

SKRIVANJE SADRŽAJA PORUKE MOŽE BITI STVAR ZABAVE ILI NUŽNE POTREBE.

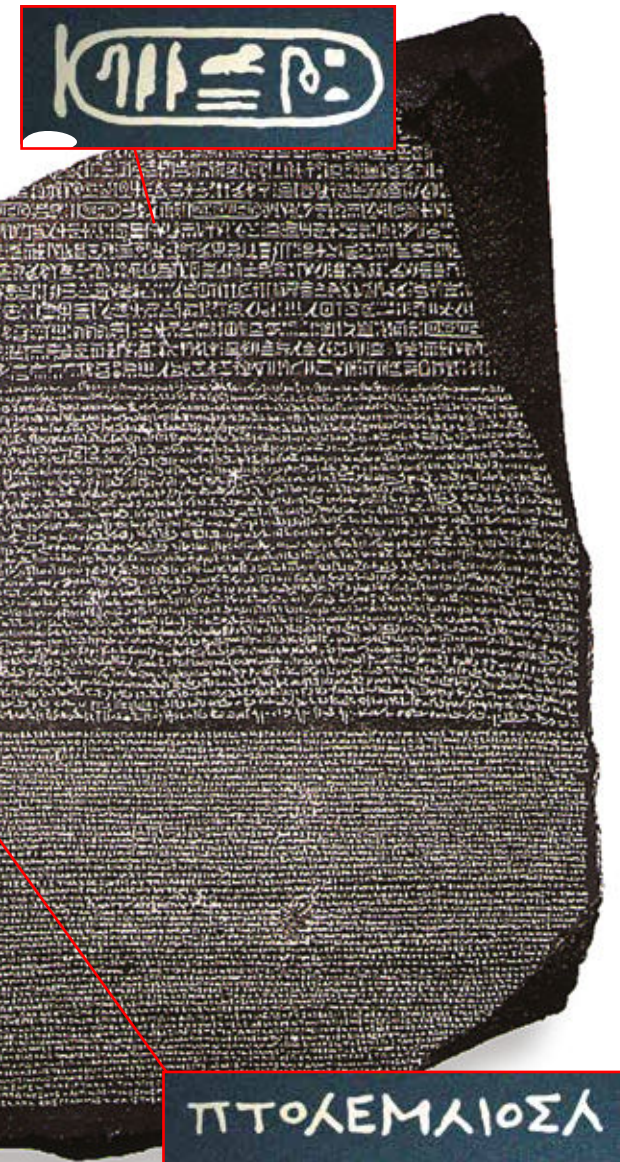
U PRVOM SLUČAJU SE MOŽDA RADI O BEZAZLENOM ZADIRKIVANJU PRIJATELJA;

U DRUGOM SE SLUČAJU PAK, MOŽE RADITI O NEPRIJATELJU KOJEG ŽELIMO IZBEĆI.

• *Kodovi i šifre*

Šifrovanje i dešifrovanje poruka

► Kamen iz Rozete, koji je slučajno otkrio vojnik Napoleonove vojske 1799. godine, postao je ključ za dešifrovanje egipatskih hijeroglifa. Ispostavilo se da je na ploči isti tekst zapisan na tri pisma: hijeroglifskom, demotskom i grčkom.



▲ Tek je 1822. godine francuzu Žanu Šampolionu pošlo za rukom da dešifruje hijeroglifsko pismo. Na slici iznad istaknuto je nekoliko hijeroglifskih znakova unutar

kartuša. Šampolion je verovao da ti znakovi predstavljaju faraonovo ime. U grčkom tekstu pojavilo se ime kralja Ptolemeja i Šampolion je postavio hipo-

tezu da se radi o imenu prikazanom gore. Bio je to prvi korak ka dešifrovanju koji je zahtevao ogroman trud, ali je na kraju i otkrio tajnu kamena.

ŠSH – iako je ova „reč” napisana na srpskom, njeno značenje ne razumemo. Ne znamo je jer njen cilj je upravo takav da je ne razume niko osim primaoca poruke. Radi se, dakle, o šifrovanj ili kodiranoj reči. Ova

dva termina u svakodnevnom govoru znače isto, tačnije, izražavaju istu nameru, a to je da na neki način sakriju informacije sadržane u nekoj poruci. Da bi primalac mogao odgonetnuti značenje reči, mora poznavati mehanizam zvani *šifra*, pomoću kojega je izvorna reč bila šifrovana. U ovom slučaju, svako slovo abecede zamenjeno je šifrovanim slovom koje se nalazi tri mesta iza njega. Shodno tome, za dešifrovanje je potrebno svako šifrovano slovo zameniti sa trećim slovom abecede koje sledi. Na taj način dobićemo reč VUK i dešifrovaćemo poruku. .

Ovaj jednostavan sistem šifrovanja korišćen je još u rimsko doba, a poznat je kao *Cezarova šifra*. Kriptografija, nauka ili umeće koje se bavi sakrivanjem informacija u određenoj poruci, stara je isto koliko i samo pismo. U izvesnom smislu, već su stari Egipćani koristili kriptografske metode u svom pismu. To dokazuje činjenica da je običan narod koristio narodno, to jest demotsko pismo, dok je sveštenstvo pisalo hijeratskim (hijeroglifskim) pismom koje je za nezamonašene bilo nerazumljivo.

