Електротехнички факултет у Београду
Катедра за рачунарску технику и информатику

Заштита података

- Пројектни задатак 2021/2022. -

Опис пројектног задатка

Циљ пројектног задатка је боље разумевање *PGP* протокола, као и могућности које он пружа и начина његовог коришћења. У ту сврху задатак подразумева пројектовање и имплементацију апликације са графичким корисничким интерфејсом у програмском језику *Java* која треба да омогући следеће функционалности:

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

При генерисању новог пара кључева од корисника тражити унос имена, мејла и одабир алгоритма за асиметричне кључеве. Након уноса свих потребних података, од корисника се тражи унос лозинке под којом ће се приватни кључ чувати. Сви генерисани и увезени кључеви треба да буду јасно видљиви на корисничком интерфејсу. При брисању приватног кључа корисника, потребно је од корисника затражити унос лозинке под којом се приватни кључ чува.

При слању поруке потребно је кориснику понудити могућност енкрипције поруке за обезбеђивање тајности, могућност потписивања поруке за обезбеђивање аутентичности, могућност компресије поруке користећи ZIP алгоритам 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 један или више јавних кључева које користи за енкрипцију поруке и избор симетричног алгоритма. Обезбедити проверу интегритета. Уколико је омогућено потписивање поруке, потребно је од корисника затражити унос лозинке под којом се приватни кључ чува. Слањем поруке се креира нова датотека *OpenPGP* структуре поруке на жељеној дестинацији коју корисник бира.

При пријему поруке корисник бира датотеку *OpenPGP* структуре поруке са жељене дестинације, а потом апликација препознаје о којим пакетима се ради и који алгоритми су коришћени за обезбеђивање тајности и аутентикације уколико су сервиси обезбеђени. Уколико је порука енкриптована јавним кључем за који корисник поседује одговарајући приватни кључ, потребно је од корисника затражити унос лозинке под којом се приватни кључ чува. У случају успешне декрипције, кориснику се приказују информације о успешности провере интегритета поруке и провере потписа, уколико је одговарајући сервис коришћен. У случају успешности провере потписа, кориснику додатно приказати и информације о аутора потписа. Након тога, кориснику омогућити да сачува поруку на жељеној дестинацији.

Алгоритми за асиметричне кључеве које апликација треба да подржи су:
Група 1: RSA за потписивање и енкрипцију са кључевима величине 1024, 2048 или 4096 бита.
Група 2: DSA за потписивање са кључевима величине 1024 и 2048 бита и *ElGamal* за енкрипцију са кључевима величине 1024, 2048 и 4096 бита.
Група 3: RSA за потписивање и енкрипцију са кључевима величине 1024, 2048 или 4096 бита.
Група 4: DSA за потписивање са кључевима величине 1024 и 2048 бита и *ElGamal* за енкрипцију са кључевима величине 1024, 2048 и 4096 бита.
Група 5: RSA за потписивање и енкрипцију са кључевима величине 1024, 2048 или 4096 бита.
Група 6: DSA за потписивање са кључевима величине 1024 и 2048 бита и *ElGamal* за енкрипцију са кључевима величине 1024, 2048 и 4096 бита.

Алгоритми за симетричне кључеве које апликација треба да подржи су:
Група 1: 3DES са EDE конфигурацијум и три кључа и CAST5 са кључем величине 128 бита.
Група 2: 3DES са EDE конфигурацијум и три кључа и IDEA.
Група 3: 3DES са EDE конфигурацијум и три кључа и AES са кључем величине 128 бита.
Група 4: 3DES са EDE конфигурацијум и три кључа и CAST5 са кључем величине 128 бита.
Група 5: 3DES са EDE конфигурацијум и три кључа и IDEA.
Група 6: 3DES са EDE конфигурацијум и три кључа и AES са кључем величине 128 бита.

Техничке информације

Све функционалности треба да се имплементирају по стандарду дефинисаном у документу RFC 4480 [1] који описује *OpenPGP* протокол. Апликација треба да буде компатибилна са свим осталим апликацијама на тржишту које имају подршку за *PGP* протокол. Студентима се препоручује да детаљно проуче наведени документ пре почетка реализације решења. За потребе провере исправности комуникације са осталим алатима истог протокола, користити апликацију *Kleopatra* [2], која је *front-end* софтвера *GnuPG* и добија се уз софтверски пакет *Gpg4win* [3].

У сваком тренутку кориснички интерфејс треба да буде довољно интуитиван, јасно назначи тренутно стање апликације, приказ постојаног модела и интерфејс за коришћење функција апликације.

Сваки студент треба да направи пакет `etf.openpgp.<username>` где `<username>` представља конкатенацију корисничких имена студената у тиму на порталу еСтудент (у формату *piGGBBBBx*, где су *pi* иницијали - презиме и име, ознака *GG* представља последње две цифре године уписа факултета, ознака *BBBB* представља четвороцифрени број индекса, проширен водећим нулама, а ознака *x* представља ниво студија *d* или *m*). Студенти су обавезни да у том пакету имплементирају комплетан код, а не ван њега.
Поред тога, треба написати извештај, који описује како је проблем решен. Извештај треба да садржи:

- Кратак приказ имплементираних алгоритама и њихових функција;
- Кратке описе свих реализованих класа, са потписима и описима метода.

Извештај приложити уз код, у фолдеру */documentation* и именовати га као: *Prezime_Ime_Prezime_Ime_ZP_Projekat_2022.pdf*.

Напомене:

- Пројектни задатак се ради у паровима од по два студента. Самостални рад је такође могућ, али се не препоручује јер не доноси додатне поене. Студенти су у обавези да решење прилагоде групи која им је додељена по следећој формули: $grupa = (zbirBrojevaIndeksa \; mod \; 6) + 1$, где је $grupa$ број групе која је додељена студентима у тиму, а $zbirBrojevaIndeksa$ је збир бројева индекса студената у тиму или број индекса студента који пројекат ради самостално без године уписа (нпр. студенти са индексом 2016/0987 и 2015/0789 треба да раде групу $1 = ((987 + 789) \; mod \; 6) + 1$.
- 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.
- На усменој обрани кандидат мора самостално да покрене своје решење које је предато 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.
- Није дозвољено коришћење готових алата у реализацији пројектног решења.
- Рок за предају и термини одбране пројекта ће бити накнадно објављени.
- Пројектни задатак може да се брани искључиво у јунском или августовском испитном року, неколико дана пре испита. 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 20 поена који не могу да се надокнаде другом предиспитном или испитном обавезом.
- 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.
- Евентуална питања послати асистентима на мејл као једну поруку (другог асистента обавезно ставити у копију - CC поруке): aki@etf.bg.ac.rs, majav@etf.bg.ac.rs

Корисна литература:

[1] OpenPGP Message Format, 2007, доступно на: https://tools.ietf.org/html/rfc4880

[2] Kleopatra – Certificate Manager and Unified Crypto GUI, доступно на: https://kde.org/applications/utilities/org.kde.kleopatra/

[3] Gpg4win, доступно на: https://www.gpg4win.org/

[4] PGP Message Exchange Formats, 1996, доступно на: https://tools.ietf.org/html/rfc1991

[5] Bouncy Castle Crypto APIs, 2000, доступно на: https://www.bouncycastle.org/

[6] https://docs.oracle.com/javase/7/docs/api/java/security/package-summary.html

[7] https://docs.oracle.com/javase/7/docs/api/javax/crypto/package-summary.html