Programsko sučelje za demonstraciju kriptografskih primitiva

Tehnička dokumentacija

Verzija 1.3

Studentski tim: Bojan Novković
Ninoslav Kukovačec
Ivan Vuković
Kristijan Palić

Nastavnik: prof. dr. sc. Marin Golub

Sadržaj

Tehnička dokumentacija

Tehnička dokumentacija

1. Uvod

Kriptografija je znanost koja se bavi logičkom promjenom podataka. Njen primarni cilj je zaštiti korisnike i njihove privatne datoteke ili poruke od napadača. Školski primjer koji zorno pokazuje što se tu zapravo događa je sljedeći. Neka postoje dvije osobe koje razmjenjuju podatke, Osoba1 i Osoba2, a neka Osoba3 bude nepoželjni promatrač koji se pokušava ubaciti u komunikacijski kanal i čitati sve poruke. Proces je sljedeći, Osoba1 napiše poruku koja je čitljiva njemu, ali se zatim kriptira i u takvom formatu se šalje Osobi2. Osoba2 prima kriptiranu poruku, koju program lokalno na njegovom računalu dekriptira i prikazuje u izvornom obliku. Pokuša li Osoba3 pročitati poruku tijekom njenog slanja, bit će u mogućnosti vidjeti samo niz naizgled nasumičnih bitova iz kojih on bez odgovarajućih informacija ne može nikako dobiti smisleni sadržaj. Tako načelno funkcionira kriptografija, no stvari su ipak malo kompleksnije, ali više o tome u poglavljima koji slijede.

Kriptografski algoritmi su od začetaka računarstva u samom centru istraživanja i konstantnog razvoja. Pojavom prvog modernog računala koje se uvlačilo u sve više kućanstava potreba za razvojem kriptografije rasla je svakim danom. Pogledamo li situaciju danas, gdje gotovo svi posjeduju pametni telefon i koriste barem jedan moderni alat za komunikaciju (a nerijetko i nekoliko njih) poput WhatsAppa, Facebookovog Messengera, Vibera, Skypea, Slacka, mailova i sl. Bez kriptografije, privatnost korisnika bilo kojeg od navedenih tehnologija bila bi nepostojeća. Uz malo znanja o internetskim protokolima koji se koriste, svatko bi mogao čitati sve. Naravno da je danas takav scenarij nezamisliv, no bez raznih kriptografskih algoritama to bi bila realnost.

Cilj ovog projekta je približiti funkcionalnost tih algoritama te pomoću jednostavnog grafičkog sučelja demonstrirati njihov rad.

2. Opis razvijenog proizvoda

Sučelje razvijenog programa sastoji se od četiri kartice, od kojih svaka predočava funkcionalnosti i način rada jedne vrste kriptografskih algoritama. Obrađeni su asimetrični i simetrični kriptografski algoritmi, te funkcije za hashiranje i digitalni potpis.

3. Tehničke značajke

U kriptografiji postoji nekoliko algoritama kriptiranja podataka. Mi smo u našem sučelju omogućili Asimetričan i Simetričan algoritam, Hash sažimanje i Digitalan potpis.

Asimetričan algoritam radi na principu javnog i tajnog ključa. Svaki sudionik u komunikaciji ima svoj javni i privatni ključ. Kako bi se sadržaj neke kriptirane poruke dekriptirao, potrebno je imati javni ključ primatelja. Pošiljatelj sadržaj poruke kriptira javnim ključem primatelja, a primatelj sadržaj dekriptira svojim privatnim ključem.

Simetričan algoritam koristi isti ključ za kriptiranje i dekriptiranje. U početku su algoritmi radili na način da se uzimao znak po znak, ili blok po blok podataka i kriptirali su se neovisno jedan o drugome. S vremenom je to postalo nedovoljno kompleksno pa su se uvele razne metode gdje idući kriptirani blok ovisi o prijašnjem bloku. Iako su simetrični algoritmi brzi i efikasni, najveći problem predstavlja dijeljenje ključeva. Primjerice, ako napadač nekim slučajem sazna ključ kojim se neka datoteka kriptirala, bez puno muke može doći do originala. Stoga se u praksi vrlo rijetko koristi isključivo korištenje takvog načina kriptiranja. Najčešće je to neka kombinacija simetričnih i asimetričnih algoritama, gdje se kriptira simetričnim algoritmom, dok se ključ dijeli asimetričnim. Takav način se pokazao izuzetno efikasan i učinkovit te danas pronalazi najširu upotrebu u praksi.

