Opis projekta:

- Projekat je zamišljen kao aplikacija sa mogućnošću registracije i logovanja, kreiranja RSA para ključeva, uvoza i izvoza ključeva, kao i slanja i primanja poruke šifrovane 3DES ili AES algoritmom.

Svaki korisnik u sistemu može da vidi samo svoje ključeva

odnosno svoje parove javnih i privatnih ključeva, kao i one ključeva koje je uvezao.

Pregled klasa i njihovih funkcionalnosti

(izostavljene su klase iz paketa GUI - sluÅ¾e za prikaz implementirane logike) :

1. Main:

- Sadrži main metodu kojom se aplikacija pokreće.

2. User:

- Čuva sve podatke vezane za korisnika sistema.

3. UserProvider:

- Singleton klasa, čuva sve korisnike sistema, omogućava kreiranje korisnika i dohvatanje

trenutno ulogovanog korisnika.

4. HashText:

- Računa heš korisnikove šifre za logovanje, koristi se pri čuvanju korisnika u fajl users.txt.

5. Pair:

- Generička klasa, koristi se za čuvanje para ključeva.

6. KeyFormatter:

- Singleton klasa, sluÅ¾i za ispis ključeva, ispisuje se ID kljuca, ID korisnika i vreme kreiranja ključa.

7. GenerateRSAKeys:

- Klasa realizovana kao Singleton omogućava kreiranje RSA ključeva duÅ¾ine 1024, 2048 ili 4096 bita, dodavanje istih u prsten ključeva, kao i upis u ključeva u fajl dodeljen korisniku.

8. Keys:

- Klasa za rad sa ključevima, uključuje uvoz i izvoz javnih i privatnih ključeva trenutno ulogovanog korisnika, dohvatanje javnih i privatnih ključeva, kao i njihovu pretragu po ID. Takođe vrši i brisanje para ključeva.

9. ZipRadix:

- Uslužna klasa sa statičkim metodama koje omogućavaju kompresiju, dekompresiju, konverziju u radix64, dekonverziju iz radix64, kao i proveru da li je poruka komprimovana.

10. SignedFileProcessor:

- Omogućava proveru da li je poruka potpisana, potpisivanje i verifikaciju iste, kao i vraćanje u originalni format bez potpisa.

11. MessageEncryption:

- Singlton klasa - šifrovanje poruke odabranim simetričnim algoritmom, kao i provera da li je ista šifrovana.

12. MessageDecryption:

- Singlton klasa - dešifrovanje poruke