

DIGITALNA TVRĐAVA

Tanja Kralj, Mali Zdenci

Slika 1. Dan Brown
(karikatura)

Dan Brown (Exeter, New Hampshire, 22. lipnja 1964.) američki je pisac triler-romana, poznat po bestselleru *Da Vincijev kod* za koji ste svi, vjerujem, čuli. Vrijeme svog školovanja proveo je u kampusu gdje je razvio zanimanje za odnos znanosti (i otac mu je bio matematičar) i religije, koji su glavna tema svih njegovih romana i koji svakodnevno potiču rasprave diljem svijeta. Neki od romana koje je napisao su: *Anđeli i demoni*, *Izgubljeni simbol* i *Inferno*, a *Digitalna tvrđava* njegov je prvi roman.

Sigurno se pitate kakve veze navedene knjige imaju s matematikom. *Digitalna tvrđava* je roman kojemu je glavna tema kriptografija. Kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih može pročitati samo onaj kome su namijenjene. Sama riječ *kriptografija* je grčkog podrijetla i mogla bi se doslovno prevesti kao *tajnopis*.

LKGXD<7 JG G<VDS8<



Prvi poznati šifrant u povijesti bio je Julije Cezar čiji se trikovi šifriranja pojavljuju i u knjizi. Kada su mu počeli presretati tajne poruke koje je slao svojim vojnicima, razvio je primitivan način šifriranja svojih naredbi. Preslagivao je tekst poruka na način da je djelovao posve besmisleno. No to nije bilo tako. Svaka poruka imala je točno određen broj slova koji je činio savršeni kvadrat – šesnaest, dvadesetpet, stotinu – ovisno o tome koliko je Cezar imao za reći. Svoje časnike potajice je uputio da primljene poruke moraju prepisati u obliku kvadrata (pišući vodoravno, red po red). Kada bi tako učinili i čitali tekst odozgo nadolje (stupac po stupac), pojavila bi se poruka.

Zadatak 1. Radnja romana *Digitalna tvrđava* odvija se na nekoliko mjesta. Jedno od njih je i: AAOITAGGZNGOKREAAUDRANNLRJIFCANNE-PIICUOLTJJISSZOU. Poslužite se Cezarovim trikom i otkrijte naziv mjesta koje se skriva iza ove zbrke slova.

Susan Fletcher, glavna junakinja ovoga romana, mlada je primijenjena matematičarka i strastvena kriptografkinja. Njezin partner, David Becker, sveučilišni je profesor koji predaje jezike, a iz znatiželje se bavi i simbologijom.

Zadatak 2. Susan je od Davida starija dvije godine. Ako broju Susaninih godina dodamo Davidove, dobit ćemo broj 72. Koliko godina ima Susan, a koliko David?



Susan je većinu svog života provela u Odjelu za kriptografiju (zvanom *Kriptografski*). Kao i većina zaposlenih, davala je sve od sebe kako bi uspjela u poslu i bila odana svojoj zemlji i njenoj sigurnosti. Glavni cilj Kriptografskog bio je borba protiv terorizma, tajnih akcija, presretanje tajnih poruka i slično. Računalo *Translatr* stvoreno je kako bi pomoglo u tome. Bio je to snažan stroj američke tajne službe za dešifriranje tajnih poruka, ujedno najveća tajna Kriptografskog. Susanin nadređeni, Strathmore, najviše je bio ponosan na izum koji je nastao pod njegovim vodstvom. Bio je jedan od onih koji se najviše zalagao da sve ostane u tajnosti, a onaj tko bi mu se suprotstavio, nije dobro prošao.

Translatr je svakodnevno savršeno obavljao svoj posao, sve do jednog dana kada je bivši zaposlenik, protivnik stvaranja Translatra, ostvario svoju prijetnju o pisanju neprobojnog algoritma koji će zaustaviti presretanje svih poruka u svijetu. Ensei Tankado bio je invalid, Japanac kojemu je majka umrla na porođaju. Razboljela se od radijacije u ratu. Ensei se zakleo da će se osvetiti zemlji koja je kriva za dva velika bombaška napada na njegovu zemlju. Usprkos svojim fizičkim nedostacima, bio je izvrstan informatičar. Od Agencije je tražio da svijetu obznani postojanje *Translatra*, inače će ga zauvijek onesposobiti.

Ensei, ljutit jer nisu vjerovali njegovim prijetnjama i odlučnosti, napisao je svoj savršeni algoritam koji je trebao uništiti *Translatr*. Taj algoritam nazvao je *Digitalna tvrđava*, a trebao je uništiti Kriptografski odjel. Stvaranjem *Digitalne tvrđave* počinju problemi za sve. Posebno za *Translatr* koji je sve kodove svakodnevno „probijao” za nekoliko minuta. Enseiov algoritam ga je „blokirao” jer ga nikako nije mogao dešifrirati.

Strathmore se bojavao trenutka u kojemu će svijet saznati za postojanje *Translatra*. Pratio je Enseiov rad i znao što će ovaj u svakom trenu učiniti. Barem je mislio da zna. Namjeravao je iskoristiti tajne koje je doznao i proslaviti se pred mirovinu, no prevario se. Neke su stvari pošle po zlu. Kada je shvatio da je prekasno, pozvao je Susan u pomoć. Susan nije mogla ni zamisliti da je Strathmore taj koji joj je uništio odmor u planinama koji je namjeravala provesti s Davidom, a još manje da je Davida poslao na „tajni zadatak”.

