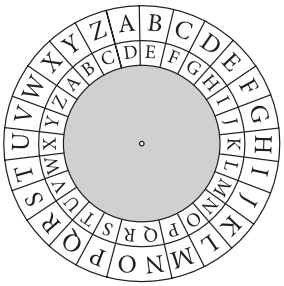
KAKO ŠIFRIRATI PORUKU?

Jelena Hunjadi, Donja Dubrava

Kako možemo prijateljima slati poruke tako da ih nitko drugi osim njih ne može pročitati? Odgovor sigurno znate: tako da poruke šifriramo. Poruku moramo prije slanja na neki način izmijeniti, ali tako da samo prijatelj kojemu šaljemo poruku zna na koji će je način pročitati. Da bi to bilo moguće, moramo se s njim dogovoriti kako ćemo je šifrirati. Ali kako ćemo se dogovoriti za šifru? Ako nas netko drugi prisluškuje, saznat će na koji smo način šifrirali poruku i lako će je dešifrirati, zar ne? Ne nužno. U nastavku ćemo naučiti kako možemo slati poruke tako da možemo biti sigurni da ih neće razumjeti nitko drugi osim onoga kome su namijenjene.

Još prije 3000 godina ljudi su imali potrebu za sigurnim prenošenjem poruka. Obično su to bile vrlo važne poruke iz svijeta politike ili strategije ratovanja. Egipćani i Indijci prvi su pokušali zaštititi poruke koje su prenosili. Koristili su drvene štapove na koje bi namotali vrpcu po kojoj se pisalo. Nakon upisivanja poruke, vrpca bi se odmotala, a na njoj bi ostali izmiješani znakovi koje je mogao pročitati samo onaj tko je imao štap jednake debljine.

Znameniti rimski vojskovođa i državnik Gaj Julije Cezar u komunikaciji s prijateljima koristio je poseban način šifriranja koji danas po njemu nazivamo Cezarova šifra. On je slova otvorenog teksta zamjenjivao slovima koja se nalaze tri mjesta dalje od njih u abecedi (A→D, B→E, C→F itd.). Abeceda se ciklički nastavlja, tj. nakon posljednjeg slova ponovno dolazi prvo slovo (slika 1). U našim primjerima koristit ćemo englesku abecedu koja se sastoji od 26 slova. Ukoliko se u tekstu pojavljuju hrvatska slova, onda ćemo Č i Ć zamijeniti s C, a Đ, Dž, Lj, Nj, Š, Ž redom s DJ, DZ, LJ, NJ, S, Z. Tako poruka OVO JE TAJNA šifrirana Cezarovom šifrom glasi RYR MH WDMQD.

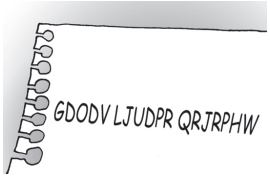


Slika 1. Cezarova šifra s pomakom za 3 mjesta unaprijed

***Zadatak* 1**. Maja želi poslati Nikolini poruku IDEMO NA SLADOLED šifriranu Cezarovom šifrom. Kako glasi poruka koju će Maja poslati?

Što ako dobijemo poruku šifriranu Cezarovom šifrom? Kako ćemo je dešifrirati? Vrlo jednostavno: obrnutim postupkom: zamijenit ćemo D sa A, E sa B, F sa C itd.

***Zadatak* 2**. Marko je od Danijela dobio poruku GDQDV LJUDPR QRJRPHW šifriranu Cezarovom šifrom. Što je Danijel htio poručiti Marku?



Poruke možemo šifrirati na ovaj način i tako da se pomaknemo za više od 3 slova u alfabetu, npr. za 5 slova. Tako ćemo A zamijeniti s F, B mijenjamo s G itd. (slika 2).

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E

Slika 2. Cezarova šifra s pomakom za 5 mjesta unaprijed

Ako želimo na ovaj način šifrirati poruku GEOMETRIJA, poslat ćemo poruku LJTRJYWNOF.

***Zadatak* 3**. Viktorija je Ivani poslala poruku BUROS SGZKSGZOQA, no poruku je pronašao Ivanin brat Mate. Mate zna da se Viktorija i Ivana dopisuju na način da svako slovo abecede pomaknu za 6 mjesta unaprijed i dešifrirao je Viktorijinu poruku. Koju poruku je Mate dobio dešifriranjem?

Ovakav način šifriranja vrlo je nesiguran. Ako smo dovoljno strpljivi i uporni, možemo pročitati svaku poruku šifriranu na ovaj način. Za neku poruku koju želimo dešifrirati prvo provjerimo je li možda šifrirana tako da je učinjen pomak za jedno slovo u abecedi. Ako ne dobijemo neku smislenu poruku, provjerimo je li napravljen pomak od dva mjesta, pa zatim tri itd.

***Zadatak* 4.** Pokušajte na ovaj način dešifrirati poruku Y PEDM WY OVEXOI RSKI.

Šaljemo li prijatelju poruku na ovaj način, moramo mu najprije javiti broj koji označava koliko smo se mjesta pomaknuli u abecedi. No, ako netko dozna taj broj, lako će pročitati našu poruku. Dakle, ovakvim šifriranjem nismo se osigurali od toga da netko drugi osim našeg prijatelja može pročitati što mu želimo poručiti.

