Matematiikkaa kaikille
Syksy 2016
Pienryhmätehtävät 6 – **Ohjaajille**

Tehtävä

(1) Rubikin kuutio – ohjeet tulevat taululle.

Huomioita.

Tämän tehtävät voi jättää tekemättä, erityisesti niissä ryhmissä, joissa ei ole yhtään ratkaisutaitoista henkilöä. Suosittelen silti kokeilemaan! Ohjeet löytyvät sekä tulostettuna ohjaajien materiaaleista että kurssin kotisivuilta.

Annetut siirtosarjat ovat sellaisia, että vain kolme palaa vaihtaa paikkaa, tai kaksi palaa kääntyy paikoillaan. Kaikki loput palat pysyvät siis paikoillaan. Kyse on vieläpä ns. 3-sykleistä: siirtosarjan toistaminen kolme kertaa peräkkäin palauttaa kuution takaisin sen alkuperäiseen tilaan. Tätä voi hyödyntää erityisesti ryhmissä, joissa kuutioita ei riitä kaikille. Näin ohjaajan ei tarvitse ratkaista kuutiota siirtosarjojen välissä. (Teoriassa voisi tehdä esimerkiksi kaikki siirtosarjat ja jatkaa jotain 3-sykleistä "loppuun". Kuution sekoittumisen välttämiseksi suosittelen kuitenkin vahvasti, että opiskelijat eivät 3-syklin havainnollistamisessa vaihda siirtosarjaa kesken kaiken.)

Tehtävä

(2) Caesar-salaus. Ohessa taulukko kirjainten "numerovastaavuuksista"

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
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Pura seuraavat salaukset:

(a) NBUFNBUJJLLB (Salattu menetelmällä Caesar-1)

(b) OWLLWMAVWBXTIGLQKM (Salattu menetelmällä Caesar-8)

Huomioita.

Ensimmäinen viesti on MATEMATIIKKA ja toinen GOD DOES NOT PLAY DICE. Jälkimmäinen on Albert Einsteinin kommentti kvanttisuperposition käsitteeseen.

Voitte myös keksiä omia salaviestejä tai laittaa opiskelijat hommiin. Kurssin kotisivuilla on linkki yhteen monista Caesar-salauksien generoimiseen ja purkamiseen soveltuvaan sivustoon.

Tehtävä

(3) Vigenèren salaus (Liitteenä Vigenèren neliö.)

(a) Salaa viesti TORSTAI avainsanalla HEI.

(b) Pura viesti COZDSSFXRQDIG, kun tiedät avainsanan olevan KOODI.

Huomioita.

Viesti TORSTAI salattuna avainsanalla HEI on ASZZXIP, ja viesti COZDSSFZRQDIG on purettuna SALAKIRJOITUS.

Tehtävä

(4) Tutki (pikku-)Enigman mallia ja toimintaa.

Huomioita.

Tarkoituksena on tehdä oma Enigma. Opiskelijat voivat tehdä joko pikku-Enigman tai ison Enigman. Kannattaa lukea Enigma-ohjeet. Hyllyssä laatikossa on molemmille versioille sopivia salaviestejä purettavaksi.

Tehtävä

(5) Suuryhtiön kassaholvin pin-koodi on jokin nelinumeroinen luku. Kolme pääjehua luottavat melkein toisiinsa. He haluavat kehittää menetelmän, jonka avulla holvi voidaan lukita siten, ettei kukaan saa holvia auki yksin, mutta ketkä tahansa kaksi kolmesta pääjehusta saavat sen auki yhdessä.

Käytännössä pääjehuilla voi olla vaikka tietokone, joka jokaisen avauksen jälkeen asettaa holviin uuden pin-koodin ja jakaa pääjehuille uudet henkilökohtaiset koodit. Mistä tahansa kahdesta henkilökohtaisesta koodista tulee siis voida päätellä varsinainen pin-koodi. Miten tämän voisi toteuttaa?

Lisärajoite 1: Järjestelmän pitää toimia myös pääjehujen lukumäärän kasvaessa kymmeneen.

Lisärajoite 2: Jos joku ulkopuolinen saa käsiinsä yhden avaimen, niin koodin arvaamisen pitää olla yhtä hankalaa kuin jos hänellä ei olisi yhtään avainta,

Lisärajoite 3: Kymmenen pääjehua, joista kenen tahansa kolmen pitää saada holvi auki yhdessä. Se, että käsillä on yksi tai kaksi avainta, ei saa tehdä holvin luvatta avaamisesta helpompaa, kuin jos käsillä olisi vain yksi avain.

Huomioita.

Perusidea on piilottaa koodi y-akselille. n-asteen funktiolle tarvitaan $n + 1$ kappaletta pisteitä, jotta funktion kuvaaja on yksikäsitteinen. Esimerkiksi jos sinulla on yksi piste, voit piirtää sen kautta äärettömän monta suoraa. Jos kaverillasi on toinen piste, näiden kahden pisteen kautta voi piirtää täsmälleen yhden suoran. Suora leikkaa y-akselin pisteessä, joka on haluttu koodi.

Googlaa "Shamir's algorithm" tai "Shamir's secret sharing".