Hash algoritam koristi se za sažimanje i identificiranje podataka. Sažetak se računa matematičkim algoritmima. Važno je napomenuti da je SHA-3 jedini Hash algoritam koji do sada nije “probijen” i koji se smatra sigurnim.

Idealan Hash algoritam bi trebao imati 5 svojstva:

1. Trebao bi biti deterministički algoritam koji mora za istu poruku izračunati isti sažetak
2. Trebao bi se brzo izračunat za proizvoljnu duljinu teksta ili veličinu datoteke
3. Ne bi se smjelo moći napraviti inverz sažetka
4. Malene promjene u sadržaju teksta ili datoteke trebale bi dati veliku razliku u izračunatom sažetku
5. Ne bi smjelo biti moguće pronaći dvije različite poruke sa istim sažetkom.

Digitalan potpis koristi prethodno opisane hash i asimetrične algoritme da bi osigurao autentičnost poslane poruke. Sadržaj poruke se najprije sažme nekim od hash algoritama, i taj sažetak se zatim kriptira pošiljateljevim tajnim ključem koristeći bilo koji od asimetričnih algoritama. Kriptirani sažetak, odnosno “digitalni potpis” se dodaje na kraj poruke, i tada se ona šalje primatelju. Primatelj koristi svoj javni ključ da bi dekriptirao potpis, i zatim sam računa hash primljene poruke. Ako su ta 2 sažetka jednaki, primatelj može biti siguran da je poruka poslana od strane pošiljatelja zbog korištenja pošiljateljevog tajnog ključa za kriptiranje, kao i da ta poruka nije mijenjana jer poslani sažetak odgovara sažetku izračunatom od strane primatelja.

4. Upute za korištenje

ASIMETRIČNI ALGORITMI

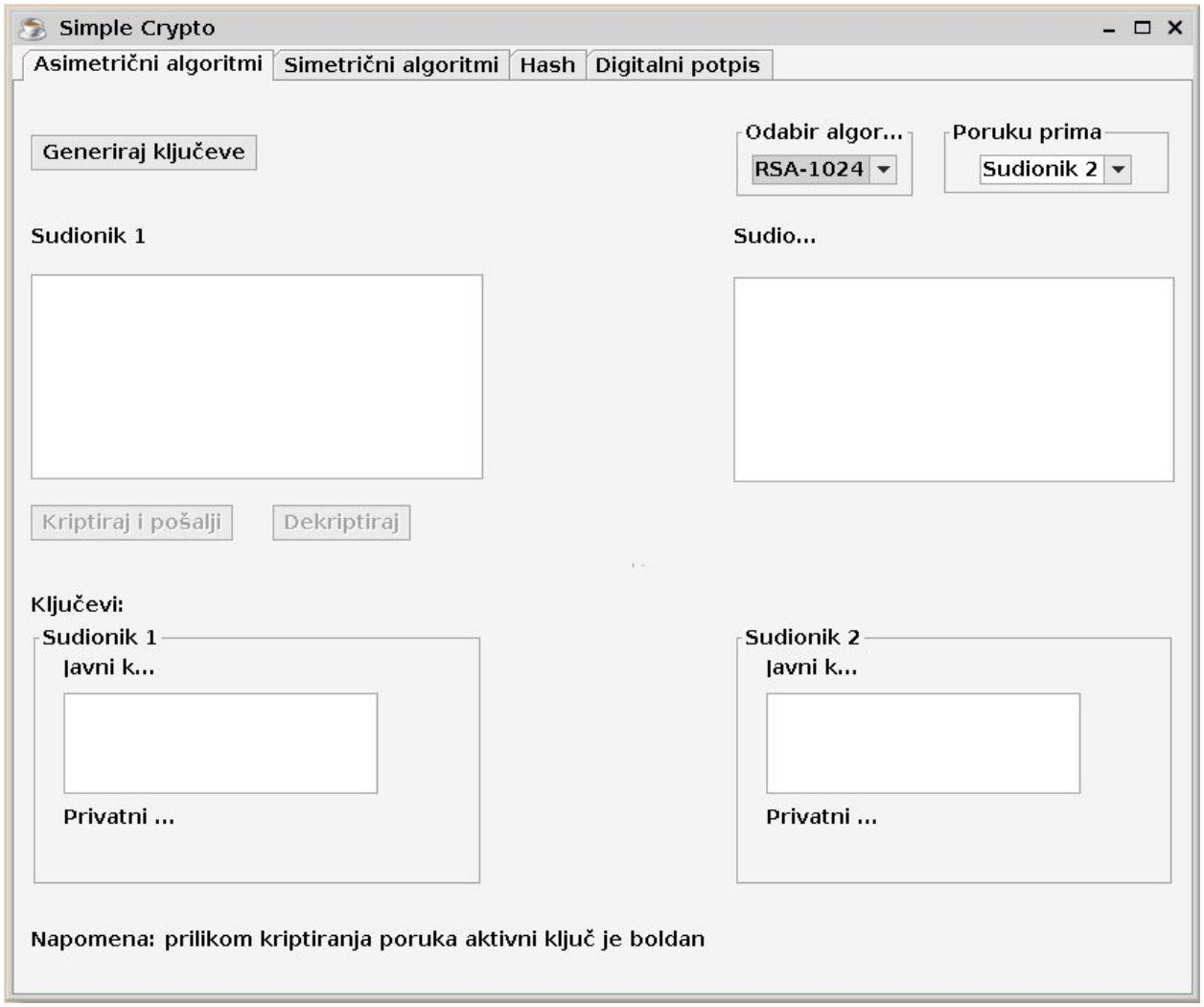
Prozor je dizajniran i osmišljen tako da na jasan način prikazuje postupak kriptiranja i slanja poruke između dva sudionika u komunikaciji kriptiranoj sa asimetričnim algoritmima.

