TAJNO PISMO

Jelena Hunjadi, Donja Dubrava

U Matki broj 95 naučili ste kako prijateljima možete slati poruke tako da ih nitko drugi osim njih ne može pročitati. Ideja je bila da pošiljatelj poruke ima svoj javni i tajni ključ. Prisjetimo se.[1]

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.

Tako smo na ovaj način šifrirali samo numeričke vrijednosti. U ovom broju naučit ćemo kako možemo na ovaj način šifrirati i slati tekstualne poruke. Prisjetimo se jednoga od najpoznatijih načina šifriranja pomoću javnog ključa.

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

$$M = a \cdot b - 1$$

$$e = c \cdot M + a$$

$$f = d \cdot M + b$$

$$n = \frac{e \cdot f - 1}{M}$$

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

Ako Irena želi poslati Maji poruku *x*, gdje je *x* neki prirodan broj manji od *n*, najprije će pomnožiti brojeve *e* i *x*. Neka je $k = e \cdot x$. Nakon toga Irena 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 = ostatak pri cjelobrojnom dijeljenju broja *k* brojem *n*

Irena će zatim poslati Maji poruku *y*.

[1] Više u članku Kako šifrirati poruku? objavljenom u Matki broj 95.

Nakon što dobije poruku, Maja 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 Irena poslala Maji.

Dakle, ovako dešifriramo poruku y:

$l = f \cdot y$.

x = ostatak pri cjelobrojnom dijeljenju broja l brojem n

Nakon što provede ovaj račun, Maja će pročitati Ireninu poruku.

Pretpostavimo da je Maja odabrala brojeve: $a = 7$, $b = 8$, $c = 10$, $d = 6$.

Koje će brojeve M, e, f, n Maja izračunati?

Maja će izračunati:

$$M = 7 \cdot 8 - 1 = 55$$
$$e = 10 \cdot 55 + 7 = 557$$
$$f = 6 \cdot 55 + 8 = 338$$
$$n = \frac{557 \cdot 338 - 1}{55} = 3\ 423$$

Pretpostavimo da Irena želi poslati Maji poruku MATIJA. Prvo ovu poruku treba pretvoriti u numeričku vrijednost. Kako ne bismo dobili prevelike brojeve, pretvaranje ćemo vršiti po blokovima veličine 2 slova. U našem slučaju, prvo ćemo šifrirati poruku «MA", zatim «TI" i «JA". Pretvaranje vršimo u bazi 27; slovu A pridružujemo broj 1, slovu B broj 2..., slovu Z broj 26. Praznom mjestu pridružujemo broj 0.

$$x_1 = (MA)_{27} = 13 \cdot 27^1 + 1 \cdot 27^0 = 352$$
$$x_2 = (TI)_{27} = 20 \cdot 27^1 + 9 \cdot 27^0 = 549$$
$$x_3 = (JA)_{27} = 10 \cdot 27^1 + 1 \cdot 27^0 = 271$$

Sada će Irena svaki od ovih triju brojeva zasebno, na prethodno opisani način, šifrirati i poslati Maji.

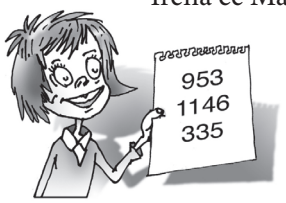
Prvo šifrira broj 352.

Računa: $k_1 = e \cdot x_1 = 557 \cdot 352 = 196\ 064$, a zatim i ostatak pri dijeljenju broja 196 064 brojem 3 423. Budući da je 196 064 : 3 423 = 57 i ostatak 953, Irena će Maji dojaviti broj 953.

Nakon toga, na jednak način šifrira i preostala dva broja.

Računa: $k_2 = e \cdot x_2 = 557 \cdot 549 = 305\ 793$, a zatim i ostatak pri dijeljenju broja 305 793 brojem 3423. Budući da je 305 793 : 3 423 = 89 i ostatak 1146, Irena će Maji dojaviti broj 1146.

Nadalje, računa: $k_3 = e \cdot x_3 = 557 \cdot 271 = 150\,947$, a zatim i ostatak pri dijeljenju broja 150 947 brojem 3 423. Budući da je 150 947 : 3 423 = 89 i ostatak 335, Irena će Maji dojaviti broj 335.



