje in lahko rešujemo mnogo večje in težje probleme kot v preteklosti.

Ko se ljudje učimo jezika, začenjamo z besedami: poskušamo razumeti njihov pomen, jih povezujemo s podobnimi besedami in razvijamo občutek kontekstualne primernosti besede. Postopno si gradimo besednjak, združujemo besede v manjše stavke in se učimo slovnice in strukture jezika. Končno smo zmožni izraziti zapletene misli. Razumevanje naravnega jezika iz besedil z globokimi nevronskimi mrežami posnema ljudi. Zaporedje mrežnih slojev postopno gradi pomensko predstavitev besedila: začne z znaki ali besedami in skozi sloje napreduje v vse bolj abstraktno predstavitev pomena.

Napake pri postavljanju vejice so najpogostejše napake pri pisanju v slovenščini, kjer je vejica močno povezana s skladnjo. Strukturi slovenščine prilagojene globoke nevronske mreže bomo uporabili za izdelavo pripomočka za postavljanje vejice v slovenščini. Kot množico podatkov, na kateri se bomo naučili pravilne rabe vejice, bomo uporabili množico zanesljivih in lektoriranih besedil iz velike zbirke slovenskih besedil *Gigafida*. Pripomoček bomo vgradili v orodje *LanguageTool* in bo tako dostopen vsem, ki uporabljajo prostodostopno zbirko orodij *LibreOffice*.

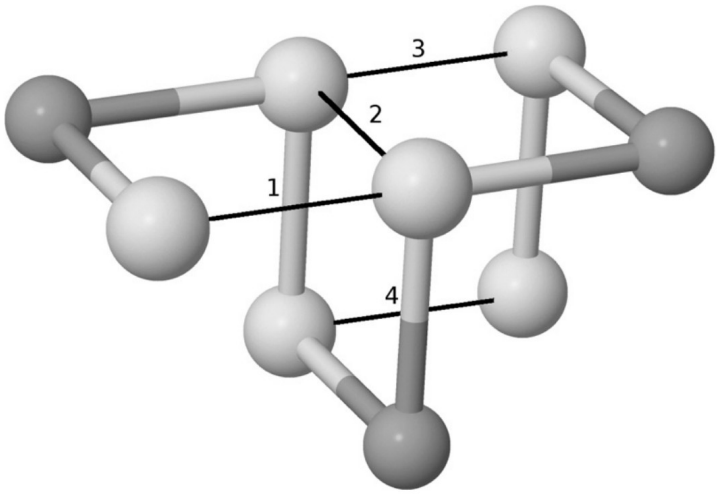
Delo bo potekalo v jeziku python in s knjižnico *Keras*. Osnove področja vam bomo predstavili in vas uvedli v delo sodelavci Laboratorija za kognitivno modeliranje Fakultete za računalništvo in informatiko Univerze v Ljubljani. V laboratoriju so voljo GPU strežniki za učenje globokih nevronskih mrež iz velikih zbirk besedi in kartica Nvidia Titan X za poskuse doma.

Mentor: prof. dr. Marko Robnik-Šikonja, Univerza v Ljubljani, Fakulteta za računalništvo in informatiko
E-Pošta: marko.robnik@fri.uni-lj.si

Zvijanje proteinov

Zvijanje proteinov je eden od največjih izzivov stoletja. Zaradi tega privablja raziskovalce iz različnih področij. Na področju računalništva raziskovalci izdelujejo algoritme, ki simulirajo zvijanje proteinov s pomočjo računalnika in tako napovedujejo nativno stanje proteina. Proteini so sestavljeni iz aminokislin in nativno stanje predstavlja tisto obliko oz. postavitev aminokislin v prostoru, ko protein izvaja svojo biološko funkcijo oz. ima najmanjšo energijo. V nasprotnem primeru lahko povzroča različne bolezni.

V okviru te naloge izdelajte program, ki bo uporabil poenostavljen model HP in poskušal poiskati čim boljšo postavitev aminokislin v 3D prostoru za podano zaporedje aminokislin. Zaporedje aminokislin je sestavljena iz črk. V primeru modela HP so aminokisline razdeljene v dve skupini H (hidrofobne) in P (hidrofilen). Podano zaporedje predstavlja povezano verigo aminokislin, ki jo je potrebno postaviti v kubično mrežo na tak način, da je njena energija čim manjša. Pri tem je potrebno upoštevati, da lahko eno aminokislino postavimo le v eno vozlišče kubične mreže. Energija pa predstavlja število hidrofobnih povezav med dvema aminokislinama, ki nista sosednji. Da dobimo končno vrednost energije, dobljeno število hidrofobnih povezav pomnožimo z -1. Npr. zaporedje HPHHPHPHH lahko postavimo v kubično mrežo tako, da zasede naslednja vozlišča: {(0, 0, 0), (0, 0, −1), (1, 0, −1),(1, −1, −1), (1, −1, 0), (1, 0, 0), (2, 0, 0), (2, 0, −1), (2, −1, −1)} in je prikazana na sliki. Vidimo, da so hidrofobne aminokisline predstavljene s temnejšimi in hidrofilne s svetlejšimi kroglicami. Na osnovi teh informacij lahko ugotovimo, da imamo 4 hidrofobnih povezav, kar pomeni, da je energija te postavitve enaka -4.



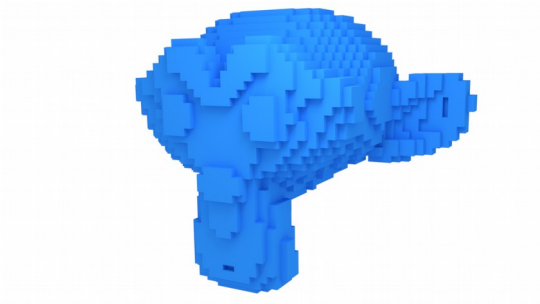
Torej cilj naloge je izdelati program, ki prejme zaporedje aminokislin modela HP in poskuša poiskati najboljšo možno njihovo postavitev znotraj kubične mreže. Boljša postavitev, je tista, ki ima več hidrofobnih povezav oz. manjšo energijo.

