Εθνικό Μετσόβιο Πολυτεχνείο

Σχολή Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών

Σημειώσεις Διαλέξεων

Στοιχεία Θεωρίας Αριθμών

&

Εφαρμογές στην Κρυπτογραφία

Επιμέλεια σημειώσεων:
Ελένη Πύλια
Κατερίνα Σωτηράκη

Διδάσκοντες:
Στάθης Ζάχος
Άρης Παγουρτζής

7 Δεκεμβρίου 2012

1 Διακριτός λογάριθμος στο $\mathbb{Z}_p^*$, p πρώτος , $p = 2^m + 1$ (Sophie Germain Primes)

Γνωρίζουμε g γεννήτορα της $\mathbb{Z}_p^*$.
Δίνεται $a \in \mathbb{Z}_p^*$ και ζητείται $x \in [0, ..., p-1)$, τέτοιο ώστε: $g^x \equiv a \bmod p$ ($x \in [0, ..., p-1)$ άρα $0 \leq x < 2^m$).

ΛΥΣΗ

Μπορούμε σε κάθε περίπτωση να υπολογίσουμε το τελευταίο bit του x.
Ισχύει ότι $x = 2k$ ή $x = 2k+1$, άρα $a \equiv g^{2k}$ ή $a \equiv g^{2k+1} \equiv g^{2k} g$.
Επίσης, για κάθε p πρώτο ισχύει ότι $g^{\frac{p-1}{2}} \equiv -1 \bmod p$.
Επομένως, υψώνοντας το a στο μισό της τάξης της ομάδας, προκύπτει:

$$a^{\frac{p-1}{2}} \equiv \begin{cases} 1, & \text{αν } x = 2k \\ -1, & \text{αν } x = 2k+1 \end{cases}$$

Αν ο x είναι περιττός, θέλουμε $a_1 \equiv g^{2k}$, οπότε $a_1 \equiv a g^{-1} \equiv g^{2k} \bmod p$.
Αν ο x είναι άρτιος,τότε $a_1 \equiv a \equiv g^{2k} \equiv (g^2)^k$.
Συνεχίζουμε αναδρομικά με εύρεση διακριτού λογαρίθμου στην ομάδα $< g^2 >$ τάξης 2^{m-1}.
Έστω $k = 2\lambda + b_1, b_1 \in \{0, 1\}$.
Θέλουμε να βρούμε το τελευταίο ψηφίο του k.
$a_1 \equiv (g^2)^{2\lambda + b_1} \equiv (g^{2^2})^{\lambda} (g^2)^{b_1}$.
Υψώνοντας στο μισό της τάξης της ομάδας,προκύπτει:

$$a_1^{2^{m-2}} \equiv (g^{2^m})^{\lambda} (g^{2^{m-1}})^{b_1} \equiv (g^{2^{m-1}})^{b_1} \equiv \begin{cases} 1, & \text{αν } b_1 = 0 \\ -1, & \text{αν } b_1 = 1 \end{cases}$$

Αν $b_1 = 0$, τότε $a_2 \equiv a_1$.
Αν $b_1 = 1$, τότε $a_2 \equiv a_1 g^{-2} \bmod p$.

Παράδειγμα
Δίνεται $p = 17$ και γνωρίζουμε ότι το 7 είναι γεννήτορας της ομάδας $\mathbb{Z}_{17}^*$.
Να βρεθεί x, τέτοιο ώστε $7^x \equiv 13 \bmod 17$.

ΛΥΣΗ

Έστω ότι $x = b_3 2^3 + b_2 2^2 + b_1 2 + b_0$. Το μισό της τάξης της ομάδας είναι 8 και $a = 13$,επομένως:
$13^8 \equiv 1$,άρα $b_0 = 0$ και $a_1 \equiv 13$
$13^4 \equiv 1$,άρα $b_1 = 0$ και $a_2 \equiv 13$
$13^2 \equiv -1$,άρα $b_2 = 1$ και $a_3 \equiv 13 \cdot 7^{-4} \equiv 13 \cdot 13 \equiv -1$
Το τελευταίο ισχύει,επειδή $7^{b_3 2^3 + 2^2} \equiv 13 \bmod 17 \Rightarrow 7^{b_3 2^3} \equiv 13^2 \equiv -1 \bmod 17$.
Επίσης, ισχύει ότι $7^{-4} \equiv 5^4 \equiv 13$.

Επομένως, $b_3 = 1$.
Άρα, $x = 12 = (1100)_2$.
Πράγματι, $7^{12} \equiv (7^4)^3 \equiv 4^3 \equiv -4 \equiv 13 \bmod 17$.

