2 SALAKIELET

LEIKKIKIELET

Kielellä ja sanoilla leikittely on ikivanha huvi, jota ovat harrastaneet niin lapset kuin aikuiset. Lapset ovat siinä usein aikuisia parempia, sillä juuri lapsenahan opitaan puhumaan. Lapset, joiden ympäristössä puhutaan useampaa kieltä, oppivat usein itsekin puhumaan kahta tai kolme kieltä jo kolme- neljävuotiaina. Jos aikuinen alkaa opetella uutta kieltä, siihen yleensä menee vuosia, eikä hän koskaan lausu sitä kunnolla, yhtä hyvin kuin ne, jotka ovat sen kielen oppineet jo lapsina.

Joskus lapsilla ei ole tarpeeksi puheliasta seuraa, jolloin heillä on huonot mahdollisuudet oppia edes äidinkieltään. 1970-luvulla Yhdysvalloissa eli kaksostytöt, Grace ja Virginia, joita hoiti vanha isoäiti, joka puhui saksaa. Tyttöjen molemmat vanhemmat olivat päivät töissä, eivätkä paljon puhuneet heille, eikä lähiseudulla asunut muita lapsia. Koska heillä ei ollut tilaisuutta oppia kunnolla mitään kieltä, he kehittivät aivan oman, kahdenkeskisen "salakielen". Siihen kuului, että he kutsuivat toisiaan nimillä Poto ja Cabenga. Aikuiset luulivat, että he ovat niin jälkeenjääneitä, etteivät opi kunnolla puhumaan, eivätkä sen vuoksi enää yrittäneetkään puhua heille. Lopulta tyttöjen kieltä alettiin tutkia, ja todettiin, että he olivat kehittäneet uuden kielen. Siihen oli lainattu sanoja englannista ja isoäidin puhumasta saksasta, mutta osa sanoista oli aivan uusia. Muiden ihmisten oli hyvin vaikea oppia ymmärtämään tätä kieltä, koska he puhuivat sitä niin nopeasti ja rytmikkäästi.

Tove Janssonin muumikirjassa Taikurin hattu esiintyvät pienet otukset Tiuhti ja Viuhti. Hekin puhuvat omaa kieltään, jota kaikki maailman Tiuhtit ja Viuhtit puhuvat. "Mitäti sinäti ajatteletti?" Muumeilla on vaikeuksia ymmärtää heidän puhettaan, mutta Hemuli hoksasi heti, miten kieli toimii. Hemuli, joka halusi kiusata Nipsua, käytti tulkin asemaansa hävyttömästi hyväksi.

Suomalaisia leikkikieliä on keksitty monia. "Siansaksaa" olet varmaan joskus kuullutkin:

SIANSAKSA: Heiska lavonen keti verran kuolasuormaa sirven jävyitse. = Laiska hevonen veti kerran suolakuormaa järven sivuitse.

KONTINKIELI Konamintti koinsöntti kokokontti komenaontti. = Minä söin koko omenan.

RISAKIELI Rinäsisä ristavasa riletosa riika-asa reitikkavisa. = Sinä vasta olet aika veitikka.

PUNKAKIELI Pulettonka puummemanka purmahinanka puomensunka puumanka. = Olet maamme armahin Suomenmaa.

RAAPPAKIELI Ränämiippa rasanooppa rahuapuuppa räättäviippa räältäkiippä. = Minä osaan puhua viittä kieltä.

LEKKERIKIELI Leisin sokkeri leelelläni mikkeri, lettä ekkeri levisitte käkkeri letsomassa kakkeri. = Soisin mielelläni, että kävisitte katsomassa.

19.7.2015 J. Holvikivi
Salatieto

VER-kieli Tuuver siiver vaaver miiver kaaver. (tai) Tuuver leever siivernääver vaaver miivernuuver kaaversaaverniiver. = Tule sinä vain minun kanssani.

TAIAISEN KIELI Mitivitä sitivinä utivuutta titiviedät? =Mitä uutta sinä tiedät?

RENGONKIELI Nosa nasa katarimpe, tensit märrätym tuoaren. (tai) Nosa nasa katarimpe, tensit rätmärym aturen. = Sano sana takaperin, sitten ymmärrät rentua.

PREERIAN MERKKIKIELI

Ennen kuin eurooppalaiset saapuivat Pohjois-Amerikkaan, oli manner suhteellisen harvaan asuttu. Intiaanien yhteiskunnat olivat hallinnoltaan kevyitä ja löyhiä, eikä heillä ollut suuria kaupunkeja. Heimot puhuivat satoja eri kieliä, jotka kuuluivat kymmeniin kielikuntiin, toisin sanoen ne erosivat toisistaan enemmän kuin eurooppalaiset kielet keskenään. Monet osasivat puhua äidinkielensä lisäksi paria naapuriheimojenn kieltä. Yleisessä heimojen välisessä käytössä tehokkain oli kuitenkin viittomakieli, jonka merkit olivat laajalti tunnettuja mantereen etelä- ja keskiosissa. Koska preeriaintiaanit, jotka liikkuivat puhvelilaumojen perässä laajalla alueella, käyttivät paljon viittomista, on kieltä kutsuttukin "Preerian merkkikieleksi". Sitä käyttäen pystyivät eri kieliä puhuvat ihmiset keskustelemaan keskenään. Varsinkin vanhat miehet, jotka kävivät heimojen välisiä neuvotteluja, osasivat pitää pitkiä puheita viittomalla. Viittomista käyttivät myös tarinankertojat, ja jopa perheenjäsenet keskenään. Viittomalla myös huviteltiin: viittomatanssissa nainen menee piirin keskelle tanssimaan, ja viittoo valitsemalleen miehelle ehdotuksen ryhtyä lemmenleikkiin. Miehen pitää osata viittoa siihen älykäs vastaus, jollei halua joutua muiden naurun kohteeksi.

