

Tehtävä 1: Palvelujen personointi

Lue oheinen teksti, jossa kuvataan palvelujen personointia. Vastaa personointi-esimerkkejä sisältäviin kysymyksiin 1.1.–1.9. tekstin pohjalta. Vastaa lisäksi esseetyyppisiin kysymyksiin 1.10.–1.11. sekä tekstin että omien tietojesi pohjalta.

Asiakkaiden henkilökohtaisten tarpeiden tunnistaminen on keskeinen osa yritysten asiakaspalvelua. Ennen vanhaan kauppias saattoi tuntea asiakkaansa nimeltä ja pystyi suosittelemaan hänelle sopivia tuotteita ja tarjouksia. Henkilökohtainen asiakaspalvelu perustui pitkään ainoastaan vuorovaikutukseen myyjän ja asiakkaan välillä. Nykyään Internetin avulla voidaan kerätä reaaliaikaista tietoa asiakkailta, ja teknologian kehittyminen mahdollistaa yhä yksilöllisempien palvelukokemusten tarjoamisen. Tätä vuorovaikutuksen muokkaamista yksilöllisen palvelukokemuksen tarjoamiseksi kutsutaan **personoinniksi**. Sen avulla yritysten on mahdollista mm. suositella asiakkaalle tiettyjä tuotteita, tuotekategorioita, brändejä ja tarjouksia sekä muokata asiakkaan käyttämän nettisivun rakennetta tai hänen näkemäänsä hakutuloksia. Tavoitteena on, että kun asiakas kokee tulevaisuutta yksilöllisesti kohdelluksi, yritysten myynti kasvaa.

Personointia voidaan hyödyntää myös osana kasvokkain, puhelimitse tai sähköpostitse tehtävää asiakaspalvelua. Asiakaspalvelussa teknologiavälitteistä personointia voidaan käyttää asiakkuudenhallintaa tukevien ohjelmistojen avulla. Esimerkiksi hotellin vastaanottovirkailija voi tarjota asiakkaalle niitä palveluja, joita ohjelmisto arvioi sopiviksi juuri kyseiselle asiakkaalle. Personoinnin avulla asiakkaiden odotetaan liittävän myönteisiä mielikuvia yrityksen asiantuntijuuteen sekä palvelujen laatuun ja tehokkuuteen. Tämän myötä yrityksen odotetaan saavan entistä tyytyväisempiä ja lojaalimpia asiakkaita.

Personointia käytetään sekä hyötyä että viihdettä painottavissa mobiili- ja nettisovelluksissa. Hyötysovelluksissa personoinnilla tavoitellaan toiminnan tehostumista, käytettävyyden parantumista tai muuta konkreettisten tavoitteiden saavuttamista. Esimerkiksi verkkokaupassa personoinnin avulla tunnistetaan ja hyödynnetään asiakkaan ostohistoriaan perustuvia yksilöllisiä tarpeita. Viihteellistä käyttöä painottavissa sovelluksissa personoinnin avulla voidaan tavoitella entistä laadukkaampaa käyttökokemusta. Personointia voidaan hyödyntää esimerkiksi verkkopelien suunnittelussa luomalla käyttäjän mieltymyksiä vastaavia toimintaympäristöjä ja sosiaalisia verkostoja.

Personoinnin toteuttamisessa voidaan erottaa kolme ulottuvuutta:

- (1) Personoinnin toteutustapa: mikä on personoinnin automaattisuuden aste?
 - a) Käyttäjälähtöisessä personoinnissa **automaattisuuden aste on matala**, jolloin personointi toteutuu enimmäkseen palveluiden käyttäjän tietoisesti ja aktiivisesti personoimalla palvelua mieleisekseen.
 - b) Järjestelmälähtöisessä personoinnissa **automaattisuuden aste on korkea**, jolloin järjestelmä toteuttaa personointia enimmäkseen automaattisesti. Käyttäjä voi joissakin tapauksissa myös tietoisesti tarjota informaatiota käyttäjälähtöisen personoinnin toteuttamiseksi.
- (2) Personoinnin kohderyhmä: kenelle personoidaan ja minkä tyyppisen tiedon perusteella? Personointi voidaan kohdistaa
 - a) tiettyyn yksilöön tämän aikaisemman verkkokäyttäytymisen, tekemien arvostelujen tai mielenkiinnon kohteiden perusteella tai
 - b) tiettyyn ihmisryhmään siihen liitettävien huomioiden pohjalta (mm. ikä, sukupuoli, perhetilanne, ammatti, asuinpaikka).

