A31 ΚΡΥΠΤΟΓΡΑΦΙΑ
Σημειώσεις

Θεόδουλος Γαρεφαλάκης

10 Απριλίου 2022

1 Το πρόβλημα του διακριτού λογαρίθμου

Όπως έχουμε δει, η ασφάλεια του πρωτοκόλλου Diffie-Hellman εξαρτάται από τη δυσκολία υπολογισμού διακριτών λογαρίθμων. Θυμίζουμε ότι στο πρόβλημα του διακριτού λογαρίθμου (DL) μας δίνεται μία πεπερασμένη αβελιανή ομάδα $(G, \cdot)$, ένα στοιχείο $g \in G$ και ένα $y \in \langle g \rangle$. Η τάξη, n, του στοιχείου g μπορεί να θεωρείται δεδομένη. Το ζητούμενο είναι να υπολογιστεί ο ακέραιος $0 \leq x < n$ με την ιδιότητα $y = g^x$. Θα δούμε κάποιους αλγόριθμους που μπορούν να εφαρμοστούν σε κάθε πεπερασμένη αβελιανή ομάδα G, αρκεί φυσικά να υπάρχει αποτελεσματικός αλγόριθμος για τον υπολογισμό της πράξης της G. Τέτοιους αλγορίθμους τους ονομάζουμε γενικούς. Είναι φενερό ότι το x μπορεί να υπολογιστεί υπολογίζοντας διαδοχικά τα $g, g^2, g^3, \ldots, g^i, \ldots$ και ελέγχοντας σε κάθε βήμα εάν $y = g^i$. Αυτός ο αλγόριθμος χρειάζεται, στη χειρώτερη περίπτωση, $n - 2$ πράξεις στην ομάδα. Στόχος μας είναι να το βελτιώσουμε.

2 Ο αλγόριθμος Baby-step/Giant-step του Daniel Shanks

Τα δεδομένα μας είναι τα $g \in G$ τάξης n και $y \in \langle g \rangle$. Έστω $1 < q < n$ ένας ακέραιος. Τότε από την Ευκλείδια διαίρεση του n με το q, έχουμε

$$x = q \cdot i + j, \quad \text{για κάποια} \quad 0 \leq i < \frac{n}{q} \quad \text{και} \quad 0 \leq j < q.$$

Φυσικά τα i και j δεν τα γνωρίζουμε. Όμως ξέρουμε ότι υπάρχουν και είναι μοναδικά. Ο αλγόριθμος που θα περιγράψουμε υπολογίζει τα i, j και από αυτά το x. Έχουμε

$$y = g^{qi+j} \quad \Longleftrightarrow \quad yg^{-qi} = g^j.$$

Η τελευταία εξίσωση υποδεικνύει τον παρακάτω αλγόριθμο:

1. Υπολόγισε το $u = g^{-q}$.
2. Για $i = 0, 1, \ldots, \lfloor n/q \rfloor$ υπολόγισε το yu^i και αποθήκευσε σε ένα hash table A το $A[yu^i] = i$. Το yu^i ονομάζεται κλειδί και το i είναι η τιμή που σχετίζεται με το κλειδί yu^i.
3. Για $j = 0, 1, \ldots, q - 1$ υπολόγισε το g^j και για κάθε μία τιμή που υπολογίζεις έλεγξε εάν το g^j είναι κάποιο κλειδί που έχεις υπολογίσει το βήμα (2).
4. Όταν βρεις j τέτοιο ώστε το κλειδί g^j υπάρχει στο hash table , θέσε $i = A[g^j]$ και απάντησε $x = qi + j$.

Η ορθότητα του αλγορίθμου είναι φανερή από όσα είπαμε παραπάνω. Πόσες πράξεις κάνει ο αλγόριθμος; Έχουμε $O(\log(q))$ πράξεις στο βήμα (1), $\lfloor n/q \rfloor + 1$ πράξεις στο βήμα (2) και το πολύ q πράξεις στο βήμα (3). Συνολικά έχουμε $O(q + n/q)$ πράξεις στην ομάδα. Έχουμε την ελευθερία να επιλέξουμε τον ακέραιο q στο διάστημα $(1, n)$. Το $q + n/q$ ελαχιστοποιείται για $q = \sqrt{n}$, οπότε επιλέγουμε $q = \lfloor \sqrt{n} \rfloor$ και έχουμε $O(\sqrt{n})$ βήματα.