Upoznajmo još jedan način šifriranja sličan Cezarovoj šifri. Problem Cezarove šifre je u tome što svako slovo u poruci pomičemo za jednak broj mjesta. Kada otkrijemo koji je taj broj, možemo pročitati cijelu poruku. Pokušajmo riješiti ovaj problem na način da svako slovo u našoj poruci pomaknemo za različit broj mjesta.

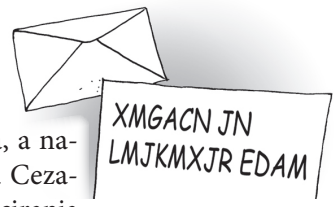
Kako ćemo odrediti koje ćemo slovo pomaknuti za koji broj mjesta? Kako što smo već rekli, koristimo englesku abecedu. Slova ćemo numerirati od 0 do 25, odnosno A je nulto slovo, B prvo slovo, C drugo slovo itd. Odabrat ćemo ključnu riječ, npr. LAV. Slovo L je 11. slovo abecede, A je 0. slovo abecede, V je 21. slovo abecede. Sada ćemo prvo slovo naše poruke pomaknuti za 11 mjesta dalje, drugo slovo za 0 mjesta dalje, treće za 21 mjesto dalje, četvrto opet za 11 mjesta, peto za 0 mjesta itd. Nakon posljednjeg slova ponovno dolazi prvo slovo.

Na primjer, uzmimo riječ ZEC kao ključnu riječ. Z je 25. slovo abecede, E je 4. slovo abecede i C je 2. slovo abecede. Ako želimo šifrirati poruku PAS FLOKI, pomaknut ćemo slovo P za 25 mjesta, slovo A za 4 mjesta, slovo S za 2 mjesta, slovo F ponovno za 25 mjesta, slovo L ponovno za 4 mjesta itd. Šifrirana poruka glasit će NEU DPQIG.

***Zadatak* 5.** Pomoću ključne riječi NADA šifrirajte poruku SUTRA IDEMO NA IZLET.

Kako bismo, koristeći ovakav postupak, pročitali šifriranu poruku ako znamo ključnu riječ? Vrlo jednostavno: obrnutim postupkom. Ako je ključna riječ ZEC, prvo slovo u poruci pomaknut ćemo za 25 mjesta unazad, drugo slovo 4 mjesta unazad, treće slovo 2 mjesta unazad, četvrto opet 25 mjesta unazad itd.

***Zadatak* 6.** Pokušajte na ovaj način, s ključnom riječi ZMAJ, dešifrirati poruku XMGACN JN LMJKMXJR EDAM.



Ovaj način šifriranja poruka izmišljen je prije petstotinjak godina, a nazivamo ga Vigenèreova šifra. Ovakvo šifriranje poruka sigurnije je od Cezarove šifre, no ipak nije u potpunosti sigurno. Pri ovom načinu komuniciranja također moramo javiti osobi kojoj šaljemo poruku koja je ključna riječ kojom smo šifrirali poruku. Ako nas netko prisluškuje, doznat će ključnu riječ i zatim šifriranu poruku, i vrlo će lako pročitati našu poruku.[1] Na koji bismo način s nekim mogli komunicirati preko šifriranih poruka, bez da smo se prethodno dogovorili kako ćemo šifrirati poruke?

Godine 1976. pronađeno je rješenje ovog problema. Ideja je da pošiljatelj poruke ima svoj javni i tajni ključ. Javni i tajni ključ međusobno moraju biti takvi da se poruka, kada je netko šifrira javnim ključem, može pročitati pomoću tajnog ključa. Javni ključ ne skrivamo nego ga objavimo svima koji nam žele poslati poruku. Pomoću javnog ključa pošiljatelj će šifrirati poruku koju nam želi poslati. No, tajni ključ moramo zadržati samo za sebe jer ćemo pomoću njega dešifrirati dobivene poruke. Ako samo mi imamo tajni ključ, jedino ćemo mi moći pročitati skrivenu poruku.

Pogledajmo jedan od najpoznatijih načina šifriranja pomoću javnog ključa.

Nikola želi od prijatelja dobivati šifrirane poruke koje će samo on moći pročitati. Zbog toga će izabrati 4 prirodna broja – *a, b, c* i *d* – pa nakon toga izračunati:

[1]Više o šifriranju poruka korištenjem Cezarove i Vigenèreove šifre moći ćete pročitati u članku Skrivene poruke Andreje Igrec u sljedećem broju Matke.

$$M = a \cdot b - 1$$
$$e = c \cdot M + a$$
$$f = d \cdot M + b$$
$$n = \frac{e \cdot f - 1}{M}$$

Brojeve e i n Nikola će javiti svojim prijateljima. Oni čine njegov *javni ključ*. No broj f zadržat će samo za sebe. To je njegov *tajni ključ* pomoću kojeg će moći pročitati poruke svojih prijatelja.