Γενικά: Έστω ότι $x = b_{m-1}2^{m-1} + ... + b_1 2 + b_0$.
Θέτουμε $a_0 \equiv a$ και παίρνουμε το $a_0^{2^{m-1}}$.

αν $a_0^{2^{m-1}} \equiv 1 \Rightarrow b_0 = 0, a_1 \equiv a_0$

αν $a_0^{2^{m-1}} \equiv -1 \Rightarrow b_0 = 1, a_1 \equiv a_0 g^{-1}$

$\vdots$

αν $a_i^{2^{m-i-1}} \equiv 1 \Rightarrow b_i = 0, a_{i+1} \equiv a_i$

αν $a_i^{2^{m-i-1}} \equiv -1 \Rightarrow b_i = 1, a_{i+1} \equiv a_i g^{-2^i}$

Γενίκευση:
Στην περίπτωση που η τάξη της ομάδας είναι 3^m (δηλαδή $p = 3^m + 1$) τότε μπορούμε να κάνουμε κάτι ανάλογο με το προηγούμενο.
Έστω $g^x \equiv a \bmod p$ με $x = 3k + t_0, t_0 \in \{0, 1, 2\}$.
Αφού $3 \mid p - 1$, $(g^{\frac{p-1}{3}})^3 \equiv 1 \bmod p$ και
$a^{\frac{p-1}{3}} \equiv (g^{3k+t_0})^{\frac{p-1}{3}} \equiv g^{t_0 \frac{p-1}{3}} \bmod p$.
Άρα, αρκεί να υπολογίσουμε τα: $g^{\frac{p-1}{3}} \bmod p$ και $g^{2\frac{p-1}{3}} \bmod p$

2 Αλγόριθμος Pohlig-Hellman

Ιδέα: Έστω $p - 1 = \prod_i q_i^{e_i}$ και ψάχνω x τέτοιο ώστε $g^x \equiv b \bmod p$.

1. Υπολογίζω τα $x_{q_i} \equiv x \bmod q_i^{e_i}$ με $0 \leq x_{q_i} \leq q_i^{e_i} - 1$.
2. Κινέζικο Θεώρημα Υπολοίπων $\rightarrow$ Υπολογίζω το x.

Υπολογισμός των x_q με $q^e \mid p - 1, q^{e+1} \nmid p - 1$:
$x_q = \sum_{i=0}^{e-1} a_i q^i = a_0 + a_1 q + a_2 q^2 + ... + a_{e-1} q^{e-1}$
$x \equiv x_q \bmod q^e \Rightarrow x = x_q + sq^e = \sum_{i=0}^{e-1} a_i q^i + sq^e, s \in \mathbb{Z}$
Βήμα 1 (Υπολογισμός του a_0):
Ισχυρισμός: $b^{\frac{p-1}{q}} \equiv g^{a_0(\frac{p-1}{q})}$

ΑΠΟΔΕΙΞΗ

$b^{\frac{p-1}{q}} \equiv g^{x\frac{p-1}{q}} \equiv (g^{(a_0+a_1q+...+a_{e-1}q^{e-1}+sq^e)})^{\frac{p-1}{q}} \equiv g^{a_0(\frac{p-1}{q})}(g^{p-1})^{a_1+a_2q+...+sq^{e-1}} \equiv g^{a_0(\frac{p-1}{q})}$ επειδή $ord(g^{\frac{p-1}{q}}) = q$

Η $b^{\frac{p-1}{q}} \equiv g^{a_0(\frac{p-1}{q})}$ έχει μοναδική λύση $modulo\ p$.
Ελέγχω $k \in \{0, 1, ..., q-1\}$ τέτοιο ώστε $(g^{\frac{p-1}{q}})^k \equiv b^{\frac{p-1}{q}} \bmod p$, τότε $k = a_0$.

$\vdots$

Βήμα e (Υπολογισμός του a_{e-1}):
$b_{e-1} \equiv b_{e-2}g^{-a_{e-2}}q^{e-2}$ (με $b_0 \equiv b$).
Υψώνουμε $(b_{e-1})^{\frac{p-1}{q^e}} \equiv g^{a_{e-1}(\frac{p-1}{q})}$ και βρίσκουμε το a_{e-1}.
Με Shanks $O(\sqrt{q})$ ανά βήμα (ή κάνουμε q ελέγχους για το a_{e-1}).
Αυτό πρέπει να γίνει $\forall q_i \mid p-1, x_{q_i} \equiv x \bmod q_i^{e_i}$.
Αν $q = \max\{q_i : q_i \mid p-1, q_i$:πρώτος$\}$, πολυπλοκότητα: $O(q(\log_q p)) = \hat{O}(q)$.
Με Shanks: $\tilde{O}(\sqrt{q})$ χρόνος και $\tilde{O}(\sqrt{q})$ χώρος