Salakirjoituksia

Avainsanat: salakirjoitus, suoraan numeroiksi, Atblash, Caesar-salakirjoitus, ruudukko-salakirjoitus, julkisen avaimen salakirjoitus, RSA-salakirjoitus

Luokkataso: 3.-5. luokka, 6.-9. luokka, lukio

Välineet: kynä ja paperia, sakset, haaraniitti

Kuvaus: Tehtävässä esitellään erilaisia ja eritasoisia salakirjoitustapoja. Mukana on myös muutamia salausharjoituksia. Tehtävä toimii erinomaisesti yksin tai vaihtoehtoisesti johdatuksena salakirjoituskone Enigman toimintaan.

Aluksi

Salakirjoitusta tarvitaan monissa eri paikoissa kun halutaan, ettei yksityisiä tai salaisia tietoja joudu sivullisten käsiin. Salakirjoitusmenetelmiä on hyvin monia erilaisia. Niitä tarvitaan nykyään melkein kaikessa tietoliikenteessä. Useat tällä hetkellä käytössä olevista menetelmistä ovat niin monimutkaisia, ettei salauksia voida muodostaa ilman tietokoneita. Nykyiset salakirjoitusjärjestelmät ja niiden murtaminen perustuvatkin melkein pelkästään korkeampaan matematiikkaan. Matematiikan osa-alueista erityisesti lukuteoria ja algebra ovat tärkeässä asemassa.

Toteutusehdotus

Tutustutaan ensin yhdessä alla esiteltyihin salausmenetelmiin. Salausmenetelmistä kannattaa valita ikäryhmälle sopivimmat.

Muodostetaan salaviestirinkejä. Ringissä tulisi olla kolmesta kuuteen henkilöä, paria tai pientä ryhmää. Rinkejä voi myös muodostaa erilaisia, jolloin voidaan lopuksi vertailla erilaisten rinkien tehokkuutta salaviestien purkamisessa. Pelataan muutama harjoituskierros ennalta sovituilla salakirjoitusmenetelmällä. Salaviestin purkamisen haastavuutta saa muunneltua kerrottavan tiedon määrällä. Keskeisiä tietoja ovat esimerkiksi käytetty salausmenetelmä, miltä väliltä salausnumero on, miten usein salausnumeroa on vaihdettu jne. Lopuksi salauksen saa tehdä vapaavalintaisella menetelmällä. Salakirjoitusmenetelmiä on helppo keksiä myös itse yhdistelemällä tunnettuja menetelmiä omiin ideoihin. Tavoitteena on saada oma viesti kulkemaan salausringissä mahdollisimman pitkään siten, ettei kukaan ole saanut sen sisältöä purettua.

Ohjeet:

1. Keksi jokin viesti ja salaa se. Merkitse itsellesi muistiin alkuperäinen viesti ja sen


salaamiseen käytetty menetelmä. Älä näytä näitä tietoja kenellekään.
2. Lähetä salattu viesti eteenpäin. Liitä viestiin haluamasi määrä tietoa.
3. Yritä purkaa saamasi salaviesti. Jos saat viestin purettua, jätä se omalle pöydällesi. Jos taas et saa viestiä purettua, lähetä se eteenpäin. Viestin purkuun käytettävä aika kannattaa rajata esimerkiksi viiteen minuuttiin riippuen käytössä olevista salausmenetelmistä ja niiden haastavuudesta.
4. Onnistutko saamaan jonkin lähettämistäsi viesteistä takaisin?

Kysymyksiä pohdittavaksi:

Millainen oli liian helppo tai liian vaikea salattu viesti? Minkälaiset viestit kiersivät pisimmän matkan? Minkälainen salakirjoitus on siis hyvä salakirjoitus? Minkälaisia menetelmiä hyvät salaajat eli kryptografit käyttivät? Entä minkälaisia menetelmiä viestien purkamisessa onnistuneet henkilöt käyttivät? Minkälainen on siis hyvä salakirjoituksen purkaja eli kryptoanalyytikko? Tässä voidaan myös pohtia ringin pituuden vaikutusta salaviestin purkamisen onnistumiseen. Entä vaikuttiko se, purettiinko viestejä yksin, pareittain vai ryhmissä?

Hieroglyfejä tai roomalaisia numeroita ei käytetä enää yleisesti. Ovatko ne siis salakirjoitusta, jos kerran valtaosa niitä ei ymmärrä? Vastaavasti onko suomen kieli salakirjoitusta englantilaisille?

