

Пројекат из Заштите података

2020/2021. година

*Студенти:*

Душан Стијовић 0145/2017

Филип Царевић 0065/2017

Садржај

[О пројекту 2](#_Toc74189009)

[Имплементирани алгоритами- DSA 3](#_Toc74189010)

[Имплементирани алгоритами- ElGamal 5](#_Toc74189011)

[Референце 7](#_Toc74189012)

# О пројекту

Идеја пројекта јесте имплементација PGP сервиса:

* Увоз и извоз јавних/приватних кључева

Кључеви се увозе из .*asc* формата. Аналогно, кључеви се извозе у исти формат.

* Креирање приватних кључева
  + За потписивање

Подржано креирање *DSA* парова приватни/јавни кључ величине *1024* или *2048* бита.

* + За енкрипцију

Подржано креирање *ElGamal* парова приватни/јавни кључ величине *1024*, *2048* или *4096* бита

* Дигитално потписивање

Подржан Digital signature algorithm- *DSA* са кључевима величине *1024* и *4096* бита.

* Компресија

Подржан *ZIP* алгоритам компресије.

* Шифровање

Порука се шифрује једним од симетричних алогритама: *3DES* или *IDEA*.

Сесијси кључ се генерише за сваку поруку. Приликом слања шифрује се *ElGamal* јавним кључем величине *1024*,*2048* или *4096* бита.

* Компатибилност са осталим мејл сервисима

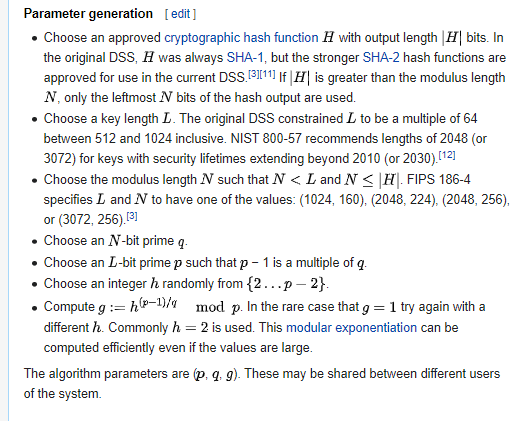
Подржана конверзија *radix64*.

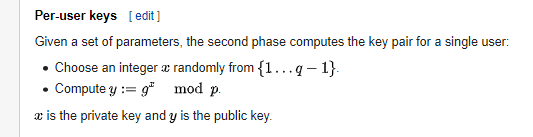
Приликом имплементације коришћенa је библиотека *Bouncy Castle.*

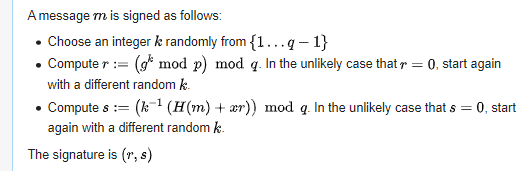
# Имплементирани алгоритами- DSA

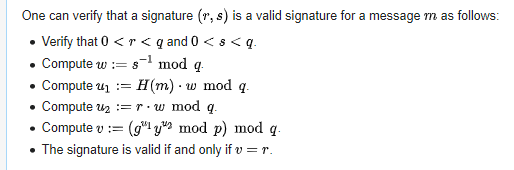
* Генерисање кључева:

Састоји се из 2 фазе. Прва фаза је генерисање параметара који су дељени између корисника, док се у другој фази генеришу сами кључеви.



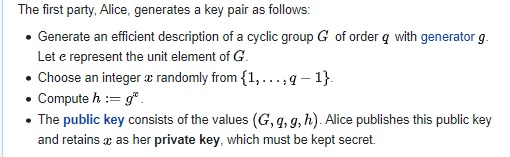


* Генерисање потписа: 
* Верификација потписа:

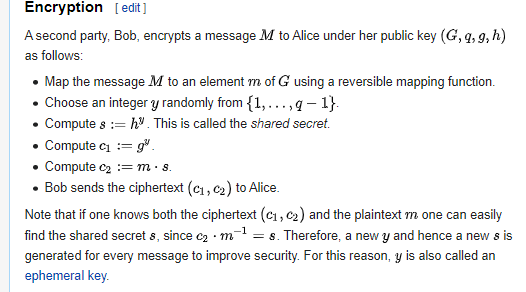


# Имплементирани алгоритами- ElGamal

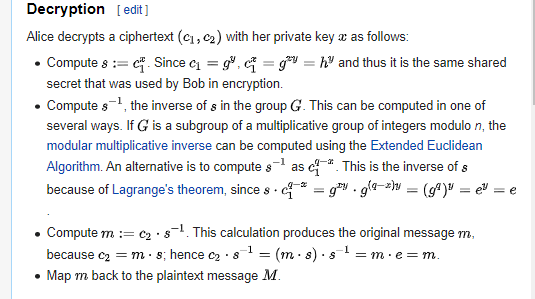
* Генерисање кључева:



* Енкриптовање података



* Декритовање података:



# Референце

* *https://en.wikipedia.org/wiki/Digital\_Signature\_Algorithm*
* *https://en.wikipedia.org/wiki/ElGamal\_encryption*