Dakle, Irena će Maji poslati redom brojeve 953, 1146 i 335.

Nakon toga, Maja mora redom dešifrirati ove poruke korištenjem svoj tajnog ključa *f*.

Dešifrirajmo poruku 953.

Uz gore navedene oznake, Maja će prvo izračunati $l_1 = f \cdot y_1 = 338 \cdot 953 =$ $= 322\,114$. Nakon toga izračunat će ostatak pri dijeljenju broja 322 114 brojem 3423. Budući da je 322 114 : 3423 = 94 i ostatak 352, Maja je izračunala da je $x_1 = 352$, odnosno da joj je Irena htjela dojaviti broj 352.

Preostaje još pretvoriti ovu numeričku vrijednost u riječ. Pretvaranje vršimo u bazi 27, na način da dijelimo broj sa 27 i promatramo ostatke pri tom dijeljenju. Broju 1 pridružujemo slovo A, broju 2 slovo B..., broju 26 slovo Z. Broju 0 pridružujemo prazno mjesto.

Budući da je 352 : 27 = 13 i ostatak 1, traženo slovo je slovo A. Dalje je 13 : 27 = 0 i ostatak 13 pa je drugo traženo slovo M. Slova ćemo pročitati od kraja prema početku, tj. prvi dio poruke koju je Irena poslala Maji glasi „**MA**".

Nakon toga, Maja na jednak način dešifrira i preostala dva broja i pretvara ih u riječi.

Pri dešifriranju broja 549, uz gore navedene oznake, Maja će prvo izračunati $l_2 = f \cdot y_2 = 338 \cdot 1\,146 = 387\,348$. Nakon toga izračunat će ostatak pri dijeljenju broja 387 348 brojem 3423. Budući da je 387 348 : 3 423 = 113 i ostatak 549, Maja je izračunala da je $x_2 = 549$, odnosno da joj je Irena htjela dojaviti broj 549.

Preostaje joj ovu numeričku vrijednost pretvoriti u riječ.

Budući da je 54 : 27 = 20 i ostatak 9, traženo je slovo I; odnosno 20 : 27 = 0 i ostatak 20, traženo je slovo T. Drugi dio poruke koju je Irena poslala Maji glasi „**TI**".

Konačno, Maja dešifrira broj 271. Uz gore navedene oznake, Maja će prvo izračunati $l_3 = f \cdot y_3 = 338 \cdot 335 = 113\,230$. Nakon toga izračunat će ostatak pri dijeljenju broja 113 230 brojem 3 423. Budući da je 113 230 : 3 423 = 33 i ostatak 271, Maja je izračunala da je $x_3 = 271$, odnosno da joj je Irena htjela dojaviti broj 271.

Preostaje još i ovu numeričku vrijednost pretvoriti u riječ.

Budući da je 271 : 27 = 10 i ostatak 1, traženo je slovo A; odnosno 10 : 27 = 0 i ostatak 10, a traženo je slovo J. Treći dio poruke koju je Irena poslala Maji glasi „**JA**".

Maja na ovaj način dobiva od Irene poruku MATIJA, odnosno uspješno rekonstruira njezinu poruku.

Što ako duljina poruke nije višekratnik broja 2? U tom slučaju nadopunit ćemo je jednim praznim mjestom čija će numerička vrijednost biti 0. Primjerice, Toni želi šifrirati riječ TAJNA. Pretvorit će u numeričku vrijednost zasebno dio „TA", zatim „JN" i „A_".

$$x_1 = (TA)_{27} = 20 \cdot 27^1 + 1 \cdot 27^0 = 541$$
$$x_2 = (JN)_{27} = 10 \cdot 27^1 + 14 \cdot 27^0 = 284$$
$$x_3 = (A\_)_{27} = 1 \cdot 27^1 + 0 = 27$$

Zatim će, prema opisanom postupku, zasebno šifrirati brojeve 541, 284 i 27. Kako će glasiti šifrirani brojevi ako pretpostavimo da je Tonijev javni ključ $e = 187$ i $n = 651$?

Toni prvo šifrira broj 541. Računa: $k_1 = e \cdot x_1 = 187 \cdot 541 = 101\,167$, a zatim i ostatak pri dijeljenju broja 101 167 brojem 651. Budući da je 101 167 : 651 = 155 i ostatak 262, prvi dio šifrirane poruke glasi 262.