Entä kannattaako aina kertoa, jos toisen käyttämän salausmenetelmän on saanut purettua?

Vinkki: Salakirjoituksiin voi tutustua myös ilman salausrinkiä. Esimerkiksi pelkästään Caesar-salauskiekkojen valmistus on mukavaa puuhaa!

Suoraan numeroiksi

Yksi tapa muodostaa salakirjoitus on muuttaa jokainen kirjain numeroksi seuraavalla tavalla:

Kirjain	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**
Vastaava numero	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Kirjain	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**Å**	**Ä**	**Ö**	
Vastaava numero	16	17	18	19	20	21	22	23	24	25	26	27	28	29	

Tällä salakirjoituksella esimerkiksi sana KISSA olisi numerosarja 11-9-19-19-1. Salakirjoitus puretaan muuttamalla jokainen numero takaisin sitä vastaavaksi kirjaimeksi käyttämällä yllä olevaa taulukkoa apuna.

Tehtävä:

1. Salakirjoita sanat
    a. KOIRA
    b. SUMMAMUTIKKA
    c. TIIKERI
    d. HEVONEN
2. Pura salakirjoitetut sanat
    a. 11-5-19-28
    b. 18-1-4-9-15
    c. 16-29-25-20-28

Atblash

Atbash-salakirjoitus on myös hyvin vanha salakirjoitusmenetelmä, jossa jokainen kirjain korvataan aakkosten "vastakkaisella" kirjaimella. Nämä on esitetty alla olevassa taulukossa.

Kirjain	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**
Vastaava numero	Ö	Ä	Å	Z	Y	X	W	V	U	T	S	R	Q	P	O
Kirjain	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**Å**	**Ä**	**Ö**	
Vastaava numero	N	M	L	K	J	I	H	G	F	E	D	C	B	A	

Atblash-salauksella salakirjoitettu sana KISSA olisi siis kirjainyhdistelmä SUKKÖ.

Tehtävä:

1. Kirjoita oma nimesi Atbash-koodilla.
2. Ratkaise seuraavat salatut sanat:
    a. HUVSO
    b. OQYPÖ
    c. RÖQQÖK
    d. SÖLJJÖ

Jos viesteissänne esiintyy lukuja, voi nekin salakirjoittaa numero kerrallaan samalla tekniikalla seuraavasti:

Numero	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**0**
Atblash	0	9	8	7	6	5	4	3	2	1

Tehtävä:

1. Mitä nyt on salakirjoitettuna: PUHELINNUMERONI ON 4122455

2. Mitä on suomeksi seuraava viesti: KÖRÖSOOZU OP 8-4-3-3-0

Jos haluaa saada tekstistä oikein hämärän näköistä, niin numerot voi pistää aakkosten perään saman pötköön, jolloin kirjainten muuntotaulukko näyttää tältä:

Merkki	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
Atblash	0	9	8	7	6	5	4	3	2	1	Ö	Ä	Å
Merkki	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
Atblash	Z	Y	X	W	V	U	T	S	R	Q	P	O	N
Merkki	Å	Ä	Ö	1	2	3	4	5	6	7	8	9	0
Atblash	**M**	**L**	**K**	**J**	**I**	**H**	**G**	**F**	**E**	**D**	**C**	**B**	**A**

Tässä kohtaa pitää olla erittäin tarkkana, etteivät nolla ja kirjain O mene sekaisin.

Tehtävä:

1. Mitä on salakirjoitettuna: 16 OMENAA
2. Mitä on suomeksi Ö0UU0Ö00X2Z O372UT6ÄÅL YZ FC-G-JAJ-JE

Caesar-salarkirjoitus

Seuraavaa salakirjoitusmenetelmää käytti jo Caesar muinaisessa Roomassa. Caesar-salakirjoituksessa käytetään osittain samoja temppuja kuin suoraan numeroiksi -menetelmässä.

M-A-K-K-A-R-A	Alkuperäinen sana
13-1-11-11-1-18-1	Muutetaan numeroiksi
16-4-14-14-4-21-4	Lisätään jokaiseen numeroon valittu numero, esimerkiksi kolme
P-D-N-N-D-U-D	Muutetaan numeroista takaisin kirjaimiksi

Salauksen purku tapahtuu tekemällä sama uudestaan, mutta tällä kertaa vähentämällä tai lisäämällä jokaiseen numeroon valittu luku. Tämä voi olla hieman työlästä ja tylsää käsin tehtäväksi, joten tätä koodausta varten on laadittu salauskiekko ohjeineen.