David se, otputovavši u Seville, našao u vrtlogu čudnih događanja koja nije mogao ni zamisliti. To što je bio osoba „izvana”, Strathmoreu je najviše odgovaralo. Potraga za Enseiom i njegovim prstenom (na kojemu je, svi su vjerovali, bila napisana lozinka za zaustavljanje *Digitalne tvrđave*) pretvorio se u igru života i smrti. Strathmore nije bio posve iskren. Njegove su namjere sve iznenadile. David je od lovca postao meta. U želji da pomogne drugima, jer je znao da bi to puno značilo i za Susan, gotovo je izgubio život. Strathmore ga je unajmio kako bi pronašao lozinku, ali ga se želio i riješiti. Želio je svoju najbolju kriptografkinju, Susan, samo za sebe. David se našao u zamršenom labirintu ubojstava i praćenja, minute su ga dijelile od smrti, ali na kraju je



uspio pronaći prsten koji je sadržavao šifru. Problem je bio što je onaj koji ga je poslao u tu tajanstvenu potragu umro. I Ensei je u međuvremenu izgubio bitku za život. Dvojice suparnika više nije bilo, a *Translatru*, kao i glavnoj banci Kriptografskog, bližila se katastrofa.

Ensei je bio opsjednut svime što je vezano za rat, a s matematičke je strane bio opsjednut prostim brojevima. Sve je pomno proučio. Znao je sve o bombama kojima su napadnuti Hiroshima i Nagasaki. Iako je većina ljudi mislila da su te dvije atomske bombe bile različite, sastojale su se od sličnog punjenja, urana 238 i urana 235. Svoje znanje uključio je i u izradu šifre za *Digitalnu tvrđavu*. Šifra je glasila: *Primarna diferencija između elemenata odgovornih za Hiroshimu i Nagasaki*.

Zadatak 3. Odredite broj koji „otključava” Digitalnu tvrđavu.

Radnja opisana na posljednjih pedesetak stranica knjige odvija se u 15 minuta. Pokušaj spašavanja NASA-inih podataka otkrivanjem šifre uspješno je odrađen. David se sretno vratio kući, nacionalna sigurnost je spašena, a Susan je još jednom dokazala svoje veliko znanje iz kriptografije. Zanimaju vas detalji? Nećemo vam sve otkriti.

Knjigu u ruke i krenite s čitanjem, uvjereni sam da će vam se svidjeti ☺!

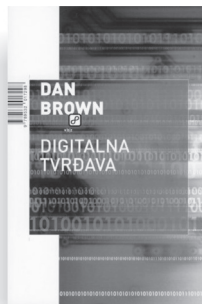
Zadatak 4. Za čitanje knjige bila su mi potrebna četiri dana. Prvi sam dan pročitala trećinu ukupnog broja stranica. Drugi dan dvostruko manje nego prvog dana, a trećeg dana trećinu broja stranica koje sam pročitala u prva dva dana skupa. Za četvrti su mi dan ostale 122 stranice. Koliko stranica ima knjiga? Koliko sam pročitala svaki dan? Koliko je dana potrebno za čitanje knjige ako se svaki dan pročita 61 stranica?

Na nastavi matematike ili informatike upoznali ste se s različitim brojevnim sustavima kao što dekadski, binarni ili heksadekadski. Prikaz brojeva u raznim brojevnim sustavima također je jedna vrsta „kodiranja” podataka (brojeva). Brojevi koje „koristimo” u svakodnevnom životu zapisani su u dekadskom brojevnom sustavu. S druge strane, binarni sustav predstavlja pozicijski brojevni sustav s bazom 2, što znači da u tom brojevnom sustavu za označavanje brojeva koristimo 2 znamenke, i to 0 i 1.

Kako broj koji je zapisan u binarnom brojevnom sustavu prikazati u dekadskom? Pokažimo na primjeru:

$$1010_2 = 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = 1 \cdot 8 + 0 \cdot 4 + 1 \cdot 2 + 0 \cdot 1 = 10_{10}.$$

Još jedan manje poznati brojevni sustav je onaj faktorijelni. Poznat je i pod nazivom faktorijelne baze. No, faktorijeli u ovom brojevnom sustavu nemaju ulogu baze, kao na broj 2 u binarnom brojevnom sustavu. Faktorijeli u faktorijelnom brojevnom sustavu označavaju mjesnu vrijednost znamenke. Na



Slika 2. Naslovnica romana



primjeru ćemo pokazati kako broj koji je zapisan u faktorijelnom brojevnom sustavu prikazati u dekadskom:

$$341010_1 = 3 \cdot 5! + 4 \cdot 4! + 1 \cdot 3! + 0 \cdot 2! + 1 \cdot 1! + 0 \cdot 0! = 463_{10}.$$

Zadatak 5. *Digitalnu tvrđavu*, svoj prvi roman, Dan Brown objavio je 2431000₁ godine. Prije koliko je godina roman objavljen?

Literatura:

1. Binarni brojevni sustav; <http://www.ic.ims.hr/brojevni-sustavi/bs5.html> (19.10.2013)
2. Dan Brown (biography); <http://www.danbrown.com/#author-section> (19.10.2013)
3. Dan Brown, *Digitalna tvrđava*, V.B.Z. d.o.o., 2007.
4. Factorial number system;
http://en.wikipedia.org/wiki/Factorial_number_system (20.10.2013)
5. Klasična kriptografija – osnovni pojmovi;
<http://web.math.pmf.unizg.hr/~duje/kript/osnovni.html> (19.10.2013)

