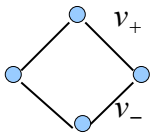
12. Hierarchia modularna

$G=(V,E)$ – graf skierowany
P,Q,R – parami rozłącznie zbiory liczb pierwszych (nieskończone),
oraz takie że:
$P \cap Q = \emptyset$, $P \cap R = \emptyset$, $Q \cap R = \emptyset$

P - aspekt – odpowiedzialny zasadniczo za bezpieczne usuwanie wierzchołków grafu
Q – aspekt – zasadniczo odpowiedzialny za dodawanie nowych wierzchołków do grafu

Załóżmy dla uproszczenia, że V jest grafem takim że:
$v_- \leqslant v \leqslant v_+$

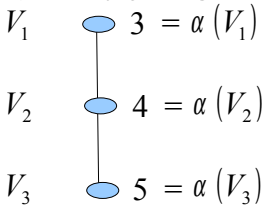
Na rysunku można to przedstawić w następujący sposób:



P - aspekt
$\forall p \in P$ rozważmy funkcje $\alpha_p : V \to N_0$ (N_0 - zbiór liczb całkowitych nieujemnych), która spełnia następujące warunki:
1) $v_1 \leq v_2 \Rightarrow \alpha_p(v_1) \geqslant \alpha_p(v_2)$
2) min $\alpha_p(v) > \alpha_p(v_-) - \alpha_p(v_+)$, przy założeniu że $v_- \leqslant v \leqslant v_+$

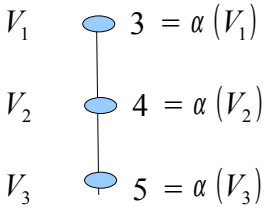
<u>Przykład</u>

1) Dany jest graf $G(V, E)$, należy sprawdzić czy spełnione są warunki 1) i 2)



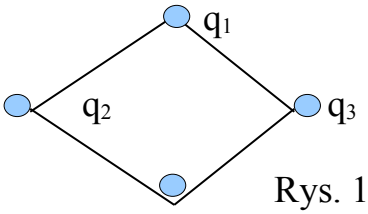
Pierwszy warunek jest spełniony (1 < 2 < 3) natomiast 2) już nie gdyż 1 < 3 – 1 = 2.

2) Dany jest graf *G(E,V)*, należy sprawdzić czy spełnione są warunki arytmetyki modularnej.

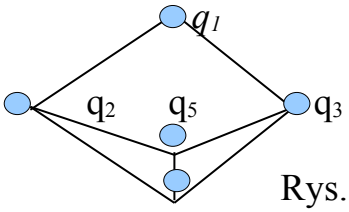


W tym grafie pierwszy warunek jest spełniony (3 < 4 < 5), jak i również warunek drugi (4 > 5 – 3 = 2)

12.1 Q – aspekt (odpowiedzialny za dodawanie wierzchołków)



Rys. 1



Rys. 2

Rysunek nr 1 to hierarchia przed dodaniem nowego wierzchołka:

$Q_1 = q_1\ q_2\ q_3\ q_4$

$Q_2 = q_2\ q_4$

$Q_3 = q_3\ q_4$

$Q_4 = q_4$

Następnie dodajemy nowy wierzchołek:

$q_5 \in Q \setminus \{ q_1, q_2, q_3, q_4 \}$

Rysunek 2 przedstawia hierarchię z nowym wierzchołkiem:

$Q_1 = q_1\ q_2\ q_3\ q_4\ q_5$

$Q_2 = q_2\ q_4\ q_5$

$Q_3 = q_3\ q_4\ q_5$

$Q_4 = q_4$

$Q_5 = q_5\ q_4$

12.2 Dodawanie nowych wierzchołków – dzielenie funkcji dostępu

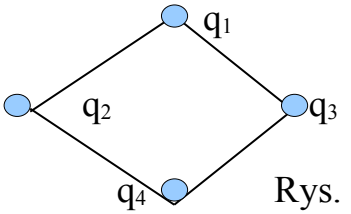
Załóżmy, że dodajemy nowy wierzchołek $v_0 \in V$, wtedy przypisujemy mu liczbę pierwszą $q_0 \in V$ i definiujemy rozszerzenie :