Za početak se u gornjem desnom vrhu prozora preko padajućeg izbornika bira vrsta asimetričnog algoritma kojim će se kriptirati sadržaj poruke, te preko drugog padajućeg izbornika sudionik koji tu poruku prima. Nakon tih akcija, preostaje generirati ključeve za oba sudionika putem gumba “Generiraj ključeve”. Omogućen je i pregled ključeva svakog sudionika u donjem dijelu prozora (sadržaj privatnog ključa se ne ispisuje).

Nadalje, ovisno o odabranom primatelju, se u jedno od dva polja za unos teksta unosi poruka. Ukoliko je kao primatelj odabran sudionik 2, onda je omogućen unos teksta u polju sudionika 1, a ukoliko je kao primatelj odabran sudionik 1, onda je obrnuto.

Nakon što je sadržaj poruke unesen, ona se može kriptirati pomoću gumba “Kriptiraj i pošalji”, nakon čega će kriptirani sadržaj poruke biti prikazan i na primateljevom polju za unos teksta. Prilikom svih akcija koje kriptiraju/dekriptiraju sadržaj poruke je odgovarajući ključ koji se za tu akciju koristi otisnut masnim slovim (boldan).Nakon što smo poruku kriptirali i poslali, njen sadržaj možemo saznati pomoću gumba “Dekriptiraj”.

Svako novo generiranje ključeva briše sadržaj svih polja za unos teksta.


Simple Crypto
Asimetrični algoritmi
Simetrični algoritmi
Hash
Digitalni potpis
Generiraj ključeve
Odabir algor...
RSA-1024
Poruku prima
Sudionik 2
Sudionik 1
Sudio...
Kriptiraj i pošalji
Dekriptiraj
Ključevi:
Sudionik 1
Javni k...
Privatni ...
Sudionik 2
Javni k...
Privatni ...
Napomena: prilikom kriptiranja poruka aktivni ključ je boldan

