Tehtävä 3. Ongelmanratkaisutehtävä – Salakirjoitus

Kysymys 3.1. Eräässä yksinkertaisessa salakirjoituksessa jokainen kirjain korvataan sitä vastaavalla numerolla (A = 1, B = 2, jne.). Käytetään tehtävässä tavallista suomalaista aakkostoa, jossa on 29 kirjainta: 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. (Yhteensä 7 p.)

(a) Erään Suomen paikkakunnan nimi on salattu edellä kuvatulla yksinkertaisella salakirjoituksella, jolloin salakirjoitettu viesti on seuraava:
16 9 5 11 19 28 13 28 11 9
Pura tämä viesti. Mikä on salakirjoitettu sana? (1 p.)

(b) Tässä on salakirjoitettu sama viesti, mutta on käytetty vaikeutettua salakirjoitusta. Siinä numeroiden alkamispaikkaa on siirretty sopiva määrä eteenpäin, jolloin esim. D = 1, E = 2, jne., ja viimeisen aakkosen jälkeen jatketaan alusta niin, että kaikille kirjaimille saadaan vastaava salakirjoitusnumero. Nyt salakirjoitettu viesti on seuraava:
14 7 3 9 17 26 11 26 9 7.
Kuinka paljon numeroiden alkamispaikkaa on siirretty eteenpäin? (1 p.)

(c) Jos et tietäisi mikä salakirjoitettu sana on kysymyksessä 3.1.(b), mutta tiedät että salauksessa on käytetty juuri tätä menetelmää ja et tiedä siirron määrää, niin esitä täsmälliset ohjeet salakirjoituksen purkamiseksi. Esitä ohjeet niin selkeästi ja täsmällisesti, että kuka tahansa lukioikäinen nuori osaisi seurata niitä. (5 p. Arvioinnissa otetaan huomioon ratkaisun selkeys, johdonmukaisuus ja toimivuus.)

Kysymys 3.2. Toisessa salakirjoituksessa kirjaimet korvataan toisilla kirjaimilla, jotka ovat käänteisessä järjestyksessä (A = Ö, B = Ä, jne.). (Yhteensä 10 p.)

(a) Pura seuraava salakirjoitettu viesti, joka sisältää paikkakunnan nimen: KOQYLO (1 p.)

(b) Seuraava viesti on salakirjoitettu vaikeutetulla versiolla tästä salakirjoituksesta. Siinä kirjaimille on tehty vastaava siirto kuin kysymyksessä 3.1.(b), jolloin J ei olekaan salakirjoitettuna T, vaan tietyllä siirrolla W. Pura seuraava salakirjoitettu viesti, joka sisältää paikkakunnan nimen: MKTUBJB. Et siis tiedä kuinka paljon kirjaimia on siirretty, joten sinun pitää selvittää se. (3 p.)

(c) Jos et tietäisi mikä salakirjoitettu sana on kysymyksessä 3.2.(b), mutta tiedät että salauksessa on käytetty juuri tätä menetelmää ja et tiedä siirron määrää, niin esitä täsmälliset ohjeet salakirjoituksen purkamiseksi. Esitä ohjeet niin selkeästi ja täsmällisesti, että kuka tahansa lukioikäinen nuori osaisi seurata niitä. (5 p. Arvioinnissa otetaan huomioon ratkaisun selkeys, johdonmukaisuus ja toimivuus.)

(d) Kuinka monta vaihtoehtoa siirrolle sinun pitää enintään testata, että saat purettua salakirjoituksen? (1 p.)

Kysymys 3.3. Tarkastellaan julkisen avaimen salakirjoitusjärjestelmää, jossa salauksessa käytettävä avain on julkinen, mutta purkamiseen tarvittavan avaimen tietää vain viestin vastaanottaja. Tätä menetelmää käytetään nykyisin yleisesti viestien salaamisessa. Salausjärjestelmässä salataan lukuja, jolloin myös kirjaimet ja muut merkit koodataan ensin numeroiksi ja salataan sen jälkeen.

Julkisen avaimen salakirjoitusjärjestelmä toimii seuraavasti. Valitaan ensin kaksi alkulukua p ja q. Alkuluvulla tarkoitetaan luonnollista lukua > 1, joka on jaollinen vain luvulla 1, mutta ei millään muulla itseään pienemmällä luvulla. Alkulukuja ovat siten 2, 3, 5, 7, 11, 13, 17, 19, jne.

Lasketaan lukujen tulo $p * q = N$. Valitaan sitten luku d siten, että $1 < d < N$, ja niin ettei luvuilla d, $(p-1)$ ja $(q-1)$ ole yhteisiä tekijöitä. Luvuilla on yhteinen tekijä, jos luvut ovat jaollisia samalla luvulla.

Valitaan sitten luku x siten, että kun $d*x$ jaetaan luvulla $(p-1)*(q-1)$, niin jakojäännös on 1.

Nyt meillä on selvillä julkisen salauksen salausavaimet N ja x, ja purkuavaimet N ja d. Avaimet N ja x voidaan julkaista vaikka netissä, mutta avain d täytyy pitää salassa, ettei kukaan asiaton pysty purkamaan viestiä.

Tarkastellaan tätä vielä esimerkin avulla. Valitaan $p = 3$ ja $q = 11$, jolloin $N = p*q = 33$ ja $(p-1)*(q-1) = 20$. Nyt täytyy olla niin, että $1 < d < 33$, ja d:llä ei saa olla yhteisiä tekijöitä lukujen 2 ja 10 kanssa. Tällainen arvo d:lle on esimerkiksi luku 3. Nyt täytyisi valita x siten, että luvun $3*x$ jakojäännös luvun 20 kanssa on 1. Sopivaksi luvuksi voidaan valita $x = 7$.

Julkinen avainpari on siten $N = 33$ ja $x = 7$. Salainen avainpari on $N = 33$ ja $d = 3$.

Viesti salakirjoitetaan korottamalla se potenssiin x ja ottamalla sitten jakojäännös jaosta luvun N kanssa. Tämä salakirjoitettu viesti puretaan korottamalla se potenssiin d ja ottamalla sitten jakojäännös jaosta luvun N kanssa. (Yhteensä 8 p.)

(a) Kari haluaa edellä esitetyn esimerkin tiedoilla lähettää Tainalle viestin, joka kertoo missä junavaunussa he tapaavat. Salakirjoita viesti 2 edellä kuvatulla julkisen avaimen salakirjoitusmenetelmällä. (3 p.)

(b) Taina vastaa Karille viestillä, joka kertoo tapaamisajan tunnin tarkkuudella. Salakirjoitettu viesti on 6. Pura viesti ja selvitä tapaamisaika. (5 p.)