MAT-KOL (Banja Luka)
ISSN 0354-6969 (p), ISSN 1986-5228 (o)
Vol. XVII (2)(2011), 43-52

DISKRETNI LOGARITAM

Bernadin Ibrahimpašić[1], Dragana Kovačević[2]

Abstract

U ovom članku se opisuje pojam diskretnog logaritma i navode algoritmi za rješavanje problema diskretnog logaritma (DLP) koji ne ovise o svojstvima grupe.

Ključne riječi i fraze: Diskretni logaritam, DLP, algoritmi za rješavanje DLP.

In this paper we describe discrete logarithm and we give algorithms for the DLP which work in arbitrary group.

AMS Mathematics Subject Classification (2010): 11Y99

Key words and phrases: Discrete logarithm, DLP, Algorithms for DLP.

1 Uvod

Kriptografija je naučna disciplina koja se bavi proučavanjem metoda za slanje poruka u takvom obliku, da ih samo onaj kome su namijenjene može razumjeti. Riječ kriptografija je sastavljena od grčkih riječi Kriptos ($K\rho\iota\pi\tau o\zeta$ – sakriven, tajan) i Grafein ($\Gamma\rho\alpha\varphi\varepsilon\iota\nu$ – pisati) i znači tajnopis. Pojam kriptografije, kao tajnog pisanja, se proširuje i na tajno prenošenje govora i slika. Na taj način se dolazi do općeg pojma tajnog sporazumijevanja ili sakrivanja informacija.

Kod simetričnih kriptosistema, tj. kriptosistema s tajnim ključem, pošiljalac i primalac bi tajno izabrali ključ K pomoću kojeg su generisali funkcije e_K za šifriranje i d_K za dešifriranje. U ovom slučaju je d_K isti kao i e_K ili se iz njega može jednostavno izračunati. Iz tog razloga, sigurnost simetričnih kriptosistema leži u tajnosti ključa, što i predstavlja veliki nedostatak, jer pošiljalac i primalac prije šifriranja moraju biti u mogućnosti da razmijene tajni ključ preko nekog sigurnog komunikacijskog kanala, pomoću kurira ili se lično sresti. To je nekada teško izvodivo, naročito ako su oni na velikoj udaljenosti i ako su komunikacijski kanali, koji su im na raspolaganju, poprilično nesigurni. Pored toga, tajni ključ se mora često mijenjati, jer šifriranje više puta istim ključem smanjuje sigurnost.

Whitfield Diffie i Martin Hellman su 1976. godine predložili algoritam za razmjenu ključeva preko nesigurnog komunikacijskog kanala, čija je sigurnost

[1]Pedagoški fakultet Univerziteta u Bihaću, Bosna i Hercegovina,
e-mail: bernadin@bih.net.ba
[2]Katolički školski centar, Opća–realna gimnazija, Sarajevo, Bosna i Hercegovina,
e-mail: draganabrcina@yahoo.com

bila zasnovana na teškoći nalaženja diskretnog logaritma. To u suštini nije kriptosistem, ali je predstavljao ideju za novu klasu kriptosistema. To su asimetrični kriptosistemi ili kriptosistemi s javnim ključem. Ideja se sastojala u tome da je iz funkcije za šifriranje e_K praktično nemoguće, u nekom razumnom vremenu, izračunati funkciju za dešifriranje d_K. U tom slučaju bi funkcija za šifriranje e_K mogla biti javna.

2 Pojam i definicija diskretnog logaritma

S pojmom logaritma učenici se upoznaju u drugom razredu srednje škole.

Definicija 2.1 Logaritam *realnog broja* $a > 0$, *za zadanu bazu* $0 < b \neq 1$, *je realan broj* x *kojim treba stepenovati bazu logaritma* b *da bi dobili broj* a, *tj.*

$$\log_b a = x \Leftrightarrow b^x = a.$$

Posmatrajmo sada $\log_b a = x$, ali takav da su $a, b, x \in \mathbb{Z}$, $0 < b \neq 1$, $a > 0$. Ovaj logaritam je definisan na skupu $\mathbb{Z}$ i on može, ali i ne mora da ima rješenje. Tako je npr. $\log_2 8 = 3$, jer je $2^3 = 8$, međutim $\log_2 7$ nema rješenja, jer ne postoji cijeli broj kojim bi stepenovali 2 i dobili vrijednost 7.

