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

1. Polni naslov projekta: Interaktivna e-knjiga Kriptografija (akronim eKripto)

- **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
6 – Informacijske in komunikacijske tehnologije, (IKT) tehnika

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
- Društvo kriptologov Slovenije

3. Besedilo:

- Opredelite problem, ki se je razreševal tekom izvajanja projekta

Moderna družba je vse bolj odvisna od računalnikov, interneta in pametnih naprav. Pri tem je varna uporaba teh sistemov ključnega pomena za uporabnike. V ta namen je vsaj osnovno znanje računalniške varnosti nepogrešljivo. Kriptografija je področje računalniške varnosti, ki se ukvarja z zagotavljanjem varne komunikacije dveh uporabnikov prek nezaščitnega kanala (npr. mobilni telefon, računalniško omrežje, pametna naprava), tako da nepooblaščena oseba ne razume vsebine sporočila in ga hkrati ne more niti spreminjati.

Glavni problem, na katerega smo se osredotočili na projektu, je dvig zavedanja in znanja o problematiki varne komunikacije prek nezavarovanih omrežij in varne uporabe moderne tehnološke opreme. Cilj projekta je bil širiti znanje kriptografije prek vabljivih vsebin, ki pri uporabniku sprožijo vedoželjnost po spoznavanju novih konceptov.

- Opišite potek reševanja problema oz. kratek povzetek projekta

V okviru projekta smo razvijali interaktivno e-knjige, katere vsebina so osnove kriptografije. Ekipo desetih študentov in treh mentorjev smo razdelili v več skupin, pri čemer je vsaka dobila nalogo napisati eno poglavje v e-knjigi, ki temelji na podajanju tematik prek interaktivnih aplikacij. Na rednih sestankih smo se dogovarjali o konkretnih vsebinah, ki naj bodo prisotne v e-knjigi in preizkušali razvite aplikacije. V zadnjem delu projekta smo delo vseh skupin poenotili, tako da smo poenotili izgled in uredili vrstni red vsebin. V e-knjigi uporabnik najde osnovne koncepte vseh tematik, nato pa lahko prek interakcije aktivno pridobi praktično znanje iz teh vsebin. Poleg tega ima možnost komentiranja in deljenja novih informacij s preostalimi uporabniki.

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

Razvita e-knjiga je še posebej namenjena izobraževanju 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.

Naša e-knjiga združuje dva najpopularnejša načina za pridobivanje informacij, to sta branje knjig v fizični obliki in brskanje po spletu. Knjigo lahko uporabljamo na računalniku, tablici ali mobilni napravi. Interaktivni del knjige uporabniku omogoča testiranje in utrjevanje znanja, uporabo znanja v nalogah ali pa samo igranje kriptografskih iger. S tem predstavljeno teoretično znanje utrdi na praktičnih primerih. Prednost naše e-knjige pred navadno je v njeni interaktivnosti, pred vsebinami na spletu pa to, da za uporabo ne potrebujemo povezave s strežnikom in vse informacije najdemo na enem mestu.

Še nekaj konkretnih vsebini v naši e-knjigi so klasične šifre, varna gesla, skrivanje šifer v sliko, digitalni podpisi, časovno žigosanje, moderni kriptografski protokoli (AES, RSA, koncept digitalnega denarja), matematične vsebine (modularna aritmetika, končni obsegi, itd.).

Prek aplikacije želimo uporabnikom olajšati način pridobitve znanja varne računalniške komunikacije, saj je ta danes ključnega pomena. Vse več sestankov in dogovorov se dogaja kar prek naprav. S tem populariziramo kriptografijo in predstavimo zapletene tematike na poljuden način, tako da uporabniki razumejo glavne koncepte in znanje lahko uporabljajo v vsakdanjem življenju. Mnogokrat zadošča že zavedanje določenega problema, s čimer preprečimo napake, ki bi jih lahko naredili.