Ihmisryhmään kohdistuvassa personoinnissa oletetaan, että ryhmään kuuluvilla on samoja tarpeita ja mielenkiinnon kohteita ja kukin yksilö tyydytetään tiettyyn ryhmään ominaisuuksiensa perusteella automaattisesti ennakko-oletusten pohjalta. Personoinnin toteuttamisessa voidaan hyödyntää myös koneoppimiseen perustuvaa automatiikkaa yksilön käyttäytymisen analysoimisessa, ryhmien välisten erojen tunnistamisessa ja uusien potentiaalisten ryhmien löytämisessä ilman varsinaisten ennakko-oletusten tekemistä.
- (3) Personoinnin kohdistuminen: mitä personoidaan? Personoinnin avulla voidaan vaikuttaa palvelujen
 - a) sisältöön: mitä informaatiota tarjotaan käyttäjälle ja/tai miltä informaatio näyttää käyttöliittymässä tai
 - b) toiminnallisuuteen: mitä käyttäjä voi tehdä palvelun avulla.

Tietojenkäsittelytieteen valintakoe 28.5.2018

Vastaa kysymyksiin 1.1.–1.9. edellä olevan tekstin pohjalta. Lue kukin esimerkki ja valitse a-, b- tai c-kohdista yksi paikkansapitävä vaihtoehto. Kirjoita valitsemasi vaihtoehto ylös vastauspaperiin seuraavaan tyyliin:

”Kysymys 1.1: x”.

Kysymys 1.1. Vuoden kuluttua asiakkaan edellisestä matkasta matkatoimistosta lähetetään postikortti, jossa suositellaan matkaa sen perusteella, miten asiakas on käyttänyt matkatoimiston nettisivua. Jokaiselle asiakkaalle tarjotaan juuri hänelle sopivaksi arvioitua matkaa. Tässä esimerkissä personointia toteutetaan (1 p.)

- a) enimmäkseen järjestelmälähtöisesti,
- b) enimmäkseen käyttäjälähtöisesti, tai
- c) personointia ei tehdä.

Kysymys 1.2. Matkapuhelimeen ladattava Matkaopas-karttasovellus opastaa käyttäjää kiinnostavien matkakohteiden paikantamisessa. Mobiilisovellus hyödyntää GPS-teknologiaa käyttäjien paikantamisessa ja suosittelee kiinnostavia kohteita ja lähialueen palveluita käyttäjän aikaisemman toiminnan perusteella. Käyttäjä voi valita, haluaako hän löytää ensisijaisesti nähtävyyksiä, ravintoloita tai muita matkakohteita. Hän pystyy lisäksi tarkentamaan suosituksia hintaluokan tai asiakasarvioiden mukaan. Tässä esimerkissä personoinnin kohderyhmänä on (1 p.)

- a) tietty yksilö,
- b) tietty etukäteen määritelty ryhmä, tai
- c) ei kumpikaan.

Kysymys 1.3. Videomateriaalia jakava nettisivusto tarjoaa uutta sisältöä reaaliaikaisesti käyttäjän katseluhistorian ja mieltymysten mukaan. Sivusto tunnistaa käyttäjän päätelaitteen ja muuttaa näkymän siihen sopivaksi. Tässä esimerkissä personointi kohdistuu (1 p.)

- a) palvelun sisältöön,
- b) palvelun sisältöön ja palvelun toiminnallisuuteen, tai
- c) personointia ei tehdä.

Tietojenkäsittelytieteen valintakoe 28.5.2018

Kysymys 1.4. Taidemuseon asiakkaille tarjotaan lipunmyynnissä tabletti-tietokone, jonka kanssa museota on tarkoitus kiertää. Tablettiin asennettu sovellus sisältää lisätietoa eri teoksista, taiteilijoista ja tyylistä. Tässä esimerkissä personointia toteutetaan (1 p.)

- a) enimmäkseen järjestelmälähtöisesti,
- b) enimmäkseen käyttäjälähtöisesti, tai
- c) personointia ei tehdä.

Kysymys 1.5. Kuljetusyrityksen nettisivustolla vieraillessa käyttäjän täytyy ensimmäiseksi valita, onko hän asiakas (tarjouspyynnöt), yrityskumppani (rahtia koskevat asiat) vai ammattikuljettaja (työtuntien sähköinen raportointi). Sivuston sisältö ja ulkoasu mukautuvat valinnan mukaan. Tässä esimerkissä personoinnin kohderyhmänä on (1 p.)

