Problém DL v Z_n^*

1. Z_n^* je cyklická práve vtedy, keď $n = 2, 4, p^k, 2p^k$, kde p je nepárne prvočíslo a $k \geq 1$.

Problém DL v Z_n^*

1. Z_n^* je cyklická práve vtedy, keď $n = 2, 4, p^k, 2p^k$, kde p je nepárne prvočíslo a $k \geq 1$.
2. Nech $a \in Z_n^*$ je generátor potom $b = a^i \bmod n$ je generátor práve vtedy, keď $\gcd(i, \varphi(n)) = 1$. Z toho vyplýva, ak Z_n^* je cyklická grupa, tak počet jej generátorov je $\varphi(\varphi(n))$.

Problém DL v Z_n^*

1. Z_n^* je cyklická práve vtedy, keď $n = 2, 4, p^k, 2p^k$, kde p je nepárne prvočíslo a $k \geq 1$.
2. Nech $a \in Z_n^*$ je generátor potom $b = a^i \bmod n$ je generátor práve vtedy, keď $\gcd(i, \varphi(n)) = 1$. Z toho vyplýva, ak Z_n^* je cyklická grupa, tak počet jej generátorov je $\varphi(\varphi(n))$.
3. Platí $\frac{\varphi(n)}{n} \approx \frac{6}{\pi^2} \approx 0,608$ a generátor je jeden z $\varphi(n) - 1$ prvkov

$$\frac{\varphi(n)}{n} \approx \frac{\varphi(\varphi(n))}{\varphi(n)} \approx \frac{\varphi(\varphi(n))}{\varphi(n) - 1} \approx 0,608.$$

Problém DL v Z_n^*

1. Z_n^* je cyklická práve vtedy, keď $n = 2, 4, p^k, 2p^k$, kde p je nepárne prvočíslo a $k \geq 1$.
2. Nech $a \in Z_n^*$ je generátor potom $b = a^i \bmod n$ je generátor práve vtedy, keď $\gcd(i, \varphi(n)) = 1$. Z toho vyplýva, ak Z_n^* je cyklická grupa, tak počet jej generátorov je $\varphi(\varphi(n))$.
3. Platí $\frac{\varphi(n)}{n} \approx \frac{6}{\pi^2} \approx 0,608$ a generátor je jeden z $\varphi(n) - 1$ prvkov

$$\frac{\varphi(n)}{n} \approx \frac{\varphi(\varphi(n))}{\varphi(n)} \approx \frac{\varphi(\varphi(n))}{\varphi(n) - 1} \approx 0,608.$$

4. Ak n je prvočíslo a existuje prvočíslo p také, že $n = 2p + 1$, tak $\frac{\varphi(\varphi(n))}{\varphi(n)-1} = \frac{\varphi(n-1)}{n-2} = \frac{p-1}{2p-1} \approx 0,5$.

Problém diskrétneho logaritmu:

Nech a je generátor Z_n^* a $c \in Z_n{}^*$. Treba nájsť číslo b také, že $0 \leq b \leq \varphi(n) - 1$ a

$$a^b = c \bmod n.$$

Označujeme $b = \log_{a,n} c$.

Problém diskrétneho logaritmu:

Nech a je generátor Z_n^* a $c \in Z_n{}^*$. Treba nájsť číslo b také, že $0 \leq b \leq \varphi(n) - 1$ a

$$a^b = c \bmod n.$$

Označujeme $b = \log_{a,n} c$.

1. $c = a^{\log_{a,n} c} \bmod n.$
2. $\log_{a,n} 1 = 0 \bmod \varphi(n).$
3. $\log_{a,n} a = 1 \bmod \varphi(n).$
4. $\log_{a,n} xy = \log_{a,n} x + \log_{a,n} y \bmod \varphi(n).$
5. $\log_{a,n} c^r = r.\log_{a,n} c \bmod \varphi(n).$

Aby sa predišlo známym útokom, ktoré riešia problém diskrétneho logaritmu, n by malo byť aspoň 150-ciferné a $n-1$ by malo mať aspoň jeden "veľký"prvočíselný faktor. V súčasnosti najrýchlejšie algoritmy pre výpočet diskrétneho logaritmu udávajú pre prvočíslo p časovú zložitosť ohraničenú hodnotou

$$\mathcal{O}(e^{((\ln p)^{1/3}\ln(\ln p))^{2/3}}).$$

V prípade, že n je ľubovolné číslo, tak udávaná časová zložitosť je ohraničená číslom

$$\mathcal{O}(e^{\sqrt{(\ln n)(\ln(\ln n))}}).$$

Ak n je 200–bitové číslo, hodnota v zátvorke dosahuje $2,7 \times 10^{11}$. Ak n je 664-bitové číslo, tak $1,2 \times 10^{23}$. V prípade, že $p-1$ sa dá faktorizovať na malé faktory, existuje Pohling -Hellmanov algoritmus.

