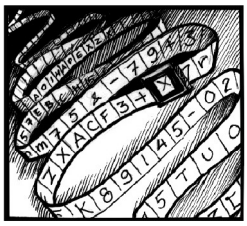

Tehtävä: dekryptaus

Anne-Maria Ernvall-Hytönen
Åbo Akademi

Caesarin kryptosysteemi on hyvin tunnettu: Ajatus on se, että jokainen kirjain kryptataan toiseksi siirtäen aakkosia aina saman verran eteenpäin tai taaksepäin. Esimerkiksi jos siirretään kolme pykälää eteenpäin, niin A muuttuu kirjaimeksi D, B kirjaimeksi E, C kirjaimeksi F ja niin edespäin.

Tunnettu esimerkki populaarikulttuurissa tämän kryptojärjestelmän käytöstä on Avaruusseikkailu 2001 -kirjassa. Siinä tietokoneen nimi on HAL. Luultavasti kone on saanut nimensä Caesarin kryptosysteemin avulla merkistä IBM. Kun jokaista kirjainta siirretään yksi taaksepäin, tulee kirjaimesta I kirjain H, kirjaimesta B kirjain A ja kirjaimesta M kirjain L, eli IBM muuttuu sanaksi HAL.

Järjestelmä on onnettoman heikko: erilaisia vaihtoehtoja, miten kryptaus on voitu tehdä, on vain aakkosten lukumäärän verran. Nämä käy läpi kokeilemalla hyvin vauhdikkaasti.

Hieman kehittyneempi versio on sellainen, jossa aakkoset korvataan toisillaan ilman vastaavaa vakiosiirtymän systemaattisuutta. Kirjaimet korvataan saman tekstin sisällä aina samoilla merkeillä (kirjaimilla), mutta siirtymä vaihtelee. Esimerkiksi siis kirjaimesta A voisi tulla vaikka H ja kirjaimesta B kirjain Ö ja kirjaimesta C kirjain A ja niin edelleen.

Nyt vaihtoehtoja on jo paljon: kirjainten lukumäärän kertoman verran. Tälläkin järjestelmällä on kuitenkin heikkoutensa: kirjainten yleisyys kielen sisällä on hyvin tunnettu. Esimerkiksi suomen kielen yleisin kirjain on A, toiseksi yleisin I. Luultavasti siis kryptatussa tekstissä on varsin paljon kirjainta A vastaavaa merkkiä, samoin kirjainta I. Vastaavan päättelyn voi yleistää muillekin kirjaimille. Kirjaimia Q, Z ja W vastaavia merkkejä esiintyy luultavasti puolestaan varsin vähän. Tämän kanssa pitää tietenkin olla varovainen: jos teksti kertoo vaikkapa qatarilaisten Volkswagenin omistajien banaanikaupoista, voi tekstissä olla epätavallisia kirjaimia hieman tavallista enemmän. Toinen ongelma on tietenkin se, että jos teksti on liian lyhyt, voivat kirjaimien esiintymien määrät olla melkein mitä tahansa. Jos teksti on aivan valtavan lyhyt, ei sanoja välttämättä edes voi erottaa toisistaan. Yksittäiset sanat ei, en ja on voidaan esimerkiksi kryptata samoiksi sanoiksi eri kryptauksilla.

En kerro tämän enempää, jottei lukijalta mene täysin ilo tehtävän ratkaisusta. Joka tapauksessa tehtävänä on dekryptata oheinen teksti. Numeroita ei ole kryptattu, vain kirjaimet. (Vihje: jos luet tätä Solmua paperilta, kannattaa kaivaa verkkoversio esiin Solmun kotisivuilta, sillä teksti on selvästi miellyttävämpää purkaa tietokoneella tekstinkäsittelyohjelmaa ja muita sopivia ohjelmia käyttäen kuin käsin.)