3 Ο αλγόριθμος των Pohlig καιHellman

Ο στόχος του αλγορίθμου των Pohlig και Hellman δεν είναι ο (άμεσος) υπολογισμός του διακριτού λογαρίθμου, αλλά η αναγωγή του προβλήματος σε μικρότερα προβλήματα (διακριτού λογαρίθμου). Για την αναγωγή χρειαζόμαστε την παραγοντοποίηση του n, την οποία θα θεωρήσουμε δεδομένη.

Ας υποθέσουμε ότι $n = p_1^{e_1} \cdots p_k^{e_k}$ είναι η κανονική ανάλυση του n σε πρώτους. Ο διακριτός λογάριθμος x ορίζεται modulo n. Έαν καταφέρουμε να υπολογίσουμε a_i, $i = 1, \ldots, k$, τέτοια ώστε $x \equiv a_i \pmod{p_i^{e_i}}$, για $i = 1, \ldots, k$, τότε με το Κινέζικο Θέωρημα Υπολοίπων μπορούμε να υπολογίσουμε $0 \le a < n$ τέτοιο ώστε $x \equiv a \pmod{n}$, που είναι το ζητούμενο.

Παρατηρήστε ότι

$$y = g^x \ \Rightarrow \ y^{n/p_i^{e_i}} = g^{(n/p_i^{e_i})x},$$

όπου $\mathrm{ord}(g^{n/p_i^{e_i}}) = p_i^{e_i}$. Έχουμε ένα πρόβλημα διακριτού λογαρίθμου στην ομάδα $\langle g^{n/p_i^{e_i}} \rangle$. Αν το λύσουμε και υπολογίσουμε a_i τέτοιο ώστε $y^{n/p_i^{e_i}} = g^{(n/p_i^{e_i})a_i}$, τότε θα έχουμε $x \equiv a_i \pmod{p_i^{e_i}}$. Αυτό θα κάνουμε για κάθε $i = 1, \ldots, k$. Ο διακριτός λογάριθμος a_i μπορεί να υπολογιστεί με $O(\sqrt{p_i^{e_i}})$ πράξεις στην ομάδα χρησιμοποιώντας τον αλγόριθμο Baby-step/Giant-step. Στη συνέχεια θα δούμε πώς μπορούμε να βελτιώσουμε αυτό το χρόνο σε $O(e_i \sqrt{p_i})$.

Έστω ότι έχουμε ένα πρόβλημα διακριτού λογαρίθμου $y = g^x$, με $\mathrm{ord}(g) = p^e$. Η μικρότερη, μη τετριμμένη υποομάδα της $\langle g \rangle$ είναι η $\langle g^{p^{e-1}} \rangle$, τάξης p. Στόχος μας είναι να υπολογίσουμε διακριτούς λογαρίθμου μόνο σε αυτή την υποομάδα. Η ιδέα είναι να γράψουμε το x στη βάση p. Γενικά θα έχουμε

$$x = x_0 + x_1 p + \cdots x_{e-1} p^{e-1}, \quad \text{με} \quad x_i \in \{0, \ldots, p-1\}.$$

Έχουμε $y = g^{x_0 + x_1 p + \cdots x_{e-1} p^{e-1}}$. Για να υπολογίσουμε το x_0 υψώνουμε στη δύναμη p^{e-1} τα δύο μέλη και έχουμε

$$h_0 = y^{p^{e-1}} = g_o^{x_0},$$

όπου $g_o = g^{p^{e-1}}$. Λύνουμε το πρόβλημα διακριτού λογαρίθμου στην $\langle g_o \rangle$ και υπολογίζουμε το x_0. Στη συνέχεια έχουμε

$$h_1 = (y g^{-x_0})^{p^{e-2}} = g_o^{x_1}$$

και υπολογίζουμε το x_1 βρίσκοντας το διακριτό λογάριθμο του h_1 ως προς τη βάση g_o. Έχοντας υπολογίσει τα $x_0, \ldots, x_{i-1}$, έχουμε

$$h_i = (y g^{-(x_0 + \ldots + p^{i-i} x_{i-1})})^{p^{e-i-1}} = g_o^{x_i}$$

και υπολογίζουμε το x_i ως το διακριτό λογάριθμο του h_i ως προς τη βάση g_o. Βλέπουμε ότι χρειαζόμαστε $O(\sqrt{p_i})$ πράξεις στην ομάδα για τον υπολογισμό κάθε ψηφίου και έχουμε e ψηφία, άρα συνολικά $(e\sqrt{p})$ πράξεις στην ομάδα.