Neka su data dva prirodna broja b i n takvi da je $b < n$. Uzmemo li proizvoljan prirodan broj $a < n$, cilj nam je naći cijeli broj x za koji važi

$$b^x \equiv a \pmod{n}.$$

Tako npr. za $b = 2, n = 25$ i $a = 7$, imamo $2^5 \equiv 7 \pmod{25}$, pa je traženi broj jednak 5.

Dakle, nas interesuju strukture u kojima je moguće riješiti dani problem.

Za grupu G kažemo da je *konačna* ili *beskonačna*, već prema tome da li skup G ima konačno ili beskonačno elemenata. Kardinalni broj skupa G nazivamo *red grupe*. Neka je $g \in G$, bilo koji element grupe G. Posmatrajmo skup svih njegovih stepena $\{\ldots, g^{-2}, g^{-1}, g^0, g^1, g^2, \ldots\}$. Ako među tim stepenima nema jednakih, kažemo da je element g *beskonačnog reda*. Ako među tim stepenima ima jednakih, tj. ako je za neke $k \neq l$, $g^k = g^l$, tada je $g^{k-l} = e$, tj. postoje netrivijalni stepeni od g koji su jednaki neutralnom elementu grupe. U tom slučaju kažemo da je element g *konačnog reda*. Najmanji prirodan broj k, takav da je $g^k = e$, nazivamo *red elementa* g. Ako u grupi G postoji element g takav da je $G = \{g^k \ : \ k \in \mathbb{Z}\}$, tada za grupu G kažemo da je *ciklička*, a element g se zove *generator* grupe G.

Ako posmatramo skup $\mathbb{Z}_n$ ostataka pri dijeljenju prirodnim brojem n, onda je $\mathbb{Z}_p^* = \{a \in \mathbb{Z}_p \ : \ \text{nzd}\,(a, p) = 1\} = \{1, 2, \ldots, p-1\}$, gdje je p prost broj, multiplikativna ciklička grupa reda $p - 1$.

Definicija 2.2 *Neka je* G *konačna ciklična grupa reda* n. *Neka je* α *generator grupe* G *i* β *proizvoljan element iz* G. *Pod* diskretnim logaritmom *od* β *po bazi* α, *u oznaci* $\log_\alpha \beta$, *podrazumijevamo jedinstveni cijeli broj* x, $0 \leq x \leq n-1$, *takav da je* $\beta = \alpha^x$.

U konačnoj multiplikativnoj grupi G reda n, za svako $b \in G$ i svako $x \in \mathbb{Z}$ lako je izračunati b^x, dok je nasuprot tome, za zadano $a \in G$ pronaći broj $x \in \mathbb{Z}$, kojim treba stepenovati b da bi dobili a, tj. riješiti problem diskretnog logaritam (DLP), teško.

Inače, nije samo po sebi jasna lakoća računanja b^x, jer kada bismo to morali računati kao $b \cdot b \cdots b$, uz $x-1$ množenja, tada nam stepenovanje ne bi bilo ništa lakše od logaritmiranja (bilo bi potrebno $O(n)$ operacija). Međutim, postoje vrlo efikasne metode za stepenovanje primjenjive u proizvoljnoj grupi od kojih treba posebno istaknuti vrlo jednostavnu metodu *kvadriraj i množi* ([1, 4]), koja koristi binarni zapis broja x, pa se naziva i binarna metoda.

Najinteresantnije grupe koje se koriste u praksi su multiplikativna grupa konačnog polja $\mathbb{F}_q$, uključujući i specijalne slučajeve multiplikativne grupe $\mathbb{Z}_p^*$, te multiplikativne grupe $\mathbb{F}_{2^m}^*$ konačnog polja $\mathbb{F}_{2^m}$ karakteristike 2.

Osobine logaritma u skupu realnih brojeva se odnose i na diskretni logaritam, tj. ako je α generator cikličke grupe G reda n, i $\beta, \gamma \in G$ proizvoljni elementi, tada vrijedi

- $(\log_\alpha \beta\gamma) \equiv (\log_\alpha \beta + \log_\alpha \gamma) \pmod{n}$,
- $\log_\alpha \left(\beta^k\right) \equiv k \cdot \log_\alpha \beta \pmod{n}$.

