Määrittelydokumentti

Aineopintojen harjoitustyö: Tietorakenteet ja algoritmit

2016 (Periodi II)

Markus Auvo

1 Toteutettavat algoritmit ja tietorakenteet

Harjoitustyössä toteutetaan symmetriseen avaimeen perustuva lohkosalausalgoritmi DES (Data Encryption Standard). Algoritmin toiminta perustuu selväkielisen viestin pilkkomiseen lohkoihin, joista jokainen annetaan syötteeksi salausalgoritmille. Koska kyseessä on symmetriseen avaimeen perustuva algoritmi, sekä viestin salaus että salauksen purku toteutetaan samalla avaimella. DES-salauksessa selväkielinen viesti pilkotaan 64 bitin lohkoiksi, joista jokainen salataan algoritmilla. Seuraavassa esitetään yleisellä tasolla salausavaimen muodostus ja DES-algoritmin käyttö.

1.1 Salausavaimen muodostus

Alkuperäisestä 64-bittisestä avaimesta luodaan permutaatio-operaation PC1 kautta 56 bitin jono. 56-bittinen jono jaetaan kahteen 28-bittiseen osaan, minkä jälkeen kummankin osan bittejä siirretään vasempaan. Siirtooperaation jälkeen osat yhdistetään takaisin 56-bittiseksi jonoksi, josta luodaan permutatio-operaatiolla PC2 16 kappaletta 48-bittisiä osa-avaimia. 56 bittiä on avaimen pituutena riittämätön, mikä tekee DES-algoritmista turvattoman. Tässä harjoitustyössä ei kuitenkaan oteta asiaan tämän enempää kantaa.

1.2 Viestin salaus ja salauksen purku

Jokainen alkuperäisestä viestistä luotu 64-bittinen lohko salataan jokaista osa-avainta käyttäen. Jokaiseen alkuperäisestä viestistä luotuun 64-bittiseen lohkoon kohdistetaan alustuspermutaatio-operaatio (Initial Permutation), minkä jälkeen lohko jaetaan kahteen 32-bittiseen osalohkoon L ja R. Osalohkoon R kohdistetaan salauskierros (Round.)

Kierroksen alussa osalohkoon R kohdistetaan laajennusfunktio (Expansion function), jolloin lohko kasvatetaan 48-bittiseksi. 48-bittiseksi laajennettu osalohko salataan 48-bittisella osa-avaimella. Salauksen jälkeen 48-bittinen lohko jaetaan kahdeksaan 6-bittiseen lohkoon. Jokaiseen 6-bittiseen osalohkoon kohdistetaan

korvausfunktio (Substitution function). Jokaiselle 6-bittiselle lohkolle on oma taulukkonsa, jonka mukaan korvausfunktio suoritetaan. Korvausfunktion tuloksena saadaan kahdeksan 4-bittistä osalohkoa, jotka yhdistetään yhdeksi 32-bittiseksi lohkoksi. 32-bittiseen lohkoon kohdistetaan permutaatio-operaatio (Permutation). Kierroksen lopussa 32-bittiseen lohkoon ja ja salauksen alussa muodostettuun osalohkoon L kohdistetaan XOR-operaatio. Kierros toteutetaan jokaiselle salattavalle lohkolle jokaisella 16 osa-avaimella.

Kierroksen jälkeen 32-bittiset lohkot yhdistetään 64-bittiseksi lohkoksi, johon kohdistetaan käänteinen alustuspermutaatio (Inverse initial permutation). Operaation tuloksena saadaan 64-bittinen salattu lohko.

Salattu viesti puretaan suorittamalla salattuihin lohkoihin edellä kuvattu lohkosalausoperaatio, mutta soveltamalla kierrosten osa-avaimia päinvastaisessa järjestyksessä, jolloin tulokseksi saadaan alkuperäinen salaamaton 64-bittinen lohko.

2 Ongelman ratkaisu ja motivaatio

Harjoitustyössä ratkaistaan triviaali viestin salaus, jossa viestin sisältö koostuu .jpg-muotoisista kuvista. Harjoitustyössä toteutettavaksi algoritmiksi valittiin DES. DES-algoritmin tekee historiallisesti mielenkiintoiseksi se, että vuoden 1973 puolivälissä NBS (National Bureau of Standards), joka nykyään tunnetaan nimellä NIST (National Institute of Standards and Technology), julkaisi pyynnön, jossa etsittiin salausalgoritmia. Vuoden 1974 lopulla IBM esitteli algoritmin nimeltä "Lucifer", jonka NSA muokkasi vuoden 1976 lopulla muotoon, joka nykyään on DES. Ilmestymisensä aikoihin DES oli erittäin turvallinen, helposti ymmärrettävä, muokattavissa ja tehokas.[1]

[1] Introduction to encryption with DES.
http://ccm.net/contents/134-introduction-to-encryption-with-des

3 Ohjelman syötteet ja niiden käyttö

Alunperin ohjelman syötteenä oli määrä käyttää eripituisia merkkijonoja, joista pisimmät ovat megatavujen luokkaa. Salauksen purkamisen onnistumisen tarkastelu ei kuitenkaan osoittautunut mielekkääksi muutamaa miljoonaa merkkiä tarkastelemalla.

Tässä harjoitustyössä ohjelmalle annetaan syötteeksi kuvatiedostoja, jotka salataan ja joiden salaus puretaan algoritmia käyttäen. Kuvatiedostot ovat erikokoisia muutaman sadan kilotavun kokoluokasta aina usean megatavun kokoluokkaan. Eri kokoluokilla on määrä tarkastella algoritmin suorituskykyä.

4 Tavoitteena olevat aika- ja tilavaativuudet

Useimmissa lohkosalausalgoritmeissa lohkon koko on vakio, ja täten salausalgoritmin aikavaatimus riippuu salattavan viestin koosta eli salattavien lohkojen määrästä n. Jokainen lohko salataan 16 osa-avaimella, jolloin viestin salaukseen kuluva aika on $16n$, ja DES-salausalgoritmin aikavaatimukseksi muodostuu $O(n)$.