Συνολικά, εάν $n = p_1^{e_1} \cdots p_k^{e_k}$, και $p = \max\{p_1, \ldots, p_k\}$, έχουμε χρόνο

$$O\left(\sum_{i=1}^{k} e_i \sqrt{p_i} \right) = O\left(\sqrt{p} \sum_{i=1}^{k} e_i \right) = O(\sqrt{p} \log(n)).$$

Παράδειγμα (Pohlig-Hellman) Ας δούμε ένα παράδειγμα υπολογισμού διακριτού λογαρίθμου με τη μέθοδο Pohlig-Hellman. Η ομάδα μας είναι η $\mathbb{F}_{29}^*$ και μας δίνονται τα $y = 10$ και $g = 3$. Βλέπουμε ότι η τάξη του στοιχείου g είναι $n = 29 - 1 = 28 = 2^2 \cdot 7$, δηλαδή $\langle g \rangle = \mathbb{F}_{29}^*$. Θέλουμε να υπολογίσουμε $0 \le x \le 28$ τέτοιο ώστε $y = g^x$ δηλαδή $10 \equiv 3^x \pmod{29}$. Το x υπολογίζεται modulo 28.

Σύμφωνα με τον αλγόριθμο θα υπολογίσω a και b τέτοια ώστε

$$\begin{aligned} x &\equiv a \pmod{2^2} \\ x &\equiv b \pmod{7}. \end{aligned}$$

Θα υπολογίσω αρχικά το a. Έχουμε

$$y^{n/4} = g^{(n/4)x} \ \Rightarrow \ 10^7 \equiv 3^{7x} \pmod{29} \ \Rightarrow \ 17 \equiv 12^x \pmod{29}.$$

Θα υπολογίσουμε το a ως το διακριτό λογάριθμο του 17 ως προς τη βάση 12 (modulo 29). Το γράφω σε βάση 2, $a = a_0 + 2a_1$, με $0 \le a_0, a_1 \le 1$. Έχουμε

$$17 \equiv 12^{a_0 + 2a_1} \pmod{29}.$$

Για το a_0 υπολογίζω:

$$17 \equiv 12^{a_0 + 2a_1} \pmod{29} \ \Rightarrow \ 17^2 \equiv 12^{2a_0} \equiv 28 \mod 29 \ \Rightarrow \ 28 \equiv 28^{a_0} \pmod{29},$$

οπότε $a_0 = 1$. Συνεχίζουμε,

$$17 \equiv 12^{1+2a_1} \pmod{29} \;\Rightarrow\; 17 \cdot 12^{-1} \equiv 12^{2a_1} \pmod{29} \;\Rightarrow\; 28 \equiv 28^{a_1} \pmod{29}.$$

οπότε $a_1 = 1$. Έτσι έχουμε $a = 1 + 1 \cdot 2 = 3$.

Προχωρούμε στον υπολογισμό του b. Καθώς το 7 εμφανίζεται στη δύναμη 1 στην κανονική ανάλυση του $n = 28$ σε πρώτους, έχουμε να υπολογίσουμε ένα μόνο ψηφίο, το ίδιο το b. Έχουμε

$$y^{n/7} = g^{(n/7)x} \;\Rightarrow\; 10^4 \equiv 3^{4x} \pmod{29} \;\Rightarrow\; 24 \equiv 23^x \pmod{29}.$$

Θα υπολογίσουμε το b ως το διακριτό λογάριθμο του 24 ως προς τη βάση 23 (modulo 29). Για το διακριτό λογάριθμο $24 \equiv 23^b \pmod{29}$ μπορούμε να χρησιμοποιήσουμε το αλγόριθμο Baby-step/Giant-step και βρίσκουμε $b = 6$.

Έτσι έχουμε να λύσουμε το σύστημα

$$\begin{aligned} x &\equiv 3 \pmod{4} \\ x &\equiv 6 \pmod{7}. \end{aligned}$$

Η λύση του συστήματος είναι $x \equiv 3 \cdot 7 \cdot s + 6 \cdot 4 \cdot t \pmod{28}$, όπου $s \equiv 7^{-1} \pmod{4}$ και $t \equiv 4^{-1} \pmod{7}$. Με τον επεκτεταμένο Ευκλείδιο αλγόριθμο υπολογίσουμε $s = 3$ και $t = 2$. Οπότε $x \equiv 3 \cdot 7 \cdot 3 + 6 \cdot 4 \cdot 2 \equiv 27 \pmod{28}$.