Viittomakielen alkuperästä tai kehittäjistä ei ole tietoa, mutta se on vuosisatoja vanha, koska jo ensimmäiset espanjalaiset seikkailijat Pohjois-Amerikan eteläosissa 1500-luvulla kertoivat siitä. Parhaimmillaan arvellaan jopa yli sadan tuhannen intiaanin osanneen puhua sitä käyttäen. Merkit olivat kaikkialla samat, joten väärinkäsityksiä ei syntynyt. Kuuluisat savumerkit taas vaihtelivat heimolta toiselle, ne olivat pikemminkin salakieli kuin yleiskieli.

Suuri osa viittomista oli käsimerkkejä: eteenpäin taivutetut kädet ohimoille nostettuina kuvasivat puhvelinsarvia ja siis puhvelia. Suuta kohti liikkuva käsi merkitsi syömistä. Viittomisen yhteydessä pidettiin kasvot peruslukemilla eikä ilmehditty. Kaikki ilmaistiin käsien avulla, ja käsieleiden tuli olla kauniita ja pyöreitä. Merkkejä oli niin paljon erilaisia, että niillä pystyi käymään täydellisesti keskustelun, eli viittomakieli oli todellinen kieli. Nykyaikaista kuurojen kieltä lukuunottamatta maailmassa on tiettävästi vain yksi toinen täydellinen viittomakieli, ja sen ovat kehittäneet Australian alkuasukkaat.

Esimerkkejä:

Mikä on nimesi?	KYSYMYS - SINÄ- KUTSUTAAN
Kuinka vanha olet?	KYSYMYS -KUINKA MONTA - SINÄ - TALVI
Hän nimensä on Pikku Majava.	HÄN - KUTSUTAAN - PIENI- MAJAVA
Hän on rohkea.	HÄN - SYDÄN -VAHVA
Minulla on hauskaa.	MINÄ-OMISTAA-SYDÄN-AURINGONNOUSU

Voit jopa opiskella Youtuben avulla preerian merkkikielen käyttöä.

19.7.2015 J. Holvikivi
Salatieto

VARKAIDEN SALAKIELET

Euroopassa oli keskiajalla paljon kodittomia ja maattomia ihmisiä, jotka kiertelivät kerjäämässä, kaupustelemassa tai varastelemassa. Heidän parissaan syntyi salakieliä, jotka olivat sekoituksia eri seutujen murteista ja kielimuodoista. Saksassa kiertolaisten kieltä kutsuttiin kerjurinlatinaksi eli 'Rotwelsch', ruotsissa 'rotvälska'. Siinä oli sanoja myös maattomien kansojen kielistä eli mustalaisten kielestä ja juutalaissaksasta. Vähitellen siitä tuli rikollisten salakieli. Muita tunnettuja varkaiden salakieliä oli "Thief Talk" Lontoossa, ja Bombayn kaupustelijoiden slangi. Rikollisten salakielet säilyivät salaisina, koska sanojen paljastamisesta seurasi ankara rangaistus. Kielitieteilijä, joka oli tutkinut Bombayn kaupustelijoiden kieltä ja julkaissut siitä tutkimuksen, hakattiin pahasti, kun hän erehtyi palaamaan Bombayihin.

Lontoon varkaiden kieltä puhuttiin muuten kuin englantia, mutta siinä oli peitesanoja, kuten:

apple pies	englanniksi	eyes,	silmät,
forks,		fingers,	sormet,
pride and joy,		boy,	poika,
Twist and twirl,		girl eli	tyttö.

Suomessakin on ainakin vankilaslangi, eli kieli, jota vankiloissa käytetään. Siinäkin on runsaasti kiertoilmauksia rikoksille, poliiseille, ja muille alan sanoille. Vanhaa vankilakieltä ovat 'puhaltaa, honata, pohmia', joilla tarkoitettiin varastamista, 'taikina' merkitsemässä dynamiittia, ja 'taulu' tarkoittamassa kasvoja.

PAREMMAN VÄEN SALAKIELET

Mikä on salakielen tarkoitus? Paitsi, että sen avulla pidetään tietojenvaihto salaisena, sillä myös erotutaan muista ja sen puhujat osoittavat toisilleen kuuluvansa jengiin. Siksi salakielet eivät rajoitukaan pelkästään rikollisten harrastukseksi. Myös ylhäisö ja hallitseva luokka ovat halunneet erottua tavallisesta kansasta puhumalla hienommin tai jopa aivan eri kieltä. Suomessakin aikoinaan hallituksen edustajat puhuivat ruotsia ja kansa suomen eri murteita.

Muinaisessa Meksikossa oli aateliston salakieliä. Misteekki-kansan parissa kutsuttiin tavallista kansaa 'maan väeksi', joka ei osannut puhua oikeaa kieltä. Ylhäisön sanottiin laskeutuneen puista, koska he olivat jumalien jälkeläisiä. Ylhäisö puhui hyvin hienostelevaa kieltä, joka oli tulvillaan vertauskuvia: kun tavalliset ihmiset yksinkertaisesti kuolivat, sanottiin aatelisten 'pyörtyneen'. Tavalliset naiset ruokkivat lapsia rintamaidolla, mutta aatelisnaiset vuodattivat 'hunajaa' vauvoilleen. Aateliset eivät myöskään pissanneet vaan 'pirskottivat kastetta'.

Misteekkien naapurikansalla mayoilla oli aatelisten salakieli, jonka päälliköt opettivat pojilleen. Ennenkuin mies saattoi päästä kylän päälliköksi, hänen piti läpäistä tutkinto tässä kielessä osoittaakseen, että todellakin on jaloa sukua, koska on oppinut kielen isältään. Kokeessa ylipapit kyselivät kokelailta arvoituksia tällä kielellä.

19.7.2015 J. Holvikivi
Salatieto

TAIKASANAT

Itä-afrikkalaisessa swahilin kielessä ja länsiafrikkalaisessa jorubassa sana 'baba' tarkoittaa isää. Sen sijaan puolassa se tarkoittaa vanhaa naista, ja japanissa 'baba' on vanha nainen tai imettäjä. 'Mama' puolestaan merkitsee äitiä swahilissa ja ranskassa, mutta isää georgiassa ja autralialaisessa pitjanjatrara-kielessä, ja enoa Intiassa puhutussa tamilissa. Tuntuisiko oudolta kutsua miestä mamaksi?

