Povzetek projekta Študentski inovativni projekti za družbeno korist 2016-2020 za študijski leti 2018/2019 in 2019/2020 2. odpiranje za namen objave in predstavitve na spletni strani sklada

1. Polni naslov projekta: Interaktivna e-knjiga Kriptografija, 2. del.

- **V katero področje na prvi klasifikacijski ravni KLASIUS-P-16 se uvršča projekt glede na vsebinsko zasnovo** (neustrezno področje izbrišite)**:**

5 – **Naravoslovje, matematika in statistika**

2. V sodelovanju z: (navede se univerza oz. samostojni visokošolski zavod, ki je prijavil projekt in članica, ki je nosilka projekta ter partner/ja – podjetje/ji oz. organizacija, ki je/sta bilo/i vključeno/i v projekt)

Univerza v Ljubljani, Fakulteta za računalništvo in informatiko in Društvo kriptologov Slovenije

3. Besedilo:

- Opredelite problem, ki se je razreševal tekom izvajanja projekta

Cilj projekta je bil z interaktivnimi metodami in problemsko motivacijo bralca širiti znanje kriptografije prek vabljivih in poenostavljenih vsebin, ki pri uporabniku sprožijo vedoželjnost in ga motivirajo za uporabo in nadaljnje osvajanje novih konceptov. V prvih dveh predhodnikih tega projekta smo razvijali portal Kriptogram, kjer so predstavljene kriptografske tematike, kot so klasične šifre, vizualne sheme za deljenje skrivnosti, varna gesla, časovni žigi, itd. V zadnjem projektu (ŠIPK) pa smo kriptografske vsebine predstavili v obliki interaktivne e-knjige, a smo pokrili poleg osnovne aritmetike šele tri večja področja (ključi, zgoščevanje in šifre). V 2. delu so bile na vrsti kode, kriptografski protokoli in digitalni podpisi. Možno pa je tudi nadaljevanje (3. del).

Naša e-knjiga bo še posebej namenjena izobraževanju in ozaveščanju mladih do 25 let, saj so ti najpogostejši uporabniki sodobnih medijev in bodo najbolj občutili problem računalniške varnosti v prihodnosti. Predstavlja samostojno učno gradivo, njene prednosti pred običajno tiskano knjigo pa so v dostopnosti (ni omejitev glede naklade), prenosljivosti, prilagodljivosti bralcu, povečevanju kreativnosti bralca, odziva avtorja na informacije uporabnikov in prijaznosti do okolja.

Glavni problem, na katerega smo se osredotočili na projektu, je nov način za dvigovanje zavedanja in znanja o problematiki varne komunikacije prek nezavarovanih omrežij in varne uporabe moderne tehnološke opreme (čeprav je morda še večjega pomena povsem nova oblika interaktivnega prenašanja znanja, ki deluje tudi v "off-line" načinu, tj. brez neposredne povezave s strežnikom - kot zgled drugim področjem).

V prejšnjem projektu smo na poljuden način predstavili kriptografske vsebine, kot so klasično šifriranje, zgoščevalne funkcije in sestavljanje močnih gesel ali varnih ključev. V sedanjem projektu pa smo se osredotočili na kode za odpravljanje napak (in s tem večjo zanesljivost delovanja računalniških sistemov), digitalno podpisovanje in infrastruktura javnih ključev ter moderni kriptografski protokoli (npr. za verodostojnost, pooblaščanje,...). Kot smo že omenili, je ravno pomanjkanje algoritmičnega razmišljanja in matematičnega znanja velikokrat glavni problem, da poljudni uporabnik ne more priti do dovolj poglobljenega razumevanja. Oba je potrebno razvijati še naprej na čim več primerih.

- Opišite potek reševanja problema oz. kratek povzetek projekta

V 1. delu knjige (predhodni ŠIPK projekt) smo se odločili za naslednji pristop. Besedilo je oblikovano v jeziku RMarkdown (z uporabo okolja RStudio), medtem ko so interakcije napisane v jeziku HTML/JavaScript. Za razvoj in sodelovanje (10 študentov in mentorji) smo uporabili storitev GitLab za gostovanje Git repozitorijev in njihovo upravljanje. Tehnologija se je izkazala za zelo uporabno.