Salattua viestiä ei voi purkaa, jos ei tiedä oikeata salausnumeroa, joten se pitää muistaa merkitä viestin viereen. Esimerkiksi voisimme merkitä salausnumerolla 3 salattua sanaa MAKKARA seuraavasti: PDNNDUD (3). Salausnumero laitetaan siis sulkuihin viestin perään. Tällöin se, jolle viesti on tarkoitettu, osaa käyttää oikeaa avaustekniikkaa, mutta ulkopuolinen ei edelleenkään ymmärrä viestiä.

Tehtävä:

1. Salaa salausnumerolla viisi sanat
    a. KAAKAO

b. KYNÄ
c. AUTO
d. KOIVU

2. Ratkaise seuraavat salatut sanat:
   a. DXULQNR(4)
   b. IIZZM(9)
   c. YVVZN(14)
   d. UVTTJ(2)

LISÄÄ MAHDOLLISUUKSIA

Jos haluat viestiä kaverisi kanssa ja salata viestinne vielä tarkemmin, voitte sopia koodauksen vaihdosta. Voitte esimerkiksi kirjoittaa ensimmäiset kolme sanaa salausavaimella 5, seuraavat kaksi sanaa avaimella 2 ja niin edelleen. Tätä varten on hyvä muodostaa yhteinen taulukko, josta ilmenee salausavainten vaihtelu. Taulukko ei tietenkään saa joutua ulkopuolisten käsiin.

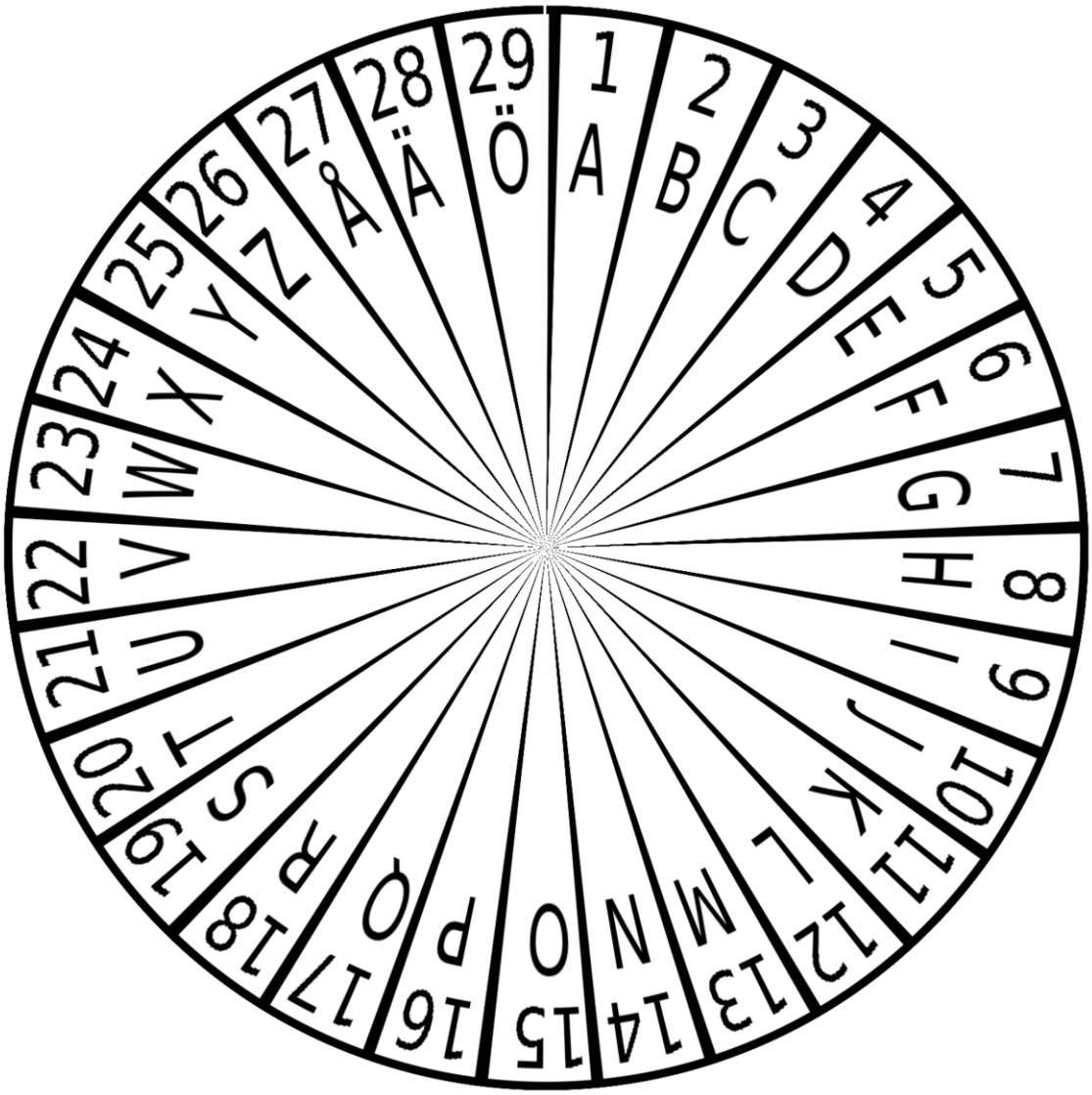
Sana	1.	3.	5.	9.	15.	16.	…
Salausavain	5	2	6	9	11	8	…