- a) tietty yksilö,
- b) tietty etukäteen määritelty ryhmä, tai
- c) ei kumpikaan.

Kysymys 1.6. Käyttäjä luo tunnukset nettisivustoon, jota hän pitää jatkossa selaimensa aloitussivuna. Hän voi muokata palvelun ulkoasua mieltymystensä mukaan ja valita sivustolle itseä kiinnostavia aihepiirejä, kuten sähköpostinsa, sosiaalisen median kanavat, blogit, keskeisimmät uutiset, urheilutulokset ja uusimman viihdesisällön. Tässä esimerkissä personointi kohdistuu (1 p.)

- a) palvelun sisältöön,
- b) palvelun sisältöön ja palvelun toiminnallisuuteen, tai
- c) personointia ei tehdä.

Tietojenkäsittelytieteen valintakoe 28.5.2018

Kysymys 1.7. Tavaratalolla on nettisivullaan palvelu, jonka avulla asiakkaan on mahdollista hyödyntää vaatteiden sovituksessa ja sopivien vaatteiden tilaamisessa virtuaalista mallinukkea. Kun asiakas lataa palveluun valokuvan itsestään, palvelu arvioi kehon mitat automaattisesti, muuttaa mallinuken asiakkaan näköiseksi ja tarjoaa näin realistisen kuvan sovitettavien vaatteiden ulkonäöstä. Palvelu ehdottaa myös muita kokonaisuuteen sopivia vaatteita ja asusteita. Tässä esimerkissä personointia toteutetaan (1 p.)

- a) enimmäkseen järjestelmälähtöisesti,
- b) enimmäkseen käyttäjälähtöisesti, tai
- c) personointia ei tehdä.

Kysymys 1.8. Vaatteita myyvä verkkokauppa tarjoaa asiakkaan maantieteellisen sijainnin perusteella ilmaston kannalta sopivimpia vaatteita ja kenkiä eri vuodenaikoina. Lisäksi verkkokauppa huomioi kunkin maan kielellisiin ja kulttuurisiin ominaispiirteisiin mukautettuja visuaalisia ominaisuuksia. Tässä esimerkissä personoinnin kohderyhmänä on (1 p.)

- a) tietty yksilö,
- b) tietty etukäteen määritelty ryhmä, tai
- c) ei kumpikaan.

Kysymys 1.9. Terveyttä ja hyvinvointia tukevan järjestön nettisivusto tarjoaa tietoa eri osa-alueista kiinnostuneille käyttäjille, kuten masentuneille, raskaana oleville, lapsiperheille ja laihduttajille. Kaikki sivuston tarjoama sisältö on julkista ja käyttäjä saa vapaasti tutkia koottua terveystietoa. Tässä esimerkissä personointi kohdistuu (1 p.)

- a) palvelun sisältöön,
- b) palvelun sisältöön ja palvelun toiminnallisuuteen, tai
- c) personointia ei tehdä.

Tietojenkäsittelytieteen valintakoe 28.5.2018

Vastaa kysymyksiin 1.10.–1.11. tehtävän alussa olevan tekstin ja omien tietojesi pohjalta. Vastaukset eivät saa olla suoraan peräisin taustamateriaalista, mutta voit johtaa niitä taustamateriaaliin perustuen. Vastausten listaamisen sijaan laadi vastaukset esseemuodossa.

Kysymys 1.10. Kuvittele olevasi Lapissa sijaitsevan hotellin omistaja. Majoituksen lisäksi hotellisi tarjoaa myös elämysmatkailupalveluita, kuten opastettuja retkiä ja liikuntapalveluita. Hotelliisi ollaan parhaillaan asentamassa uutta järjestelmää, jonka avulla on mahdollista seurata asiakkaiden ja työntekijöiden sijaintia sekä heidän käyttämiään palveluita. Pohdi, millä tavalla voisit ottaa asiakaspalveluiden personoinnin käyttöön osana hotellyrityksesi toimintaa. Kehitä kolme personoitua palvelua yrityksellesi (suunnitelma 1, suunnitelma 2, suunnitelma 3). Kuvaa kussakin suunnitelmassa **palvelun sisältö**, mitä **tietoa** sen toteuttamiseksi kerätään, ja mitkä ovat tiedon **lähteet**, eli minkäläisten teknisten ratkaisujen tai muiden keinojen avulla tiedon keräys tapahtuu. Kuvaa suunnitelmissasi myös, kuinka tehtävän alussa olleessa tekstissä kuvatut **personoinnin kolme ulottuvuutta** toteutuvat.