Aplikacija pa omogoča tudi ogled istih vsebin iz različnih zornih kotov. Teoretične vsebine so podkrepljene z interaktivnimi v obliki različnih iger in ugank. S tem ima projekt učinek na širšo skupnost, ne le študente matematike in računalništva, saj na vabljiv način podaja informacije. Zahtevne strokovne vsebine v ozadju so skrite v uganke, tako da se uporabniki sploh ne zavedajo, da se seznanjajo z njimi. Naš namen je, da se ljudje začnejo zavedati, da sta tematiki, kot sta kakovost gesel in varna komunikacija, poglavitnega pomena v sodobnem svetu, kajti sicer lahko hitro zaidemo v težave kot tarča različnih sodobnih nepridipravov.

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.).

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

eKripto-knjiga

LKRV - FRI, UNI LJ

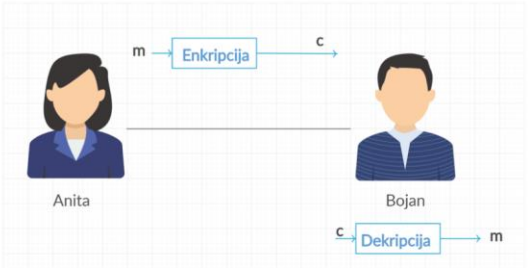
torek, 20. avgust, 2019

Uvod

Večina bralcev se je najbrž že srečala z besedo *kriptografija*, ne ve pa točno, kaj ta veda je. Na kratko povedano, gre za znanost o skrivnem pisanju in varnem dostopu do podatkov. Povedano natančneje, kriptografija poskuša omogočiti zasebnost. in še naprej zaupnost, avtentičnost, celovitost in preprečevanje zanikanja. V splošnem uporabljamo naslednja prostopa:

1. simetrična kriptografija,
2. kriptografija javnih ključev.

Glavna razlika med obema je v njunem načinu šifriranja in odšifriranja. Pustimo to za kasneje in razložimo najprej, kaj si lahko predstavljamo pod pojmom *kriptosistem*.



Obrazec za šifriranje

Vnesi čistopis za šifriranje:

To je eknjiga Kriptografija

Začni | Od začetka

Zs mh hnrmljč Ntlšzsjtčilmč

Za zgornji primer dobimo:

> žh mh lpho cd sryhgdwl ndu nrol vnulyqhjd, mh qdslvdo y šliudk, wm., v vsuhplqmdqmhp cdsruhgmd čun y dehfhgl, y ndwhul qrehqh ehvhgh ql prč xjrwrylwl.

Preverimo lahko tudi, če je rezultat odšifriranja enak začetnemu sporočilu.

Obrazec za odšifriranje

Vnesi tajnopis za odšifriranje:

Poglavje 1 Ključi

1.1 Gesla

Geslo je beseda ali znakovni niz, ki se uporablja za uporabnikov dokaz identitete ali dostopno soglasje za pridobitev dostopa do virov.

Uporaba gesel je starodavna. V preteklosti so stražarji v tiste, ki so želeli vstopiti v varovano območje, merili z orožjem, dokler le-ti niso povedali pravilnega gesla.

V sodobnem času so uporabniška imena in gesla običajen način identifikacije za dostop do zaščitenih računalniških operacijskih sistemov, mobilnih telefonov, TV sprejemnikov, ipd. Tipičen uporabnik računalnika ima gesla za veliko različnih namenov: prijavljanje v račune, pridobivanje e-pošte, dostop do aplikacij, baz podatkov, omrežij, spletnih mest in celo branje jutranjega časopisa na spletu. Kljub imenu ni potrebno, da so gesla dejanske besede; gesla, ki niso dejanske besede, je morda težje uganiti, kar je zaželena lastnost. Beseda geslo se včasih uporablja, kadar so skrivne informacije samo