Mieti:

Voimmeko sopia sanojen merkityksen aivan miten huvittaa? Mikä on sanan suhde sen tarkoittamaan asiaan? Onko sillä väliä, miksi jotain esinettä, ihmistä tai eläintä kutsutaan?

Pelkästään järjellä ajatellen näin näyttäisi olevan. Sanojen mama ja baba/papa käyttö näyttää esimerkissämme varsin mielivaltaiselta, mutta todellisuudessa se ei ole aivan näin satunnaista: suuressa osassa maailman kieliä äitiä tarkoittavassa sanassa on 'ma' tai 'na'-äänne: 'ma' kiinassa ja thaissa, 'emä' ja 'emo' suomessa, 'mother' englannissa, 'nan' mayassa, 'ammaa' tamilissa, ja niin edelleen.

Joskus sata tuhatta vuotta sitten ihmiset alkoivat puhua, he kehittivät kielen. Kielen tehtävänä on ilmaista asioita äänteiden avulla, niin että yksi äänneyhdistelmä on 'symboli' tai merkki, jolla tarkoitetaan juuri tiettyä asiaa. Äänneyhdistelmä saa informaatioarvon, se kertoo jotain. Sanomalla 'mama' lapsi ilmoittaa, että hän kaipaa äitiään: antamaan ruokaa, lohduttamaan, tai hellimään. 'Mama' on pienelle lapselle taikasana, jolla kaikki kääntyy hyväksi. Jo hyvin varhaisina aikoina ihmiset oivalsivat, kuinka hyödyllinen ja merkityksellinen kieli oli. He alkoivat kunnioittaa tätä keksintöään syvästi, ja uskoivat, että sanoilla saattoi olla suorastaan maagista voimaa. Sanat saattoivat tuoda mukanaan siunauksen, hyvää onnea, tai sanoilla saattoi kirota ja aiheuttaa pahaa. Sanoilla kutsuttiin avuksi luonnossa asuvia näkymättömiä henkiä. Joitakin sanoja oli varottava lausumasta, ettei arvaamattomia asioita alkanut tapahtua.

Ennen uskottiin, että esimerkiksi karhu on niin voimakas eläin, ettei siitä sovi puhua huolettomasti. Arveltiin, että se voisi kuulla, kun sen nimeä kutsutaan. Niinpä sen 'oikean' nimen 'oksi' sijasta sanottiin 'karhu' eli karhea eläin. Samoin englannin kielessä 'bear' tarkoitti aikoinaan ruskeaa (brown) eläintä.

Ihmisen nimen ajatellaan olevan läheisesti hänen henkilöönsä liittyvä ominaisuus. Madagaskarilla ihmiset eivät paljasta oikeaa nimeään muille, etteivät nämä voisi sen avulla tehdä vahingoittavia taikoja. Euroopassa ei kerrota lapsen nimeä ennenkuin lapsi on kastettu, ettei paholainen veisi lasta. Australiassa taas on kiellettyä lausua kuolleiden ihmisten nimiä. Pelätään, että kuolleen henki on vielä niin lähellä, että se saattaa palata takaisin aiheuttamaan harmia, jos nimi lausutaan. Niinpä ihmiset, joiden kaima on kuollut, joutuvat vaihtamaan nimensä. Vanhat naiset, joilta on monia sukulaisia kuollut, joutuvat välttämään niin monen nimen lausumista, että he joskus lakkaavat kokonaan puhumasta ääneen. Se ei estä heitä keskustelemasta vilkkaasti keskenään, sillä heillä on viittomakieli, jolla voi sanoa kaiken tarvittavan.

19.7.2015 J. Holvikivi
Salatieto

3 SALAKIRJOITUKSET

Kirjainten järjestyksen vaihtaminen sanan sisällä: TALO = OLAT. Helppoa!

Kokonaisen lauseen voi kirjoittaa takaperin hiukan eri tavoin. Seuraavat koodilauseet on muunnettu samasta viestistä kahdella eri tavalla. Mitkä ovat koodaussäännöt?

ELUT ELLIEM ALLALLI
ALLA EILL EILL ULEM T

Peilikirjoitus

HƎЯƎ YOU ƤO ?

Onko sinulla vielä tallella papereita, joille piirsit ja kirjoitit pienenä lapsena? Esiintyykö niissä peilikirjoitusta? Se on lapsilla hyvin yleistä. Peilikirjoituksessa ei ole mitään häpeämistä, sillä eräs maailman suurimpia nerojakin harrasti sitä. Leonardo da Vinci, joka oli vasenkätinen, kirjoitti mielellään oikealta vasemmalle, peilikirjoituksena. Leonardon tunnetuin työ on Mona Lisa, mutta maalamisen lisäksi hän teki paljon muutakin: suunnitteli lukuisia teknisiä laitteita ja tutustui ihmisen anatomiaan leikkelemällä ruumiita. Peilikirjoitusta on tietysti helppo lukea peilin avulla, siksi esimerkiksi hälytysajoneuvon nimi voi olla kirjoitettu takaperin, jotta se edelläajavien autojen taustapeilissä näkyisi heti oikein ja kuljettaja antaisi välittömästi tietä.