SIMETRIČNI ALGORITMI

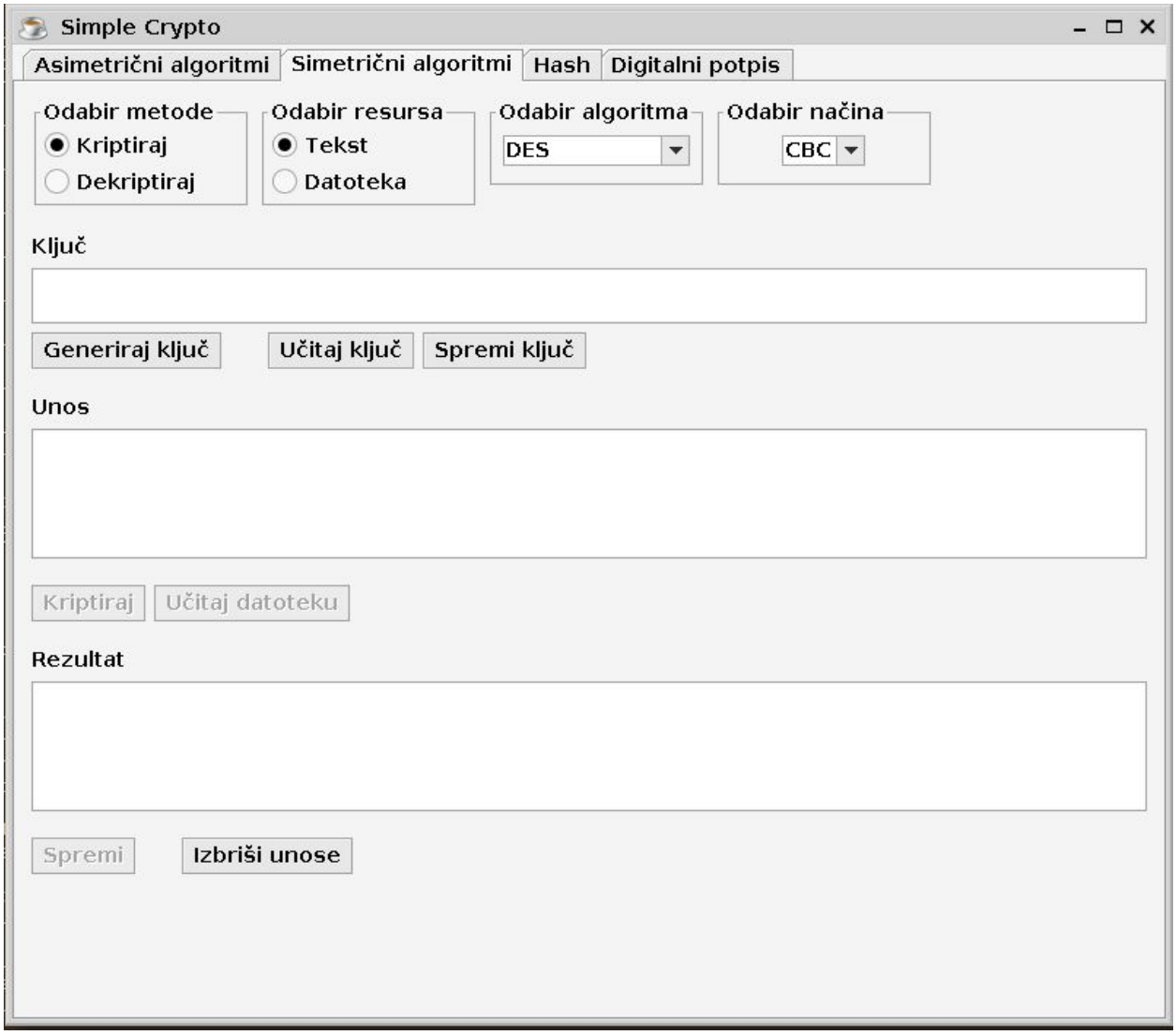
Na vrhu prozora nalazi se nekoliko izbornika kojima korisnik odlučuje što i kako želi provesti. Prvi po redu je odabir metode, odnosno hoće li to biti kriptiranje ili dekriptiranje. Zatim se bira resurs, gdje su trenutno ponuđeni samo tekst ili datoteka (koja može biti isključivo tekstualna). Slijedi odabir algoritma i načina na koji će se algoritam provesti. Od algoritama na izbor korisnik ima 5 njih te u kombinaciji sa različitom veličinom ključeva, nudi se preko 10 “različitih” algoritama. Za način kojim će se algoritam provesti u trenutnoj verziji 1.0 moguće je odabrati isključivo jedan, CBC.

