MAAILMAN

Historia

SAGA
EGMONT

VAKOOJAT, KOODIT JA MYSTISET KIRJOITUKSET

MAAILMAN

Historia

SAGA
EGMONT

VAKOOJAT, KOODIT JA MYSTISET KIRJOITUKSET

Maailman historia

Vakoojat, koodit ja mystiset kirjoitukset

SAGA Egmont

Vakoojat, koodit ja mystiset kirjoitukset

ISBN: 9788726383379

1. e-book edition, 2020
Format: EPUB 2.0

SAGA Egmont www.saga-books.com – a part of Egmont, www.egmont.com

Vakoojat, koodit ja mystiset kirjoitukset

Aikojen alusta alkaen ihminen on etsinyt totuutta – tai sitten yrittänyt kaikin keinon salata sen. Jo 11 500 vuotta sitten Siperian länsiosissa ihmiset kaiversivat lehtikuusen palaseen outoja symboleja, jotka tutkijoiden mielestä olivat historian ensimmäisiä koodeja. Voi olla, että niiden viestiä ei saada koskaan selville, mutta arkeologit eivät aio antaa periksi. Arvoitusten ratkaisemisen ja totuuden selvittämisen halu istuvat syvällä ihmisen mielessä.

Sama halu saa vakoojat riskeeraamaan henkensä ja tutkijat yrittämään keskiaikaisen Voynichin käsikirjoituksen koodin murtamista. Totuuden himo on johtanut myös siihen, että osa tutkijoista on kyseenalaistanut vanhat uskomukset Shakespearen henkilöllisyydestä. Tämä kirja kertoo historian taitavimmista vakoojista, salaisista koodeista ja oudoista kirjoituksista. Sukella tutkijoiden mukana koodien salaperäiseen maailmaan.

Mielenkiintoisia lukuhetkiä!

1. Täydellisen koodin jäljillä

Tuhansia vuosia ihmiset ovat yrittäneet peitellä syvimpiä salaisuuksiaan koodien suojaan. Yhtä kauan toiset ovat yrittäneet paljastaa totuuden. Antiikin Caesarin koodeista aina saksalaisten Enigma-laitteeseen on käyty loputonta taistoa salakirjoitustekniikoiden taitajien välillä.

Niin hurjalta kuin se kuulostaakin, salaiset koodit ovat yhtä vanhoja kuin ensimmäinen kirjakieli, ehkä jopa vanhempia. Tutkijat pohtivat, ovatko arvoitukselliset kaiverrukset niin kutsutussa Šigirin idolissa maailman vanhin salainen koodi. Šigirin idoli on korkea, lehtikuusesta veistetty ihmistä muistuttava hahmo, joka löydettiin vuonna 1894 Länsi-Siperiasta, ja saksalaiset tutkijat ovat sittemmin todenneet, että puuveistos on tehty 11 500 vuotta sitten, joten se on kaksi kertaa niin vanha kuin Egyptin pyramidit. Suonpohjan liete on suojannut puuta lahoamiselta.

Asiantuntijoiden huomion ovat korkean iän lisäksi kiinnittäneet kaiverrukset veistoksen pinnalla. Puuta peittävät kuviot ja abstraktit symbolit, joilla ilmeisesti on ollut jokin merkitys, ehkä varoittava.

”Koristelu sisältää salakirjoituksella ilmaistua tietoa”, arvelee Venäjän tiedeakatemian arkeologian professori Mihail Žilin. ”Ihmiset välittivät tärkeää tietoa puuveistoksen avulla.”

Nykyään tutkijat voivat vain arvata, mitä kaiverretut siksakviivat, pienet kasvot ja muut symbolit tarkoittivat niille, jotka osasivat purkaa koodin. Kuitenkin siitä lähtien,

kun Siperian heimot yli 10 000 vuotta sitten ensimmäisinä kaiversivat salaperäiset merkkinsä puupatsaaseen, ihmiset ovat keksineet koodeja jakaakseen salaisia tietoja – ja toiset ovat hetken kuluttua murtaneet koodit. Siperian merkit ovat tosin edelleen arvoitus.

SPARTALAISET SEKOITTIVAT KIRJAIMIA

Šigirin idolin tekijöillä ei ollut kirjakieltä, joten viestit muodostuivat kuvista. Myöhemmin tulivat egyptiläisten hieroglyfit ja sumerien nuolenpääkirjoitus, joissa kuvia käytettiin tietyn järjestelmän mukaan. Ensimmäinen foneettinen kirjakieli, joka siis perustuu kielen äänteisiin, syntyi vuoden 1050 eaa. tienoilla, kun foinikialaiset muuttivat Lähi-idässä hieroglyfit aakkosiksi, joissa oli 22 kirjainta. Foinikialaisten kielessä ja kaikissa myöhemmissä kirjoitetuissa kielissä on kieliopillisia sääntöjä siitä, miten sanat kirjoitetaan ja lauseet muodostetaan. Jos sääntöjä muutetaan, toiset eivät voi lukea kirjoitusta – elleivät he tiedä uusia sääntöjä, joiden mukaan teksti on kirjoitettu. Näin koodi toimii: kielen säännöt rikotaan vihollisen hämäämiseksi.