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

je pri nas vedno 50 (kar označuje rojstvo v Sloveniji), sledijo še tri cifre, ki določajo zaporedno številko rojstva (pri tem se razlikuje med rojstvi otrok moškega in ženskega spola). Sledi še zadnja cifra, ki je v bistvu zgoščena vrednost vseh ostalih. Tukaj lahko poskusiš generirati svojo EMŠO številko, pa tudi tisto izmišljenih oseb. Poskusi pa odgovoriti na naslednja vprašanja:

1. Kako se spremeni EMŠO, če spremeniš ime?
2. Ali lahko imata dva občana isto EMŠO številko?
3. Kaj lahko sklepaš o imetniku dane EMŠO številke, če o njem veš samo EMŠO?

2.2.3 Številke plačilnih kartic

Tudi zadnja številka naših plačilnih kartic je zgoščena funkcija prvih petnajstih. Izračunamo jo s tako imenovanim Luthovim algoritmom, ki ima podoben postopek kot zgornja dva primera: ustrezno pomnožimo cifre kartice, jih seštejemo, na koncu pa izvedemo še neko celoštevilsko deljenje. Na spletu najdemo več takih aplikacij, ki ponaredijo izmišljene kartice (v bistvu izberejo skoraj naključno prvih 15 cifer in izračunajo na koncu še kontrolno vsoto).Postopek, s katerim bi lahko trivialno preverili, ali so take kartice resnične ali ne, ne obstaja; to pa omogoča razna protizakonita obnašanja (na primer lahko vsaki mesec generiramo izmišljeno kartico in tako koristimo "brezplačni mesec" na raznih spletnih straneh kot "Netflix". Ponovimo pa da je tako obnašanje protizakonito). Nekatere spletne strani odvzamejo iz računa 1 cent in ga takoj vrnejo z namenom preverjanja pristnosti kartice. Proti takemu sistemu za preverjanje kartic seveda spodnji postopek ni odporen.

Tudi s spodnjim pripomočkom lahko generiramo izmišljene kartice: vnesi prvih 15 cifer, dobil pa boš veljavno številko kartice!

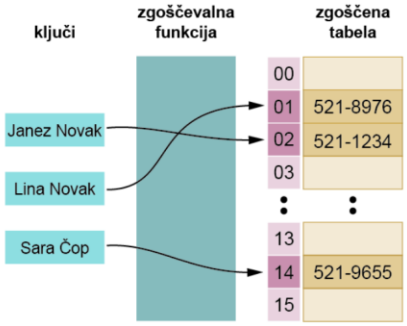
Zaključek

Iz zgoraj navedenih primerov bi moralo biti jasno, da osnovni podatki enolično določajo zgoščeno vrednost, obratno pa ne velja. Na primer, če se navežemo na zgornji primer ISBN-ja: obstaja namreč več milijonov knjig, vsaka ima enolično določeno ISBN kodo, z druge strani pa obstaja samo 11 zgoščenih vrednosti za podane osnovne podatke.

Podoben razmislek lahko uporabimo v računalništvu, tudi ko nas vsebina in naspoln pomen podatkov, ki prenašamo, sploh ne zanima. Naprimer, da želimo sporočilo dolgo 20 bitov zgostiti v vrednost dolgo 5 bitov. V takem primeru, možnih 1048576 (2^{20}) vhodnih vrednosti bo zgoščevalna funkcija razdelila v skupine, ki bodo imele isto zgoščeno vrednost; v povprečju bodo te skupine velike 32768 (2^{15}), osnovna želja pa je seveda, da so skupine čim bolj enakomerne. Trčenjem pa se seveda želimo izogniti.

2.4.2 Hashiranje gesel

Drugo področje, kjer uporabljamo zgoščevalne funkcije za zagotavljanje varnosti, je v hranjenju gesel v serverjih.



