Bezpečnost v IT

12. přednáška

Radek Janoštík

Univerzita Palackého v Olomouci

2. 5. 2024

Outline

- Aktuální (kyber)bezpečnostní situace
- Diffie-Hellman výměna klíčů
- Eliptické křivky
- Blockchain
- Doporučená četba
- Zkouška

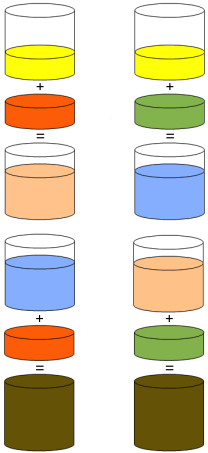
Aktuální (kyber)bezpečnostní situace

- Sledujete zprávy z dění v kyberprostoru? Co se stalo?
- Vydáno Chrome 124, které zavádí mechanismy *postkvantové kryptografie*
  - Nový ochranný mechanismus při navazování TLS 1.3 a QUIC spojení
  - Některé implementace serverů/firewallů mají problém s dodatečnými parametry
  - Chybně implementují standard
- Google vydal zprávu o boji proti škodlivým aplikacím na Play
  - V roce 2023 zablokováno přes 2.2 milionu aplikací
  - V roce 2022 zablokováno „jen“ 1.4 milionu
- V Británii začal platit nový zákon upravující výchozí hesla zařízení
  - Nesmí být pevné výchozí heslo pro zařízení
  - Musí být náhodné, bez vazby na HW identifikátor (MAC adresu)
  - Silné proti bruteforce
  - Poměrně vysoké pokuty

Diffie-Hellman výměna klíčů

- Algoritmus pro ustanovení parametrů pro šifrování
- Jak nastavit klíče pro symetrické šifrování po nezabezpečeném kanále
- Principy asymetrické kryptografie, ale konkrétní algoritmus
- Široké využití (SSL, SSH, IPSec, . . .)

Diffie-Hellman výměna klíčů – idea



Diffie-Hellmanova výměna klíče

- zásadním krokem je smíchání společné barvy s tajnými barvami
- tento proces je *jednosměrný*
- hledáme tedy funkci f, která bude tuto jednosměrnost napodobovat: vyčíslení funkce $f(x)$ by mělo být *snadné*, výpočet inverze (z daného y získat x takové, že $f(x) = y$) by mělo být *obtížné*
- kandidát na jednosměrnou funkci: umocnění v modulární aritmetice

DH – generování klíčů

- *Alice* (příjemce) vygeneruje páry klíčů
- Velké prvočíslo $p -> 1024$ bitů (*modulus*)
- Základ $g < p$ (*base*)
- Náhodné x_1 číslo délky ± 160 bitů (*private exponent*)
- Veřejná hodnota $y_1 = g^{x_1} mod p$
- Veřejný klíč: Trojice g, p, y_1
- Soukromý klíč: x_1 (Alice zachová v tajnosti)

DH – odesilatel

- *Bob* chce komunikovat s *Alicí*
- Na základě veřejného klíče Alice, zvolí hodnoty:
- Náhodný exponent x_2
- Veřejná hodnota $y_2 = g^{x_2} mod p$ (g a p z veřejného klíče Alice)
- Spočítá svou tajnou hodnotu: $s = y_1^{x_2} mod p$
- s (nebo část) může použít k symetrickému šifrování
- Odešle Alici šifrovanou zprávu + hodnotu y_2

DH – příjemce

- S první zprávou (zašifrovanou pomocí s obdrží i y_2
- Vypočítá $s = y_2^{x_1} \, mod p \Rightarrow$ také má s
- $\Rightarrow$ může dešifrovat
- s nikdy neputovalo nezabezpečeným kanálem

Příklad (na tabuli)

DH – bezpečnost

- Nalezení x_1 (a tím i klíče) z odchycených zpráv prakticky nemožné
- „Umíme řešit“, ale trvá *moc dlouho*
- $\Rightarrow$ Discrete Logarithm Problem
- Doporučuje se používat klíče délky 2048 bitů a více

