Implementacija PGP Protokola

Elektrotehnički Fakultet | Univerzitet u Beogradu

Projekat iz Zaštite Podataka

Damjan Pavlović I Uroš Ugrinić

2021

Sadržaj

[Algoritmi za Asimetričnu Enkripciju 2](#_Toc74676032)

[DSA 2](#_Toc74676033)

[ElGamal 2](#_Toc74676034)

[Algoritmi za Simetričnu Enkripciju 2](#_Toc74676035)

[3DES 2](#_Toc74676036)

[IDEA 2](#_Toc74676037)

[PGP 2](#_Toc74676038)

[Slanje Poruke 2](#_Toc74676039)

[Primanje Poruke 2](#_Toc74676040)

# Algoritmi za Asimetričnu Enkripciju

Asimetrični algoritmi su sporiji od simetričnih algoritama i zbog toga se ne koriste za enkripciju cele poruke, nego samo za enkripciju manjih delova.

## DSA

DSA algoritam koristimo za potpisivanje poruke, to jest za enkripciju heša poruke. Ovim obezbeđujemo autentikaciju korisnika. Veličina ključa nam je 1024 ili 2048 bita.

Za implementaciju DSA koristimo već gotove funkcije iz BouncyCastle-a. Funkcionalnost su implementirane unutar PGP.sign(..) funkcije.

## ElGamal

ElGamal-ov algoritam koristimo za asimetričnu enkripciju poruka, preciznije za enkripciju ključa sesije (kojim enkriptujemo samu poruku). Ovim obezbeđujemo da samo osoba sa odgovarajućim privatnim ključem može pročitati našu poruku. Veličina ključa nam je 1024, 2048 ili 4096 bita.

Za implementaciju DSA koristimo već gotove funkcije iz BouncyCastle-a. Funkcionalnost su implementirane unutar PGP.encrypt(..) funkcije, zajedno sa simetričnom enkripcijom.

# Algoritmi za Simetričnu Enkripciju

Implementirali smo 2 algoritma simetrične enkripcije. Bilo koji od njih se može koristiti za šifrovanje poruke, ovim obezbeđujemo tajnost poruke.

Za oba naredna algoritma koristimo već gotove funkcije iz BouncyCastle-a. Funkcionalnost su implementirane unutar PGP.encrypt(..) funkcije.

## 3DES

3DES je jedna od opcija koja se može koristiti za simetričnu enkripciju poruka.

## IDEA

IDEA je druga od opcija koja se može koristiti za simetričnu enkripciju poruka.

# PGP

## Slanje Poruke

Slanje poruke se radi iz maksimalno 5 koraka, i to su:

1. Pravljenje Literal Data paketa
2. Potpisivanje
3. Kompresija (ZIP algoritam)
4. Enkripcija
5. Enkodovanje u radix64 format

## Primanje Poruke