3 Algoritmi za rješavanje DLP

Definicija 3.1 *Neka je α generator od $\mathbb{Z}_p^*$, gdje je p prost broj, i neka je $\beta \in \mathbb{Z}_p^*$ proizvoljan element.* Problem diskretnog logaritma (DLP) *je naći cijeli broj x, $0 \leq x \leq p-2$, takav da je $\alpha^x \equiv \beta \pmod{p}$.*

Definicija 3.2 *Neka je α generator konačne cikličke grupe G reda n, i neka je $\beta \in G$ proizvoljan element.* Generalizirani problem diskretnog logaritma (GDLP) *je naći cijeli broj x, $0 \leq x \leq n-1$, takav da je $\alpha^x = \beta$.*

Svi algoritmi za rješavanje problema diskretnog logaritma se mogu svrstati u jednu od tri kategorije.

i) Algoritmi koji rade u proizvoljnim grupama tj. koji ne koriste nijedno specifično svojstvo grupe. To su: iscrpljujuće pretraživanje, Shanksov algoritam, te Pollardov ρ i λ algoritam.

ii) Algoritmi koji dobro rade u grupama glatkog reda, tj. grupama čiji red nema velike proste faktore. To je Silver–Pohlig–Hellmanov algoritam.

iii) Algoritmi koji koriste metode koji predstavljaju elemente grupe kao proizvod elemenata iz relativno malih skupova, tzv. faktorskih baza. Klasični predstavnici ove kategorije su algoritmi koji su varijacije Index calculus metode.

Mi ćemo opisati algoritme iz prve kategorije, tj. algoritme koji rade u proizvoljnim grupama i ne zahtijevaju nijedno specifično svojstvo grupe.

3.1 Iscrpljujuće pretraživanje

Najprostiji algoritam za traženje $\log_\alpha \beta$ u grupi G je uzastopno izračunavanje α^0, α^1, $\alpha^2, \ldots$ dok ne dobijemo β. Ovaj metod zahtijeva $O(n)$ množenja, gdje je n red od α, i zato je neefikasan za velike n. Dobra osobina je da ne zahtijeva memorisanje podataka.

3.2 Shanksov algoritam

Prvo poboljšanje algoritma, baziranog na iscrpljujućem pretraživanju, dao je Daniel Shanks. Naziva se Shanksov algoritam ili *mali korak–veliki korak* (Baby–step giant–step) i bazira se na činjenici da ako u konačnoj cikličkoj grupi G reda n, s generatorom α, za $\beta \in G$ vrijedi da je $x = \log_\alpha \beta$, tada se x može na jedinstven način zapisati u obliku $x = im + j$, gdje je $0 \leq i, j < m = \lceil \sqrt{n} \rceil$.

Napomenimo da funkcija "*najmanje cijelo*", u oznaci $\lceil t \rceil$, kao rezultat vraća najmanji cijeli broj koji je veći ili jednak realnom broju t. Slično tome, funkcija "*najveće cijelo*", u oznaci $\lfloor t \rfloor$, kao rezultat vraća najveći cijeli broj koji je manji ili jednak realnom broju t.

Prema tome imamo da vrijedi $\alpha^x = \alpha^{im}\alpha^j$, što implicira relaciju

$$\beta \left(\alpha^{-m}\right)^i = \alpha^j. \tag{1}$$

Dalje prolazeći vrijednostima i i j, $0 \leq i, j < m$ tražimo one koji zadovoljavaju relaciju (1). Time smo dobili i vrijednost x, što je upravo traženi diskretni logaritam. Opišimo sada navedeni algoritam za rješavanje DLP u grupi $\mathbb{Z}_p^*$.

1. Izračunamo $m = \lceil \sqrt{p-1} \rceil$.
2. Računamo mali korak i formiramo tabelu T_1 uređenih parova $\left(j, \alpha^j \bmod p\right)$, $(0 \leq j < m)$ i sortiramo je uzlazno po drugoj koordinati.
3. Računamo veliki korak i formiramo, uzlazno sortiranu po drugoj koordinati, tabelu T_2 uređenih parova $\left(i, \beta\left(\alpha^{-m}\right)^i \bmod p\right)$, $(0 \leq i < m)$.
4. Pronalazimo parove $(j, y) \in L_1$ i $(i, y) \in L_2$, tj. one parove koji imaju jednaku drugu koordinatu i računamo
$$x = \log_\alpha \beta = im + j.$$

Primjer 3.1 *Odrediti* $\log_5 96$ *u grupi* $\mathbb{Z}_{317}^*$*, tj. izračunati* $\log_5 96 \pmod{317}$.

