Salakirjoitusmenetelmiä

LUKUTEORIA JA LOGIIKKA, MAA 11

Salakirjoitusten historia on tuhansia vuosia pitkä. On ollut ”tarve” lähettää viestejä, joiden sisältö ei asianomaisen mielestä saanut tulla ulkopuolisten tietoon. Tämä johti viestien koodaamiseen, niin ettei ”väärä” henkilö sitä ymmärtänyt.

Yksinkertaisimpia koodauskeinoja on vaihtaa tekstissä esiintyvät kirjaimet toisiksi jollakin sovitulla tavalla. Tätä vaihtomenetelmää kutsutaan *salausavaimeksi*. Avain pitää olla sekä viestin lähettäjällä että vastaanottajalla. Ongelmia?
Helppo murtaa → kielessä esiintyvien aakkosten esiintymistiheyksiä on taulukoitu ja yleisemmin esiintyvät aakkoset on helppo paikantaa. Lisäksi, jos yksi viesti saadaan purettua → tiedetään avain ja kaikki viestit saadaan auki (jos käytetään samaa avainta).

Edellä mainitun kaltainen salausmenetelmä on Caesar-salaus → kirja.

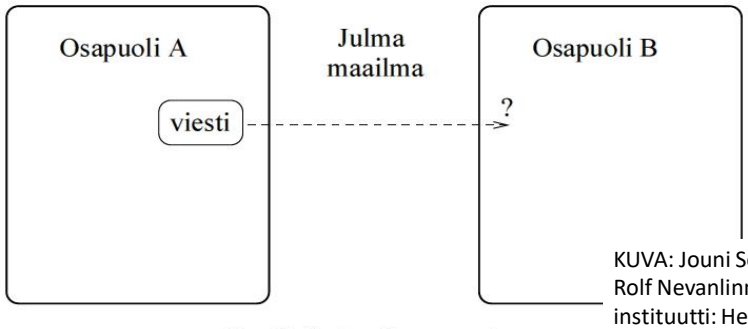
Saksalaiset käyttivät toisessa maailmansodassa Enigma-salakirjoituskonetta. Se perustui siihen, että käyttäjillä oli yhteinen, kuukausittain vaihtuva kirja, jossa mainittiin, minkälaisia asetuksia koneessa kunakin päivänä käytettiin. Lisäksi jokaisen viestin alussa kerrottiin tätä päiväsalausta käyttäen, mitkä ovat nimenomaan kyseiseen viestiin liittyvät asetukset. Kuvat: http://fi.wikipedia.org/wiki/Enigma_%28salauslaite%29

Nykyään netin ja sähköpostien aikana salausmenetelmien tarve ja käyttö on kasvanut räjähdysmäisesti. Samalla menetelmät ovat kehittyneet vaikeammin murrettaviksi. Tietysti myös koodinmurtajien keinot ja välineet ovat samalla tavoin kehittyneet. Tilanne on jatkuva ”kissa-hiiri leikki”.

Useimmat nykyaikaiset salausmenetelmät perustuvat lukuteorian käyttöön. Lähtökohtana on, että teksti muutetaan ensin numeeriseen muotoon, esim. käyttämällä ASCII- standardia, jonka jälkeen salataan numeerinen tieto.

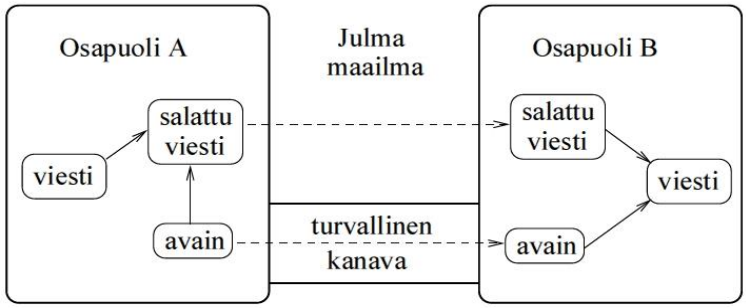
→ Monisteen (tunnilla jaettava) sivut 247 – 251 kertovat lyhyesti idean. Tarvitaan niin sanotut avainluvut.

Perinteinen ratkaisu



KUVA: Jouni Seppänen
Rolf Nevanlinna instituutti: Helsingin Yliopisto

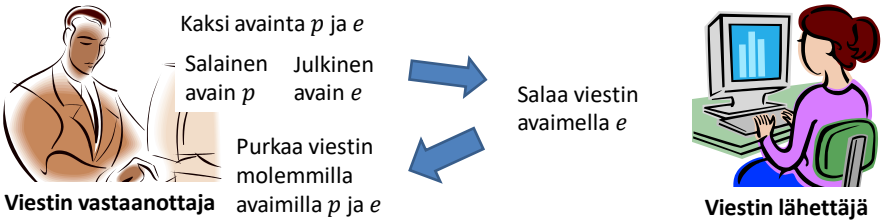
Kuva I.1: Kryptografian perusongelma



Julkisen avaimen salakirjoitus

Palataan vielä salausmenetelmien perusluonteeseen. Nimittäin joskus voi olla tilanne, että viestin lähettäjä ja vastaanottaja eivät pysty vaihtamaan käytettävä avaimia. Miten tällöin toimitaan?