U prostoru gdje se zahtjeva od korisnika da unese ključ za odabrani algoritam, ponuđeno mu je da taj ključ upiše sam, prepusti programu da potpuno nasumično odabere ključ ili da ga učita iz tekstualne datoteke spremljene lokalno na računalu. Isti taj ključ korisnik može pohraniti na računalo za daljnju upotrebu.

Slično je i za unos teksta, osim što nije moguće nasumično generirati tekst. Valja napomenuti kako će tipka za kriptiranje/dekriptiranje biti onemogućena u slučaju da je prostor za upis ključa ili teksta prazan. Također, tipka *“Učitaj datoteku”* u polju *“Unos”* će biti onemogućena ako je za resurs odabran tekst.

Za kraj, polje rezultat će program ispuniti dobivenim rezultatom. Tek tada će taj rezultat korisnik moći spremiti na računalo, budući da je onemogućeno spremanje dok god je rezultat prazan. Na samom dnu nalazi se i tipka *“Izbriši unose”* koja će poništiti sve korisnikove unose.

Ako je korisnik odabrao ili upisao pogrešan ključ (ključ koji ne odgovara odabranom algoritmu i veličini), tada će se prilikom pokušaja kriptiranja ili dekriptiranja pojaviti pogreška u vidu skočnog prozora.

