**MATEMATIČKA LEKTIRA  
PRIČA O ŠIFRAMA**

Šifriranje je postupak kojim skrivamo naše poruke tako da ih ne može bilo tko pročitati. Dvije osobe koje žele komunicirati dogovore postupak skrivanja i otkrivanja poruka. Važno je da dogovoreni postupak ostane tajan. U nastavku ove priče opisat ćemo neke značajne događaje u povijesti koji su povezani sa šifriranjem.

Otkada je civilizacije, ljudi imaju tajne te postoji potreba za skrivanje tajni. Jednu od prvih naprava za šifriranje koristili su Spartanci. Ta se naprava zvala skital. Skital je štap oko kojeg je namotana vrpca od pergamenta na koju se zapisivala poruka duž štapa. Nakon što se vrpca odmotala, sadržaj poruke je bio skriven za svakoga tko nije imao isti štap.

Veliki rimski vojskovođa Gaj Julije Cezar koristio je šifre kako bi skrivao poruke od svojih neprijatelja. Cezar je poruke skrivao tako da je svako slovo u poruci zamijenio slovom koje je tri mjesta nakon njega u abecedi (A je zamijenio sa D, B sa E, itd.). U to je vrijeme jako malo ljudi znalo čitati i pisati pa je Cezar ovim jednostavnim šiframa uspješno čuvao svoje tajne.

Skoro 2000 godina nakon Cezara ljudi su uspješno skrivali tajne različitim šiframa, na sličan način kako je to i Cezar radio. Kroz vrijeme postupci šifriranja postajali su sve složeniji.

Prije oko 200 godina engleski matematičar Charles Babbage izradio je mehanički stroj na temelju kojega su se razvila današnja računala. Prvo pravo računalo osmislila je i izradila grupa matematičara i inženjera predvođena velikim matematičarom Alanom Turingom. Oni su izradili računalo kako bi mogli s njim čitati tajne koje su skrivane poznatom napravom za šifriranje koja se zove Enigma. Opis prvog pravog računala objavljen je 1946. godine. Prvo osobno računalo nastalo je 17 godina nakon toga.

Nakon pojave prvih računala ljudi su morali smisliti nove načine skrivanja tajni koje se ne mogu otkriti uz pomoć računala. Matematičari su osmislili mnoge načine šifriranja koji danas uspješno čuvaju naše tajne.

PITANJA:

1. Kako se zove naprava za šifriranje koju su koristili Spartanci?
2. Opiši kako je Cezar skrivao poruke?
3. Pokušaj sakriti sljedeću poruku na isti način kako je to Cezar radio: ANA.

PITANJA (NAKON OBRADE LENTE VREMENA):

1. U kojem stoljeću je Charles Babbage osmislio svoj stroj?
2. U kojem stoljeću je Alan Turing napravio prvo pravo računalo?
3. Prije koliko godina je nastalo prvo osobno računalo?