Na začetku projekta smo pripravili uvodni sestanek na sedežu Društva kriptologov Slovenije (DKS). Pedagoška mentorja in strokovni sodelavec smo udeležencem predstavili zasnovo projekta (namen, cilje, potek). Organizirali smo se v skupine, vsaki določili naloge in zadolžitve pri projektu, ter se dogovorili za termin tedenskih srečanj na sedežu društva.

Prvi del projekta je bil namenjen preučevanju literature in internetnih gradiv. Prek delavnic, ki smo jih organizirali na sedežu društva DKS in na Fakulteti za računalništvo in informatiko (FRI), smo mentorji študentom predstavili glavne kriptografske koncepte in njihovo uporabo. Naloga študentov v tem delu je bila pridobitev dobrih osnovnih znanj na področju kriptografije in iskanja novih idej za njihov interaktiven prenos naprej širšemu krogu uporabnikov.

V drugem delu projekta smo določili ogrodje 2. dela e-knjige. Dogovorili smo se, katere naj bodo funkcionalnosti interakcij in katere vsebine naj bodo vključene. Poskrbeli smo za poenoten grafičen izgled različnih delov aplikacije. Strokovni sodelavec je s svojimi izkušnjami (še posebej praktičnimi primeri) pomagal pri pripravi izvedljivega načrta v danem časovnem okviru.

Tretji del tega projekta je bil namenjen pripravi strokovnih vsebin in implementaciji programske opreme. Pedagoška mentorja sta študentom nudila pomoč pri pripravi vsebin (svetovanje o primerni literaturi, izgledu vsebin, primerni zahtevnosti), pa tudi pri sami implementaciji. Dobivali smo se na skupnih sestankih in delali tudi individualno. Ves čas smo pregledovali združljivost vsebin različnih skupin v povezano celoto. Tekom projekta smo dodajali nove tematike.

V zadnjem delu projekta smo združili delo vseh skupin. Sledilo je testiranje, del časa pa smo namenili tudi dokumentaciji, saj samo na ta način lahko zagotovimo možnost nadaljnjega razvoja vsebin. Poudarek je bil na primerni grafični podobi in dobri uporabniški izkušnji.

Na zaključnem sestanku smo si ogledali končni izdelek, se dogovorili o kanalih za popularizacijo našega izdelka in se pogovorili o možnem nadaljnjem razvoju.

- Navedite in opišite rezultate projekta ter njihov doprinos k družbeni koristnosti

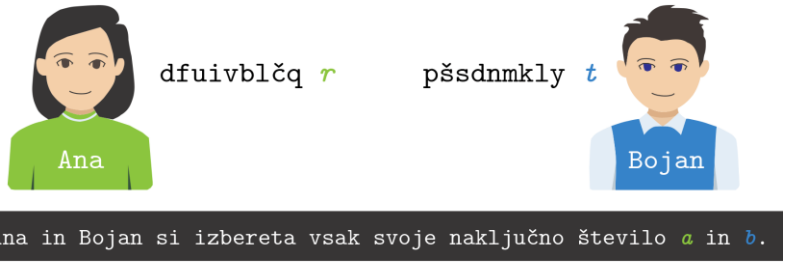
Cilj projekta je popularizacija kriptografije in računalniške varnosti. Rezultat projekta je 2. del interaktivne knjige, ki združuje dva najpopularnejša načina za pridobivanje informacij, to sta branje knjig v fizični obliki in brskanje po spletu. Interaktivno knjigo lahko uporabljamo na računalniku, tablici ali mobilni napravi, omogočena pa je tudi uporaba brez neprestane povezave s strežnikom. Poleg osnovne vsebine ima e-knjiga tudi interaktivni del, ki uporabniku omogoča testiranje in nadaljnji razvoj svojega znanja, uporabo pridobljenega znanja v nalogah ali pa samo igranje kriptografskih iger. S tem pridobimo teoretično znanje in ga utrjujemo na praktičnih primerih. Prednost e-knjige pred navadno je v njeni interaktivnosti, pred vsebinami na spletu pa to, da za uporabo ne potrebujemo povezave s strežnikom in najdemo vse informacije na enem mestu.