Mentor: Borko Bošković, Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko
E-Pošta: borko.boskovic@um.si

Predstavitev 3D objektov z verižnimi kodami in osmiškimi drevesi

Štiriško drevo in verižna koda sta dva izmed načinov opisa rasteriziranih 2D objektov. Medtem ko z verižnimi kodami opišemo obod objekta s pomikanjem po njegovem zunanjem robu v 2D rastrski mreži, s štiriškimi drevesi opišemo območja, ki jih prekriva notranjost objekta. Obe metodi je možno razširiti v 3D tako, da z verižnimi kodami opišemo lupino objekta po rezinah v izbrani koordinatni smeri, namesto štiriških dreves pa uporabimo osmiška drevesa. Pri tem je potrebno upoštevati možnost pojavitve lukenj ali nepovezanih območij v posameznih 2D rezinah.

V okviru naloge se implementira predstavitev vokseliziranih 3D objektov z verižnimi kodami in osmiškimi drevesi ter izvede primerjava njihove prostorske in časovne učinkovitosti.



Mentor: Damjan Strnad, Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko
E-Pošta: damjan.strnad@um.si

Kroglice, zaporniki in konsenz

Predstavljajmo si, da je več divizij bizantinske vojske obkolilo sovražno mesto in vsako divizijo vodi svoj general. Slednji lahko med seboj komunicirajo le preko kurirja. Sprva si sovražnika dobro ogledajo, nato pa morajo narediti skupen načrt za napad. Dodatni problem je, da so med generali lahko tudi izdajalci, ki želijo preprečiti zvestim generalom, da bi dosegli enoten dogovor. Za potrebe generalov torej potrebujemo poseben algoritem, ki poskrbi za naslednja dva pogoja (recimo jima A in B).

A: Vsi zvesti generali se po določenem usklajevalnem času odločijo za isti načrt.
Zvesti generali se bodo vsi odločili na podlagi rezultatov algoritma, izdajalci pa se bodo odločili po svoje. Pri tem mora algoritem zagotoviti pogoj A, ne glede na dejanja izdajalcev. Ker pa ni dovolj, da se zvesti generali le strinjajo med sabo, ampak je pomembno tudi to, da je načrt za katerega se odločijo smiseln, je potrebno zagotoviti tudi to, da:

B: majhna številka izdajalcev ne more povzročiti, da bi zvesti generali prevzeli slab načrt.

Zgornji *Problem Bizantinskih generalov* je namenoma zastavljen zelo široko in očitno je, da bi za natančno matematično formulacijo potrebovali vsaj definicijo pojmov, kaj je slab načrt, kaj pomeni majhna številka izdajalcev, na kakšen način poteka komunikacija preko kurirjev. Spodaj je naveden na prvi pogled popolnoma drugačen problem, ki pa je v svojem bistvu zelo podoben zgornjemu:

V zloglasnem zaporu Alcatraz so ujetniki ves čas zaprti v svoji celici, brez medsebojne komunikacije. Nekega dne se po zvočniku zasliši naslednje obvestilo glavnega nadzornika:

> Spoštovani zaporniki!
>
> Od danes naprej bomo v zaporu igrali ti. »igro devetih barv«. Za naš zapor sem pripravil veliko vrečo kroglic v devetih različnih barvah, ki so v tem trenutku v barvnem razmerju 2:1:1:1:1:1:1:1:1 – prve barve je torej na začetku malo več, vendar ne veste katere.
>
> Vsako uro bo v vašo celico paznik prinesel to vrečo, pri čemer lahko vsakič na slepo izvlečete novo kroglico, jo (po dogovoru s paznikom) zamenjate s poljubno drugo barvo, ter jo nato vrnete nazaj v vrečo.
>
> Po nekaj dneh bo vsak od vas poskusil uganiti začetno dominantno barvo. Tistim ki uspe, bodo izpuščeni.

Izkaže se, da lahko tudi v primeru ko je zapor še tako velik, po nekaj dnevih vsi ujetniki z visoko verjetnostjo uganejo pravo barvo, vendar je pot do rešitve vse prej kot majhen matematični trik. Kljub vsemu je družina teh in podobnih problemov izjemnega pomena v sodobnem času, uporablja se že pri sinhronizaciji vsakega več-jedrnega procesorja, v porazdeljenih podatkovnih bazah, doseganju skupinskih konsenzov, ter nenazadnje v tehnologiji veriženja blokov (*Blockchain*), na kateri temelji večina poznanih kriptovalut.

Pri igranju z omenjenimi problemi bomo spoznali osnove verjetnosti, tj. veja matematike ki preučuje verjetnost, da se zgodi naključni dogodek. Pri računanju verjetnosti nam pogosto pomaga kombinatorika. Za lažjo analizo se bomo morali poglobiti med drugim tudi v teorijo grafov. Ta zavzema koristne tehnike za reševanje različnih optimizacijskih problemov, ter pogosto nudi nov pogled na izbrani problem. Z grafi lahko opazujemo povezanost stvari med seboj in tudi interakcijo med njimi. Velik plus za spopad s problemom pa je seveda poznavanje osnov programiranja.

Mentor: dr. Matjaž Krnc, Univerza na Primorskem, Fakulteta za matematiko, naravoslovje in informacijsko tehnologijo
E-Pošta: matjaz.krnc@upr.si