Antiikin kansat äkkäsivät pian mahdollisuuden kätkeä tietoja muutoin tuttujen kirjainten taakse. Kreikkalaiset ottivat ensimmäisenä käyttöön sanan, joka yhä viittaa koodeihin, eli kryptologian, ”salaisuuden opin”. Kreikassa sotaisat spartalaiset käyttivät niin sanottua skytalea armeijan yksiköiden viesteissä. Pergamentti-, nahka- tai kangassuikaleeseen merkittiin kirjaimet näennäisesti sattumanvaraisessa järjestyksessä. Kun suikale kiedottiin oikean paksuisen sauvan ympärille, kirjaimet muodostivat sanoja. Spartalaisten koodia kutsutaan siirtoalgoritmiksi, koska kirjaimia ei lisätä eikä poisteta, vain niiden paikkaa vaihdetaan. Skytalea oli helppo käyttää, mutta koodi oli

myös melko helppo purkaa. Jos vihollinen sai viestisuikaleen käsiinsä, hänen tarvitsi vain kietoa se eripaksuisten sauvojen ympärille, kunnes halkaisija oli oikea. Spartalaiset koodasivatkin viestejä vihollisen hidastamiseksi, eivät pitääkseen viestit ikuisesti salaisina. Sama koskee monia uudempia ja kehittyneempiä koodijärjestelmiä ja myös yhtä historian kuuluisimmista koodinlaatijoista.

CAESAR MUOKKASI AAKKOSET UUSIKSI

Myös antiikin roomalaiset lähettivät salaisia viestejä, ja erityisesti Julius Caesar oli kuuluisa monista erilaisista koodeistaan. Kokonainen teos kirjoitettiin pelkästään Caesarin koodeista, mutta kirja on sittemmin kadonnut, ja nykyään koodeista tunnetaan vain yksi. Niin kutsutun Caesarin koodin kuvaili kirjailija Suetonius vuonna 121.

”Aina, kun hän halusi kertoa jotain salaista, hän kirjoitti sen koodilla”, Suetonius kertoi.

Caesar-koodissa koko teksti siirretään tietyn kirjainmäärän verran aakkosissa. Määrä on avain, joka vastaanottajan on tunnettava voidakseen purkaa viestin. Jos avain on esimerkiksi kolme, A:n tilalle vaihdetaan D, B:n tilalle E ja niin edelleen.

Caesar-koodia kutsutaan korvausalgoritmiksi, koska siinä kirjaimet korvataan toisilla kirjaimilla. Spartalaisten skytalen lailla koodi on helppo purkaa, ja usein se sujuu myös nopeammin. Lukijan ei tarvitse käydä läpi kaikkia aakkosia alusta loppuun esimerkiksi siirtämällä kirjaimia ensin vain yhden paikan verran, sitten kaksi ja sitten kolme, kunnes teksti tarkoittaa jotakin. Sen sijaan hän voi keskittyä kirjaimiin, jotka esiintyvät tiheimmin koodatussa viestissä. Ne vaihdetaan useimmiten vokaaleihin tai yleisimpiin konsonantteihin.

Koodinpurkumenetelmää kutsutaan frekvenssianalyysiksi. Sitä on perusteellisesti kuvaillut Bagdadissa 800-luvulla elänyt suuri ajattelija Al-Kindi. Häntä pidetään arabialaisen filosofian isänä, mutta hän kirjoitti myös tieteellisiä teoksia antiikin Kreikan oppien pohjalta. Yksi Al-Kindin lukuisista kirjoituksista oli historian ensimmäinen kryptoanalyysin eli koodien purkamisen käsikirja. Hänen mukaansa useimmat koodit voitiin ratkaista tutkimalla, miten usein tietyt kirjaimet esiintyivät kooditekstissä, koska niin muodostui yhtymäkohtia tavalliseen tekstiin. Satoja vuosia monet yrittivät päätellä, miten koodeja voitiin paljastaa frekvenssianalyysin avulla, mutta he epäonnistuivat – joskus jopa kuolettavin seurauksin, kuten Skotlannin kuningatar Maria Stuart joutui toteamaan.

ENTINEN KUNINGATAR UHKASI RAUHAA

”Mary, Queen of Scots”, kuten britit häntä kutsuvat, eli kuohuvana ja sekasortoisena aikana. Katolilaisena hän oli alati riidoissa mahtavien protestanttisten aatelisten kanssa, ja vuoden 1567 kapinan jälkeen hän pakeni maasta. Skotlannin kuningatar hakeutui turvaan lähisukulaisensa Englannin Elisabet I:n luokse, mutta se osoittautui suureksi virheeksi. Maria Stuartilla oli nimittäin myös vaatimuksia Englannin kruunuun, ja maan katolinen vähemmistö suunnitteli jatkuvasti, miten Maria saataisiin nostettua valtaan. Siksi protestanttinen Elisabet lukitsi ei-toivotun vieraansa linnaan, missä tällä ei ollut mitään yhteyksiä ulkomaailmaan. Näin kului 18 vuotta, mutta sitten Maria Stuart alkoi saada salaisia kirjeitä. Katolinen aatelismies Anthony Babington halusi jakaa ovelan juonen Maria Stuartin kanssa. Babingtonin viestit oli piilotettu oluttynnyreihin, joita toimitettiin säännöllisesti linnaan.