V e-knjigi smo razvili poglavja in interakcije za vse najpomembnejše koncepte kriptografije, v tem projektu pa pripravili dobro zasnovo in razvili nekaj novih konceptov. V 1. delu se že nahajajo poleg modularne aritmetike še poglavja o klasičnih šifrah, o varnih geslih in o zgoščevalnih funkcijah, v 2. delu pa smo predstavili kode, digitalne podpise in moderne kriptografske protokole. V prihodnosti želimo e-knjigo dopolniti še s konceptom digitalnega denarja, verigami blokov itd. Te tematike zahtevajo še več matematičnega predznanja (npr. končne obsege, eliptične krivulje itd). Nov pristop bo uporaben tudi pri drugih študijskih predmetih.

Dunajska cesta 20, 1000 Ljubljana t 01 434 10 81 e info@sklad-kadri.si www.srips-rs.si

4. Priloge:

- Slikovno gradivo: Priložite vsaj dve sliki npr. sliko končnega produkta, sliko študentov pri delu na projektu, sliko s sestankov ipd. Pri pošiljanju slik bodite pozorni, v kolikor gre za končni produkt, da bo zadoščeno zahtevam glede informiranja in obveščanja (ustrezni logotipi itd.).



Ana in Bojan si izbereta vsak svoje naključno število a in b.

gheriosdp ž xcnmklweh l as i sdioghcve v

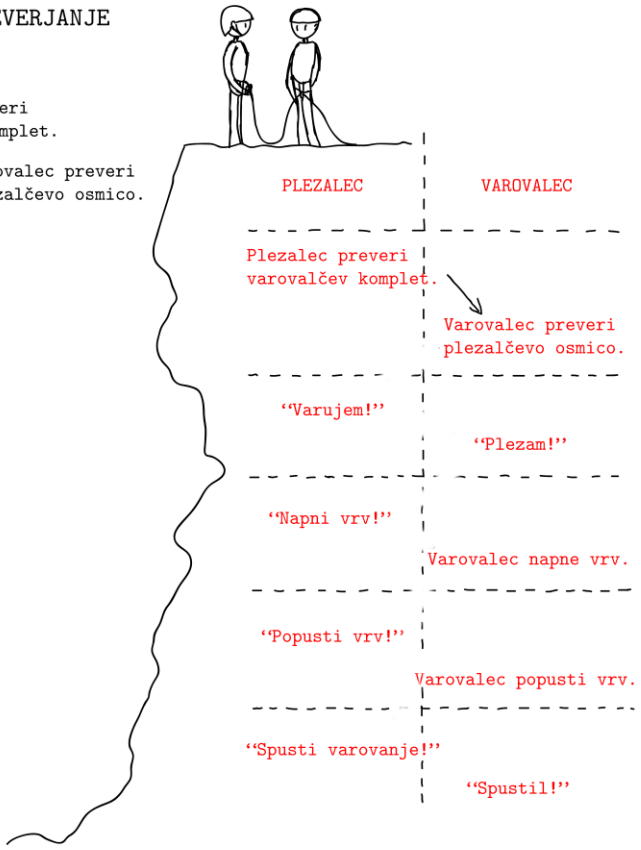
Ana in napadalec si izbereta naključni a in c.

Bojan in napadalec si izbereta naključni b in d.

Dunajska cesta 20, 1000 Ljubljana t 01 434 10 81 e info@sklad-kadri.si www.srips-rs.si

DVOJNO PREVERJANJE

1. Plezalec preveri varovalčev komplet.
2. Varovalec preveri plezalčevo osmico.



Dunajska cesta 20, 1000 Ljubljana t 01 434 10 81 e info@sklad-kadri.si www.srips-rs.si