Mali kriptografi

NASTAVLJAMO SA ŠIFRIRANJEM PORUKA

Vaši zadaci

Dragi učenici 4. razreda, vaši zadaci su sljedeći:

1. Pročitajte tekst koji se nalazi na sljedećim stranicama ovog dokumenta.

2. Riješite zadatke koji se nalaze na zadnjoj stranici ovog dokumenta.

Rješenja pošaljite u obliku privatnih poruka na Yammeru.

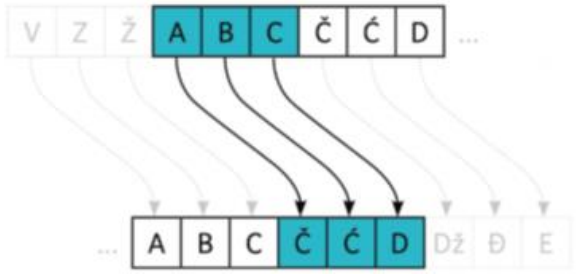
Rješenja možete poslati do sljedećeg utorka.

Cezarova šifra

Julije Cezar bio je jedan od najpoznatijih rimskih careva i vojskovođa.

Često je svojim vojnicima trebao slati poruke. Kako bi bio siguran da neprijatelji ne bi pročitali sadržaj tih poruka, koristio je šifriranje koje je poznato pod nazivom **Cezarova šifra**.

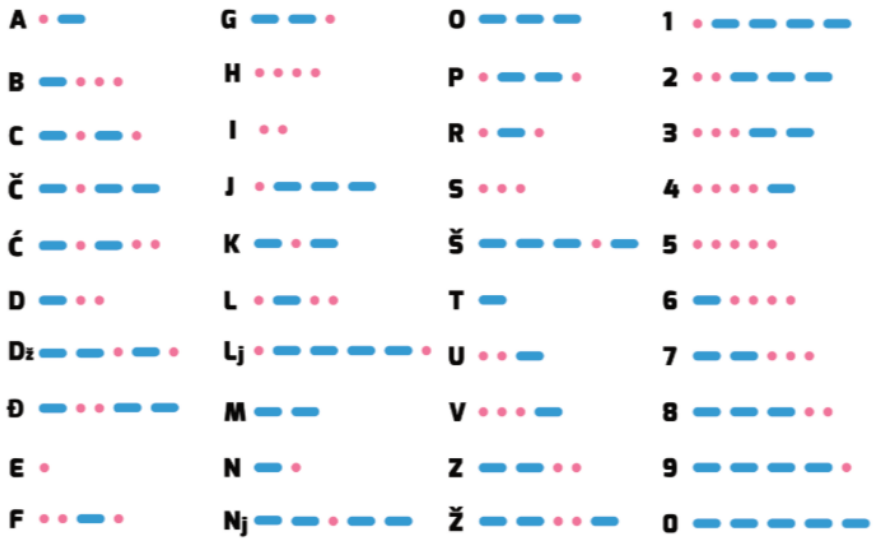
Kod ovog šifriranja, svako slovo iz izvorne abecede se zamijeni nekim drugim slovom iz abecede. Broj koji se zove **pomak** određuje s kojim se slovom treba zamijeniti svako slovo iz izvorne abecede. Primjerice, ako je pomak 3, onda će se slovo A zamijeniti sa slovom Č jer je slovo Č za tri mjesta udaljeno od slova A. Slovo B će se zamijeniti sa slovom Ć jer je slovo Ć za tri mjesta udaljeno od slova B. Slovo C će se zamijeniti sa slovom D itd. Dakle kao da abeceda počinje slovom Č. Pritom će se slovo Ž zamijeniti sa slovom C jer je sada C na kraju abecede. Promotrite sljedeću sliku:



Morseova abeceda

Samuel Morse bio je poznati američki izumitelj koji je osmislio jedan od najpoznatijih načina šifriranja. Po njemu se taj način šifriranja zove **Morseova abeceda**, a razvijen je u 19. stoljeću. Pomoću Morseove abecede šifrirale su se poruke koje su se slale preko električnih telegrafa. Ovaj sustav šifriranja su najviše koristili vojnici, pomorci i izviđači.

Svako slovo u Morseovoj abecedi predstavljeno je nizom točkica ili crtica:



Još malo o Morseovoj abecedi

Morseova abeceda se može koristiti i u komunikaciji svjetlosnim signalima. Takvu komunikaciju su često koristili pomorci jer je bila učinkovita, brza i jeftina (nisu bile potrebne žice za prijenos podataka ni uređaji koji bi ih slali i primali). Svaki brod je obično imao jedan svjetlosni reflektor. Kada bi se s tog reflektora uputio kratak svjetlosni signal, to bi predstavljalo točku iz Morseove abecede. Kada bi se pak uputio dugi svjetlosni signal, to bi predstavljalo crtu iz Morseove abecede.

Morseova abeceda se koristi i danas. Primjerice, Google je u svojim tipkovnicama ugradio Morseovu abecedu i na taj način osigurao osobama s invaliditetom sporazumijevanje putem pametnih telefona.

Zadaci

1. Koristeći Cezarovu šifru s pomakom od **3** slova, šifrirajte svoje ime. Slovo A se zamjenjuje slovom Č, slovo B se zamjenjuje slovom Ć i tako redom. Slovo V se zamjenjuje slovom A, slovo Z se zamjenjuje slovom B i slovo Ž se zamjenjuje slovom C.

2. Koristeći Morseovu abecedu, napišite svoje ime u obliku niza točkica i crtica.