Asymetrické šifry

Pavla Henzlová

FJFI ČVUT v Praze

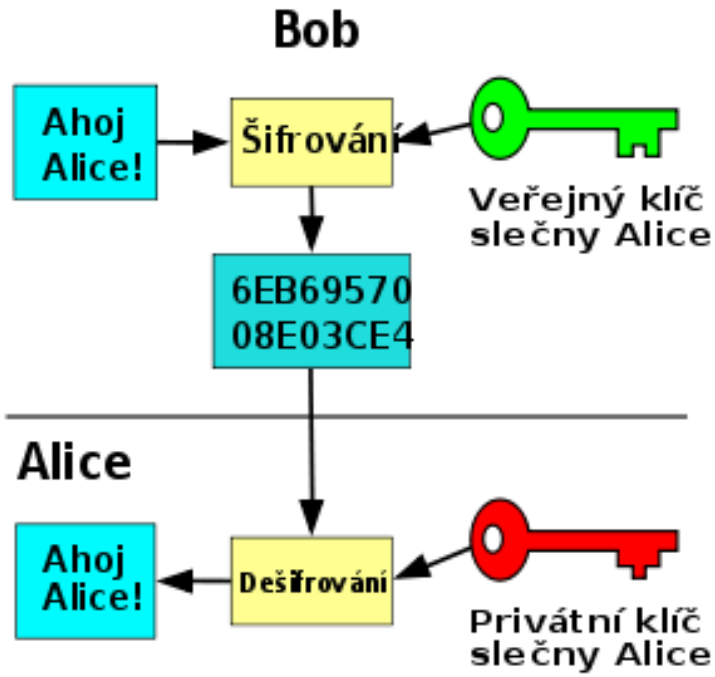
28.3.2011

Obsah

1. Asymetrická kryptografie
2. Diskrétní logaritmus
3. Baby step - Giant step
4. El Gamal
5. Diffie - Hellman

Asymetrická kryptografie

- pro šifrování a dešifrování se používají rozdílné klíče
- nejběžnější je verze s veřejným a soukromým klíčem
- šifrovací a dešifrovací klíč musí být matematicky provázány, ale je nutné, aby bylo prakticky nemožné ze znalosti šifrovacího klíče spočítat dešifrovací



Asymetrická kryptografie

Matematicky tedy asymetrická kryptrografie postupuje následujícím způsobem:

Šifrování $c = f(m, e)$

Dešifrování $m = g(c, d)$

e je šifrovací klíč a d je dešifrovací klíč V principu se mohou šifrovací a dešifrovací funkce lišit, zpravidla jsou však matematicky velmi podobné

Asymetrická kryptografie

- AK je založena na tzv. jednocestných funkcích - operace, které lze snadno provést pouze v jednom směru: ze vstupu lze snadno spočítat výstup, ale nikoliv naopak.
- Běžně využívané jednocestné funkce:
  - násobení (faktorizace) (na tomto principu funguje RSA)
  - diskrétní logaritmus
  - problém batohu
- žádná metoda AK se neukázala bezpečná při použití nekonečného výpočetního výkonu (na rozdíl od Vernamovy šifry), ale když počítáme s omezeným výkonem, lze např. říci, že metoda je nerozluštitelná pomocí osobního počítače za 1000 let

Diskrétní logaritmus

Definice

Buďte $m, g, Y \in \mathbb{N}$. Pak každé číslo $k \in \mathbb{N}$ takové, že

$$Y \equiv g^k \mod m$$

nazveme **diskrétní logaritmus o základu** g **z čísla** Y **vzhledem k** *modulum*. Protože k není určeno jednoznačě, někdy se definice upravuje tak, že se vybere ze všech možných k to nejmenší.

Definici lze zobecnit na libovolnou cyklickou konečnou multiplikativní grupu G s generátorem g. Zatímco spočítat Y ze znalosti k, m, q je snadné, spočítat diskrétní logaritmus je velmi obtížné. Jedním z algoritmů, který se k výpočtu používá je Baby step - Giant step.

Baby step - Giant step

Použití:Výpočet diskrétního logaritmu

Mějme cyklickou grupu G řádu n a generátor grupy g, prvek grupy h.

Úkolem je najít přirozené číslo x takové, že

$$g^x = h.$$

Baby step - Giant step algoritmus je založen na zapsání čísla x jako $x = im + j$, kde $m = \left\lceil \sqrt{n} \right\rceil$, $0 \leq i < m$, $0 \leq j < m$.

Tedy $h(g^{(} - m))^i = g^j$.

Algoritmus předpočítá g^j pro několik hodnot j, pak zafixuje m a testuje hodnoty i, zda je pro některou hodnotu i, j splněna kongruence.

Baby step - Giant step

Algoritmus

Vstup: Cyklická grupa G řádu n s generátorem g a prvkem h.