ElGamalov kryptosystém

Je to nedeterministický krytosystém, lebo zašifrovaný text závisí od pôvodného textu x a aj hodnoty náhodne generovného kľúča k.

1. $\mathcal{P} = Z_p^*$ je množina OT a

ElGamalov kryptosystém

Je to nedeterministický krytosystém, lebo zašifrovaný text závisí od pôvodného textu x a aj hodnoty náhodne generovného kľúča k.

1. $\mathcal{P} = Z_p^*$ je množina OT a
2. $\mathcal{C} = Z_p^* \times Z_p^*$ je množina ZT

ElGamalov kryptosystém

Je to nedeterministický krytosystém, lebo zašifrovaný text závisí od pôvodného textu x a aj hodnoty náhodne generovného kľúča k.

1. $\mathcal{P} = Z_p^*$ je množina OT a
2. $\mathcal{C} = Z_p^* \times Z_p^*$ je množina ZT
3. $\mathcal{K} = \{(p, a, b, c) \mid c = a^b \bmod p\}$, a je generátor

ElGamalov kryptosystém

Je to nedeterministický krytosystém, lebo zašifrovaný text závisí od pôvodného textu x a aj hodnoty náhodne generovného kľúča k.

1. $\mathcal{P} = Z_p^*$ je množina OT a
2. $\mathcal{C} = Z_p^* \times Z_p^*$ je množina ZT
3. $\mathcal{K} = \{(p, a, b, c) \mid c = a^b \bmod p\}$, a je generátor
4. Hodnoty p, a, c sú verejné a b je tajné

Šifrovanie:

$$e_K(x, k) = (y_1, y_2) \in Z_p^* \times Z_p^*,$$

kde

$$y_1 = a^k \bmod p \quad y_2 = xc^k \bmod p.$$

Šifrovanie:

$$e_K(x, k) = (y_1, y_2) \in Z_p^* \times Z_p^*,$$

kde

$$y_1 = a^k \bmod p \quad y_2 = xc^k \bmod p.$$

Dešifrovanie:

$$d_K(y_1, y_2) = y_2({y_1}^b)^{-1} \bmod p = x.$$

Prílad: tajné $b = 765$, verejné $p = 2579$, $a = 2$,
$c = 2^{765} \bmod p = 949$.
Alica chce poslať správu $x = 1299$ *Bobovi*.
Zvolí $k = 853$ a počíta $y_1 = 2^{853} \bmod 2579 = 435$, a
$y_2 = 1299 \times 949^{853} \bmod 2579 = 2396$.

Prílad: tajné $b = 765$, verejné $p = 2579$, $a = 2$,
$c = 2^{765} \bmod p = 949$.
Alica chce poslať správu $x = 1299$ *Bobovi*.
Zvolí $k = 853$ a počíta $y_1 = 2^{853} \bmod 2579 = 435$, a
$y_2 = 1299 \times 949^{853} \bmod 2579 = 2396$.
Bob obdrží $(y_1, y_2) = (435, 2396)$ a počíta
$(435^{765})^{-1} \bmod 2579 = 1980$, a potom
$x = 2396 \times 1980 \bmod 2579 = 1299$.

Tento postup je možné zovšeobecniť pre ľubovoľné prvočíslo p, ako aj pre ľubovoľnú cyklickú (pod)grupu G s generátorom α. Podstatné je, aby bol problém nájdenia diskrétneho logaritmu v tejto grupe nezvládnuteľný v reálnom čase. Pre praktické potreby sa uvažujú dve triedy grúp:

1. Multiplikatívna grupa poľa $GF(p^n)$. Ak $p = 2$ potom $2^n - 1$ musí mať aspoň jeden veľký prvočíselný deliteľ. Boli realizované čípy pre $n = 593, 1186$.
2. Grupa generovaná eliptickou krivkou nad konečním poľom. Boli realizované čípy pre $GF(2^{155})$. Zaberajú menej ako 4% z $20mm^2$ rezervovaních na inteligentních kartách.