•Dobra šifra

Sistem šifrovanja funkcioniše samo ako pošiljalac i primalac znaju sledeće:

1. *Algoritam*. To je računaska metoda koja se primenjuje pri šifrovanju ili dešifrovanju poruke.
2. *Ključ*. Radi se o tajnoj informaciji koju algoritam koristi za šifrovanje i dešifrovanje poruke.
3. *Rok važenja*. Predstavlja period u kojem je ključ važeći.

Pretpostavimo da su stanovi u nekoj zgradi dati na korišćenje rukovodiocima jedne kompanije. Stanovi su zaštićeni bezbednosnim sistemom koji za otvaranje vrata zahteva unošenje numeričkog koda. U ovom slučaju, *algoritam* je niz komandi koji odlučuje da li će se vrata otvoriti ili neće. Ispravnii kod predstavlja tajnu šifru. *Rok važenja* označava period u kojem menadžer koristi stan. Po isteku tog perioda, potrebno je šifru promeniti da bi stan mogao koristiti sledeći korisnik. .



◀ Problem udvajanja kocke poznat je i kao problem delfskog proročišta. Legenda kaže da se bog Apolon već ko zna koji put razgnevio na ceo svet. Proročište u Delfima odlučilo je savetovati Atinjanima da bogu podignu novi oltar koji će biti dva puta veći od prethodnog. U to vreme, matematika je znala da služi i za smirivanje gnevni bogova. Međutim, kada su se matematičari prihvatili zadatka, shvatili su da oltar ima oblik kocke. Našli su se pred problemom koji nisu uspeali da reše.

tematičar Ferdinand fon Lindeman dokazao da je nemoguće konstruisati kvadrat koji ima istu površinu kao zadati krug, a da se pri tome koristi isključivo lenjir i šestar. Moralo je proći više od 23 veka iscrpljujućih pokušaja, jer je u matematici često teže dokazati da problem nema rešenje, nego pronaći rešenje onog problema, koji ga ima. Gore pomenuti problem je najpoznatiji od tri klasična problema konstruisanja pomoću lenjira i šestara. Druga dva su „trisekcija ugla” i „udvajanje kocke”, oba veoma slična prvom problemu. Trisekcija ugla podrazumeva podelu ugla na tri jednaka dela, a udvajanje kocke odnosi se na konstrukciju kocke čija je zapremina dvostruko veća od zapremine zadate kocke. Naravno, sve to samo pomoću lenjira i šestara.

•Za kraj

Trebalo je da prođe mnogo vremena, dok se nije pronašlo zadovoljavajuće rešenje ovog tipa problema. Delimično je to bilo i zato što problemi nisu mogli biti formulisani isključivo geometrijskim pojmovima, nego je bilo potrebno zaroniti i u oblasti koje su mnogo kasnije nazvane teorija grupa. Osnove ove discipline postavio je francuski matematičar Evarist Galoa sredinom 19. veka. Zaključak te teorije glasi da isključivo pomoću lenjira i šestara nije moguće rešiti kvadraturu kruga, trisekciju ugla niti udvajanje kocke.

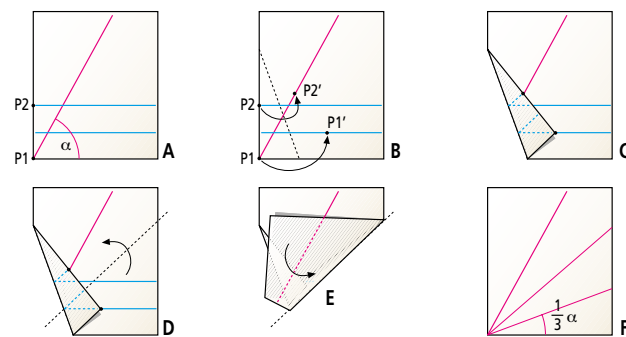
ZANIMLJIVOSTI

■ I dalje postoje oni koji veruju da su rešili problem kvadrature kruga (kao i poznati problem perpetuum mobile). Procenjuje se da se u svakoj akademskog godini na svim fakultetima širom sveta pojavi 50 do 100 „rešenja” ovog tipa.

■ Napoleon je bio strastveni ljubitelj matematike, pa je vreme između vojnih pohoda provodio rešavajući matematičke probleme. Da nije imao samo strast, već i istinski talenat, svedoči činjenica da nije samo umeo da rešava probleme, već je neke i sam osmislio. Jedan od njih, poznat kao „Napoleonova teorema” glasi ovako: „Da li je moguće odrediti centar kruga služeći se isključivo šestarom?” Taj problem je, zanimljivo, rešiv.

■ Pitagorejske škole pripisivale su metafizičko značenje kvadraturi kruga, a kasnije su ga preuzeli evropski okultni pravci. Oni su matematičko značenje nerešivosti problema prenosili na okultnu simboliku: tražili su način da tačno predvide mesto i vreme smrti čoveka. To je, naravno, nemoguće.

Trisekcija i origami



Presavijanje papira, to jest umetnost poznatija kao origami, krije duboke tajne geometrije, a može da izvede i trisekciju ugla. Uzmimo list papira po želji, obeležimo ugao α , pa nacrtajmo dve jednake paralelne linije na donjem delu papira (slika A). Sada presavijemo donji ugao P1 na prvu paralelnu liniju tako da kraj drugog vrha P2 dodiruje stranu ugla (slike B i C). Pravimo novi pregib na prvoj paralelnoj liniji koji će se rasprostirati od gornjeg vrha lista papira do temena ugla (slika D). Taj ugao ćemo podeliti na dva dela (slika E) i time dobiti, nakon rasklapanja papira, početni ugao podeljen na tri jednaka dela (slika F).