Výstup: Hodnota x splňující $g^x = h$

1. $m := \lceil \sqrt{n} \rceil$
2. for j= 0 to m

   spočítat g^j a uložit (j, g^j) do paměti
3. spočítat g^{-m}
4. $y := h$
5. for i = 0 to m-1
   1. zkontrolova, zda y není již někde mezi uloženými hodnotami g^j
   2. jestli ano, vrátit $im + j$
   3. jestli ne, $y := y * g^{-m}$

El Gamal

- navrhnul roku 1985 Taher El Gamal
- je méně používaný než RSA
- šifrovaná data mají dvojnásobnou délku než otevřený text
- tento algoritmus může být definován nad libovolnou cyklickou grupou G (velmi často je G multiplikativní grupa $\mathbb{Z}_p^\star$ module $p \in \mathbb{P}$)
- bezpečnost algoritmu závisí na volbě grupy G a na náročnosti vyřešení problému diskrétního logaritmu

El Gamal

Veřejné parametry: Generátor g multiplikativní cyklické grupy G řádu n

Tajný klíč: Náhodné číslo $x \in \{0, 1, \ldots, n-1\}$

Veřejný klíč: $h = g^x$

El Gamal - šifrování

Zašifrujeme zprávu m pomocí veřejného klíče (h, G, g, n):

- Vybereme náhodné $y \in \{0, 1, \ldots, n-1\}$
- $c_1 = g^y$
- $s = h^y$ (tzv. jepičí klíč)
- převedeme zprávu m na zprávu $\bar{m} \in G$
- $c_2 = s \cdot \bar{m}$
- odešleme šifrový text (c_1, c_2)
- je nutné dobře utajit nebo zničit jepičí klíč s

El Gamal - dešifrování

- dostaneme šifrový text (c_1, c_2)
- spočítáme $\bar{m} = c_2 \cdot ((c_1)^x)^{-1}$
- převedeme na původní zprávu m

El Gamal

Bezpečnost:

- pokud chceme prolomit algoritmus El Gamal, je třeba při daném $p, g, h = g^x, c_1 = g^y, c_2 = h^y$ vypočítat $m = c_2 \cdot (g^x y)^{-1}$
- kdybychom uměli vyřešit diskrétní logaritmus, stačilo by pouze dosadit
- je třeba pro zašifrování různých zpráv volit různé jepičí klíče y
- s výjovem algoritmů pro řešení diskrétního logaritmu a se zvětšující se výpočetní silou je potřeba volit čím dál větší klíče
- V roce 1996: alespoň modul p o 768 bitech a 1024 bitů pro dlouhodobé šifry
- V roce 2003: Pro dlouhodobé šifry je potřeba alespoň 2000 bitů

Diffie - Hellman

- algoritmus navrhnutý roku 1976 Witfieldem Diffiem a Martinem Hellmanem
- umožňuje přes nezabezpečený komunikační kanál vytvořit mezi komunikujícími stranami šifrované spojení
- vytvoří se symetrický klíc, který lze použít pro následnou šifrovanou komunikaci, ale přes nezabezpečený kanál není tento klíč nikdy posílán v otevřené formě
- pomocí tohoto protokolu nelze ověřit identitu komunikujících, je tedy potřeba jej kombinovat s jinými metodami nebo používat pouze tam, kde nemůže do komunikace „nepřátelská“ strana aktivně zasáhnout

Diffie - Hellman

1. Alice a Bob se domluví na společné multiplikativní cyklické konečné grupě G s generátorem g (obvykle je to $\mathbb{Z}_p^\star$)
2. Alice si zvolí náhodné přirozené číslo a a odešle g^a Bobovi
3. Bob si zvolí náhodné přirozené číslo b a odešle g^b Alici
4. Alice si vypočte $(g^b)^a$
5. Bob si vypočte $(g^a)^b$

Oba nyní vlastní tajný klíč g^{ab}, který může sloužit pro další šifrování

Diffie - Hellman

- Aby třetí strana získala tajný klíč $g^a b$, musela by umět vyřešit problém diskrétního logaritmu. Potřebuje totiž ze známého g^a a g^b získat $g^a b$.
- Tento protokol je bezpečný, pokud se zvolí p alespoň se 300 ciframi nebo a, b alespoň se 100 ciframi. Generátor grupy G se volí malý, nejčastěji 2 nebo 5.
- p se volí tak, že $p = 2q + 1$, kde $p, q \in \mathbb{P}$
- pro generování a, b se užívá generátoru náhodných čísel
- Nebezpečí prostředníka: pokud někdo zachytí komunikaci mezi Alicí a Bobem, může jim podvrhnout své hodnoty klíčů a odposlouchávat, případně modifikovat jejich komunikaci
- nutné autentizovat účastníky komunikace