Rješenje: Imamo da je $\alpha = 5$, $\beta = 96$ i $p = 317$.

Kako je $m = \lceil \sqrt{316} \rceil = 18$, to radimo za $0 \leq i, j < 18$.

Odredimo sada $\alpha^{-m} = \left(\alpha^{-1}\right)^m$. Kako je

$$5^{-1} \equiv 127 \pmod{317},$$

to je

$$\alpha^{-m} = \left(5^{-1}\right)^{18} \equiv 127^{18} \equiv 7 \pmod{317}.$$

Formirajmo T_1.

j	0	1	2	8	9	6	10	3	7
$5^j \pmod{317}$	1	5	25	81	88	92	123	125	143
j	17	13	14	15	16	**12**	5	11	4
$5^j \pmod{317}$	154	159	161	171	221	**222**	272	298	308

Formirajmo sada T_2.

i	7	4	1	14	12	8	17	0	11
$96 \cdot 7^i \bmod 317$	11	37	38	64	66	77	79	96	100
i	15	13	**9**	6	5	2	3	16	10
$96 \cdot 7^i \bmod 317$	131	145	**222**	228	259	266	277	283	286

Uočimo da se druge komponente poklapaju za $i = 9$ i $j = 12$ pa je

$$x = im + j = 9 \cdot 18 + 12 = 174 \qquad \Rightarrow \qquad \log_5 96 \equiv 174 \pmod{317}.$$

♢

Napomenimo da je postupak moguće prekinuti i ranije čim se pojavi poklapanje drugih komponenti u L_1 i L_2.

Kao što vidimo, ovaj algoritam zahtijeva pohranjivanje podataka i nerijetko se u literaturi za ovaj algoritam može pronaći i naziv *Time–memory trade off*. Ovaj algoritam zatijeva $O(\sqrt{n})$ mjesta u listi. Za kreiranje liste je potrebno još $O(\sqrt{n})$ množenja, a za sortiranje je potrebno $O(\sqrt{n}\ln n)$ operacija i $O(\sqrt{n})$ pogleda u listu. Sve ovo pokazuje da ovaj algoritam nije primjenjiv na grupe velikog reda.

3.3 Pollardov ρ algoritam

Ovo je algoritam koji zahtijeva isto vrijeme izvršavanja kao i Shanksov, ali mu treba mnogo manje prostora. Pretpostavimo da je $f\colon G \to G$ slučajno preslikavanje, gdje je G ciklička grupa čiji je red n prost broj. Odaberemo slučajno $x_0 \in G$ i računamo

$$x_{i+1} = f(x_i), \qquad i \geq 0.$$

Tako dobijamo slučajan niz $x_0, x_1, x_2, \ldots$. Kako je G konačan skup, to se mora dogoditi $x_i = x_j$, za neke $i \neq j$, pa je dalje

$$x_{i+1} = f(x_i) = f(x_j) = x_{j+1}.$$

Dakle, dobijamo da se niz $x_0, x_1, x_2, \ldots$ ciklički ponavlja. Ako bismo to grafički predstavili, dobili bismo oblik slova ρ, pa otuda i dolazi naziv ovog algoritma. Jedan od načina da se pronađu i i j takvi da je $x_i = x_j$, je sljedeći. Uzimamo (x_1, x_2) i računamo (x_2, x_4), a zatim (x_3, x_6). Na isti način nastavljamo dalje. Tačnije, za dani par (x_i, x_{2i}), računamo

$$(x_{i+1}, x_{2i+2}) = (f(x_i), f(f(x_{2i}))).$$

Zaustavljamo se kada dobijemo da je $x_m = x_{2m}$.