Suunnitelmien arviointiperusteet:

- a) Personoidun **palvelun** kuvaus ja sen realistisuus (3 p., 1 p./suunnitelma)
- b) Kerättävän **tiedon** kuvaus (3 p., 1 p./suunnitelma)
- c) Kerättävän **tiedon lähteiden** kuvaus (3 p., 1 p./suunnitelma)
- d) **Personoinnin kolmen ulottuvuuden** erittely (3 p., 1 p./suunnitelma)
- e) Tekstin sujuvuus kokonaisuutena (1 p.)

HUOM! Jos kirjoitat useamman kuin kolme suunnitelmaa, vain kolme ensimmäistä tullaan arvioimaan.

Kysymys 1.11. Pohdi personoinnin mahdollisia negatiivisia puolia tai toteuttamisen haasteita yleisellä tasolla. Sinun ei tarvitse käyttää edellisen kysymyksen 1.10. kuvausta pohjana. Mainitse ja perustele kolme negatiivista puolta tai haastetta. (3 p.)

Tehtävä 2: Liukuhihna

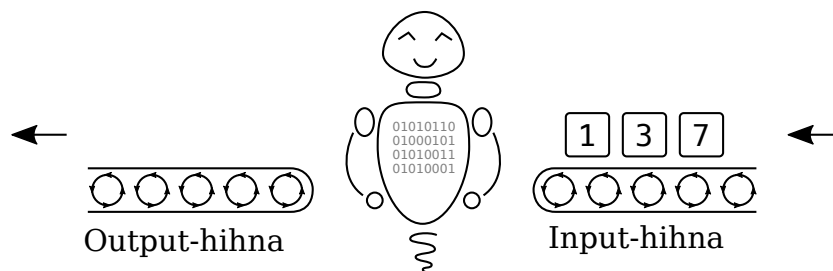
Olkoon käytössä väsymätön robotti, jonka tehtävänä on käsitellä liukuhihnalla sille syötettäviä kokonaislukuja. Robotti ottaa vastaan luvun, käsittelee sen annetulla ohjeella, ja siirtää käsitellyn luvun valmiiden lukujen liukuhihnalle. Nimitetään sisääntulevien lukujen hihnaa input-hihnaksi ja valmiiden lukujen output-hihnaksi. Robotille voi antaa ohjeita seuraavien komentojen avulla:

Komento	Toiminnon kuvaus
INPUT	Ota yksi luku input-hihnalta.
OUTPUT	Siirrä luku output-hihnalle.

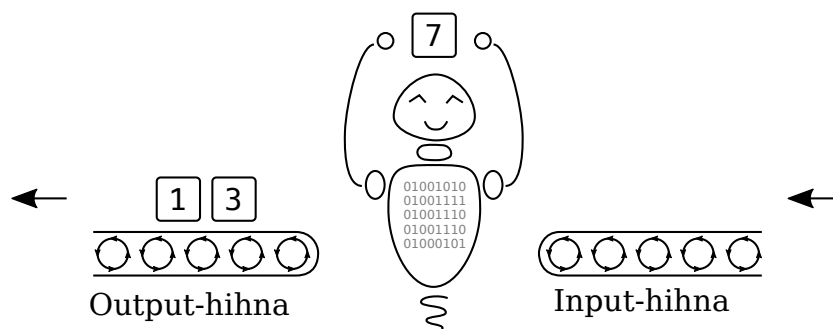
Ohje koostuu robotille annettavasta suoritettavien komentojen sarjasta ja voi sisältää useita komentoja. Komennot suoritetaan yksi kerrallaan, ja robotilla voi olla kädessä vain yksi luku kerrallaan. Robotin työsuoritus päättyy, kun kumpi tahansa seuraavista ehdoista täyttyy: (a) ohjeessa ei ole enää suoritettavia komentoja, tai (b) input-hihnalla ei ole enää lukuja yritettäessä suorittaa INPUT-komentoa.

