Dokumentacija projekta

Implementacija OpenPGP standarda

Milan Akik 2018/0688

Milena Đurić 2018/0630

(0688+0630)mod6+1=5

RSA za enkripciju i potpisivanje sa kljucevima velicine 1024, 2048 i 4096

3DES sa EDE konfiguracijom i 3 kljuca i IDEA

Sama dokumentacija se nalazi u podfolderu doc Eclipse projekta.

Osnovni paket je etf.openpgp.am180688ddm180630d. U njemu se nalazi klasa Main koja sadrzi main metodu. Unutar tog paketa se nalaze jos tri podpaketa: data, gui i util.

Table

Description automatically generated

Paket data sadrzi klase za privatni i javni kljuc i njihove prstenove i podpaketi enumerators, packet, subpacket i types.

Table

Description automatically generated

Podpaket types sadrži samo jednu klasu MPI koja predstavlja MPI(Multi precision integer) iz OpenPGP standarda. Table

Description automatically generated

Podpaket enumerators sadrži java Enumeratore za kompresione algoritme, heš algoritme, tag paketa, algoritme asimetrične enkripcije, tipove potpisa i tipove potpisnih podpaketa.

Table

Description automatically generated

Podpaket packet sadrži klase Packet, PublicKeyPacket, SignaturePacket i UserIDPacket. Klasa Packet sadrži zajedničku strukturu svih paketa, dok se ostale tri klase izvode iz nje. Ostale tri klase sadrže pojedinosti svakog od tipova paketa.

Table

Description automatically generated

Podpaket subpacket u sebi sadrži implementiranu klasu SignatureSubpacket, kao i preostalih 23 tipova podpaketa paketa za potpisivanje. SignaturSubpacket sadrži zajedničku strukturu svih podpaketa paketa za podpisivanje.

Graphical user interface, text, application, email

Description automatically generated

Paket gui sadrzi jednu klasu MainMenu koja se bavi celim sistemom prozora.

Table

Description automatically generated

Paket util sadrzi 4 pomocne klase: ASCReader, CRCUtil, Radix64Util i RSAUtil. ASCReader sluzi da procita fajl koji je u Armored ASCII formatu i pretvori ga u niz bajtova i proveri njegov CRC. CRCUtil sluzi da bi se za niz bajtova izracunao CRC24-Radix64 kod opisan u RFC4880 standardu. Radix64Util ima metode za enkodovanje i dekodovanje niza bajtova u radix64 String i radix64 Stringa u niz bajtova. RSA sluzi za generisanje javnog kljuca(eksponenta i modulusa) odredjene velicine/duzine u bitovima.

Table

Description automatically generated