Kada računamo $x = \log_\alpha \beta$, prvo grupu G podijelimo u 3 skupa G_1, G_2 i G_3, koji su u parovima disjunktni i čija je unija skup G. Formiramo ih na proizvoljan način, ali da budu približno iste veličine i da $1 \notin G_2$. Zatim, uzimajući da je $x_0 = 1$, za $i \geq 0$ definiramo niz

$$x_{i+1} = f(x_i) = \begin{cases} \beta \cdot x_i \ , & x_i \in G_1, \\ x_i^2 \ , & x_i \in G_2, \\ \alpha \cdot x_i \ , & x_i \in G_3. \end{cases} \tag{2}$$

Podaci koje pamtimo su trojke (x_i, a_i, b_i), gdje vrijedi da je $x_i = \alpha^{a_i} \cdot \beta^{b_i}$. Nizove $a_0, a_1, a_2, \ldots$ i $b_0, b_1, b_2, \ldots$, stavljajući $a_0 = b_0 = 0$, dobijamo iz niza $x_0, x_1, x_2, \ldots$ na sljedeći način:

$$a_{i+1} = \begin{cases} a_i \ , & x_i \in G_1, \\ 2a_i \bmod n \ , & x_i \in G_2, \\ a_i + 1 \bmod n \ , & x_i \in G_3, \end{cases} \tag{3}$$

i

$$b_{i+1} = \begin{cases} b_i + 1 \bmod n \ , & x_i \in G_1, \\ 2b_i \bmod n \ , & x_i \in G_2, \\ b_i \ , & x_i \in G_3. \end{cases} \tag{4}$$

Ako startujemo s $a_0 = 1$, tj. s trojkom $(a_0, x_0, y_0) = (1, 0, 0)$, tada za svako i imamo

$$\log_\alpha x_i = a_i + b_i \cdot \log_\alpha \beta = a_i + b_i x.$$

Kada posmatramo $x_m = x_{2m}$, imamo

$$\begin{aligned} a_m + b_m x &= a_m + b_m \cdot \log_\alpha \beta = \log_\alpha x_m \\ &= \log_\alpha x_{2m} = a_{2m} + b_{2m} \cdot \log_\alpha \beta \\ &= a_{2m} + b_{2m} x. \end{aligned}$$

Sada imamo

$$(b_m - b_{2m})\, x = a_{2m} - a_m$$

i ako je $b_m \neq b_{2m}$, tada je

$$x = \frac{a_{2m} - a_m}{b_m - b_{2m}}, \tag{5}$$

gdje dijeljenje s $b_m - b_{2m}$ znači množenje s $(b_m - b_{2m})^{-1}$.

Vjerojatnost da je $b_m = b_{2m}$ je zanemarivo malena. Ukoliko ipak dođe do toga, procedura se ponavlja izborom slučajnih a_0 i b_0 iz segmenta $[1, n-1]$ i postavlja se $x_0 = \alpha^{a_0} \cdot \beta^{b_0}$.

Primjer 3.2 *U podgrupi G grupe $\mathbf{Z}_{59}^*$, reda 29, čiji je generator 5, izračunajmo* $\log_5 28$.

Podijelimo G u tri skupa i to

$$\begin{aligned} G_1 &= \{g \in G \ : \ g \leq 19\} \\ G_2 &= \{g \in G \ : \ 20 \leq g \leq 39\} \\ G_3 &= \{g \in G \ : \ 40 \leq g \leq 58\} \end{aligned}$$

Koristeći relacije (2), (3) i (4), uz start $(x_0, a_0, b_0) = (1, 0, 0)$, imamo:

i	x_i	a_i	b_i	x_{2i}	a_{2i}	b_{2i}
1	28	0	1	17	0	2
2	17	0	2	53	0	4
3	4	0	3	15	2	8
4	53	0	4	19	2	10
5	29	1	4	28	2	12
6	15	2	8	4	4	25
7	7	2	9	29	5	26
8	19	2	10	7	10	53
9	**1**	**2**	**11**	**1**	**10**	**55**

Dobili smo da je

$$x_9 = x_{18} = 1, \qquad a_9 = 2, \qquad a_{18} = 10, \qquad b_9 = 11, \qquad b_{18} = 55,$$

pa je na osnovu (5), uzimajući u obzir da radimo u podgrupi reda 29,

$$x = \frac{a_{18} - a_9}{b_9 - b_{18}} \bmod 29 = \frac{10 - 2}{11 - 55} \bmod 29.$$

Kako je

$$(11 - 55)^{-1} \equiv (-44)^{-1} \equiv 14^{-1} \equiv 27 \pmod{29},$$

to je

$$x = 8 \cdot 27 \equiv 13 \pmod{29}.$$

To znači da je

$$\log_5 28 = 13 \qquad \Rightarrow \qquad 5^{13} \equiv 28 \pmod{59}.$$

$\diamondsuit$

3.4 Pollardov λ algoritam

Ovaj algoritam je naročito koristan ako znamo interval $[w_1, w_2]$ kojem pripada naš diskretni logaritam $x = \log_\alpha \beta$. Neka je $w = w_1 - w_2$, dužina intervala kojem pripada naš diskretni logaritam x, te neka je $N = \lfloor \sqrt{w} \rfloor$ i $k \approx \frac{1}{2} \log_2 w$.