Hyvin helppo koodi käyttää on 'höpö-höpö'-kirjoitus: siinä ei tarvitse muuttaa mitään, vaihtaa kirjainten paikkoja tai muistaa salasanoja. Lisätään vain yhdentekeviä kirjaimia, yksi jokaisen kirjaimen eteen. Poista seuraavasta sanasta ensimmäinen, kolmas, jne. joka toinen kirjain:

SYRÖITSYEÖKLVÄRINNIEAN

Jos valitsee peitekirjaimet sopivasti, ei alkuperäinen koodi "näy" läpi. Jos viesti on pidempi, huomaa siitä heti, että sanat ovat hirmu pitkiä, ja silloin voi koodin arvaaminen olla helppoa. Viesti kannattaakin ryhmitellä neljän tai viiden kirjaimen pituisiksi pätkiksi:

AKIAS TESRO WKYEG TOTFU JA

SEKOITUSMENETELMÄT

Kirjainten sekoittamiseen tutustuimme jo alussa, jossa viestit kirjoitettiin takaperin. Merkkien perinpohjaiseen sekoittamiseen on kehitetty monenlaisia sääntöjä, jotta viesti olisi vaikeampi selvittää. Ruudukon käyttö apuna on varsin yksinkertaista sekä koodaus- että lukemisvaiheessa. Siihen ei tarvita kuin ruutupaperia, eikä menetelmän avainta tarvitse tallettaa paperille, koska se on helppo muistaa. Sitä voi helposti muunnella eri tavoin.

Tee ruudukko, jossa on kuusi riviä ja kuusi saraketta. Kirjoita ruutuihin viesti riveittäin:

TAPAAMME AAMUNKOITTEESSA VENEVAJALLA. L.B.

Älä jätä tyhjiä ruutuja, äläkä merkitse pisteitä. Nyt voit poimia kirjaimet sarake kerrallaan ja kirjoittaa yhteen pötköön. Viesti on helppo purkaa kirjoittamalla se takaisin ruudukkoon. Menetelmää voi muunnella poimimalla sarakkeet eri järjestyksessä, esimerkiksi ensin toinen,

sitten viides, ensimmäinen, neljäs ja kolmas. Tai vaikkapa "kerimällä" kirjaimet ruudukon sisältä alkavana spiraalina, jolloin salakoodiksi tulisi: ISSOAA MTAAVE NEKEAP AAMUTV JBLALL AEENMT.

KORVAUSMENETELMÄT

Numerokoodi:

A	B	C	D	E	F	G	H	I	J	K	L	M
9	3	18	29	7	20	24	27	13	21	16	8	28

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	1	5	11	22	15	19	2	26	17	24	6	12

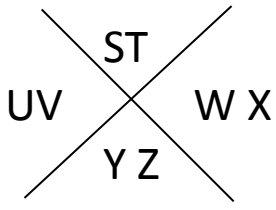
Å	Ä	Ö
23	4	10

Mitä söisit välipalaksi:
5 1 22 16 16 9 14 9
21 4 4 19 7 8 10
8 9 16 2 14 9 2 27 9?

Numeroiden sijasta voit käyttää mitä tahansa merkkejä, joita ei ole liian vaikea piirtää. "Sikolätti"koodi näyttää varsin hauskalta, ja sitä voi muunnella eri tavoin. Sen toinen nimi on "muurarisalakirjoitus", joka kertoo siitä, että Vapaamuurarien veljeskunta joskus käytti sitä aikaisempina vuosisatoina. Vapaamuurarit on satoja vuosia vanha eurooppalainen miesten salaseura, jonka jäsenet eivät suinkaan kaikki olleet muurareita, vaikka järjestö käyttikin tunnuksinaan lastaa ja muita muurarin työvälineitä. Sillä on ollut monia kuuluisia henkilöitä jäseninään. Kuten kunnon salaseuralla, sillä on salaisia menoja ja symboleita. Sen jäsenyys on pidetty salassa ulkopuolisilta, ja jäsenet ovat sitoutuneet auttamaan 'veljiään' kaikin tavoin. Siksi sitä on joskus epäilty rikollisista puuhista.

Sikolättikoodi

A B	C D	E F
G H	I J	K L
M N	O P	Q R



A ilmaistaan sen sijainnilla kulmassa __| ja

B pisteellä kulman lisäksi •_|

19.7.2015 J. Holvikivi
Salatieto

JULIUS CAESAR

Ennen Jeesuksen syntymää vaikuttanut roomalainen sotapäällikkö Julius Caesar on antanut nimen yhdelle salakirjoitusmenetelmälle. Caesar oli hyvin menestyksellinen taisteluissaan Galliassa (Ranskassa), Iberiassa (Espanjassa) ja Britanniassa. "Veni, vidi, vici'" eli 'tulin, näin, voitin'. Hän taisteli myös germaaneja vastaan, mutta ei onnistunut valloittamaan näiden maita. Joka tapauksessa Caesarin toimia ihailtiin Roomassa niin paljon, että hän onnistui valituttamaan itsensä ennen niin tasavaltaisen Rooman ensimmäiseksi keisariksi.

Caesarin salakirjoitus yksinkertaisimmassa muodossaan (jota keisari Augustuksen väitetään käyttäneen) syntyi siten, että aakkonen korvattiin sitä seuraavalla kirjaimella: esim. APINA olisi BQJOB. Kehitetyssä muodossa hypätään sitä seuraavaan kirjaimeen tai vieläkin edemmälle aakkosissa.

Ratkaise: Montako kirjainta eteenpäin on seuraavassa salakirjoituksessa hypätty:

ONGELMA

RQJHOPD?

Caesarin koodi on hyvin yksinkertainen vai mitä? Voisi kuvitella, että vihollinen ratkaisee sen hyvinkin nopeasti. Hänen aikanaan ei kuitenkaan tarvittu kovin mutkikkaita menetelmiä: monet hänen sotilaistaankaan eivät osanneet lukea, ja viholliskansojen parissa lukutaito oli vieläkin harvinaisempi.

Koodista tulee paljon vaikeampi ratkaista, jos soveltaa jokaiseen sanaan eri muunnosta. Valitaan koodin avaimeksi sana PURJE - nyt P kertoo, että ensimmäisessä sanassa siirros on:

A B C D E F ... alkutekstissä

P Q R S T U ... koodissa

Seuraavassa sanassa

A B C D E F G H I J ..

U V W X Y Z O Ä Ö A ..