Pre porovnanie RSA-číp zaberá 20%.

D-H protokol na výmenu kľúča

Diffie–Hellmanova schéma bol prvý prakticky upotrebiteľný protokol na výmenu kľúčov pre *Alicu* a *Boba* (banku). Ďalšie sú napr. ElGamalova schéma, resp. systémy na báze eliptických kriviek. Všetky tieto schémy sú výpočtovo veľmi náročné.

D-H protokol na výmenu kľúča

Diffie–Hellmanova schéma bol prvý prakticky upotrebiteľný protokol na výmenu kľúčov pre *Alicu* a *Boba* (banku). Ďalšie sú napr. ElGamalova schéma, resp. systémy na báze eliptických kriviek. Všetky tieto schémy sú výpočtovo veľmi náročné.

Základná verzia DH protokolu.

Alica a *Bob* sa dohodnú na veľkom prvočísle p a čísle a takom, že a je primitívny prvok podľa modulu p. Čísla p a a nemusia byť tajné. *Alica* a *Bob* sa môžu na nich dohodnúť prostredníctvom verejného informačného kanála. Tieto čísla môžu byť dokonca spoločné pre celú väčšiu skupinu používateľov. Protokol má nasledujúci tvar:

1. *Alica* vyberie náhodným spôsobom veľké číslo x a na adresu *Bob* odošle číslo
$$X = a^x \bmod p.$$
2. *Bob* vyberie náhodným spôsobom veľké číslo y a na adresu *Alica* odošle číslo
$$Y = a^y \bmod p.$$
3. *Alica* počíta
$$k = Y^x = a^{yx} \bmod p.$$
4. *Bob* počíta
$$k' = X^y = a^{xy} \bmod p.$$

Je zrejmé, že $k = k'$. Toto číslo je šifrovacím kľúčom, ktorý je známy len *Alici* a *Bobovi*. Každý iný pozorovateľ pozná len hodnoty p, a, X, Y. Bez toho, aby vypočítal diskrétne logaritmy x a y, nie je schopný nájsť k.

DL problém: či je určenie g^{ab} zo znalosti g, g^a a g^b rovnako ťažký problém, ako je problém diskrétneho logaritmu vo všeobecnosti.

DL problém: či je určenie g^{ab} zo znalosti g, g^a a g^b rovnako ťažký problém, ako je problém diskrétneho logaritmu vo všeobecnosti.

Na diskrétnom umocňovaní je založený aj U.S. Digital Signature Algorithm – DSA. V ňom je generovanie verejného kľúča Y tiež založené na obtiažnosti riešenia problému diskrétneho logaritmu. Uvažuje sa o konečnej grupe G a jej prvku g rádu q. Pre podpisovanie je vygenerovaný tajný kľúč X taký, že $0 < X < q$, pričom $\gcd(X, q) = 1$. Ku X vypočítame $Y = g^X$.

Eliptické krivky

Nech $p > 3$ je prvočíslo. Eliptická krivka E nad Z_p je množina riešení $(x, y) \in Z_p \times Z_p$ kongruencie

$$y^2 = x^3 + ax + b \pmod{p},$$

kde $a, b \in Z_p$ sú konštanty spĺňujúce podmienku $\Delta = 4a^3 + 27b^2 \neq 0 \bmod p$, spolu s adjungovaným bodom $\mathcal{O}$ v nekonečne.

Eliptické krivky

Nech $p > 3$ je prvočíslo. Eliptická krivka E nad Z_p je množina riešení $(x, y) \in Z_p \times Z_p$ kongruencie

$$y^2 = x^3 + ax + b \pmod{p},$$

kde $a, b \in Z_p$ sú konštanty splňujúce podmienku $\Delta = 4a^3 + 27b^2 \neq 0 \bmod p$, spolu s adjungovaným bodom $\mathcal{O}$ v nekonečne.

Podmienka $\Delta \neq 0 \bmod p$ zaručuje, že neexistujú viacnásobné riešenia. Dostaneme ju výpočtom

$$\gcd(y^2, (y^2)') = \gcd(x^3 + ax + b, 3x^2 + a) = \frac{\Delta}{27b}.$$

Na množine bodov $P, Q \in E$ eliptickej krivky definujeme súčet takto:

- $\mathcal{O} + P = P + \mathcal{O} = P$
- Ak $P = (x_1, y_1) \neq \mathcal{O}$, potom $-P = (x_1, -y_1)$ a $P + (-P) = \mathcal{O}$. Teda P a $-P$ sú jediné body E s rovnakou x-ovou súradnicou.