Esimerkiksi, jos input-hihnalle tulisivat luvut 1, 3 ja 7 (joista luku 1 tulee ensimmäisenä käsittelyvuoroon), niin seuraava ohje siirtäisi ne output-hihnalle. Kuvat 1 ja 2 havainnollistavat esimerkin robotin toimintaa.

INPUT
OUTPUT
INPUT
OUTPUT
INPUT
OUTPUT



Kuva 1: Ohjeen alkutilassa input-hihnalla ovat luvut 1, 3 ja 7.



Kuva 2: Ohjeen viimeisessä OUTPUT-komennossa luku 7 on käsiteltävänä.

Jotta robottia voidaan käyttää erilaisiin tehtäviin, sisällytetään robotin tunnistamiin komentoihin seuraavassa taulukossa esiteltyt komennot. Lisäksi robotilla on käytettävissä rajoittamattomasti muistipaikkoja lukujen ja niistä laskettujen välitulosten varastointia varten. Muistipaikat on nimetty kokonaisluvulla nollasta alkaen, joten muistipaikkojen nimet ovat 0, 1, 2, 3, ja niin edelleen.

Komento	Toiminnon kuvaus
ADD(n)	Laske yhteen muistipaikassa n oleva luku ja kädessä oleva luku. Yhteenlaskun lopputulos tulee käteen.
SUB(n)	Vähennä kädessä olevasta luvusta muistipaikassa n oleva luku. Laskun lopputulos tulee käteen. Jos esimerkiksi kädessä on 10 ja muistipaikassa 2 on luku 4, niin tällöin SUB(2)=6.
COPYTO(n)	Kopioi kädessä pideltävä luku muistipaikkaan n .
COPYFROM(n)	Kopioi muistipaikassa n olevan luku käteen. Jos kädessä oli jokin luku, se tuhoutuu.
Paikka:	Määrittelee ohjeeseen merkityn kohdan, johon robotti voi siirtyä JUMP-komentojen avulla. Ohjeen suorittamista jatketaan kohdasta Paikka eteenpäin.
JUMP(Paikka)	Siirry kohtaan Paikka.
JUMPIFZERO(Paikka)	Siirry kohtaan Paikka vain siinä tapauksessa, että kädessä on luku 0. Muussa tapauksessa jatka seuraavaan komentoon.
JUMPIFNEG(Paikka)	Siirry kohtaan Paikka vain siinä tapauksessa, että kädessä on negatiivinen luku ($-1, -2, \dots$). Muussa tapauksessa jatka seuraavaan komentoon.

Esimerkit

Esimerkki 1. Tehdään ohje, joka siirtää input-hihnalta output-hihnalle vain nollasta eroavat luvut. Ohjeen vieressä on ohjeen toimintaa kuvaava selitys.

Alku: INPUT JUMPIFZERO(Alku) OUTPUT JUMP(Alku)	<i>Määritellään kohta "Alku". Otetaan luku input-hihnalta. Jos luku on 0, hypätään kohtaan "Alku". Siirretään luku output-hihnalle. Siirrytään kohtaan "Alku".</i>
--	--

Jos input-hihnalla olisivat esimerkiksi luvut

1, 0, 7, 9, 0, 4

olisi output-hihna ohjeen suorittamisen jälkeen:

1, 7, 9, 4

Esimerkki 2. Tehdään ohje, joka ottaa input-hihnalta ensimmäiset kaksi lukua ja siirtää ne output-hihnalle käänteisessä järjestyksessä. Ohjeen komentoja toistetaan niin kauan kuin input-hihnalla on lukuja. Lukuja oletetaan olevan parillinen määrä. Ohjeen vieressä on ohjeen toimintaa kuvaava selitys.

Alku: INPUT COPYTO(0) INPUT OUTPUT COPYFROM(0) OUTPUT JUMP(Alku)	<i>Määritellään kohta "Alku". Otetaan luku input-hihnalta. Kopioidaan luku muistipaikkaan 0. Otetaan luku input-hihnalta. Siirretään luku output-hihnalle. Kopioidaan muistipaikan 0 sisältö. Siirretään luku output-hihnalle Siirrytään kohtaan "Alku".</i>
---	--

Jos input-hihnalla olisivat esimerkiksi luvut

1, 0, 7, 9, 0, 4

olisi output-hihna ohjeen suorittamisen jälkeen:

0, 1, 9, 7, 4, 0

Huomautuksia

- Jos INPUT-komentoa suoritettaessa robotin kädessä on jo jokin luku, niin kyseinen luku häviää.
- OUTPUT-komennon antamisen jälkeen robotin kädessä ei ole mitään lukua.
- Output-hihna on aina tyhjä ennen ohjeen suorittamista. Vastaavasti muistipaikat ovat tyhjiä, ellei kysymyksessä muuta ole sanottu.
- Kysymyksissä 2.3–2.10 edellytetään, että ohjeen suorittamisen jälkeen input-hihnalle ei jää lukuja.