$$\tilde{f} : V \cup v_0 \Rightarrow Q$$

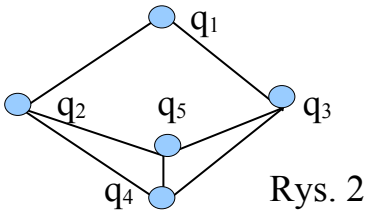
$$\tilde{Q}(v) = \begin{cases} Q(x)\ jeśli\ v \geq v_0 \\ q_0 Q(v)\ jeśli\ v \leq v_0 \end{cases}$$

$$\tilde{a}(x) = \frac{P(v)}{\tilde{Q}(v)} \quad mod\ m$$

Przykład:



Rys. 1



Rys. 2

$Q(v_1) = q_1\ q_2\ q_3\ q_4$

$Q(v_2) = q_2\ q_4$

$Q(v_3) = q_3\ q_4$

$Q(v_4) = q_4$

$\tilde{Q}(v_5) = q_4 q_5$

$\tilde{Q}(v_4) = q_4$

$\tilde{Q}(v_3) = q_3 q_4 q_5$

$\tilde{Q}(v_2) = q_2 q_4 q_5$

$\tilde{Q}(v_1) = q_1 q_2 q_3 q_4 q_5$

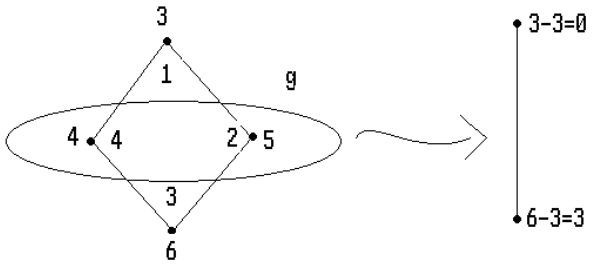
12.3 Usuwanie wierzchołków i określenie k(v)

Niech . $V(G) = \{w : v_- \leq w : v_+\}, S = \{v_1, v_2, \ldots, v_r\} \subset V$ Mamy $\alpha = \alpha_p\ (p \in P)$ i definiujemy $\delta = \delta(S) = \alpha_p(v_-) - \min_{v \in S} \alpha_p(v_+) + 1$

Nowe funkcje :

$$\tilde{\alpha}_p : V \setminus S \to \mathbb{N}_0$$
$$\tilde{\alpha}_p = \alpha_p - \delta$$

Przykład:



Definicja Klucz w hierarchii:

Wartość klucza dla wierzchołka *v* wynosi $k(v) = \gamma^{a(v)} \pmod m$ gdzie $m = \lambda(n)$, natomiast γ jest elementem rzędu $\lambda(n)$ w grupie Z_n^* .

$$a(v) = \frac{P(v)}{Q(v)} \pmod m$$

12.4 P –aspekt (odpowiedzialny za usuwanie wierzchołków)

Budujemy funkcję $\alpha_p : V \to N_0$ ($p \in P$), taką że

1) $v \geqslant w \Rightarrow \alpha(v) \leqslant \alpha(w)$
2) Dla dowolnego podgrafu $G' \subset G$, $V' \subset V$,
   takiego że $V' = \{w : v_- \leqslant w \leqslant v_+\}$ zachodzi warunek $2\alpha(v_-) > \alpha(v_+)$

W praktyce warunek 2) będziemy zastępować warunkiem 2')

2') $min\ \alpha_p(v) > \alpha_p(v_-) - \alpha_p(v_+)$

Jeżeli ścieżka ma długość *N* to możemy definiować:

$\alpha(v_+) = N + 1$

$\alpha(v_-) = 2N$

$2\alpha(v_+) = 2N + 2 > 2N$

Funkcje dostępu wyglądają następująco:

$k(v) = q^{a(v)} \pmod n$

$a(v) = P(v) / Q(v)$

$P(v) = P^{\alpha p(v)}$

teraz:

$a(v_1) = P(v_1) / Q(v_1) = P^3 / q_1q_2q_3q_4$

$a(v_2) = P^4 / q_2q_4$

$a(v_3) = P^5 / q_3q_4$

$a(v_4) = P(v_4) / Q(v_4) = P^6 / q_4$

$k(v_2) = (k(v_1))^{pq_1q_3}$

Przykład

Wyrazić przez potęgowanie klucz k_4 za pomocą kluczy k_1, k_2, k_3.