Koodia on helpointa käyttää siten, että kirjoittaa kahdelle paperille listan aakkosista tasaiselle etäisyydelle toisistaan. Koodatessa sijoitetaan toinen lista toisen alle niin, että A:n kohdalle tulee avainkirjain, ja korvataaan aina ylärivissa oleva kirjain sen alapuolella olevalla. Koodi luetaan päinvastaisella menettelyllä. Se on varsin yksinkertaista, mutta menetelmässä on helppo mennä sekaisin, joten keskittymistä siinä vaaditaan! Jos nauhan käyttö tuntuu hankalalta, kokeile kahta pahvikiekkoa, joista toinen on vähän pienempi ja sijoita ne päällekkäin. Kiekkoa kääntelemällä saat helposti kirjaimet kohdalleen. Kuva. Lue seuraava teksti käyttäen avaimena sanaa PURJE.

TULE HETI KUN VOIT, ÄITI.

FGÅT ÄYKÖ ÄIB BXRÖ CMXM.

HARJOITUS: Käytä avainsanana KÖNGÄS, ja koodaa sillä joku teksti.

Vaihda ystäväsi tai työparisi kanssa viestejä, jotka on kirjoitettu käyttäen avainsanoja TYÖVUORO, HEPO. Voitte valita itsekin avainsanat, mutta huomatkaa, että esimerkiksi AAMU tai KAARINA eivät ole hyviä valintoja, koska.. Niin miksi?

19.7.2015 J. Holvikivi
Salatieto

Jos käytät ystäviesi kanssa edellä esitettyä menetelmää pidempään, voitte poimia avainsanan koodikirjasta. Voit valita minkä tahansa kirjan, ja yhdessä sovitun säännön avulla valitsette sieltä avainsanan. Avainsanasta ilmoitetaan sivunumero - rivi - sana; tai sivunumero ja sanan järjestysnumero sivulla. Tietysti kirjan sanoja voisi sellaisenaankin käyttää viestintään. Silloin salakirjoitus toimii niin, että etsit kirjasta kaikki tarvitsemasi sanat, ja merkitset ne salaiseen koodiin numeroyhdistelmällä. Kokeile! Huomaat, että menetelmä vie koodaajalta paljon aikaa, lukeminen sen sijaan sujuu hiukan nopeammin. Jos pidät tärkeänä, että viestit säilyvät salaisina, on tämä menetelmä erittäin varma niin kauan kuin koodauksessa käytetty kirja pysyy salaisena.

KRYPTOGRAFIA

Koodaaminen on kehittynyt vaativaksi tieteeksi sitten muinaisten roomalaisten. Ceasarin menetelmästä siirryttiin monimutkaisempiin koodeihin ja operaatioita sisältäviin koodikirjoihin, joita vielä sata vuotta sitten armeijoiden tiedusteluosastot käyttivät. Ne oli suunniteltu varta vasten sotilaallisten viestien lähetykseen. Jokaisella operaatiolla oli numero, ja numerosarjan lähettäminen riitti viestiksi. Jos tiedusteluosastolle oli soluttautunut vihollisen vakooja, joka paljasti koodiston omalle puolelleen, koodikirja tuli hetkessä hyödyttömäksi.

Kehitettiin myös koodauskoneita, jotka olivat erikoisrakenteisia kirjoituskoneita, tai laitteita kirjainten sekottamiseksi. Yhdysvaltain sisällissodassa viestejä sekotettiin sylinterillä, joka oli eräänlainen muunnelma edellä esitetystä kiekko/ nauhamenetelmästä. Kirjoitusta voi salata myös tekemällä siitä "näkymätöntä" eli kirjoittamalla se siveltimen avulla käyttäen sitruunamehua tai maitoa. Kun paperia hiukan lämmittää hehkulampulla tai kuumaa patteria vasten, muuttuu mehulla kirjoitettu teksti näkyväksi. Maidolla kirjoitetun tekstin saa esiin ripottelemalla tuhkaa tai kynäpölyä paperin päälle.

Kun luonnontieteitä, tietoliikennetekniikkaa ja matematiikkaa kehitettiin nopeasti tämän vuosisadan alkupuolella, sovellettiin näitä tietoja myöskin koodaamiseen. Viisikymmentä vuotta sitten päättyi toinen maailmansota, joka oli monessa suhteessa erilainen kuin aikaisemmat sodat. Siinä tietoliikennetekniikka ja vakoilutekniikka ratkaisivat monia päätöksiä ja taisteluita. Armeijat lähettivät viestinsä radioteitse, ja koska viholliset tietenkin salakuuntelivat toisiaan, piti viestit koodata. Kaikki sotaa käyvät maat sijoittivat parhaita matemaatikkojaan ja kielitieteilijöitään näihin tehtäviin. Englannilla oli ainakin 30,000 henkilöä koodien murtamistehtävissä.

Japani oli kehittänyt salakirjoituskoodia tuottavan koodauskoneen, joka oli niin edistynyttä tekniikkaa, että sitä pidettiin mahdottomana selvittää. Amerikkalaisten tiedustelu onnistui kuitenkin murtamaan sen koodin, ja kykeni tämän jälkeen lukemaan japanilaisten viestejä. Sotaa vastustanut sanomalehti, The Chicago Tribune, julkaisi uutisen koodin murtamisesta. Japanilaiset eivät suostuneet uskomaan sitä todeksi, vaan jatkoivat onnettomuudekseen koodin käyttöä koko sodan ajan!

19.7.2015 J. Holvikivi
Salatieto

HARJOITUS: Tavallista näppäimistöä voi käyttää koodauskoneena siten, että korvaa näppäimen sen vieressä tai yläpuolella olevalla näppäimellä. Kokeile viestin kirjoittamista ja selvittämistä tällä tavalla!

KOODIN MURTAMINEN

Koodit, joissa kirjainten järjestys on sekoitettu, mutta niitä ei ole muutettu, ovat sitä helpompia ratkaista, mitä lyhyempi viesti on. Ne voi selvittää melko nopeasti pelkästään kokeilemalla ja arvaamalla. Montako eri viestiä voisit saada seuraavasta kirjainsarjasta: ÄÄÄTNN? Kun viesti pitenee, tehtävä mutkistuu, jos sekoitus on hyvin tehty. Sen sijaan kaikki sellaiset koodit, joissa kirjaimet on vaihdettu muiksi merkeiksi, tulevat helpommiksi selvittää, kun sanoma on pitkä. Tämä perustuu siihen, että kirjoitettu teksti noudattaa tiettyjä sääntöjä.