Kysymykset

Kysymys 2.1. Input-hihnalla ovat seuraavat luvut:

1, 2, 3, 4, 5, 6

Miltä output-hihna näyttää, kun luvut käsitellään alla olevalla ohjeella? (1 p.)

```
Alku :  
INPUT  
INPUT  
OUTPUT  
JUMP (Alku)
```

Kysymys 2.2. Input-hihnalla ovat seuraavat luvut:

8, 3, 5, 0, 0, 6

Muistipaikassa 0 on valmiina luku 1. Miltä output-hihna näyttää, kun luvut käsitellään alla olevalla ohjeella? (1 p.)

```
Alku :  
INPUT  
ADD (0)  
OUTPUT  
INPUT  
SUB (0)  
JUMPIFNEG (VainNeg)  
JUMP (Alku)  
  
VainNeg :  
OUTPUT  
JUMP (Alku)
```

Tietojenkäsittelytieteen valintakoe 28.5.2018

Kysymys 2.3. Tee ohje, joka siirtää ensimmäisen luvun output-hihnalle ja hylkää kaksi seuraavaa. Toista niin kauan kuin input-hihnalla on lukuja. Oletetaan, että käsiteltäviä lukuja on kolmella jaollinen määrä. (2 p.)

Kysymys 2.4. Tee ohje, joka siirtää output-hihnalle pelkät nollat ja hylkää muut luvut. Toista niin kauan kuin input-hihnalla on lukuja. (2 p.)

Kysymys 2.5. Tee ohje, joka ottaa ensimmäiset kaksi lukua input-hihnalta, laskee ne yhteen ja siirtää tuloksen output-hihnalle. Toista niin kauan kuin input-hihnalla on lukuja. Oletetaan, että käsiteltäviä lukuja on parillinen määrä. (2 p.)

Kysymys 2.6. Tee ohje, joka täyttää seuraavat ehdot. Ota kaksi lukua input-hihnalta, vähennä toisesta luvusta ensimmäinen ja siirrä tulos output-hihnalle. Sitteen vähennä ensimmäisestä luvusta toinen ja siirrä tämäkin tulos output-hihnalle. Toista niin kauan kuin input-hihnalla on lukuja. Oletetaan, että käsiteltäviä lukuja on parillinen määrä. (2 p.)

Kysymys 2.7. Tee ohje, joka ottaa kaksi lukua input-hihnalta. Mikäli luvut ovat samat, siirrä yksi näistä output-hihnalle. Hylkää kaikki sellaiset luvut, joiden arvot ovat keskenään erisuuria. Toista niin kauan kuin input-hihnalla on lukuja. Oletetaan, että käsiteltäviä lukuja on parillinen määrä. (3 p.)

Kysymys 2.8. Tee ohje, joka siirtää jokaisen input-hihnan luvun output-hihnalle muuntaen kunkin negatiivisen luvun vastaluvukseen (positiiviseksi). (3 p.)

Kysymys 2.9. Oletetaan, että input-hihnalle tulee pelkästään positiivisia lukuja ja viimeisenä lukuna 0. Lisäksi oletetaan, että input-hihnalle tulee vähintään yksi positiivinen luku ja 0. Tee ohje, joka siirtää output-hihnalle pienimmän luvun nollaa edeltävistä luvuista. Output-hihnalle ei saa sijoittaa muuta. (4 p.)

Kysymys 2.10. Tee ohje, joka kertoo kaksi ei-negatiivista lukua keskenään ja siirtää kertolaskun lopputuloksen output-hihnalle. Voit tässä olettaa, että input-hihnalle tulee täsmälleen kaksi lukua. Lisäksi muistipaikassa 0 on valmiiksi luku 0 ja muistipaikassa 1 on valmiiksi luku 1. (5 p.)

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 ($A = \text{Ö}$, $B = \text{Ä}$, 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.)

Tietojenkäsittelytieteen valintakoe 28.5.2018

- (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.)