Rozwiązanie:

$$k(v_4)=(k(v_3))^{pq_3}$$
$$k(v_4)=(k(v_2))^{p^2q_2}$$
$$k(v_4)=(k(v_1))^{p^3q_1q_2q_3}$$

Przykład

$n = p*q \quad p-1 = 2q' \qquad (p,q,p',q' - \text{liczby pierwsze} \in R)$

$n = \lambda(n) = NWW(p-1,q-1) = NWW(2p',2q') = 2p'q' = \frac{\varphi(n)}{2}$

γ - element rzędu $\frac{\varphi(n)}{2}$,

$k(v)=\gamma^v \pmod n$

Obliczanie funkcji Eulera

$\phi(p)=p-1$

$\tilde{\phi}(p)=p^{\alpha-1}(p-1)$

$\phi(p,q^0)=p^{\alpha-1}(p+1)q^{\beta-1}(q-1)=\phi(p^\alpha)\phi(q^\beta)$

$\phi(p^\alpha,q^\beta)=p^{\alpha-1}(p-1)+q^{\beta-1}(q-1)=\phi(p^\alpha)\phi(q^\beta)$

Przykład

N=pq=3*11

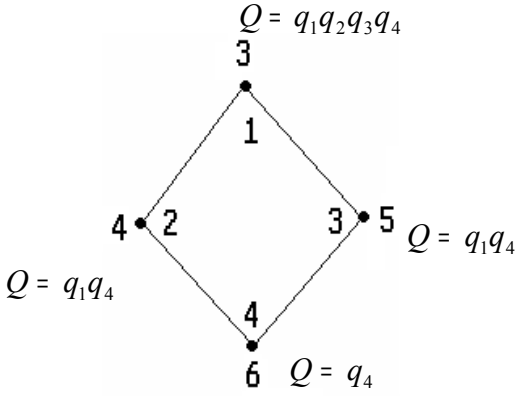
p-1=2=2*1=2p`

q-1=11=11-1=10=2*5=2q`

$$\varphi(n) = \varphi(pq) = \varphi(p)\cdot\varphi(q) = (p-1)(q-1) = 20$$
$$m = \lambda(n) = \frac{\phi(n)}{2} = \frac{20}{2} = 10$$

γ jest elementem rzędu 10 w grupie Z_{33}^{*}

Przykład: Obliczanie kluczy w hierarchii



$$P(v) = p^{\alpha_p(v)} \qquad (p=7)$$
$$k(v) = \gamma^{\frac{P(v)}{Q(v)}} = \gamma^{\frac{p^{\alpha_p(v)}}{Q(v)}}$$
$$k(v_1) = \gamma^{\frac{P(v)}{Q(v)}} = \gamma^{\frac{7^3}{q_1 q_2 q_3 q_4}}$$
$$k(v_2) = \gamma^{\frac{7^4}{q_2 q_4}}$$
$$k(v_3) = \gamma^{\frac{7^5}{q_3 q_4}}$$
$$k(v_4) = \gamma^{\frac{7^6}{q_4}}$$

13. Hierarchia potęgowa

Problem I (logarytmu dyskretnego dla G)

Dana jest multiplikatywna grupa G i generator g ∈ G oraz
A ∈ G. Znaleźć (o ile istnieje) wartość $\log_g(A)=x : g^x = A\,(w\,grupie\,G)$.

Problem II

Niech $s=\{k_1, k_2, ..., k_r\}\setminus\{k_j\},\ j\in r \quad x=x_1\,x_2\,...\,x_r$
Dane: $g^{x/x_j},\ j=1,2,...r\,(w\,grupie\,G)$
Szukamy: g^x

Problem obliczenia g^x na podstawie g^{x/x_j} jest obliczeniem trudnym – decyzyjny problem D-H (Diffie-Hellmana).