Vaikka kaikki testit ovatkin erilaisia, on niillä myös yhteisiä piirteitä. Ensinnäkin ne koostuvat sanoista. Kaiken lisäksi vieläpä usein samoista sanoista. Jotkut sanat esiintyvät aivan kaikenlaisissa teksteissä melko usein: ja, on ,ovat, se, ne, mutta, ei, eli, on, ovat. Jos otetaan oikein suuri joukko suomenkielisiä kirjoja ja lehtiä, voidaan laskea, mitkä ovat kielemme yleisimmät sanat. Suuresta tekstijoukosta voidaan laskea myös eri kirjainten esiintyminen. Suomessa yleisimmät kirjaimet ovat tässä järjestyksessä i, t, a, s, n, l, k, o ja u. Kun sanojen ja kirjainten esiintymistaajuudet tunnetaan, voidaan tietoa käyttää salakielisten viestien selvittämisessä. Parhaiten se onnistuu tietenkin silloin, kun yhtä merkkiä vastaa aina sama koodi, ja sanojen välit on jätetty näkyviin.

Kun lähdet selvittämään korvaussalakirjoitusta, katso ensin tekstin "hahmoa": usein toistuvat merkit, usein toisiaan seuraavat merkit, jne. Tieto kirjainten esiintymistiheyksistä on hyödyllinen, koska se auttaa arvaamaan yleisimmin esiintyvät koodit. Toisekseen suomenkielen rakenne on sellainen, että vokaalit ja konsonantit vuorottelevat sanoissa varsin säännön-mukaisesti: vokaaleja on peräkkäin korkeintaan kaksi (vain joissakin poikkeustapauksissa kolme: ruoan, reiät), eikä konsonanttejakaan ole koskaan enempää kuin kolme, ja silloin jo kahden pitää olla samat (pan<u>kk</u>i, ton<u>tt</u>i). Sanojen viimeisenä kirjaimena voi olla vain vokaali tai t, n tai s, harvoin muu konsonantti. Tietyt vokaalit kuuluvat yhteen: ä, ö ja y, jotka eivät esiinny samoissa perussanoissa a:n, o:n ja u:n kanssa.

HARJOITUS 1: Valitse täynnä tekstiä oleva sivu jostain kirjasta ja laske siitä yleisimmät sanat ja eri kirjainten esiintymistiheys. Yhden sivun perusteella saatuja tuloksia ei vielä voi yleistää kovin varmasti, mutta mitä useampi sivu lasketaan, sen parempi tulos on. Jos teitä on monta henkeä, valitkaa erilaisia tekstejä: sanomalehden juttuja, tietokirjoja, nuorten kirjoja, jne. Saatteko kovin erilaisia tuloksia keskenänne?

Jos tekstissä on vieraskielisiä sanoja, muuttuu kirjainten yleisyys tietysti toiseksi: esimerkiksi englannissa, ranskassa ja saksassa on yleisin kirjain E, sen jälkeen seuraavat englannissa T, A, I, O ja N.

19.7.2015 J. Holvikivi
Salatieto

HARJOITUS 2:

Ratkaise päättelemällä ja kokeilemalla, mitkä koodit ja sanat kuuluvat yhteen:

VARJO	17 4 4 24 15
SUURI	29 11 11 1 4
HAAMU	28 11 24 23 3

Täytä ratkaisemasi kirjaimet avaintaulukkoon.
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

Seuraavassa on lisää vihjeitä, viisi yhteenkuuluvaa salakirjoitettua ja selväkielistä sanaa. Täydennä avaintaulukko. Kaikki koodimerkit eivät näiden perusteella selviä, joten avaimeesi jää tyhjiä kohtia.

KATTO	15 31 3 10 15
PELTO	17 9 15 16 6
PYÖRÄ	18 11 21 21 3
SEINÄ	7 9 10 21 3
IDOLI	7 8 12 24 6

HARJOITUS 3:

Seuraavassa luettelossa on kuusi sanaa tai sanaparia, jotka ovat Suomen kansan antamia lempinimiä karhulle. Pystytkö selvittämään ne ilman enempiä vihjeitä. Tee itsellesi avaintaulukko, johon täytät ratkaistut kirjaimet.

O@J#(@	K$E(O=KK$J	K$#E=J @K$JW
EWP@J W%KWE	@#E@	K*E#E*OOWJ$J

HARJOITUS 4:

Edellä olevissa tehtävissä tiesit, millainen koodi on kyseessä, nimittäin yksinkertainen merkin korvaaminen toisella. Salasanoman selvittäminen on paljon vaikeampaa, jos ei tiedä käytettyä menetelmää. Silloin pitää käydä läpi eri vaihtoehdot. Helpoimpiakin koodeja kannattaa kokeilla, sillä ainahan voi luottaa siihen, että useimmat meistä ovat liian laiskoja soveltamaan kovin monimutkaisia menettelyjä. Hyvin vaikeasti ratkaistavaa koodia voi tuottaa esimerkiksi sekoittamalla ensin kirjaimet ja sitten vielä muuttamalla merkit toisiksi, mutta se vaatii aika paljon työtä sekä koodaajalta että vastaanottajalta.

19.7.2015 J. Holvikivi
Salatieto

TIETOKONEKOODIT

Tietokonetekniikkaa kehitettiin nopeasti sodan jälkeisenä aikana. Koska tietokoneilla pystyttiin suorittamaan laskelmia paljon nopeammin kuin koskaan aikaisemmin, alettiin salakirjoituksessakin käyttää yksinomaan matemaattisia menetelmiä. Suuria lukuja kerrotaan, jaetaan ja pilkotaan osiin, ja näiden avulla muutetaan alkuperäisen viestin kirjaimet ja numerot toisiksi. Sitä mukaa kun tietokoneiden nopeus ja teho kasvavat, paranevat myös mahdollisuudet koodien murtamiseen, sillä tehokkailla tietokoneilla voidaan kokeilla miljoonia vaihtoehtoja varsin nopeasti. Niinpä myös salakirjoituksessa käytettävien lukujen suuruuden ja laskuoperaatioiden monimutkaisuuden pitää kasvaa.