Ako Borna želi poslati Nikoli poruku x, gdje je x neki prirodan broj manji od n, prvo će pomnožiti brojeve e i x. Neka je $k = e \cdot x$. Nakon toga Borna će izračunati ostatak pri cjelobrojnom dijeljenju broja k brojem n. Nazovimo taj ostatak s y.

Dakle, ovako šifriramo poruku x:

$$k = e \cdot x$$
$$y = \text{ostatak pri cjelobrojnom dijeljenju broja } k \text{ brojem } n$$

Borna će zatim poslati Nikoli poruku y.

Nakon što dobije poruku, Nikola će računati: $l = f \cdot y$. Nakon toga izračunat će ostatak pri cjelobrojnom dijeljenju broja l brojem n. Taj ostatak upravo je poruka x koju je Borna poslao Nikoli.

Dakle, ovako dešifriramo poruku y:

$$l = f \cdot y.$$
$$x = \text{ostatak pri cjelobrojnom dijeljenju broja } l \text{ brojem } n$$

Nakon što provede ovaj račun, Nikola će pročitati Borninu poruku.

Pogledajmo jedan konkretan primjer.

a) Nikola je odabrao brojeve: $a = 4$, $b = 7$, $c = 10$, $d = 8$, a zatim je prema gore navedenim „formulama" izračunao javne ključeve i tajni:

$$M = 4 \cdot 7 - 1 = 27$$
$$e = 10 \cdot 27 + 4 = 274$$
$$f = 8 \cdot 27 + 7 = 223$$
$$n = \frac{274 \cdot 223 - 1}{27} = 2\,263.$$

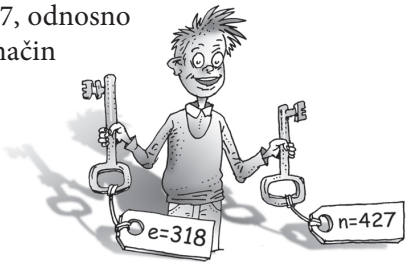
Prijateljima je javio svoje javne ključeve $e = 274$ i $n = 2\,263$.

b) Borna želi Nikoli dojaviti broj 17. Kako glasi šifrirana poruka koju će Borna poslati Nikoli?

Uz ranija objašnjenja, u ovom je slučaju $x = 17$. Borna računa: $k = e \cdot x = 274 \cdot 17 = 4\,658$, a zatim i ostatak pri dijeljenju broja 4 658 brojem 2 263. Budući da je $4\,658 : 2\,263 = 2$ i ostatak 132, Borna će Nikoli dojaviti broj $y = 132$.

c) Dešifrirajmo Borninu poruku. Hoće li Nikola zaista na ovaj način dobiti Borninu originalnu poruku?

Pri dešifriranju poruke, Nikola će iskoristiti svoj tajni ključ *f*. Uz gore navedene oznake, prvo će izračunati: $l = f \cdot y = 223 \cdot 132 = 29\,436$, a nakon toga izračunat će ostatak pri dijeljenju broja 29 436 brojem 2 263. Budući da je $29\,436 : 2\,263 = 13$ i ostatak 17, Nikola je izračunao da je $x = 17$, odnosno da je 17 je broj koji mu je Borna želio dojaviti. Dakle, na ovaj način Nikola zaista može dešifrirati poruku koju mu je poslao Borna.



***Zadatak* 7.** Sljedećeg dana Nikola je objavio novi javni ključ: $e = 318$ i $n = 427$. Ako mu Borna želi dojaviti broj 25, kako će glasiti šifrirana poruka?

Što ako Nikola želi na jednak način odgovoriti Borni na poruku? U tom slučaju Borna mora odabrati svoje brojeve *a, b, c, d*, izračunati i objaviti svoj javni ključ kako bi Nikola mogao šifrirati poruku. Nakon toga Borna će je na jednak način dešifrirati svojim tajnim ključem.

***Zadatak* 8.** Borna je za računanje javnog i tajnog ključa odabrao brojeve $a = 9$, $b = 12$, $c = 21$, $d = 4$. Nakon što je objavio svoj javni ključ, dobio je od Nikole poruku $y = 1\,497$. Što je Nikola „poručio" Borni?

Na ovaj se način mogu šifrirati i tekstualne poruke. O tome ćete imati priliku pročitati u nekome od sljedećih brojeva Matke.

Literatura:

1. Dujella, A., Maretić, M. (2007.). *Kriptografija*. Zagreb: Element
2. Barun, M. (2008.). *Kriptografija u školi*. Diplomski rad. Zagreb: PMF Matematički odsjek
3. http://csunplugged.org/wp-content/uploads/2014/12/18-Kriptografija.pdf (15. 10. 2015.)
4. http://lukyanenko.net/teaching/2015/MMSS/Lab4.pdf (15. 10. 2015.)
5. https://www.math.washington.edu/~koblitz/crlogia.html (15. 10. 2015.)
6. http://sigurnost.zemris.fer.hr/algoritmi/2008_ceri/ispis/zavrsni.pdf (15. 10. 2015.)

Rješenja zadataka provjerite na stranici 214.