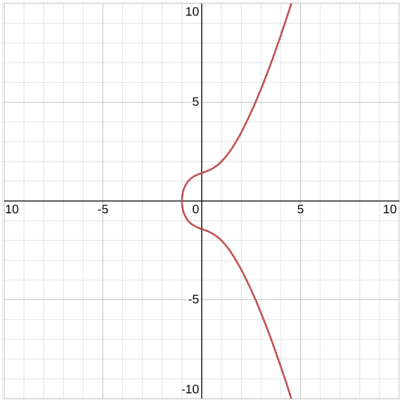
Eliptické křivky – úvod

- „Moderní“ kryptografická metoda, která „konkuruje“ RSA
- Výrazně kratší veřejné a privátní klíče ($\approx$ 200 bitů) při podobné bezpečnosti jako RSA
- $\Rightarrow$ Potřeba méně paměti pro ukládání (*smart cards*)
  - Rychlejší podepisování (EC DSA), ověřování však pomalejší
  - Méně přenosu při DH
- Ale – pro efektivní algoritmy se předpočítávají hodnoty (vyšší nárok na paměť)
- Aritmetika vystavěna nad „sčítáním“ bodů na eliptické křivce

Eliptická křivka – definice

- Eliptické křivky jsou dány rovnicí:

$$y^2 = x^3 + Ax + B$$



Eliptické křivy – body na křivce

- Prvky x, y, A, B brány z nějakého *pole* ($\mathbb{R}, \mathbb{C}, \mathbb{Z}_p$)
- Body na křivce L jsou: $E(L) = \{\infty\} \cup \{(x, y) \in L \times L \mid y^2 = x^3 + Ax + B\}$
- Křivky z jiných polí než $\mathbb{R}$ se velmi těžko kreslí, musíme se od toho odprostit
- Dodefinujeme si operaci sčítání dvou (a více) bodů
- Pro kryptografii se opět hodí křivky s modulární aritmetikou
- Tvar: $y^2 mod\ p = (x^3 + Ax + B) mod\ p$
- Kde p je opět nějaké prvočíslo

Eliptické křivky – sčítání bodů

- Mějme body $P_1 = (x_1, y_1)$ a $P_2 = (x_2, y_2)$, pokud nejsou stejné nebo ∞,
  - Proložíme mezi nimi přímku, někde protne křivku $\rightarrow$ bod P_3'
  - Tento bod překlopíme přes osu $X \rightarrow$ bod P_3
  - Definujeme $P_1 + P_2 = P_3$
- (nikdy) Se nejedná o obyčejné sčítání „po složkách“
- Určitě byste byli schopni dát dohromady obecnou rovnici
- Pro $x_1 \neq x_2$
  - Směrnice přímky: $m = \frac{y_2 - y_1}{x_2 - x_1}$
  - $P_3 = (x_3, y_3)$:

$$x_3 = m^2 - x_1 - x_2$$
$$y_3 = m(x_1 - x_3) - y_1$$

Eliptické křivky – sčítání bodů – pravidla

- Mějme křivku E definovanou jako $y^2 = x^3 + Ax + B$, body na křivce E: $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, $P_1, P_2 \neq \infty$, definujme sčítání bodů $P_1 + P_2 = P_3$:
  1. Pokud $x_1 \neq x_2$, pak