Definirajmo skup $T = \{t_0, t_1, \ldots, t_{k-1}\}$, gdje je $t_i = 2^i$, $(0 \leq i < k)$.

Grupu G čiji je generator α, reda prost broj p, podijelimo u k, u parovima disjunktnih, podskupova G_i, $(i = 0, 1, \ldots, k-1)$, a nakon toga radimo sljedeće.

1. Krenuvši od $r_0 = \alpha^y$, formiramo niz

$$r_i = r_{i-1} \cdot \alpha^{t_j}, \qquad i = 1, \ldots, N$$

gdje je t_j takav da $r_{i-1} \in G_j$.

Logaritmirajući, dobijamo niz

$$c_{i+1} = c_i + t_j \pmod{p}, \qquad c_0 = y.$$

Pamtimo samo vrijednost c_N. Za c_N vrijedi da je $c_N = \log_\alpha r_N$.

2. Krenuvši od $s_0 = \alpha^x = \beta$, formiramo drugi niz

$$s_{i+1} = s_i \cdot \alpha^{t'_j}$$

gdje je t'_j takav da $s_i \in G_j$.

Na isti način, u ovom slučaju dobijamo niz

$$d_{i+1} = d_i + t'_j \pmod{p}, \qquad d_0 = 0.$$

Vrijedi da je $\log_\alpha s_i = x + d_i$.

Nizovi r_i i s_i, koji kreću odvojeno, sreću se na jednom mjestu kao kraci od slova λ, a zatim nastavljaju istim putem. Otuda i potiče naziv ovog algoritma. Cilj nam je pronaći M takav da je $s_M = r_N$, jer je tada

$$c_N = \log_\alpha r_N = \log_\alpha s_M = x + d_M$$

pa je

$$x = c_N - d_M \bmod p.$$

U slučaju da se ova dva niza ne sretnu, povećava se N i nastavlja s računanjem oba niza, r_i i s_i, na isti način.

Očekivano vrijeme izvršavanja je $O(\sqrt{w})$.

Primjer 3.3 *U grupi G, reda $p = 101$, koja je podgrupa cikličke grupe $\mathbf{Z}^*_{607}$, čiji je generator $\alpha = 64$, izračunajmo $\log_{64} 8$, tj. odredimo takav x za koji vrijedi da je $64^x \equiv 8 \pmod{607}$.*

Rješenje: Uzmimo da je $x \in [0, 100]$, pa imamo da je

$$w = 100 - 0 = 100, \qquad N = \lfloor \sqrt{100} \rfloor = 10, \qquad k = 4,$$

$$T = \{t_0, t_1, t_2, t_3\}, \qquad t_i = 2^i, \quad i = 0, 1, 2, 3,$$

$$G_i = \{g \in G \ : \ g \equiv i \pmod{4}\}.$$

1. $r_0 = 64^{100} \pmod{607} = 313, \;\; c_0 = 100$

   Za $i = 1, \ldots, 10 = N$, računamo

i	0	1	2	3	4	5	6	7	8	9	10
r_i	313	64	454	330	288	222	271	204	309	69	**369**
c_i	100	1	2	6	10	11	15	23	24	26	**28**

2. $s_0 = 8, \;\; d_0 = 0$

   Računamo s_i i d_i sve dok ne dobijemo da je $s_M = r_N = r_{10} = 369$.

i	0	1	2	3	4	5	6	7	8	9	10	11	12
s_i	8	512	597	316	193	214	562	347	418	122	570	56	549
d_i	0	1	2	4	5	7	11	15	23	27	31	35	36
i	13	14	15	16	17	18	19	20	21	22	23	24	25
s_i	376	391	478	64	454	330	288	222	271	204	309	69	**369**
d_i	38	39	47	51	52	56	60	61	65	73	74	76	**78**

