UNIVERZITET U BEOGRADU - ELEKTROTEHNIČKI FAKULTET

ZAŠTITA PODATAKA

PROJEKAT – PGP

Izveštaj o urađenom projektnom zadatku

Student:

Miloš Ćirković 2017/0333

Ksenija Bulatović 2019/0730

Beograd, jun 2022.

SADRŽAJ

1. UVOD

1.1. Implementirane stvari

Implementiran je PGP algoritam za slanje i prijem poruka. U sklopu njega omogućene su sledeće funkcionalnosti:

- Generisanje novog i brisanje postojećeg ključa
- Uvoz i izvoz javnog ili privatnog ključa u .asc formatu
- Prikaz prstena javnih i privatnih ključeva sa svim potrebnim informacijama
- Slanje poruke (uz obezbeđivanje enkripcije i potpisivanja)
- Primanje poruke (uz obezbeđivanje dekripcije i verifikacije)

1.2. Korišćeni alati

Za implentaciju ovog projekta korišćena je biblioteka Bouncy Castle.

Radi testiranja ispravnosti aplikacije, korišćena je Kleopatra.

2. KORIŠĆEJNE APLIKACIJE

2.1. Odabir korisnika

U okviru taba „User settings“ moguće je registrovati korisnika pomoću:

- username-a
- email-a
- šifre.

Postojećeg korisnika je moguće izabrati iz padajuće liste.

2.2. Pregled ključeva

U okviru taba *KeyRing Edit.*

Svi privatni ključevi selektovanog korisnika se nalaze u listi *Private key ring.*

Svi javni ključevi svih korisnika se nalaze u listi *Public key ring.*

Svi DSA ključevi su zapisani kao *username <mail>*.

Svi ElGamal ključevi su zapisani kao *#KeyId.*

2.3. Generisanje novog ključa

Moguće je generisati novi ključ samo za trenutno izabranog korisnika.

Potrebno je uneti username, email i šifru.

Potrebno je izabrati da li se generiše DSA ili ElGamal ključ.

DSA ključ mora da se generiše prvi.

ElGamal ključevi su zavisni od DSA ključa.

DSA ključevi mogu biti veličine 1024 i 2048.

ElGamal ključevi mogu biti veličine 1024, 2048 i 4096.

2.4. Importovanje ključeva

Moguće je impotovati privatni ključ samo za svog korisnika.

Javne ključeve je moguće importovati od svih korisnika.

Nije moguće importovati ključeve korisnicima koji već imaju ključeve.

Nakon importovanja ključeva, taj korisnik ne može generisati nove ključeve.

2.5. Export ključeva

Radi uspešnog exportovanja potrebno je selektovati DSA (username <mail>) korisnika.

Klikom na dugme export bira se lokacija i naziv fajla u koji će ključevi biti exportovani.

2.6. Brisanje ključeva

Moguće je izbrisati jedan ElGamal ključ.

Moguće je izbrisati ceo prsten ključeva nekog korisnika ukoliko se izabere njegov DSA ključ.

2.7. Slanje poruke

Moguće je izabrati fajl koji će se slati.

Moguće je ukucati plaintext. On generiše tekstualni fajl u koji će se smestiti.

Moguće je izabrati da li želimo da Enkriptujemo i/ili potpišemo poruku.

Enkriptovanje zahteva odabir algoritma 3DES ili IDEA.

Autetikacija zahteva šifru korisnika koji potpisuje.

Enkriptovanje se vrši javnim ElGamal ključem primaoca.

Potpisivanje se vrši privatnim DSA ključem pošaljioca.

Moguće je opciono zipovati fajl.

Moguće je opciono izvršiti Radix64 konverziju.

2.8. Primanje poruke

U okviru taba *Recive message* moguć je prijem poruke.

Potrebno je izabrati fajl koji korisnik želi da primi.

Potrebno je uneti šifru korisnika koji prima poruku.

Klikom na dugme *Receive* kreira se dekriptovani fajl.

3. IMPLEMENTACIJA

3.1. View_User

Klasa koja pokreće ceo GUI i spaja ostatak aplikacije.

3.2. KeyRing

- public static String generateNewUserKeyPair(

  String algo,

  String username,

  String password,

  String mail,

  int size);

metoda generiše novi DSA ili ElGamal par ključeva.

- public static boolean importKeyRing(

  String username,

  InputStream in);

Metoda importuje keyRing nekog korisnika. Vraća *true* ako je uspešno odrađeno, odnosno *false* ako nije.

3.3. User

Klasa User čuva sve informacije o korisnicima i njihovim ključevim i prstenima ključeva.

Unutar klase postoje razne metode koje šifruju id ključa i username sa ključem, korisnikom ili prstenom ključeva.

3.4. Encryption

Klasa sadrži metodu koja enkriptuje i potpisuje fajl sa prosleđenim podešavanjima.

3.5. Decryption

Klasa sadrži metodu koja dekriptuje sadržaj poruke koju korisnik prima.