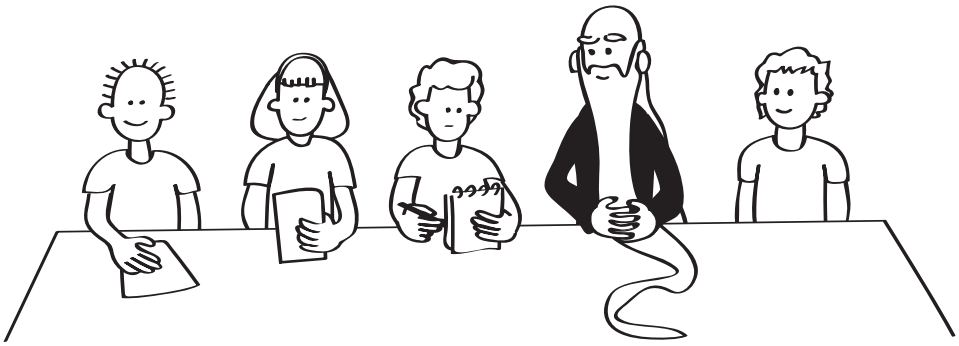
Aktivnost 16

Deljena skrivnost

Lahko skupina otrok odkrije, koliko denarja imajo vsi skupaj, če nihče noče povedati nikomur, koliko ga ima? To je posel za kriptografe, mojstre šifriranja.

Povzetek

Na internetu moramo pogosto izdati kak podatek, vendar tako, da ga nihče ne izve – niti ta, ki smo mu ga povedali. Zveni čudno in nemogoče? Recimo, da delamo anketo: imamo nekaj gospa in radi bi vedeli njihovo poprečno starost. Nevljudno bi bilo, da bi jih vprašali po njej in tudi med seboj si je nočejo zaupati. Kako naj tedaj dobimo poprečje, ne da bi poznali posamezne starosti?



Namen

Otroci spoznajo tipičen scenarij iz kriptografije: kako nekomu omogočiti, da uporabi nek naš skrivni podatek, ne da bi mu ga pri tem razkrili.

Potrebščine

Vsaka skupina otrok potrebuje

- kupček bankovcev (npr. iz monopolija ali natisnjene s pole)
- blokec papirja (ali nekaj listkov),
- pisalo.

Deljena skrivnost

V tej aktivnosti bodo otroci izračunali vsoto nekih "osebnih" podatkov, ne da bi drug drugemu izdali ta podatek.

1. Otroke razdeli v skupine. V vsaki skupini morajo biti vsaj trije, po možnosti pa več, recimo šest.

2. Vsakemu otroku daj nekaj "bankovcev". Količino denarja v igri prilagodi temu, kar so otroci sposobni bolj ali manj brez napak seštevati – glej nadaljevanje. Naroči, naj vsak zase skrivoma ugotovi, koliko denarja ima. Povej jim, da tega, koliko denarja imajo, ne smejo nikomur nikomur povedati.

3. Naroči vsaki skupini, naj ti pove, koliko denarja ima (torej vsi otroci skupaj). Ponovno jih opozori, da nihče ne sme nikomur izdati, koliko denarja ima. Pusti otrokom, naj malo razmišljajo in te poskusijo prepričati, da se to ne da.

4. Razloži jim, kako lahko izračunajo skupno vsoto denarja, ne da bi prekršili tvojo prepoved:
    a. Prvi otrok (v vsaki skupini) naj na listek skrivoma napiše naključno število, primerljivo s tem, koliko denarja imajo.
    b. K temu številu naj prišteje, koliko denarja ima. Vsoto skrivoma napiše na drug listek in ga da sosedu. Prvi listek skrije.
    c. Drugi otrok k temu skrivoma prišteje svojo količino denarja. Vsoto skrivoma napiše na nov listek in ga poda naslednjemu otroku.
    d. Tako naredijo eden za drugim vsi otroci v skupini.
    e. Na koncu dobi listek spet dobi prvi otrok. Ta od končne vsote odšteje naključno število: rezultat je pravilna vsota denarja.

    Za primer vzemimo, da so v skupini štirje otroci, ki imajo 85, 12, 34 in 50 evrov. Prvi na listek napiše naključno število, recimo 20. K temu prišteje 85; na nov listek napiše 105 in to poda drugemu otroku. Drugi vzame nov listek, napiše vsoto 105 in svojih dvanajstih evrov, torej 117 in ta listek da tretjemu. Tretji napiše 151 in poda listek četrtemu. Četrti na nov listek napiše 201 in ga poda prvemu. Prvi odšteje 20 in poroča, da imajo skupaj 181 evrov – kar je tudi res.

5. Na koncu dovoli otrokom, da preverijo rezultat: vsak naj pokaže svoj denar, skupaj naj ga preštejejo in ugotovijo, ali je postopek dal pravilen rezultat.

6. Če je potrebno, se pogovori tudi o tem, kako in zakaj postopek deluje – kako da so na koncu dobili pravilen rezultat.

7. Pogovori se, ali je kdo za kogarkoli izvedel, koliko denarja ima.

8. Je mogoče postopek izigrati? Se lahko dva od njih dogovorita, da bosta družno odkrila, koliko denarja ima kateri od sošolcev? Tega se verjetno ne bodo sami domislili, zato namigni: se lahko prvi in tretji dogovorita, da bosta odkrila, koliko denarja ima drugi? (Da, očitno: od števila, ki ga je drugi dal tretjemu, odšteta, kar je dal prvi drugemu.)

9. Lahko prvi in četrti odkrijeta, koliko denarja ima drugi? Če ne, kaj pa lahko odkrijeta? (Koliko denarja imata drugi in tretji skupaj.)

Pogovor - razlaga

Kriptografija je veda o varnem komuniciranju. Včasih se je ukvarjala s tem, kako pošiljati šifrirana sporočila (to se bomo učili v eni od prihodnjih aktivnosti). Danes se ukvarja tudi s tem, kako poskrbeti za varnost na internetu – kako shranjevati gesla, da jih nepridipravi ne morejo izvedeti, kako preverjati, da sporočil, ki jih pošiljamo po internetu, kdo ne prestreže in spremeni ter podobno.

V kriptografiji moramo velikokrat reševati probleme, ki so navidez nemogoči. Pogosto se zgodi, da moramo sporočiti nekomu podatke, ki jih ne želimo razkriti. Kriptografi si zato izmišljajo zvite postopke, kot je ta, ki smo ga spoznali v tej aktivnosti. Kot smo videli, lahko tu skupina "uporabi" naš podatek, obenem pa ga ne izve.