Varmuuden vuoksi lähettäjä oli kirjoittanut viestit salakirjoituksella, jotta raskauttava sisältö oli suojassa, jos kirje päätyi vääriin käsiin.

Babingtonin käyttämä koodi perustui korvausalgoritmiin, jossa merkit korvasivat kaikki kirjaimet. Babington täydensi koodia merkeillä, jotka tarkoittivat kokonaista sanaa tai ilmaisivat, että seuraava merkki oli kaksoiskonsonantti. Lisäksi koodiin kuului neljä merkkiä, jotka eivät tarkoittaneet mitään vaan olivat pelkkää harhautusta.

Babington kirjoitti Maria Stuartille pyytäkseen siunausta salajuonelle, joka päättäisi Marian vankeuden ja nostaisi tämän Englannin valtaistuimelle. Vietettyään 18 vuotta vankeudessa Skotlannin entinen kuningatar janosi vapautta epätoivoisesti, ja tuntemattoman pelastajan tarjous houkutti häntä. Kahden salaliittolaisen epäonneksi kolmas silmäpari luki kirjeenvaihtoa. Englannissa ei tapahtunut mitään, mistä ovela vakoilupäällikkö Francis Walsingham ei olisi kuullut. Hän tiesi, miten Babington sai kirjeet Maria Stuartille, koska hän oli itse luonut viestintäyhteyden heidän välilleen. Francis Walsingham halusi poistaa Skotlannin entisen kuningattaren aiheuttaman uhkan, ja sitä varten hän tarvitsi todisteita Mariaa vastaan.

Agenttien välityksellä vakoilupäällikkö rohkaisi vaivihkaa Babingtonia ryhtymään maanpetokseen. Valonarkoja kirjeitä maan halki kiidättänyt kuriiri oli myös Walsinghamin palkkalistoilla. Matkalla oluttynnyreihin kätketyistä kirjeistä avattiin varovasti sinetit ja sisältö kopioitiin.

”Saavun vapauttamaan sinut kymmenen aatelismiehen ja satojen maanmiestemme kanssa vihollisen käsistä”, Babington kirjoitti ensimmäisessä kirjeessään. Sillä välin toisen katolisen ryhmän oli määrä murhata kuningatar Elisabet, jotta tie valtaistuimelle olisi auki.

Babingtonin tarjous oli liian suuri kiusaus Maria Stuartille, joka vastauksessaan hyväksyi aikeet. Hän myönsi myös, että katolisen Espanjan joukkojen tuli nousta maihin Englantiin varmistamaan hänen valtaannousuaan. Entinen kuningatar Maria Stuart allekirjoitti näin oman kuolemantuomionsa, sillä Walsinghamin paras koodinmurtaja oli ratkaissut Babingtonin koodin. Valemerkit hidastivat paljastusta, mutta lopulta voittoon vei frekvenssianalyysi, jolla koodiaakkoset saatiin selville. Kokonaiset sanat joidenkin merkkien takana voitiin sitten arvata ympäröivän tekstin perusteella. Babingtonin ja Maria Stuartin kirjeenvaihdosta löytyivät Walsinghamin tarvitsemat raskauttavat yksityiskohdat. Niillä hän sai vakuutettua Elisabetin, että tämän oli luovuttava pysyvästi skottilaisesta sukulaisestaan. Maria Stuart mestattiin helmikuussa 1587.

KOODIT LOIVAT VALHEELLISTA TURVAA

Babingtonin tapaus on esimerkki siitä, miten koodit voivat luoda valheellista turvallisuudentunnetta. Lähettäjät luulevat olevansa turvassa salakirjoituksen takana, joten viestit sisältävät tarpeettoman paljon arkaluonteisia yksityiskohtia. Tapaus osoittaa myös klassisen korvausalgoritmin heikkouden frekvenssianalyysin edessä. Itse asiassa paljon turvallisempaa koodijärjestelmää ehdotettiin aikalaisteoksessa. Mikäli Babington olisi lukenut teoksen, hän olisi ehkä välttänyt pyövelin kirveen.

Euroopan hallitsijat alkoivat 1500-luvulla lähettää pysyvästi lähettiläitä toistensa hoveihin. Neuvottelemisen lisäksi diplomaatit vakoilivat minkä ehtivät, samoin kuin heitä itseään vakoiltiin. Siksi ei ollut mikään sattuma, että yksi lähettiläistä ehdotti uutta ja paljon entistä monimutkaisempaa salakirjoitusta. Ranskalainen Blaise de