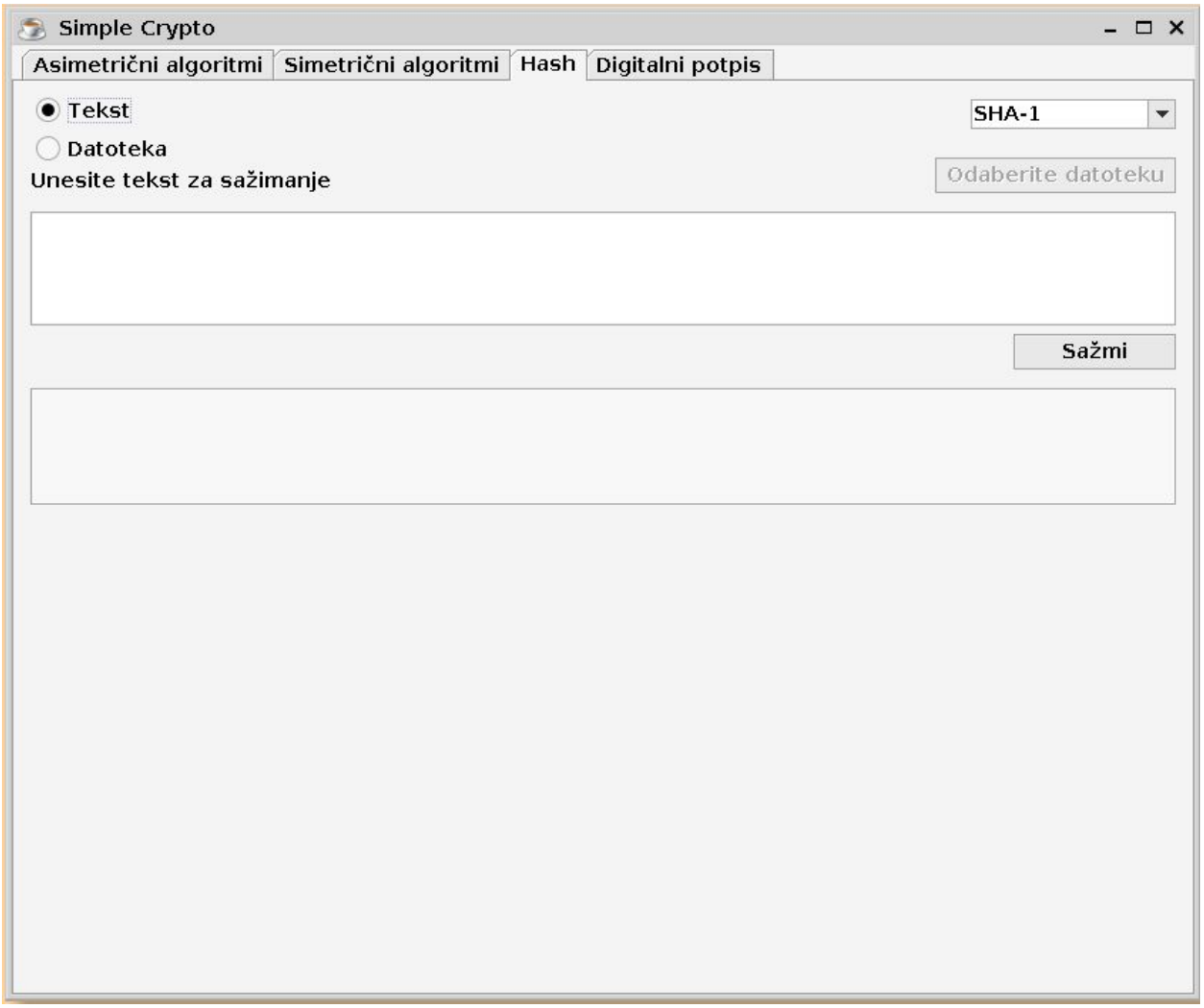

Simple Crypto
Asimetrični algoritmi
Simetrični algoritmi
Hash
Digitalni potpis
Odabir metode
Kriptiraj
Dekriptiraj
Odabir resursa
Tekst
Datoteka
Odabir algoritma
DES
Odabir načina
CBC
Ključ
Generiraj ključ
Učitaj ključ
Spremi ključ
Unos
Kriptiraj
Učitaj datoteku
Rezultat
Spremi
Izbriši unose

HASH

Na vrhu prozora nalazi se odabir resursa za sažimanje. Moguće je izabrati za sažimanje teksta ili datoteke. U desnom uglu se odabire algoritam pomoću kojeg će resurs biti sažet može se izabrati između 4 vrste algoritama sa različitim duljinama sažetka.

Kod odabira unosa teksta u gornji prozor upisuje se tekst koji se želi sažeti. Kad se tekst unese, mora se pritisnuti gumb Sažmi nakon čega se tekst sažima i rezultat se ispisuje u donji prozor.