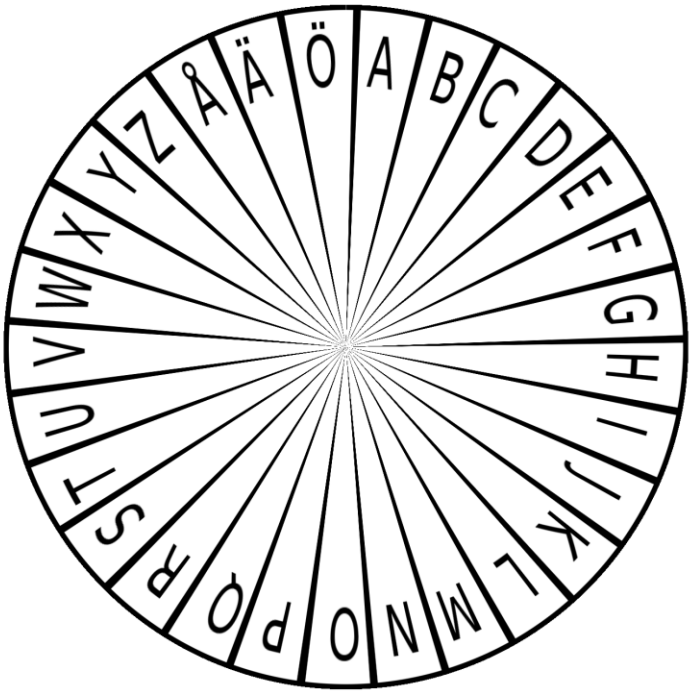
Salausavainta vaihtelemalla salakirjoitus on jo paljon hankalampi murtaa. Helposti sovittava ja salausta edelleen parantava keino on aloittaa sovitulla salausnumerolla, ja jokaisen salakirjoitetun kirjaimen jälkeen kiertää kiekkoa pykälän verran myötäpäivään. Näin jokainen salattava kirjain salataan omalla salausavaimellaan. Tätä ajatusta vie pidemmälle salakirjoituskone nimeltä Enigma (tehtävä löytyy Summamutikka-keskuksen materiaalipankista).

SALAUSKIEKON VALMISTUS JA KÄYTTÖ

Leikkaa salauskiekot huolellisesti irti paperista. Tee kummankin kiekon keskelle pieni reikä ja laita pienempi kiekko paksumman päälle siten, että molempien kiekkojen kirjaimet näkyvät. Liitä kiekot haaraniitillä yhteen.

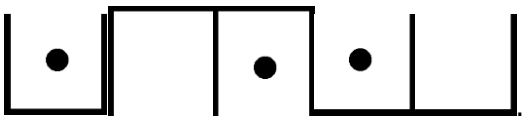
Viestiä **salatessa** valitaan ensin salausnumero. Sen jälkeen pyöritetään sisempää kiekkoa asentoon, jossa sisemmän kiekon A-kirjain on kyseisen salausnumeron kohdalla. Tämän jälkeen etsitään salattavan viestin kirjaimet sisemmästä kiekosta. Salatun viestin kirjaimet ovat silloin ulommassa kiekossa. Kun viesti halutaan **purkaa**, katsotaan ensin mitä salausnumeroa viestin salaamiseen on käytetty. Tämän jälkeen pyöritetään sisempää kiekkoa asentoon, jossa sisemmän kiekon A-kirjain on kyseessä olevan salausnumeron kohdalla. Tämän jälkeen katsotaan salatun viestin kirjaimet ulommasta kiekosta, jolloin puretun alkuperäisen viestin kirjaimet näkyvät sisemmässä kiekossa.