Esimerkki: pankkikortin tunnusluku. Tavallisesti pankkiautomaattikorteissa on nelinumeroinen tunnusluku. Se on arvottu mielivaltaisesti ja koodattu kortin magneettijuovaan. Kun kortti syötetään automaattiin, on käyttäjän ensimmäiseksi näppäiltävä tunnuslukunsa. Hän saa yrittää vain kolme kertaa, ennen kuin kortti katoaa automaatin sisään. On hyvin pieni todennäköisyys, että kukaan onnistuisi arvaamalla syöttämään oikean tunnusluvun (tosin se on paljon suurempi todennäköisyys kuin loton päävoiton saaminen). Jo ensimmäisen numeron kohdalla mahdollisuuksia on nollasta yhdeksään eli 10! Seuraavan numeron kohdalla on taas mahdollisuus yksi kymmenestä, että osuu oikeaan, eli mahdollisuus saada kaksi ensimmäistä oikein on vain yksi sadasta. Jotta kolmaskin osuisi oikeaan, on taas valittava kymmenen vaihtoehdon joukosta, eli mahdollisuuksien määrä kertautuu kymmenellä: tuhat! Numeroiden valinnassa ei auta mikään älykäs menetelmä, koska ne ovat täysin satunnaisia.

Entä jos tunnuskoodiksi saisi valita etunimensä tai jonkin muun tutun sanan? Tulisiko arvaaminen helpommaksi?

HARJOITUS 1: Arvaamispeli. Pelataan tunnusluvun arvaamista siten, että yksi valitsee luvun ja muut yrittävät arvata sitä. Pelinvetäjä kirjoittaa paperille neljän numeron sarjan, eikä näytä sitä muille. Ensimmäinen pelaaja arvaa neljän numeron sarjan, ja pelinviejä merkitsee siihen, mitkä osuivat oikeaan. Jos numero on oikein ja oikealla paikalla, merkitään se ympyrällä. Jos se esiintyy sarjassa, mutta on sijoitettu väärään kohtaan, vedetään sen alle viiva. Kaikki pelaajat saavat nähdä tämän, ja seuraava arvaaja käyttää sitä hyödykseen. Se, joka vuorollaan osuu oikeaan sarjaan, tulee seuraavaksi pelinviejäksi.

ESIMERKKI: VERNAMIN LASKENTAMENETELMÄ

Amerikkalainen C. Vernam kehitti jo vuosikymmeniä sitten koodausmenetelmän, jota on mahdoton murtaa. Se perustuu kertakäyttöisiin satunnaisten lukujen taulukoihin. Sekä koodin lähettäjällä että vastaanottajalla pitää olla samat taulukot, jotka hävitetään heti käytön jälkeen. Tämä tekee koodista varsin hankalan jatkuvassa käytössä, joten siitä ei koskaan ole tullut kovin suosittua. Bolivian viidakoissa taistellut kapinallisjohtaja Che Guevara käytti tätä menetelmää

lähettäessään sanomia Kuubaan, joka tuki hänen sissisotaansa. Vernamin menetelmä on hyvä esimerkki yksinkertaisesta laskentamenetelmästä, jota voi käyttää ilman tietokonetta.

Tarvitaan kaksi taulukkoa: ensimmäisen lukusarjan avulla muutetaan kirjaimet numeroiksi samoin kuin tavallisessa korvausmenetelmässä. Sen jälkeen otetaan toinen numerosarja ja lisätään sen numeroita ensimmäisen sarjan numeroihin yksi kerrallaan, säilyttäen vain summan oikeanpuoleinen numero (kymmenet jätetään pois), joten numeroiden määrä säilyy samana. Numerot voidaan sitten lähettää radiolla vastaanottajalle. Koodin purku tapahtuu päinvastaisella menettelyllä: 1) vähennetään saaduista numeroista toisen sarjan luvut, ja 2) katsotaan avaintaulusta, mitä kirjaimia ne vastaavat.

Yksinkertaisen englanninkielisen viestin "I like you" lähetys näyttää tältä:

Avain:

A	6	E	8	I	39	M	70	Q	71	U	52	Y	1
B	38	F	30	J	31	N	76	R	58	V	50	Z	59
C	32	G	36	K	78	O	9	S	2	W	56		
D	4	H	34	L	72	P	79	T	0	X	54		

Viesti: I L I KEYO U.
Koodattuna: 3972397881952
Numerosarja: 752964023875427615775420768 9
Summa: 0491937019606

Summarivi saadaan siis niin, että lisätään allekkain olevat numerot toisiinsa: 3+7=10, josta otetaan vain viimeinen numero eli nolla. Toiseksi numeroksi tulee 4 eli 9+5=14, ykkönen pudotetaan pois. Seuraavaksi 7+2=9, joka otetaan sellaisenaan. Tämä summarivi lähetetään vastaanottajalle.

Viestin purkaminen on melko työlästä: ensin vähennät viestirivin ensimmäisestä luvusta numerosarjan ensimmäisen eli 0-7, ei voi ottaa joten laske 10-7, josta tulee 3. Katso, onko 3 avaimessa. Ei ole, joten tarvitaan toinen numero: 4-5, eli 14-5=9. Nyt 39 löytyy avaimesta, sehän on I. Näin jatketaan.