Przykład:

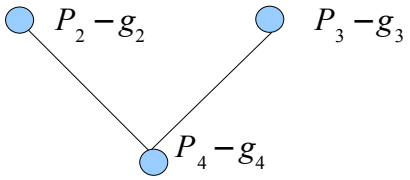
$r=2,\ x=x_1\,x_2,\ x_i\in N,\ G=Z_p^*$
Dane: $g^{x/x_1}=g^{x_2}\ oraz\ g^{x/x_2}=g^{x_1}(mod\ p)$
problem D-H to obliczenie $g^x=g^{x_1 x_2}(mod\ p)$
$[(g^{x_1})^{x_2}=(g^{x_2})^{x_1}]$ czyli trzeba obliczyć $\log x_1\ lub \log x_2$

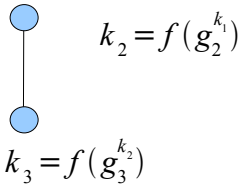
13.1 Diagram Hasse

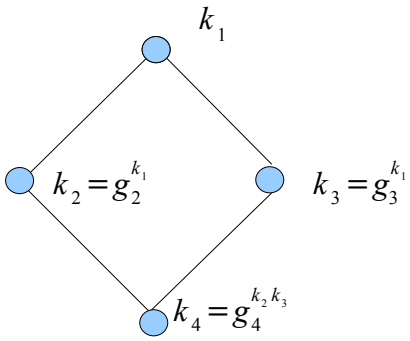
Funkcja pomocnicza: $f : G\to\{1,2,..,q\}$
G – podgrupa Z_p^* rzędu q $(q=\frac{p-1}{2})$

$$f(x)=\begin{cases} x\ jeśli\ 1\leqslant x\leqslant q \\ p-x\ jeśli\ x>q \end{cases}$$

Parametry systemu g_i – dowolny generator grupy G (odpowiadający graczowi P_i).







$K_4 = [g_4^{k_2}, g_4^{k_3}]$ P_2 *oblicza* $k_4 : (g_4^{k_3})^{k_2} = g_4^{k_2 k_3} = k_4$

13.2 Faza generacji kluczy

Algorytm

1. P_i losuje g_i – generator G
2. Jeśli P_i nie ma rodzica to k_i – losowe z przedziału {1, 2, ..., q}
3. Jeśli ma dokładnie jednego rodzica P_j , to
   $k_i = f(g_i^{k_j})$
4. Jeśli $P_{j1} \ldots P_{jn}$ są rodzicami P_i to:
   $k_i = f(g_i^{k_{j1} k_{j2} \ldots k_{jr}}) - klucz\ prywatny$
   $K_i = [h_{ij1}, h_{ij2}, \ldots, h_{ijr}] - klucz\ publiczny$

13.*3 Faza obliczania kluczy*

Jeśli P_i ma dokładnie jednego rodzica P_j to $f(g_i^{k_j})$
w przeciwnym wypadku wybieramy jako P_j dowolnego rodzica i :

$k_i = f(h_{ij}^{k_j})$

13.4 Złożoność obliczeniowa

Potęgowanie modularne

$(a, b) \rightarrow a^b \bmod n \qquad a, b \leqslant n$

zapisujemy b dwójkowo

$$c = c_0 * 2^0 + c_1 * 2^1 + ... + c_k * 2^k$$

$$k \leqslant \log_2 n$$

$$a^b = (a^{2^0})^{c_0} * (a^{2^1})^{c_1} * ... * (a^{2^k})^{c_k} (mod\ n)$$

$(a^{2^k}) = (a^{2^{k-1}})^2$ – *więc obliczenie* a^b *sprowadza się do co najwyżej* k *podnoszeń do kwadratu*

Jeśli przez M oznaczymy operację mnożenia, a P podniesienie do kwadratu modulo n, to ostatecznie mamy:

koszt $a^b (mod\ n) \leqslant kM + kP \leqslant (\log_2 n) M + (\log_2 n) P$