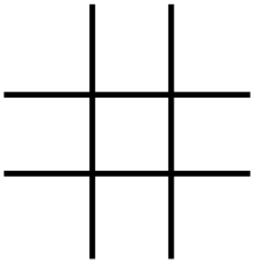

1 A
2 B
3 C
4 D
5 E
6 F
7 G
8 H
9 I
10 J
11 K
12 L
13 M
14 N
15 O
16 P
17 Q
18 R
19 S
20 T
21 U
22 V
23 W
24 X
25 Y
26 Z
27 Å
28 Ä
29 Ö

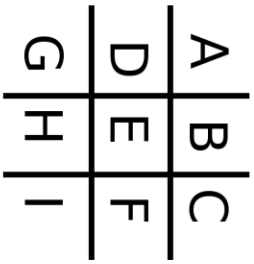

A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
P
Q
R
S
T
U
V
W
X
Y
Z
Å
Ä
Ö

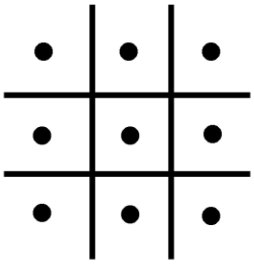
Ruukukko-salakirjoitus

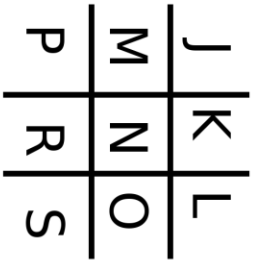
Tässä salakirjoitusmenetelmässä kirjaimet muutetaan symboleiksi. Salakirjoitusta varten tarvitset salausruudukon. Voit myös itse keksiä symboleita vastaavat kirjaimet!

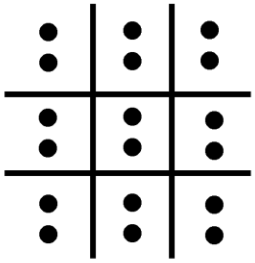
Ruudukko-salakirjoituksella sana ”kirja” on  . Keksi itse lisää salakirjoitettavia sanoja ohessa olevien ruudukoiden avulla.