cdiwajci

1. cdiwajc. acwaaw wbqwrui renievhi vczcwnc tc icrcvudicwrwnc cdvgjiccn tc gwauoarwjiccn. buwjju gn

cnnuiio thdaw tc gqcionig, tc buwfhn gn igwqwiicvc igwrwccn agbiccn vujtuefun bunyurrh. 2. cdiwajc. tgacwnun gn gwauoiuiio acwaawwn ihrrh tojwrioarurrc urwiuiiewbwn gwauoarwwn tc vczcoarwwn wjqcn qwnahhnjcwric dgioon, vhdwwn, roaozogjuun, awujuun, oragniggn, zgjwwiiwruun icw qoobon qwujwzwiuuruun, acnrcjjwruun icw ebiuwraonncjjwruun cjaozudhhn, gqcwrooiuun, reniezudhhn icw qoobon iuawthhn zudoriovcc udgioric. qwihhn udgioric uw qesrahhn zwfh iubfh run qccn icw cjouun vcjiwgjjwrun, bcjjwnngjjwrun icw acnrcwnvhjwrun cruqcn zudoriuujjc, tgbgn bunawjs aoojoo, gjwzc ihqh cjou wirunhwnun, bogjigbcjjwnngrrc, wirubcjjwnigc vcwjjc icw iherwvcjicwroofujiccn qwnah icbcnrc qoon dctgwioarun cjcwnun. 3. cdiwajc. aojjcawn earwjsjjh gn gwauor ujhqhhn, vczcoiuun tc bunawjsagbicwruun iodvcjjwrooiuun. 4. cdiwajc. auihhn uw rcc zwihh gdtcnc icw gdtooiuiionc, acwaaw gdtoofun tc gdtcacozcn qogfgi gn awujjuiihvh. 5. cdiwajc. auihhn uw rcc awfoiicc uwah agbfujjc icw dcnycwric tojqcriw, uzhwnbwqwjjwruriw icw cjunicvcriw. 6. cdiwajc. tgacwrujjc wbqwrujjh gn acwaawcjjc gwauor rwwbun, uiih bhnui bunawjsnh ionnoriuiccn jcwn ufurrh. 7. cdiwajc. acwaaw gvci icrcvudicwrwc jcwn ufurrh tc gwauoiuioi udgioaruiic ebihjhwruun jcwn rogtccn. acwawjjc gn gwauor icrcvudicwruun rogtccn ihih tojwrioric jgoaaccvcc redtwnihh vcriccn ruah acwaauc rujjcwruun redtwnihhn ihbihhvhh ejjeierih vcriccn. 8. cdiwajc. tgacwrujjc gn gwauor iubgaaccruun bevwiearuun crwcngqcwrurrc acnrcjjwrurrc iogqwgwriowqurrc bhnuun agbfwrionuwric iugwric, tgiac jgoaaccvci bhnujju vcjiwgrhhnnsjjh icw jcwjjc iodvciiotc zudorgwauoarwc. 9. cdiwajc. auihhn uw rcc qwujwvcjicwruriw zwfhiihh, vcnywic icw ctcc qccnzcaggn. 10. cdiwajc. tgacwrujjc gn iherwn icrc-cdvgwruriw gwauor rwwbun, uiih bhnih gwauofunqoacwruriw tc tojawruriw aoojjccn dwwzzoqciigqcrrc tc zogjouuiigqcrrc iogqwgwriowqurrc bhnun gwauoarwccn tc vujvgjjwrooarwccn qhhdhiihurrh icw bhnih vcriccn ngriuiioc dwagrreeiuiih rujvwiuiihurrh. 