Osnovna ideja je, da v primeru, ko nekdo uspe iz kakršnegakoli razloga dobiti dostop do računalnika, kjer so shranjena gesla, le-ta ne uspe izluščiti gesel uporabnikov. Denimo konkreten primer: Facebook ima več kot dve milijardi uporabnikov. Vsak,ki želi vstopiti v svoj račun, mora dokazati svojo identiteto s tem, da vnese svoj e-mail in neko geslo. E-mail je v večini primerov javen, z druge strani pa je geslo nekaj, kar pozna samo uporabnik. Le-ta seveda hoče, da ostane njegovo geslo tajno (še posebej če rabi isto geslo za več spletnih strani). Recimo pa primer, da bi Facebook hranil gesla v čistopisu (npr geslo uporabnika je '12345' in je na serverju geslo shranjeno kot '12345'). Ko neki uporabnik želi vstopiti, sistem preveri, ali je vneseno geslo enako tistemu, ki je hranjeno v serverju. Taki sistem deluje v redu, dokler napadalec ne uspe vstopiti v računalnik, kjer so hranjena gesla in si tako brez težav prilasti gesla vseh uporabnikov. Seveda se skušamo izogibati takemu sistemu, žal pa je še vedno veliko takih spletnih strežnikov, ki hranijo gesla v čistopisu; nenazadnje nismo omenili takega velikana kot je Facebook zaman: ravno v prvih mesecih leta 2019 smo izvedeli, da je Facebook hranil gesla stotin milijonov uporabnikov v čistopisu, lastniki gesel pa so seveda bili v nevarnosti.

b. tablica za množenje.

Drugi tabeli pravimo *poštevanka* in se jo morajo drugošolci od nekdaj naučiti na pamet ter si jo zapomniti za celo življenje. Seveda si ni potrebno zapomniti vseh 100 zmnožkov; večkratniki števil 1 in 10 so otročje lahki, množenje z 2 ni nič težje kot seštevanje, vrstni red pri množenju ni prav nič pomemben (*zakon o zamenjavi* ali *komutativnost*) (tabela 2).