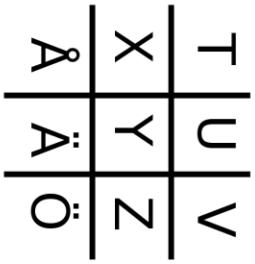


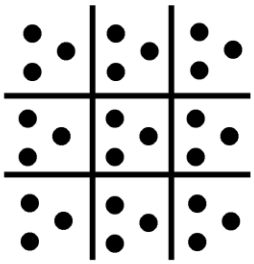

A B C
D E F
G H I

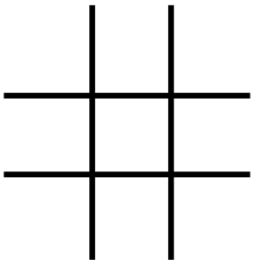


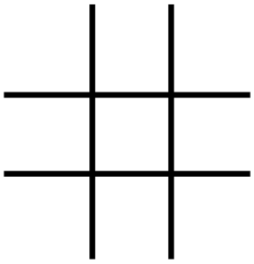
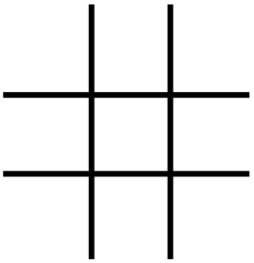
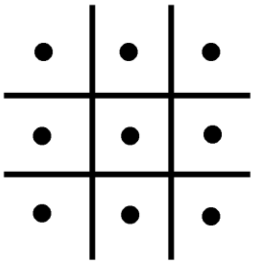
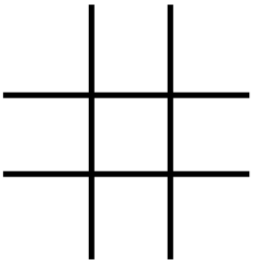
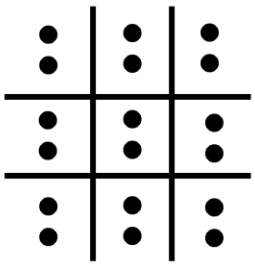
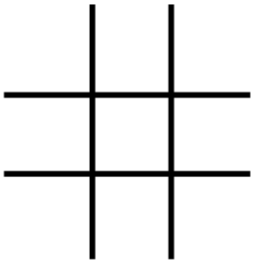
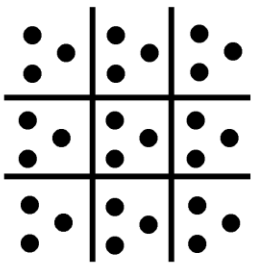
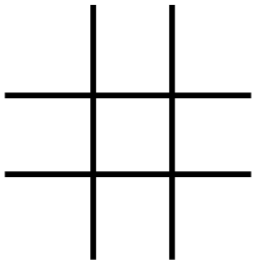

J K L
M N O
P R S




T U V
X Y Z
Å Ä Ö





Julkisen avaimen salakirjoitus

Monet muut tämän tehtäväsarjan salakirjoitukset perustuvat siihen, että kummallakin viestijällä on jokin aikaisemmin sovittu sääntö tai kone, jonka avulla he salakirjoittavat ja purkavat lähettämiään viestejä. Tutkitaan seuraavaksi kuvitteellista tilannetta, jossa Matias ja Terhi haluavat lähettää toisilleen viestejä ilman, että uteliaat ulkopuoliset pääsevät niitä tutkimaan. Leikitään, että Matiaksen ja Terhin ainut mahdollinen yhteydenpitokeino on postin lähettäminen.

Aikaisemmat salakirjoitusmenetelmät vastaavat tilannetta, jossa Matiaksella ja Terhillä on kummallakin avain lukittuun laatikkoon. Kun Matias haluaa lähettää Terhille viestin, hänen tarvitsee vain laittaa viesti laatikkoon, lukita laatikko ja laittaa se postiin. Perillä Terhi voi avata laatikon avaimellaan ja lukea viestin. Tämä on toimiva järjestelmä, mutta siinä on yksi ongelma. Nimittäin jotta järjestelmä toimii, on Matiaksen ja Terhin pakko vaihtaa avaimet jossain vaiheessa ennen viestin lähettämistä. Jos heillä on ollut mahdollisuus tavata, ei tässä ole ongelmaa, mutta entä jos ainut viestintäkanava on tosiaan posti? Jos avain on lähetetty joskus aikoinaan postin välityksellä, on joku ilkeä henkilö saattanut päästä käsiksi kirjeeseen ja kopioida avaimen matkalla. Tällöin tämä henkilö voisi kirjeitä varastelemalla avata Matiaksen ja Terhin salaisen laatikon matkalla ja lukea viestit ilman, että Matias ja Terhi arvaisivat mitään. Tämän ongelman ratkaisuksi on kehitetty niin sanottu *epäsymmetrinen salakirjoitus*, josta tässä tehtävässä puhutaan.

Epäsymmetrinen salakirjoitus vastaa sitä, että kun Terhi haluaa Matiakselta viestin, hän hankkii itselleen laatikon lukkoineen, pitää avaimen itsellään ja lähettää laatikon avattuna Matiakselle. Matias laittaa viestin laatikkoon ja sulkee laatikon. Nyt kukaan muu kuin Terhi ei voi avata laatikkoa (ei edes Matias), sillä ainoa avain laatikkoon on Terhillä. Matias postittaa laatikon Terhille ja Terhi voi lukea viestin.

RSA-salakirjoitus antaa varsin hyvän kuvan nykyisten salakirjoitusjärjestelmien toiminnasta. RSA-salakirjoitus perustuu siihen, että on helppoa laskea kahden luvun tulo, mutta isosta luvusta voi olla hankalaa sanoa, minkä kahden luvun tulo se oikein on. Asia on näin etenkin silloin, jos kyseiset kaksi lukua ovat suunnilleen samankokoisia alkulukuja. Vuoteen 2007 asti oli käynnissä haaste, jossa saattoi voittaa rahapalkintoja löytämällä tulon tekijät. Esimerkiksi luvun

25195908475657893494027183240048398571429282126204032027771378360436620
20707595556264018525880784406918290641249515082189298559149176184502808 4
89120072844992687392807287776735971418347270261896375014971824691165077 6
13379859095700097330459748808428401797429100642458691817195118746121515 1
72654632282216869987549182422433637259085141865462043576798423387184774 4
47920739934236584823824281198163815010674810451660377306056201619676256 1
33844143603833904414952634432190114657544454178424020924616515723350778 7
07749817125772467962926386356373289912154831438167899885040445364023527 3

819513786365643912120103971228221207203 57

tekijöiden löytämisellä olisi voinut voittaa 200 000 dollaria. Luvulla on oma nimikin, RSA-2048.