11. cdiwajc. 1. tgacwrun dwagjjwruric iugric reeiiuurrh gjuvcn bunawjsn ufujjeiuihhn gjuvcn reeisn rwwbun criw aonnur bhnun reejjwreeiunrh gn jcwjjwruriw igfwriuiio tojawrurrc gwauofunahennwrrh, tgrrc bhnujju iodvciccn acwaaw bhnun zogjorioriccn vcdiun icdzuujjwrui icauui. 2. auihhn uw zwfh iogqwic dcnycwricvcarw iugwric icw jcwqwnjesnnuwrih, tgiac uwvhi acnrcjjwrun icw acnrcwnvhjwrun gwauofun qoaccn gjjuui dwagjjwrwc iuagbuiaujjh. qesrahhn uw zwfh iogqwic cnacdcqzccn dcnycwrioaruun, aown qwah gjw rgvujjuiicvwrrc dcnycwricvcn iugn rogdwiorbuiaujjh. 12. cdiwajc. hjassn qwujwvcjicwruriw zooioiicag aununahhn earwiewrujhqhhn, zudbuuruun, agiwwn icw awdtuunvcwbiggn hjassnah jgoaciicag aununahhn aonnwcc tc qcwnuiic. tgacwrujjc gn gwauor jcwn rogtccn rujjcwric zooiioqwric icw jgoaacoric vcriccn. 13. cdiwajc. 1. tgacwrujjc gn gwauor jwwaaoc vczccriw tc vcjwic crownzcwaacnrc aonawn vcjiwgn rwrhjjh. 2. tgacwrujjc gn gwauor jhbiuh qccric, qesr gqcric qccriccn, tc zcjcic qccbcnrc. 14. cdiwajc. 1. tgacwrujjc vcwngn agbiuuarw tgoionuujjc gn gwauor bcauc tc ncoiiwc iodvczcwaacc qowrrc qcwrrc. 2. ihbhn gwauoiuun uw vgwfc vufgic, aon gn aereqer igrw uzhzgjwwiiwrwric dwagarwric tgbiovwric reeiiuwrih icw iugwric, tgiac gvci vcrigwn ebfwrienuwfun acnrcaoniwun zudwcciiuwic tc zhhqhhdwh. 15. cdiwajc. 1. tgacwrujjc gn gwauor acnrcjcwrooiuun. 2. aujihhn uw rcc qwujwvcjicwruriw dwwrihh acnrcjcwrooiic uwah uvhih gwauoiic acnrcjcwroofun vcwbicqwruun. 16. cdiwajc. 1. iherw-wahwrwjjh qwubwjjh tc ncwrwjjc gn gwauor rgjqwc cvwgjwwiig tc zudoricc zudbu wjqcn qwnahhnjcwrwc dgforic, acnrcjcwroofuric icw oragnngric tgbiovwc dctgwioarwc. buwjjh gn ebihjhwrui gwauofui cvwgjwwiiggn, cvwgjwwign cwacnc tc run zodacqwrun thjauun. 2. cvwgjwwign rgjqwqwnun iczcbioaggn vcwn iojuvwun cvwgzogjwrgwfun vczccric tc ihefurih rogrioqoaruric. 