- Ak $P \neq \mathcal{O}, Q \neq \mathcal{O}, Q \neq -P$, potom označme $R = (x_3, y_3)$ bod symetrický podľa osi x s "priesečníkom priamky"PQ s E. Ak $P \neq Q$, resp. bod symetrický podľa osi x s "priesečníkom dotyčnice"v bode P s E ak $P = Q$. Definujme $R = P + Q$:

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda(x_1 - x_3) - y_1$$

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & \text{ak } P \neq Q \\ \frac{3x_1^2 + a}{2y_1}, & \text{ak } P = Q \end{cases}$$

Štruktúra $(E, +)$ je abelovská grupa. Počet jej prvkov je daný Hasseho odhadom

$$p + 1 - 2\sqrt{p} \leq |E| \leq p + 1 + 2\sqrt{p}.$$

Nech $E = \{(x, y) |\ \ y^2 = x^3 + x + 6, \ \ x, y \in Z_{11}\}$. Potom body a príslušné násobenie je dané tabuľkou:

(2,7)	(3,5)	(3,6)	(5,2)	(5,9)	(7,2)	(7,9)	(8,3)	(8,8)
$\mathcal{O}$	(7,2)	(10,2)	(2,7)	(8,8)	(7,9)	(3,6)	(5,2)	(10,9)
(5,2)	(10,9)	(7,9)	(8,3)	(2,4)	(3,5)	(7,2)	(10,2)	(5,9)
(10,9)	(8,3)	$\mathcal{O}$	(8,8)	(7,9)	(5,2)	(2,7)	(5,9)	(3,6)
(7,9)	$\mathcal{O}$	(8,8)	(7,2)	(8,3)	(2,4)	(5,9)	(3,5)	(5,2)
(8,3)	(8,8)	(7,2)	(10,2)	$\mathcal{O}$	(10,9)	(3,5)	(3,6)	(2,4)
(2,4)	(7,9)	(8,3)	$\mathcal{O}$	(10,9)	(3,6)	(10,2)	(2,7)	(3,5)
(3,5)	(5,2)	(2,4)	(10,9)	(3,6)	(2,7)	$\mathcal{O}$	(8,8)	(10,2)

Za generátor grupy môžeme zvoliť napr. bod $P = (2, 7)$ ($|E| = 13$ je prvočíslo). Potom

$$\begin{array}{lllllllll} P & = & (2,7) & 2P & = & (5,2) & 3P & = & (8,3) \\ 4P & = & (10,2) & 5P & = & (3,6) & 6P & = & (7,9) \\ 7P & = & (7,2) & 8P & = & (3,5) & 9P & = & (10,9) \\ 10P & = & (8,8) & 11P & = & (5,9) & 12P & = & (2,4) \end{array}$$

Všetky singulárne eliptické krivky ($\Delta = 0$) nad Z_{11}, $E = \{(x, y) | \, y^2 = x^3 + ax + b, \, x, y \in Z_{11}\}$ dostaneme pre nasledovné hodnoty parametrov a, b:

a	2	6	7	8	10
b	$\pm$ 3	$\pm$ 1	$\pm$ 4	$\pm$ 2	$\pm$ 5

Ako nájsť body E ? Ak $p = 3 \bmod 4$, potom máme jednoduchý algoritmus:

FOR x FROM 1 TO $p-1$ DO
$z = x^3 + ax + b$
IF $\left(z^{\frac{p+1}{4}}\right)^2 = z \bmod p$ THEN $P = (x, \pm z^{\frac{p+1}{4}})$ "bod krivky"
OD;

Ak $|E|$ je prvočíslo, máme cyklickú grupu. Inak musíme nájsť vhodnú podgrupu podľa vety:
Nech E je eliptická krivka nad $Z_p, p > 3$. Potom existujú čísla n_1, n_2 tak, že $(E, +)$ je izomorfná s $Z_{n_1} \times Z_{n_2}$ s vlastnosťou $n_2 | n_1, n_2 | p - 1$.

Ako nájsť body E ? Ak $p = 1 \bmod 4$, potom máme algoritmus:

FOR x FROM 1 TO $p - 1$ DO
$z = x^3 + ax + b$
IF $z^{\frac{p-1}{2}} \bmod p = L(\frac{z}{p})$ THEN $P = (x, \pm y), y^2 = z$ "bod krivky"
OD;

Na nájdenie odmocniny zo z máme špeciálne algoritmy.

