# Programmeerimine keeles C++

## Praktikum 8: Variant 1: Failide krüpteerimine ja allkirjastamine

## Sissejuhatus

Selle ülesande käigus saate tutvuda praktilise krüptograafiaga, täpsemalt Crypto++ teegiga, mis on üks paremaid selle valdkonna teeke C++ keeles. Teegi ametlik veebileht asub aadressil http://www.cryptopp.com/. Teegi ehitamiseks kasutage make'i ja dokumentatsiooni saamiseks doxygeni.

Teie ülesandeks on nimetatud teeki kasutades kirjutada programm `filesecure`, mis lubab teha järgmiseid toiminguid:

1) krüpteerimis- ja signeerimisvõtme genereerimine ning faili salvestamine,

2) etteantud nimega faili krüpteerimine etteantud nimega failis asuvat võtit kasutades,

3) etteantud nimega faili signeerimine etteantud nimega failis asuva võtmega.

## Võimalikud käsureaparameetrid

`filesecure --help`

Väljastab kõik programmi poolt toetatavad võtmed ning nimetab ka krüptograafilised skeemid, mida kasutatakse.

`filesecure --genkey` *`pubkeyfile privkeyfile`*

Genereeritakse uus RSA võtmepaar, avalik võti salvestatakse faili *`pubkeyfile`* ja salajane võti faili *`privkeyfile`*.

`filesecure --encrypt` *`infile`* `--out` *`outfile`* `--withkey` *`pubkeyfile`*

Failide krüpteerimisel kasutage levinud hübriidkrüpteerimise meetodid, kus avaliku võtme krüptoga kaitstakse nn *sessioonivõtit*, mis on tavaliselt sümmeetriline võti. Antud ülesande puhul käituge järgmisel moel.

Genereerige uus võti või parool, millega saab teha sümmeetrilist krüpteerimist. See võti krüpteeritakse failist *`pubkeyfile`* loetud avaliku RSA võtmega ning tulemus kirjutatakse faili *`outfile`*. Seejärel krüpteeritakse faili *`infile`* sisu genereeritud võtmega ning tulemus kirjutatakse faili *`outfile`* võtme krüptoteksti järele.

`filesecure --decrypt` *`infile`* `--out` *`outfile`* `--withkey` *`privkeyfile`*

Failist nimega *`infile`* loetakse sümmeetrilise krüpto võti või parool, mis dekrüpteeritakse salajase RSA võtmega failist *`privkeyfile`*. Saadud võtmega dekrüpteeritakse ülejäänud *`infile`* sisu ning tulemus salvestatakse faili *`outfile`*.

`filesecure --sign` *`infile`* `--withkey` *`privkeyfile`* `--sigfile` *`sigfile`*

Fail nimega *infile* signeeritakse salajase RSA võtmega failist *privkeyfile*. Signatuur salvestatakse faili *sigfile*,

`filesecure --verify infile --withkey pubkeyfile --sigfile sigfile`

Kontrollitakse signatuuri *sigfile* *vastavust* failile *infile* kasutades avalikku võtit failist *pubkeyfile*.

NB! Nõutud on, et käsureaparameetrid võivad esineda ka teises järjekorras – näiteks:

```
filesecure --verify infile --sigfile sigfile --withkey pubkeyfile
```

## Hindamine

Sobiv Makefile lahenduse kompileerimiseks – kuni 1 punkt

Käsureaparameeter *--help* ja doxygeni dokumentatsioon – kuni 1 punkt

Krüpteerimine – kuni 4 punkti

Signeerimine – kuni 4 punkti

Kokku kuni 10 punkti

## Märkused

Ilma käivituva käsurearakenduseta ma programmi hindama ei hakka. Seega olge tähelepanelikud ja veenduge, et programmid kompileeruksid - vaadake, et kõik päised oleks lisatud ja Makefile oleks korralik.

## Vihje

Crypto++ teegi koosseisus on testprogramm *test.cpp*. See aitab teid kõvasti.

Palun veenduge, et te saate genereeritud võtmetega krüpteerida kokku näiteks programmi enda ning lahtikrüpteeritud programm ikka veel käima läheb.