3. zudbu gn ebiuwraonncn jognngjjwnun tc zudoricvc efwngrc tc rwjjh gn gwauor ebiuwraonncn tc vcjiwgn rogtccn. 17. cdiwajc. 1. tgacwrujjc gn gwauor gqwricc gqcwrooiic earwn icw ebfurrh igwriun acnrrc. 2. aujihhn hjassn qwujwvcjicwruriw dwwriuiihas bhnun gqcwrooiiccn. 18. cdiwajc. tgacwrujjc wbqwrujjh gn ctcioarun, gqcnionngn tc oragnngn vczcor; ihqh gwauor rwrhjihh vczcofun oragnngn icw vcacoqoarun vcwbicqwruun ruah oragnngn icw vcacoqoarun tojwricqwruun earwn icw ebfurrh igwriun acnrrc, ruah tojawruriw uiih earwiewruriw, gzuiicqcjjc ruah bcdtgwiicqcjjc bcdicoiic tc oragnngjjwrwc qungtc. 19. cdiwajc. tgacwrujjc gn gwauor qwujwzwiuun- tc rcncnvczcoiuun; ihbhn rwrhjiee gwauor bhwdwiruqhiih zwihh qwujwzwiuunrh ruah gwauor dctgwric dwwzzoqciic bcnaawc, vcriccngiicc tc juvwiihh iwuigtc acwaawun iwufgiorvhjwnuwfun acoiic. 20. cdiwajc. 1. acwawjjc gn gwauor dcobcngqcwruun agaggnioqwr- tc ebfwrieqwrvczcoiuun. 2. auihhn uw rcc zcagiicc jwwiieqhhn qwbwnahhn ebfwriearuun. 21. cdiwajc. 1. tgacwrujjc gn gwauor grcjjwrioc qccnrc bcjjwiruqwruun tgag vhjwiisqhriw icw vczccriw vcjwiiotun uforictwun vhjwiearujjh. 2. tgacwrujjc gn ebihjhwnun gwauor zhhrih qccnrc tojawrwwn igwqwwn. 3. acnrcn icbig gn bcjjwiorvcjjcn zudoric; ihqh icbig gn wjqcwricvc qhhdhcwacwrwjjc tc cwfgwjjc vccjuwjjc, tgwrrc acwawjjc gn ejuwnun tc ebihjhwnun hhnwgwauor tc tgwrrc hhnurier gn rcjcwnun icw qooic vccjwvczcofun iodvccvcc qunuiiujeh ngofciicvc. 22. cdiwajc. tgacwrujjc gn ebiuwraonncn thrununh gwauor rgrwccjwiodvccn ruah gwauor acnrcjjwriun igwqunzwiuwfun tc acnrcwnvhjwrun ebiuwriesn acoiic aonawn qccn thdturiujqh tc vgwqcvcdci bogqwggn giicun, ncoiiwc bhnun wbqwrcdvgjjuun tc bhnun earwjsjjwrun gjuqoarunrc vczccjju aubwiieqwrujju vhjiihqhiisqwh icjgofujjwrwc, rgrwccjwrwc tc rwvwrieaujjwrwh gwauoarwc. 23. cdiwajc. 1. tgacwrujjc gn gwauor iesbsn, ieszcwacn vczccruun vcjwniccn, gwauofunqoacwrwwn tc ieefeiihvwwn iesubigwbwn ruah rogtccn iesiisqeeiih vcriccn. 2. tgacwrujjc gn gwauor wjqcn qwnahhnjcwric redtwnihh rcqccn zcjaaccn rcqc-