On kuitenkin kehitetty salausmenetelmä, jossa avaimenvaihtoa ei tarvita lainkaan. (HUOM. vaihtoa, ei käyttöä, eli aina pitää salata!)
Menetelmän karkea idea on, että viestin **vastaanottaja** valitsee avaimet – joita on kaksi – ja lähettää niistä **vain toisen** viestin lähettäjälle.
Miten? Laittaa vaikka nettiin tai puhelinluetteloon, siis täysin julkiseen levitykseen. Viestin lähettäjä sitten salaa viestin tällä julkisella avaimella ja lähettää vastaanottajalle salatun viestin, joka purkaa viestin

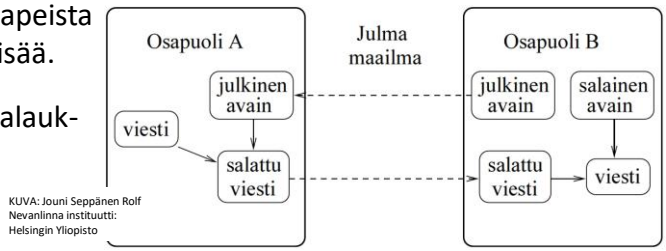


Koska toinen avain on koko ajan vain vastaanottajan hallussa, mitään avaimensiirrosta aiheutuvaa murtomahdollisuutta ei ole. Tosin nyt on mainittava se tosiasia, että viestin lähettäjän on jollakin tavoin saatava viestin saajan julkinen avain tietoon.

Periaatteessa kuku tahansa voi seurata tätä viestiliikennettä ymmärtämättä salattua viestiä. Tarkkailija/tunkeutuja saa selville toisen avaimen, kun se lähetetään vastaanottajalta lähettäjälle, samoin hän saa selville koodatun viestin, mutta ei osaa murtaa koodausta, koska häneltä puuttuu toinen avain.

Tällaista salausmenetelmää kutsutaan julkisen avaimen salakirjoitusmenetelmäksi. Näitä tunnetaan useita erilaisia (julkisesti) ja armeijoiden yms. kassakaapeista löytynee tukuttain lisää.

Tutustutaan RSA – salaukseen.



KUVA: Jouni Seppänen Rolf Nevanlinna instituutti: Helsingin Yliopisto

RSA – salausmenetelmä

Historiaa/Yleistä tietoa:

- RSA-salaus on *epäsymmetrinen julkisen avaimen salausalgoritmi*.
- RSA sai nimensä tekijöidensä sukunimien kirjaimista: Ron **R**ivest, Adi **S**hamir, Len **A**dleman, v.1977/1978.
- Perustuu suuren kokonaisluvun alkutekijöiden etsimiseen. Ison kokonaisluvun tekijöihin jako on yleisesti sekä aikavaativuudeltaan että laskennallisesti vaativa tehtävä.
- RSA-salauksessa käytetään *julkista avainta*, että *salaista avainta*.
- RSA ei sovellu suurten tietomäärien salaamiseen koska RSA-algoritmi ei ole erityisen nopea.

Matemaattiset työvälineet:

- Alkulukujen valinta.
- Eukleideen algoritmi.
- Eulerin ϕ-funktio.
- Diofantoksen yhtälö.
- Jäännösluokilla laskeminen.

Määritelmä, Eulerin φ −funktio:
Kun $n > 0$, niin määritellään joukko
$\Phi(n) = \{m \in \mathbb{Z} |\ 1 \leq m < n \text{ ja } \text{syt}(m,n) = 1\}$.
Tällöin Eulerin φ −funktion määrittelee yhtälö

$$\varphi(n) = |\Phi(n)|.$$

RSA:n algoritmin vaiheet:

1. Avainten luonti:

Julkinen avain: Valitaan suuret alkuluvut p ja q. Valitaan pienehkö luku e siten, että $\text{syt}\big(e, \varphi(pq)\big) = 1$. Ja jos valitsee luvuksi e pienehkön alkuluvun, kuten 17 tai 19, niin $\text{syt}\big(e, \varphi(pq)\big)$ on aina yksi, koska

$$\varphi(pq) \ = \ (p-1)(q-1)$$

on parillinen, p ja q ovat siis alkulukuja. Tällöin julkinen avain on lukupari (e, pq), joka julkaistaan (nettisivulla tai puhelinluettelossa).

Salainen avain: Lasketaan Diofantoksen yhtälöstä

$$ed \ \equiv \ 1 \ \big(\text{mod } \varphi(pq)\big), \qquad \text{missä siis } \varphi(pq) = \ (p-1)(q-1).$$

Tällöin salainen avain on d. Tämän jälkeen voidaan tuhota tieto luvuista p ja q!

2. Viestin kryptaaminen:

Viestin muuttaminen luvuksi M valitulla algoritmilla, jolle pätee

$$0 \ \leq \ M \ \leq \ pq - 1.$$

Viestin M salaaminen:
Salattu viesti

$$M' \equiv M^e \pmod{pq}.$$

Salatun viestin M' avaaminen:

$$M \equiv (M')^d \pmod{pq}$$

eli

$$(M')^d = M^{de} = M^{s\varphi(pq)+1} = M \cdot M^{s\varphi(pq)} \equiv M \cdot 1^s = M \pmod{pq}.$$

Esimerkki Löytyy monisteesta.
Harjoitus/kotitehtävä:
Aukaise salattu viesti kun, $M' = 13$ ja $e = 3, d = 27$ ja $pq = 55$.