ElGamal a Eliptické krivky

ElGamalov kryptosystém s použitím problému diskrétneho logaritmu na grupe $(E, +)$ je nasledovný:

$$\mathcal{P} = E, \mathcal{C} = E \times E, \mathcal{K} = \{(P, Q, b) : Q = bP\}$$

Hodnoty $(E, +), P, Q$ sú verejne známe, b je tajný exponent, k je náhodne zvolené číslo, $1 \leq k < |E|$.
Šifrovanie:

$$X \in E, \quad e_K(X) = (kP, X + kQ) = (Y_1, Y_2)$$

Dešifrovanie:

$$d_K(e_K(X)) = Y_2 - bY_1 = X + kQ - bkP = X + k(Q - bP) = X$$

Tajná hodnota je $b = 7$, náhodne zvolená hodnota $k = 3$, verejný kľúč je $P = (2, 7)$, $Q = bP = (7, 2)$. Nech správa je $X = (5, 9)$. Potom dostaneme

- $kP = 3(2, 7) = (8, 3), kQ = (3 * 7)P = 8P = (3, 5)$
- $X + kQ = (5, 9) + (3, 5) = (7, 9)$
- $e_K(X) = ((8, 3), (7, 9))$
- $d_K(e_K(X)) = (7, 9) - 7(8, 3) = 6P - 7(3P) = -15P = -2P = 11P = (5, 9)$. Pri dešifrovaní k nepotrebujeme!

Menezes – Vanstoneho algoritmus

Táto varianta ElGamalovho kryptosystému na $(E, +)$ zlepšuje prenosový pomer na pôvodnú hodnotu 2. Eliptická krivka je tu použitá na maskovanie a OT sú ľubovoľné nenulové dvojice zo Z_p.

$$\mathcal{P} = Z_p^* \times Z_p^*, \mathcal{C} = E \times Z_p^* \times Z_p^*, \mathcal{K} = \{(P, Q, b) : Q = bP\},$$

Hodnoty $(E, +), P, Q$ sú verejne známe, b je tajný exponent, číslo $k \in Z_{|H|}$ je náhodne zvolené, kde H je cyklická podgrupa $(E, +)$. Kardinalita $\mathcal{P}$ sa tiež zväčšuje z pôvodných $|E| \approx p$ na $(p-1)^2$.

šifrovanie:

odosielateľ zvolí k a vypočíta

$$kQ = (c_1, c_2)$$

$$x \in Z_p^* \times Z_p^*, \quad e_K(x) = e_K(x_1, x_2) = (R, y_1, y_2) =$$
$$= (kP, c_1 x_1 \bmod p, c_2 x_2 \bmod p)$$

šifrovanie:

odosielateľ zvolí k a vypočíta

$$kQ = (c_1, c_2)$$

$$x \in Z_p^* \times Z_p^*, \quad e_K(x) = e_K(x_1, x_2) = (R, y_1, y_2) =$$
$$= (kP, c_1 x_1 \bmod p, c_2 x_2 \bmod p)$$

dešifrovanie

adresát najprv vypočíta

$$bR = (c_1, c_2),$$

a potom

$$d_K(e_K(x)) = (y_1 c_1^{-1} \bmod p, y_2 c_2^{-1} \bmod p) = x.$$

šifrovanie:

odosielateľ zvolí k a vypočíta

$$kQ = (c_1, c_2)$$

$$x \in Z_p^* \times Z_p^*, \quad e_K(x) = e_K(x_1, x_2) = (R, y_1, y_2) =$$
$$= (kP, c_1 x_1 \bmod p, c_2 x_2 \bmod p)$$

dešifrovanie

adresát najprv vypočíta

$$bR = (c_1, c_2),$$

a potom

$$d_K(e_K(x)) = (y_1 c_1^{-1} \bmod p, y_2 c_2^{-1} \bmod p) = x.$$

Tajná hodnota je $b = 7$, náhodne zvolená hodnota $k = 6$, verejný kľúč je $P = (2, 7), Q = bP = (7, 2)$. Nech správa je $x = (9, 1)$. (Uvedomte si, že $x \notin E$.)

Tajná hodnota je $b = 7$, náhodne zvolená hodnota $k = 6$, verejný kľúč je $P = (2, 7), Q = bP = (7, 2)$. Nech správa je $x = (9, 1)$. (Uvedomte si, že $x \notin E$.)