ric iesrih. 3. tgacwrujjc iesih iuauvhjjh gn gwauor agbioojjwruun tc dwwiihvhhn zcjaaccn, tgac iodvcc bhnujju tc bhnun zudbuujjuun wbqwrcdvgn qoacwrun igwquuniojgn tc tgic icdzuun vcciwurrc ihefunihvhi qooi rgrwccjwrun rogtujon auwngi. 4. tgacwrujjc gn gwauor zudoricc cqqciiwebfwriearwh tc jwwiieh nwwbwn uiotunrc zogjoricqwruarw. 24. cdiwajc. tgacwrujjc gn gwauor juzggn tc vczcc-cwaccn, iesctcn thdauvhhn dctgwiicqwruun ruah qhhdhcwacwrwwn zcjacjjwrwwn jgqwwn. 25. cdiwajc. 1. tgacwrujjc gn gwauor ujwnicrggn, tgac gn dwwiihvh iodvccqccn bhnun tc bhnun zudbuunrh iudvuefun tc bevwnvgwnnwn dcvwnngn, vcciuioarun, cronngn, jhhawnihbogjjgn tc vhjiihqhiisqhn ebiuwraonncjjwrun bogjjgn grcjic. tgacwrujjc gn qesr gwauor iodvccn iesiisqeefun, rcwdcofun, iczciodqcn, jurauefun icw vcnboofun ruah qoon bhnun icbfgriccn dwwzzoqciic iczcbionuun igwquuniojgn qunuiearun vcdcjic. 2. hwfuwjjh tc jczrwjjc gn gwauor udwiewruun bogjiggn tc czoon. acwaawun jcriun, dwwzzoqciic rwwih, gvciag bu renienuui cvwgjwwigrrc icw run ojagzogjujjc, iojuu ncoiiwc rcqcc ebiuwraonncn rogtcc. 26. cdiwajc. 1. tgacwrujjc gn gwauor rccfc gzuioric. gzuioarun gn gjicvc cwncawn cjauwr- tc zudorgzuioarun grcjic qcaroignic. cjauwrgzuioarun gn gjicvc zcagjjwnun. iuanwrih tc cqqciiwgzuioric gn gjicvc ejuwruriw rccicvwjjc, tc agdaucqqcn gzuioarun gn gjicvc cvgwnnc ebihjhwruriw acwawjju buwfhn aeaetunrh qoaccn. 2. gzuioarun gn zedwiihvh wbqwrun zudrggncjjwroofun iheiuun aubwiihqwruun ruah wbqwrgwauoarwun tc zudorvczcoarwun aonnwgwiicqwrun vcbvwricqwruun. run iojuu ufwrihh eqqhdihqerih, rovcwiruvcwrooiic tc erihveeiih acwaawun acnrcaoniwun tc acwaawun dgio- tc oragnigdebqwun auraun ruah zedawh ufwrihqhhn ebfwrienuwfun acnrcaoniwun igwqwnicc dcobcn ejjhzwihqwruarw. 3. vcnbuqqwjjc gn unrwrwtcwnun gwauor vcjwic buwfhn jczrwjjuun cnnuiicvcn gzuioarun jccio. 27. cdiwajc. 1. tgacwrujjc gn gwauor vczccriw grcjjwrioc ebiuwraonncn rwvwrierujhqhhn, ncoiiwc icwiuwric ruah zhhrih grcjjwruarw iwuiuun ufwriearun qoacnccn iogqwric ufowric. 2. tgacwrujjc gn gwauor nwwfun bunawriun tc cwnuujjwriun uiotun rogtccqwruun, tgiac tgbiovci bhnun jogqcriccn iwuiuujjwrurih, awdtcjjwruric icw icwiuujjwruric iogicnngric. 28. cdiwajc. tgacwrujjc gn gwauor rujjcwruun ebiuwraonncjjwruun tc acnrcwnvhjwruun thdturiearuun, tgnac zowiiuwrrc ihrrh tojwrioarurrc urwiuiei gwauofui tc vujvgjjwroofui vgwvci iherwn igiuoioc. 29. cdiwajc. 1. tgacwrujjc wbqwrujjh gn vujvgjjwrooarwc ebiuwraonicc agbiccn, agrac vcwn run zowiiuwrrc bhnun earwjsjjwrun gjuqoarunrc vczcc tc iherw aubwier gn qcbfgjjwnun. 2. aheiihurrhhn gwauoarwccn tc ncoiiwurrccn vczcoarwccn aoaccn uw gju qowfun aown rujjcwriun jcwjjc rhhfuiietun dctgwioriun cjcwnun, tgwfun earwngqcwrunc icdagwioarunc gn iodvcic igwriun gwauoarwun tc vczcoarwun ionnoricqwnun tc aonnwgwiicqwnun ruah qgdccjwn, tojawrun thdturiearun tc ejuwrun bevwnvgwnnwn gwauoiuioi vcciwqoarui acnrcnvcjicwrurrc ebiuwraonncrrc. 3. nhwih gwauoarwc tc vczcoarwc uw qwrrhhn iczcoarurrc rcc aheiihh vcrigwn ebfwrienuwfun acnrcaoniwun zhhqhhdwh tc zudwcciiuwic. 30. cdiwajc. qwihhn ihrrh tojwrioarurrc uw rcc iojawic nwwn, uiih vcjiwg, debqh icw earwiewnun bunawjs vgw run zudoriuujjc acirgc gwauofuaruun iubfh rujjcwric, qwah vgwrw bhvwiihh ihrrh qhhdwiujieth gwauoarwc tc vczcoarwc.

iuariw: ea:n wbqwrgwauoarwun tojwrior

Solmun matematiikan verkkosanakirja

Solmun matematiikan verkkosanakirja on osoitteessa

`http://matematiikkalehtisolmu.fi/sanakirja/a.html`

Sekä sisältöä että tekniikkaa koskevat kokemukset ovat meille arvokkaita ja kaikenlaiset parannus- sekä korjausehdotukset tervetulleita. Palautetta voi lähettää osoitteeseen

toimitus at matematiikkalehtisolmu piste fi