Nakon toga, na jednak način šifrira i preostala dva broja.

Računa: $k_2 = e \cdot x_2 = 187 \cdot 284 = 53\,108$, a zatim i ostatak pri dijeljenju broja 53 108 brojem 651. Budući da je 53 108 : 651 = 81 i ostatak 377, drugi dio šifrirane poruke glasi 377.

Nadalje računa: $k_3 = e \cdot x_3 = 187 \cdot 27 = 5\,049$, a zatim i ostatak pri dijeljenju broja 5049 brojem 651. Budući da je 5049 : 651 = 7 i ostatak 492, treći dio šifrirane poruke glasi 492.

Dakle, da bi dojavio željenu poruku, Toni će poslati brojeve 262, 377 i 492.

Zadatak 1. Ivan je prijateljima objavio svoj javni ključ: $e = 530$ i $n = 2\,187$. Ako mu Lovro želi dojaviti poruku „NINA", kako će glasiti šifrirana poruka?

Zadatak 2. Lovro je za računanje javnog i tajnog ključa odabrao brojeve $a = 10$, $b = 4$, $c = 4$, $d = 5$. Nakon što je objavio svoj javni ključ, dobio je od Ivana poruke $y_1 = 110$, $y_2 = 213$. Što je Ivan „poručio" Lovri?

Rješenja zadataka:

Zadatak 1. Prvo poruku pretvaramo u numeričku vrijednost:

$$x_1 = (NI)_{27} = 14 \cdot 27^1 + 9 \cdot 27^0 = 387$$
$$x_2 = (NA)_{27} = 14 \cdot 27^1 + 1 \cdot 27^0 = 379$$

Za $e = 530$ i $n = 2\,187$ šifriramo zasebno poruke $x_1 = 387$ i $x_2 = 379$.

Računamo $k_1 = e \cdot x_1 = 530 \cdot 387 = 205\,110$, a zatim i ostatak pri dijeljenju broja 205 110 brojem 2187. Budući da je 205 110 : 2187 = 93 i ostatak 1 719, prvi dio poruke glasi 1719.

Nadalje računamo $k_2 = e \cdot x_2 = 530 \cdot 379 = 200\,870$, a zatim i ostatak pri dijeljenju broja 200 870 brojem 2187. Budući da je 200 870 : 2187 = 91 i ostatak 1853, drugi dio poruke glasi 1853.

Dakle, Lovro će Ivanu poslati brojeve 1 719 i 1853.

Zadatak 2. Ako je $a = 10$, $b = 4$, $c = 4$, $d = 5$, za dešifriranje Ivanove poruke prvo moramo izračunati brojeve M, e, f i n:

$$M = 10 \cdot 4 - 1 = 39$$
$$e = 4 \cdot 39 + 10 = 166$$
$$f = 5 \cdot 39 + 4 = 199$$
$$n = \frac{166 \cdot 199 - 1}{39} = 847$$

Pri dešifriranju poruke Lovro računa: $l_1 = f \cdot y_1 = 199 \cdot 110 = 21\,890$. Nakon toga izračunat će ostatak pri dijeljenju broja 21 890 brojem 847. Budući da je 21 890 : 847 = 25 i ostatak 715, zaključujemo da prvi dio poruke koji je Ivan htio dojaviti Lovri glasi 715.

Nadalje, Lovro računa: $l_2 = f \cdot y_2 = 199 \cdot 213 = 42\,387$. Nakon toga izračunat će ostatak pri dijeljenju broja 42 387 brojem 847. Budući da je 42 387 : 847 = 50 i ostatak 37, zaključujemo da drugi dio poruke koji je Ivan htio dojaviti Lovri glasi 37.

Lovro još mora pretvoriti ove numeričke vrijednosti u riječi.

715 : 27 = 26 i ostatak 9, što znači da je traženo slovo M; odnosno 26 : 27 = 0 i ostatak 26, što znači da je traženo slovo Z. Prvi dio poruke Ivanove poruke glasi „**ZM**".

32 : 27 = 1 i ostatak 10, što znači da je traženo slovo J; odnosno 1 : 27 = 0 i ostatak 1, pa je traženo slovo A. Drugi dio Ivanove poruke glasi „**AJ**". Zaključujemo da je Ivan Lovri poslao poruku ZMAJ.