SUURET ALKULUVUT

Tietokoneilla käytettäviä menetelmiä on kahta tyyppiä: toisissa salausmenetelmissä avain on salainen, mutta laskuoperaatio yleisesti tiedossa. Toisissa menetelmissä taas avain on julkinen, mutta menettely koodatun viestin purkamiseksi salainen. Alkuluvut on havaittu hyödyllisiksi, koska niiden matemaattinen käsittely on hankalaa, varsinkin jos ne ovat suuria. Alkuluvuksi kutsutaan sellaista kokonaislukua, joka voidaan jakaa vain itsellään ja ykkösellä. Sillä ei ole muita tekijöitä. Alkulukujen sarja alkaa: 1,2,3,5,7,11,13,17 ja niin edelleen. Osaatko jatkaa sarjaa?

Hyvin suosittu salausmenetelmä käyttää tunnuslukuina erittäin suuria lukuja, jotka on saatu kertomalla kaksi erittäin suurta alkulukua keskenään. Koodauksessa vuosia käytetty luku on nimeltään RSA 129, koska siinä on 129 numeroa. Se on tunnettu luku, jota käyttäen kuka

tahansa saattoi tietokoneellaan koodata ja lähettää viestin. Mutta viestin purkamiseen piti tuntea luvun kaksi tekijää, jotka molemmat ovat suuria alkulukuja, ja jotka pidettiin salassa. Uskottiin, että alkulukujen selville saaminen vaatii niin tehokkaan tietokoneen, ettei kenelläkään ole sellaista. Internet-verkon krytografia-ryhmä keksi, että yhteistyö on tässäkin voimaa. He jakoivat ongelman pieniin osiin, ja kutsuivat vapaaehtoisia apuun tekemään laskelmia. Kun sadat tietokonekäyttäjät osallistuivat laskentaan eri puolilla maailmaa, kului vain vuosi, ennenkuin ongelma oli ratkennut. Onhan sekin pitkä aika, mutta osoitti, ettei 129 numeroa ole tarpeeksi vuorenvarman koodin avaimeksi. Nykyään arvellaan, että luvussa pitäisi olla noin 230 numeroa, jotta siihen voisi luottaa viisi seuraavaa vuotta. Se käyttökin vaatii koodaukseen käytetyltä tietokoneelta jo hyvää nopeutta.

4 MORSEN AAKKOSET

…/---/…

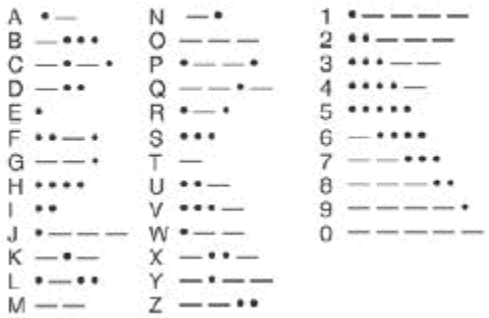
SOS = "Save Our Souls" on kansainvälinen hätäkutsu. Se on tunnettu kaikkialla maailmassa, se on helppo muistaa, ja ennen kaikkea, se on helppo ilmaista erilaisin tavoin. Lyhyitä ja pitkiä signaaleja voi lähettää lampulla, äänenä tai jopa savumerkkeinä. Toinen kansainvälinen avunpyyntö on "Mayday" (=meedee), jonka voi lähettää silloin kun puhe kuuluu.

Viestin lähettäminen on helpottunut ja nopeutunut valtavasti viimeisen sadanviidenkymmenen vuoden aikana. Miten toimisit, jos haluat kutsua toisessa kaupungissa asuvan ystävän luoksesi viikonlopuksi? Mitkä ovat vaihtoehdot, jos aikaa on kuukausi? Entä jos sanoma pitäisi saada perille heti?

Ennen nykyaikaisia viestimiä ja puhelintekniikan monia mahdollisuuksia piti jonkun ihmisen kuljettaa viesti perille. Eikä kuljetuskaan ollut nopeaa, kun ei ollut autoja, junia eikä lentokoneita. Postia kuljetettiin hevosen vetämillä vaunuilla ja purjelaivoilla. Ylhäiset ja rikkaat saattoivat käyttää henkilökohtaisia lähettejä, jotka kulkivat nopeasti ratsain, mutta tavallinen kansa saattoi joutua odottamaan, että jollakin olisi asiaa siihen suuntaan mihin kirje oli menossa. Kun viesti oli näin saatu perille, ei vierailulle lähdetty hätäillen. Kyläreissut kestivät helposti viikkoja tai kuukausia.

Samuel F. B. Morse keksi lennättimen vuonna 1835. Hänen koneellaan voitiin lähettää viestejä sähkökaapelia pitkin paikasta toiseen. Viestinnän helpottamiseksi Morse kehitti aakkoston, joka oli yhdistelmä lyhyitä ja pitkiä näpäyksiä. Lennätin saavutti pian suuren suosion, ja kaapelit vedettiin yhdistämään maailman kaikkia tärkeitä kaupunkeja. Kuusikymmentä vuotta myöhemmin onnistui nuori italialainen Guglielmo Marconi yrityksissään langattoman lennättimen keksimiseksi. Siinäkin käytettiin pitkään Morsen aakkosia, sillä ne kuuluvat selkästi, eivätkä ole yhtä herkkiä häiriölle kuin puhe.

MORSE CODE



Morsen aakkoset on helppo oppia muistamaan avainsanojen avulla. Tavussa lyhyt vokaali vastaa pistettä, ja pitkä vokaali ja diftongi vastaavat viivaa:

A A-haa
B bee-ring-me-ri
C cey-lon-saa-ri
D daa-de-li
E en
F fe-mi-nii-ni
G gee-klaa-vi
H hy-vä-hy-vä
I i-lo
J ja-tuul-koon-vaan
K kou-lu-työ
L lap-peen-ran-ta
M muu-rain
N naa-va
O oi-voi-voi
P per-heen-pie-nin
Q quu-lee-ko-maa
R re-tii-si
S si-pu-li
T tee
U u-ro-työ
V vel-vol-li-suus
W wam-pyy-reit
X tää-äk-sät-tää
Y yö-jo-pei-tää
Z zoo-loo-gi-o
Å ån-vai-kea-kir-jain
Ä äl-kää-kos-kaan
Ö öin-tuu-lee-pi

19.7.2015 J. Holvikivi
Salatieto