RSA-salauksen käyttö voi vaikuttaa monimutkaiselta, mutta kaikki laskutoimitukset ovat helppoja tehdä tietokoneella, ja tietokoneiden viestiliikenteessä tätä useimmiten käytetäänkin.

AVAIMIEN MUODOSTAMINEN

Salatun viestin lähettämisen ensimmäisessä vaiheessa pitää muodostaa sekä julkinen että salainen avain. Tämä vastaa äskeisen tekstin tilannetta, jossa Terhi haluaa Matiakselta viestin, joten hän hankkii lukittavan laatikon, johon vain hänellä on avain. Lukittavaa laatikkoa vastaa eräässä mielessä julkinen avain, ja salainen avain sen ainutta avainta. Nämä muodostetaan seuraavasti:

Yleinen ohje	**Esimerkki**
Valitaan ensin kaksi alkulukua, p ja q.	Valitaan ensin kaksi alkulukua, $p = 3$ ja $q = 11$.
Lasketaan luku $N = pq$.	Lasketaan luku $N = pq = 3 \cdot 11 = 33$.
Valitaan luku $1 < d < N$ siten, että luvuilla d ja $(p-1)(q-1)$ ei ole yhteisiä tekijöitä (eli niin, että ne ovat suhteellisia alkulukuja).	Valitaan luku $1 < d < N$ siten, että luvuilla d ja $(p-1)(q-1) = 2 \cdot 10 = 20$ ei ole yhteisiä tekijöitä. Olkoon vaikka $d = 3$.
Valitaan x siten, että $dx \equiv 1\ (mod\ (p-1)(q-1))$, eli niin, että luvun dx jakojäännös luvun $(p-1)(q-1)$ suhteen on 1.	Valitaan x siten, että $dx \equiv 1\ (mod\ (p-1)(q-1))$, eli $3x \equiv 1\ (mod\ 20)$. Tähän kelpaa $x = 7$.
Hävitetään kaikki lukuja p ja q koskeva tieto.	Hävitetään kaikki lukuja p ja q koskeva tieto.
Julkinen avain on nyt lukupari N, x ja salainen avain lukupari N, d.	Julkinen avain on nyt lukupari $33, 7$ ja salainen avain lukupari $33, 3$.

VIESTIN SALAKIRJOITTAMINEN

Yleinen ohje	**Esimerkki**
Kun Matias on saanut Terhiltä julkisen avaimen N, x, haluaa hän ensin muuttaa viestinsä luvuksi m, missä $1 < m < N$ (esimerkiksi suoraan numeroiksi -menetelmällä). Tämän vaatimuksen takia myös luvut p ja q valitaan mahdollisimman suuriksi, jotta isojakin viestejä voitaisiin lähettää.	Matias on saanut Terhiltä julkisen avaimen $33, 7$. Hän haluaa lähettää Terhille viestin 18, joka tarkoittaa heidän tapaamisensa kellonaikaa.
Lähetettävä viesti on tällöin luku $c \equiv m^x \ (mod\ N)$, eli se luku, joka jää jakojäännökseksi, kun luku m^x jaetaan luvulla N.	Matiaksen lähettämässä viestissä on siis luku $c \equiv 18^7 \ (mod\ 33) = 6 \ (mod\ 33)$.
Kun Terhi saa Matiakselta viestin c, voi hän laskea alkuperäisen viestin m kaavasta $m \equiv c^d \ (mod\ N)$, eli alkuperäinen luku on se luku, joka jää jakojäännökseksi, kun luku c^d jaetaan luvulla N.	Terhi on saanut Matiaksen viestin ”6”. Nyt hän voi purkaa viestin kaavalla $c^3 = 6^3 = 216 \equiv 18 \ (mod\ 33)$. Terhi osaa siis saapua tapaamiseen oikeaan aikaan.