   Dobili smo da je $s_{25} = 369 = r_{10}$, pa je sada

$$x = c_N - d_M = c_{10} - d_{25} = 28 - 70 = -50 \equiv 51 \pmod{101}$$

   $\Rightarrow \log_{64} 8 = 51$, tj. $64^{51} \equiv 8 \pmod{607}$. $\diamondsuit$

4 Diffie–Hellmanov algoritam za razmjenu ključeva

Sada ćemo opisati već spomenuti Diffie–Hellmanov algoritam za razmjenu ključeva putem nesigurnog komunikacijskog kanala, koji je nastao 1976. godine, a zasniva se na teškoći, skoro pa nemogućnosti, računanja g^{ab} iz poznavanja g^a i g^b. Osobe koje sudjeluju u komunikaciji imaju, za kriptografiju, standardna imena Alice i Bob.

1. Odabere se veliki prost broj p i generator g grupe $\mathbb{Z}_p^*$, i objave se kao javni.

2. Alice izabere slučajan broj $a \in \{1, 2, \ldots, p-1\}$ i pošalje Bobu dobijeni rezultat $A = g^a \bmod p$.

3. Bob izabere slučajan broj $b \in \{1, 2, \ldots, p-1\}$ i pošalje Alice dobijeni rezultat $B = g^b \bmod p$.

4. Oboje računaju $g^{ab} \bmod p$, tj. Alice računa $B^a = \left(g^b \bmod p\right)^a = g^{ab} \bmod p$, a Bob računa $A^b = \left(g^a \bmod p\right)^b = g^{ab} \bmod p$, i rezultat koriste kao privatni (tajni) ključ za buduću komunikaciju.

Protivnik koji prisluškuje razgovor Alice i Boba, sazna generator g i grupu G (tj. prost broj p), te vrijednosti g^a i g^b. Cilj mu je izračunati g^{ab}, tj. riješiti tzv. Diffie–Hellmanov problem (DHP). Ukoliko je on u mogućnosti riješiti problem diskretnog logaritma (DLP), pa iz g^a i g izračunati a, onda mu je lako, pomoću a i g^b, izračunati g^{ab}. Vjeruje se da su DHP i DLP, u većini grupa koje se koriste u kriptografiji, ekvivalentni.

Primjer 4.1 *Alice i Bob kreiraju tajni ključ preko nesigurnog komunikacijskog kanala.*

Rješenje:

1. U telefonskom razgovoru (potpuno javno) oni se dogovore da odaberu prost broj $p = 13$ i $g = 2$ kao generator grupe $\mathbb{Z}_{13}^*$.
2. Alice bira $a = 11$ i računa $A = 2^{11} \bmod 13 = 7$ i šalje Bobu rezultat $A = 7$ putem nesigurnog komunikacijskog kanala (npr. telefonski).
3. Bob bira $b = 9$ i računa $B = 2^9 \bmod 13 = 5$ i šalje Alice rezultat $B = 5$, također putem nesigurnog komunikacijskog kanala.
4. Alice računa $B^a = 5^{11} \bmod 13 = 8$.
   Bob računa $A^b = 7^9 \bmod 13 = 8$.
   Oboje su dobili isti rezultat, pa je njihov tajni ključ 8. ♢

Na prvi pogled, čini se laganim izračunati a i b, a samim tim i g^{ab}, ali to je, u ovom slučaju, samo zato što smo izabrali malen p. Za velike p, to je teško izvodivo. Tako je McCurley, za $g = 7$ i $p = 2 \cdot 739 \cdot q + 1$, gdje je $q = \left(7^{149} - 1\right)/6$, objavio 1989. godine 7^a i 7^b kao brojeve od po 129 cifara, te ponudio \$100 onome ko izračuna tajni ključ $7^{ab} \bmod p$. Zadatak su riješili tek 1998. godine Damian Weber i Thomas F. Denny.

Literatura

[1] B. Ibrahimpašić: *Matematičke osnove kriptografije javnog ključa*, Magistarski rad, PMF, Sarajevo, 2004.

[2] A. Menezes, P. van Oorschot, S. Vanstone: *Handbook of Applied Cryptography*, CRC Press, Boca Raton, 1996.

[3] A. J. McCurley: *The Discrete Logarithm Problem*, Proceedings in Applied Cryptography, Vol. 42, 13–25, AMS, Providence, 1990.

[4] S. Y. Yan: *Number Theory for Computing*, Springer–Verlag, Berlin, 2002.

Pristiglo u redakciju 22.07.2011.