$$x_3 = m^2 - x_1 - x_2$$
$$y_3 = m(x_1 - x_3) - y_1$$

     Kde $m = \frac{y_2 - y_1}{x_2 - x_1}$

  2. Jestliže $x_1 = x_2$, ale $y_1 \neq y_2$, pak $P_1 + P_2 = \infty$

Eliptické křivky – sčítání bodů – pravidla

3. Jestliže $P_1 = P_2$ a $y_1 \neq 0$, pak

$$x_3 = m^2 - 2x_1$$
$$y_3 = m(x_1 - x_3) - y_1$$

   Kde $m = \frac{3x_1^2 + A}{2y_1}$

4. Jestliže $P_1 = P_2$ a $y_1 = 0$, pak $P_1 + P_2 = \infty$
5. $P + \infty = P$ pro všechny P na křivce E

Eliptické křivky – sčítání bodů

- Definované sčítání bodů splňuje následující vlastnosti:
  1. $P_1 + P_2 = P_2 + P_1$ pro všechny P_1, P_2 na křivce E (komutativita)
  2. $P + \infty = P$ pro všechny body P na křivce E (existence nulového prvku)
  3. Pro daný bod P na E existuje P' na E, t.ž. $P + P' = \infty$, P' značeno $-P$ (existence inverzního prvku)
  4. $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$ pro všechny P_1, P_2, P_3 na E (asociativita)
- $\Rightarrow$ Sčítání bodů na křivce tvoří aditivní abelovskou grupu, kde ∞ je neutrálním prvkem
- $\Rightarrow$ Sčítání bodů „se chová rozumně“

Eliptické křivky – prvočíselný modul

- Tvar $y^2 mod\ p = (x^3 + Ax + B) mod\ p$
- Lehce komplikuje předchozí pravidla (modulární dělení)
  - Např: jaký je výsledek $4/3 mod\ 11$?
  - Hledáme takové t, které splňuje: $3 \cdot t \bmod 11 = 4$
  - Celou rovnici vynásobíme inverzním prvkem ke 3, tedy 3^{-1}
  - $3^{-1} \cdot 3 \cdot t \bmod 11 = 3^{-1} \cdot 4$
  - Dostaneme $t \bmod 11 = 3^{-1} \cdot 4$
  - Inverze ke 3 v $\mathbb{Z}_{11}$ je 4
  - Jaké t modulo 11 dává zbytek $16 \Rightarrow 5$?
  - Takže $4/3 \bmod 11 = 5$

Eliptické křivky – kryptografie

- Mějme $d \in \mathbb{N}$ bodu skalárem $d \cdot P$ můžeme definovat jako: $P + \cdots + P$, kde je sčítání provedeno d krát
- Např. $d = 3$, pak $3 \cdot P = P + P + P$
- Zvolme si eliptickou křivku E (modul p, parametry A, B) a bod P, který na ní leží
- Zvolme náhodný skalár d a najděme bod $Q = d \cdot P$, d budeme držet v tajnosti
- E, P, Q můžeme oznámit světu – mohou efektivně najít tajné d?
- Je-li modul *dostatečně velký*, tak to není prakticky možné

Diffie-Hellman na eliptických křivkách

- Alice má veřejný klíč: p – modul, A, B parametry křivky, P, Q_a body na křivce
- Alice má soukromý klíč: d_a (tajný skalár, $Q_a = d_a \cdot P$)
- Bob vezme Alicinu křivku a zvolí vlastní (náhodné) d_b a spočítá $Q_b = d_b \cdot P$
  - Veřejný klíč: p, A, B, P, Q_b
  - Soukromý klíč: d_b
- Bob odvodí tajemství: $s = d_b \cdot Q_a$
  - Ve skutečnosti $s = d_b \cdot d_a \cdot P$, ale Bob nemá znalost d_a
- Bob pošle alici Q_b a ta může spočítat tajemství: $s = d_a \cdot Q_b$
  - Ve skutečnosti opět: $s = d_a \cdot d_b \cdot P$, ale Alice nemá znalost d_b
- Oba přišli ke stejnému s

Blockchain

- Pokračování přednášky bez slidů

Doporučená četba / zdroje

- Mel H.x., Baker, D. Cryptography Decrypted. Addison-Wesley, 2001. ISBN 201616475
  - Diffie-Hellman
  - Eliptické křivky

- Washingtong L. C.: Elliptic Curves, Number Theory and Cryptography. Chapman&Hall, 2003. ISBN 1584883650
  - Eliptické křivky

Zkouška

- Zkouška bude ústní formou
- Dvě otázky
  - 1. „do hloubky“ (komplexnější téma)
  - 2. „přehledová“ (vedlejší téma, přehledově, základní principy)
- Otázky z probraných okruhů + základní otázky z KMI/POS 1
  - `https://apollo.inf.upol.cz/~janostik/bezit/`
- $\approx$ 20 minut příprava $\Rightarrow$ ústní zkoušení, doptávání, diskuze
- Předtermín v pondělí v zápočtovém týdnu?