Šifrovanie:

- $R = kP = 6(2, 7) = (7, 9), kQ = 6(7, 2) = (8, 3) = (c_1, c_2)$
- $y_1 = c_1 x_1 \bmod 11 = 8 * 9 \bmod 11 = 6$
- $y_2 = c_2 x_2 \bmod 11 = 3 * 1 \bmod 11 = 3$
- $y = (R, y_1, y_2) = ((7, 9), 6, 3)$.

Tajná hodnota je $b = 7$, náhodne zvolená hodnota $k = 6$, verejný kľúč je $P = (2, 7), Q = bP = (7, 2)$. Nech správa je $x = (9, 1)$. (Uvedomte si, že $x \notin E$.)

Šifrovanie:

- $R = kP = 6(2, 7) = (7, 9), kQ = 6(7, 2) = (8, 3) = (c_1, c_2)$
- $y_1 = c_1 x_1 \bmod 11 = 8 * 9 \bmod 11 = 6$
- $y_2 = c_2 x_2 \bmod 11 = 3 * 1 \bmod 11 = 3$
- $y = (R, y_1, y_2) = ((7, 9), 6, 3)$.

Dešifrovanie:

- $bR = bkP = k(bP) = kQ = (c_1, c_2) = (8, 3)$
- $x_1 = y_1 c_1^{-1} \bmod 11 = 9$
- $x_2 = y_2 c_2^{-1} \bmod 11 = 1$

Porovnanie algoritmov

Názov	Verejný kľúč	R
RSA	$1024 + \|e\|$	1
Rabin	$1024 + \|B\|$	> 1
ElGamal $(Z_p, +)$	$1024 + \|\alpha\| + \|\alpha^a\| \approx 3000$	2
ElGamal $(E, +)$	$\|a\| + \|b\| + \|P\| + \|Q\| \approx 3000$	4
Menezes-Vanstone $(E, +)$	$\|a\| + \|b\| + \|P\| + \|Q\| \approx 3000$	2
Merkle-Hellman	$100 \times 100 = 10000$	2
Chor-Rivest	$p \times \|c\| + \|p\| + \|h\| \approx 36000$	1,798
McEliece	$1024 \times 524(654) \approx 537(670)000$	1,96; 1,56

$|x|$ je počet bitov binárneho vyjadrenia x, $|\alpha|, |\alpha^a| \leq 1024$,
$|a|, |b| \approx 500, |P|, |Q| \approx 2 \times 500$,
$|c| \leq 183, p = 197, h = 24, |p| = 8, |h| = 5$.

Zložitosť algoritmov

- Polynomická: $\mathcal{O}(n^k)$

Zložitosť algoritmov

- Polynomická: $\mathcal{O}(n^k)$
- Subexponenciálna: $e^{o(n)}, o(n) < cn$

Zložitosť algoritmov

- Polynomická: $\mathcal{O}(n^k)$
- Subexponenciálna: $e^{o(n)}, o(n) < cn$
- $1 < \ln \ln n < \ln n < \exp(\sqrt{(}\ln n \ln \ln n)) < n^{\ln n}$

Zložitosť algoritmov

- Polynomická: $\mathcal{O}(n^k)$
- Subexponenciálna: $e^{o(n)}, o(n) < cn$
- $1 < \ln \ln n < \ln n < \exp(\sqrt{(}\ln n \ln \ln n)) < n^{\ln n}$
- RSA, DL problémy: sú subexponenciálne...

Zložitosť algoritmov

- Polynomická: $\mathcal{O}(n^k)$
- Subexponenciálna: $e^{o(n)}, o(n) < cn$
- $1 < \ln \ln n < \ln n < \exp(\sqrt{(}\ln n \ln \ln n)) < n^{\ln n}$
- RSA, DL problémy: sú subexponenciálne...

Niekedy sa pomýlime: Ruksak...

Zložitosť algoritmov

- Polynomická: $\mathcal{O}(n^k)$
- Subexponenciálna: $e^{o(n)}, o(n) < cn$
- $1 < \ln \ln n < \ln n < \exp(\sqrt{(}\ln n \ln \ln n)) < n^{\ln n}$
- RSA, DL problémy: sú subexponenciálne...

Niekedy sa pomýlime: Ruksak...
Subexponenciálne problémy budú riešiteľné QPC...