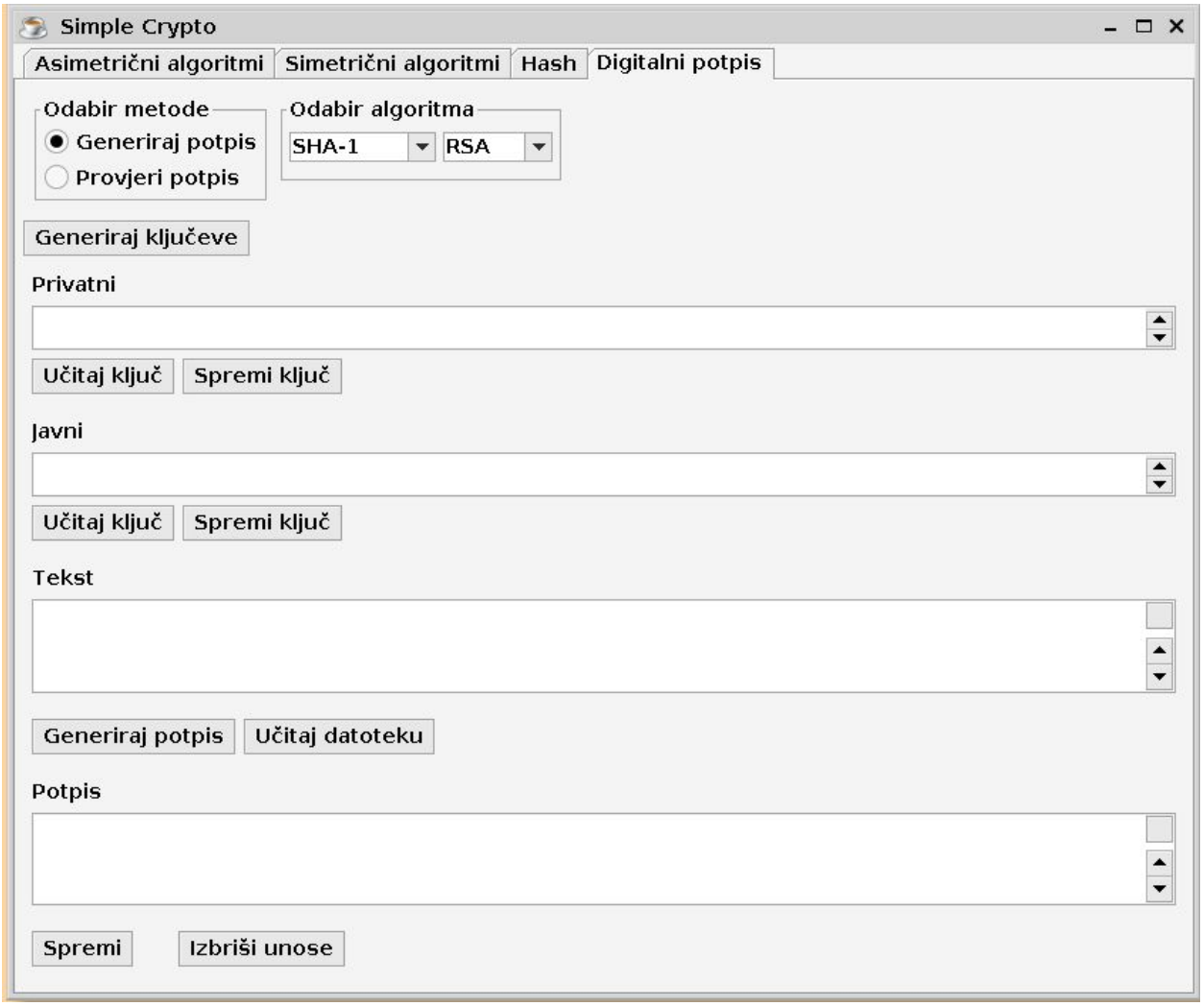
Kod odabira sažimanja datoteke omogućava se gumb Odaberite datoteku, pritiskom na njega otvara se novi prozor pomoću kojeg se odabire datoteka. Nakon odabira datoteke u gornji prozor se ispisuje putanja do te datoteke. Za izračun sažetka mora se pritisnuti gumb Sažmi nakon čega se u donji prozor izračunava sažetak.


Simple Crypto
Asimetrični algoritmi
Simetrični algoritmi
Hash
Digitalni potpis
Tekst
Datoteka
SHA-1
Unesite tekst za sažimanje
Odaberite datoteku
Sažmi

DIGITALNI POTPIS

Pri vrhu prozora korisniku se najprije nudi mogućnost generiranja ili provjere potpisa, kao i odabir asimetričnog i hash algoritma koji se koristi za potpisivanje. Korisnik zatim ima opciju generiranja ključeva, kao i njihovog učitavanja iz datoteke, spremanja u datoteku, kao i ručnog unosa. Sljedeće polje služi za unos teksta, koji se također može unijeti ručno ili učitati iz datoteke. Klikom na gumb “Generiraj potpis” se u zadnjem prozoru pojavljuje digitalni potpis dane poruke.

Kod provjere, korisniku se ne prikazuje polje s privatnim ključem. Javni ključ ostaje onaj koji je prije odabira opcije provjere bio u polju, i korisnik ga opet ima opciju promijeniti na jednak način. Gumb “Generiraj potpis” sada postaje “Provjeri potpis”, i klikom na njega se pojavljuje skočni prozor sa obavijesti odgovara li dani potpis poruci.



5. Zaključak

Po završetku projekta možemo zaključiti da su kriptografski algoritmi temelj znanja svakog računarca. Iako su algoritmi u konstantnom razvoju te se stalno predlažu neki noviteti, mislimo kako je konačan rezultat ovog projekta nešto iz čega se može dobiti dobra praktična podloga u načinu rada tih algoritama.

6. Literatura

- Dokumentacija programske knjižnice BouncyCastle
    - https://www.bouncycastle.org/documentation.html