Määrittely - Rypto
10.3.2017

Sisällys

Johdanto

Tietorakenteet ja algoritmit – harjoitustyö.

Rypto on salakirjoitusohjelma, joka salakirjoittaa ja purkaa salauksen.

Algoritmit ja tietorakenteet

Ohjelma toteuttaa AES-algoritmin[FIPS197] 128-bittisillä avaimilla ECB-moodissa.

Toteutuksessa on sekä salaus että salauksen purku.

Käytettävät tietorakenteet ovat standardissa kuvatut

- avainvektori, joka on yksiulotteinen taulukko ja
- tila, joka on kaksiulotteinen taulukko.

Lisäksi käytetään tiedostoja syötteenä ja tulosteena sekä muuttujaa komentoriviltä annettavan avaimen talletukseen.

Ratkaistava ongelma

Ratkaistava ongelma on annetun tiedoston salaus standardinmukaisella menetelmällä, sekä mainitun salauksen purkaminen. AES on laajasti käytössä oleva salausalgoritmi jota pidetään turvallisena[AESW000].

Syötteet

Syötteenä annetaan:

- Toimintamoodi, ts. salaus tai purku
- 128-bittinen avain heksalukuna (16 x 8 bittiä = 32 heksamerkkiä)
- Lähdetiedosto, joka luetaan
- Kohdetiedosto, johon kirjoitetaan tulokset

Suorituskyky

ONGELMA – Kysy!

Tilavaativuus: Ohjelman käyttämä tila ei riipu salattavan aineiston koosta.

Aikavaativuus: 10 Mbit/s yhteiskäyttöympäristössä (users.cs.helsinki.fi)

Lähteet

FIPS197: U.S. Department of Commerce/National Institute of Standards and Technology, Federal Information Processing Standard, FIPS PUB 197 Advanced Encryption Standard (AES), 2001
AESW000: Wikipedia, Wikipedia article: Advanced Encryption Standard, 2017,