*Електротехнички факултет у Београду*
*Катедра за рачунарску технику и информатику*

# Заштита података

*- Пројектни задатак 2022/2023. -*

## Опис пројектног задатка

Циљ пројектног задатка је боље разумевање *PGP* шеме за заштиту електронске поште, као и могућности које она пружа и начина њеног коришћења. У ту сврху задатак подразумева пројектовање и имплементацију апликације са графичким корисничким интерфејсом у програмском језику *Python* која треба да омогући следеће функционалности:

- Генерисање новог и брисање постојећег пара кључева
- Увоз и извоз јавног или приватног кључа у *.pem* формату
- Приказ прстена јавних и приватних кључева са свим потребним информацијама
- Слање поруке (уз обезбеђивање енкрипције и потписивања)
- Пријем поруке (уз обезбеђивање декрипције и верификације)

При генерисању новог пара кључева, од корисника тражити унос имена, мејла, алгоритма за асиметричне кључеве и величине кључа. Потребно је подржати RSA алгоритам за енкрипцију и потписивање и комбинацију DSA алгоритма за потписивање и ElGamal алгоритма за енкрипцију са величинама кључева од 1024 и 2048 бита. Након уноса свих потребних података, од корисника тражити унос лозинке под којом ће се чувати приватни кључ. Сви генерисани и увезени кључеви треба да буду јасно видљиви на корисничком интерфејсу. Сваки приступ приватном кључу треба да буде обезбеђен затраживањем уноса лозинке. Студенти треба да предложе и имплементирају структуре у којима се чувају кључеви (прстен јавних и приватних кључева).

При слању поруке потребно је кориснику понудити могућност енкрипције поруке за обезбеђивање тајности, могућност потписивања поруке за обезбеђивање аутентичности, могућност компресије и могућност конверзије података у radix-64 формат. При обезбеђивању аутентичности, омогућити кориснику да изабере приватни кључ који жели да искористи за потписивање поруке користећи SHA-1 за генерисање hash функције. При обезбеђивању тајности, омогућити кориснику да изабере јавни кључ који користи за енкрипцију поруке и симетрични алгоритам. Потребно је подржати два (по жељи) од следећа четири предложена алгоритма: TripleDES, AES128, Cast5 и IDEA. Слањем поруке се креира нова датотека на жељеној дестинацији коју корисник бира. Датотека треба да садржи све потребне информације које је потребно доставити на страну пријема. Структура датотеке треба да одговара структури која је обрађена на часовима вежби, а студенти треба да предложе и имплементирају све детаље чувања информација у датотеци.

При пријему поруке, корисник бира датотеку са жељене дестинације, а потом апликација препознаје о којим пакетима се ради и врши декрипцију и верификацију. Након пријема поруке, кориснику се приказују информације о успешности провере потписа и информације о аутору потписа, уколико је одговарајући сервис коришћен. Након тога, потребно је кориснику омогућити да сачува оригиналну поруку на жељеној дестинацији. У случају неуспешне декрипције или верификације, приказати јасну поруку о грешци на корисничком интерфејсу.

## Напомене:

- Пројектни задатак из предмета *Заштита података* се ради у тимовима од по два студента. Самостални рад је такође могућ, али се не препоручује јер не доноси додатне поене.
- Пројектни задатак може да се брани искључиво у јунском или августовском испитном року. Рок за предају и термини одбране пројекта ће бити накнадно објављени. Пројектни задатак мора да се одбрани пре изласка на испит. Студент који жели да му се поени са пројекта признају мора да:
    - одбрани пројекат у јунском испитном року, а потом положи испит у било ком року.
    - одбрани пројекат у августовском испитном року, а потом положи испит у било ком року почевши од августовског.
- Пројектни задатак није обавезан и може максимално да донесе 15 поена који не могу да се надокнаде другом предиспитном или испитном обавезом.
- На усменој одбрани кандидат мора самостално да покрене своје решење које је предао до задатог рока за израду. Кандидат мора да поседује потребан ниво знања о задатку, мора да буде свестан недостатака приложеног решења и могућности да те недостатке реши. Кандидат мора тачно да одговори и на одређен број питања која се баве тематиком домаћег задатка и успешно реализује решење модификације.
- Пре започињања реализације проблема или тражења помоћи, задатак и приложену документацију прочитати у целини и пажљиво. Уколико у задатку нешто није довољно прецизно дефинисано, од студената се очекује да уведу разумне претпоставке.
- Приликом реализације решења, студенти су у обавези да поштују следећа правила:
    - Дозвољено је да студенти преузму идеје о структури поруке и реализацији функционалности из стандарда дефинисаном у документу RFC 4480 који описује OpenPGP протокол.
    - Дозвољено је да студенти користе готове модуле за реализацију делова PGP шеме (нпр. rsa модул, cryptography модул, итд.).
    - Није дозвољено да студенти користе готове модуле који нуде готове функционалности PGP шеме (нпр. py-pgp модул).
    - Студенти унутар једног тима треба да поделе одговорности на једнаке делове.
    - Није дозвољено да студенти унутар једног тима поделе одговорности тако да један члан тима ради на реализацији логике апликације, а други члан тима ради на реализацији графичког корисничког интерфејса.
    - Забрањено је преузимање готових решења са интернета и дељење решења са другим тимовима. Сва предата решења биће пропуштена кроз апликацију за проверу сличности програмског кода. Уколико се провером установи да су два или више предатих решења са већим степеном сличности од дозвољеног, сви аутори ће бити пријављени дисциплинској комисији Факултета.
- Евентуална питања послати асистентима на мејл, али као једну поруку (другог асистента обавезно ставити у копију - CC поруке): aki@etf.bg.ac.rs, majav@etf.bg.ac.rs