# Projekat iz predmeta Zaštita podataka: Izveštaj

## Autori


1. Marko Stanojević, broj indeksa 2017/0081
2. Uroš Isaković, broj indeksa 2017/0057


## Prikaz implementiranih algoritama i funkcionalnosti

Implementirane funkcionalnosti:

1. Generisanje novog i brisanje postojećeg para ključeva
2. Uvoz i izvoz javnog ili privatnog ključa u *.asc* formatu
3. Prikaz prstena javnih i privatnih ključeva sa svim potrebnim informacijama
4. Slanje poruke (uz mogućnost enkripcije, potpisivanja, kompresije i radix-64 formatiranja)
5. Primanje poruke (uz mogućnost dekripcije, dekompresije i verifikacije integriteta i potpisa poruke)

Algoritmi korišćeni za implementiranje navedenih funkcionalnosti:

1. ElGamal i IDEA algoritam za enkripciju i potpisivanje (kao i za dekripciju)
2. ElGamal i 3DES algoritam za enkripciju i potpisivanje (kao i za dekripciju)
3. Generisanje para ključeva pomoću DSA i ElGamal algoritama

## Opis realizovanih klasa

### Klasa Encryption

Opis:
Statička klasa koja implementira logiku enkripcije i dekripcije.

Javne metode i polja:

```
public static byte[] createPgpMessage(
            byte[] message,
            PGPSecretKey senderDsaSecretKey,
```

```
            PGPPublicKey receiverElGamalPublicKey,
            EncryptionAlgorithm encryptionAlgorithm,
            char[] senderPassphrase,
            boolean addSignature,
            boolean addCompression,
            boolean addConversionToRadix64 ) throws IOException

public static void readPgpMessage( PgpMessage pgpMessage )
     throws Exception

public static void decryptPgpMessage(
            char[] passphrase,
            PgpMessage pgpMessage )

public static class PgpMessage
```

## Klasa PGPKeys

Opis:
Statička klasa koja implementira rad, operacije čitanja i pisanja  i čuvanje prstenova javnih i privatnih ključeva.

Javne metode i polja:

```
public static PGPSecretKeyRingCollection getSecretKeysCollection()

public static PGPPublicKeyRingCollection getPublicKeysCollection()

public static final void addSecretKey( PGPKeyRingGenerator
keyRingGenerator )
     throws IOException

public static final void addPublicKey( PGPKeyRingGenerator
keyRingGenerator )
     throws IOException

public static final void removePublicKey( PGPPublicKeyRing
publicKeyRing )
     throws IOException
```

```
public static final void removeSecretKey( PGPSecretKeyRing
secretKeyRing )
      throws IOException

public static void saveSecretKeysToFile() throws IOException
public static void savePublicKeysToFile() throws IOException

public static void exportPublicKey( PGPPublicKeyRing publicKeyRing,
File file )
      throws IOException

public static void exportSecretKey( PGPSecretKeyRing publicKeyRing,
File file )
      throws IOException

public static void importPublicKey( File file ) throws IOException,
PGPException

public static void importSecretKey( File file ) throws IOException,
PGPException

public static final PGPKeyRingGenerator createPGPKeyRingGenerator(
                KeyPair dsaKeyPair,
                KeyPair elGamalKeyPair,
                      String identity,
                char[] passphrase ) throws Exception

public static PGPSecretKeyRing getSecretKeyRing( long keyID )
      throws IOException, PGPException

public static String keyIdToHexString( long keyId )

public static long hexStringToKeyId( String userFriendlyHexString )

public static boolean isValidPassphrase(
      PGPSecretKeyRing secretKeyring,
      int index,
```

```
    char[] passphrase )
```

## Klasa FileUtils

Opis:
Statička pomoćna klasa za rad sa fajlovima. Implementira operacija čitanja i pisanja iz fajla, kao i dialog za izbora fajla (pomoću `javax.swing.JFileChooser` komponente).

Javne metode i polja:

```
public static void writeToFile( String filePath, byte[] content )

public static void writeToFile( String filePath, String content )

public static byte[] readFromFile( String filePath )

public static void ensureFileExists( File file ) throws
    FileNotFoundException

public static String getUserSelectedFilePath( int dialogType, int
    allowedFileType )
```

## Klasa App

Opis:
Klasa koja implementira grafički korisnički interfejs sačinjen od vizuelnih elemenata, osluškivača događaja i funkcija reakcija na događaje koristeći `javax.swing` radni okvir.

Javne metode i polja:
Sve javne metoda i polja su enkapsulirane u `javax.swing` radnom okviru.

## Klasa Main

Opis:
Klasa koja sadrži `main` metodu i pokreće aplikaciju,

Javne metode i polja:

```
public static void main( String[] args )
```