Tabela 2a

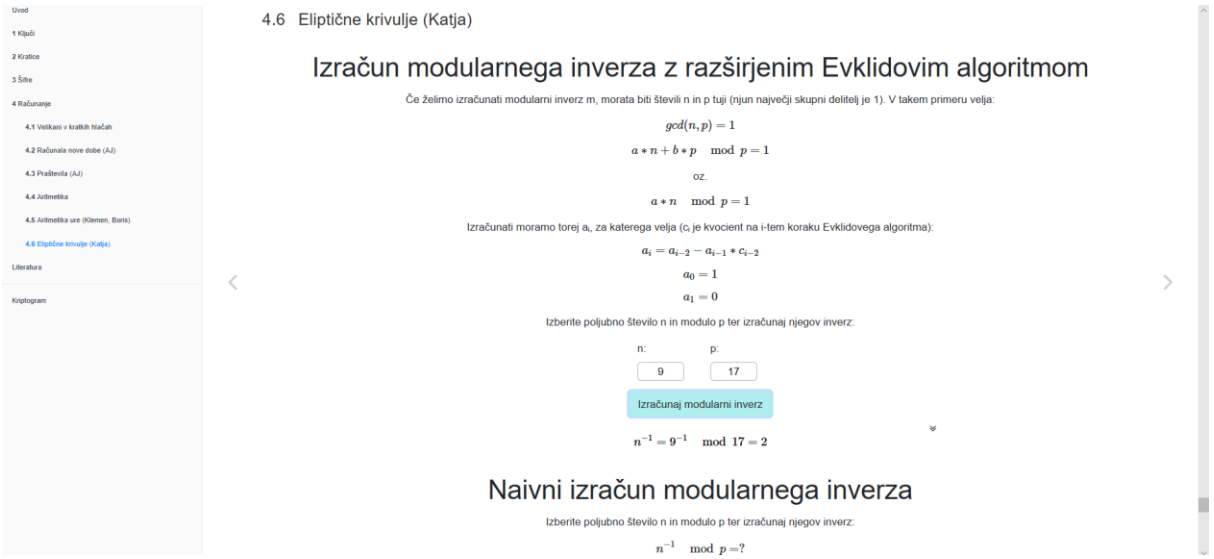
Velikost tabele: 15

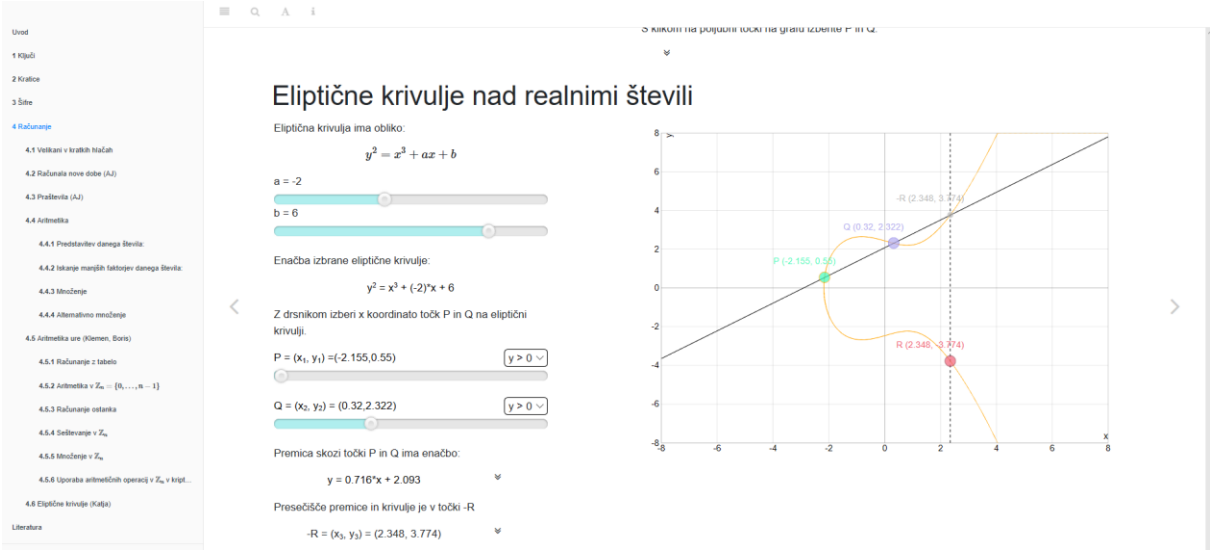
Baza: 12

Tabela za seštevanje

+	0	1	2	3	4	5	6	7	8	9	a	b	10	11	12
0	0	1	2	3	4	5	6	7	8	9	a	b	10	11	12
1	1	2	3	4	5	6	7	8	9	a	b	10	11	12	13
2	2	3	4	5	6	7	8	9	a	b	10	11	12	13	14
3	3	4	5	6	7	8	9	a	b	10	11	12	13	14	15
4	4	5	6	7	8	9	a	b	10	11	12	13	14	15	16
5	5	6	7	8	9	a	b	10	11	12	13	14	15	16	17
6	6	7	8	9	a	b	10	11	12	13	14	15	16	17	18
7	7	8	9	a	b	10	11	12	13	14	15	16	17	18	19
8	8	9	a	b	10	11	12	13	14	15	16	17	18	19	1a
9	9	a	b	10	11	12	13	14	15	16	17	18	19	1a	1b
a	a	b	10	11	12	13	14	15	16	17	18	19	1a	1b	20
b	b	10	11	12	13	14	15	16	17	18	19	1a	1b	20	21
10	10	11	12	13	14	15	16	17	18	19	1a	1b	20	21	22
11	11	12	13	14	15	16	17	18	19	1a	1b	20	21	22	23
12	12	13	14	15	16	17	18	19	1a	1b	20	21	22	23	24

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





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