ElGamal, Diffie-Hellman

Asymetrické šifrování

Martin Vlček

FJFI ČVUT Praha

22. dubna 2010

Prezentace do předmětu UKRY

Osnova

Osnova

Osnova

Osnova

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 modulu* m. *Někdy se definice upravuje tak, že se ze všech možných diskrétních logaritmů* k *vybere ten nejmenší.*

Poznámka

Definice lze zobecnit na libovolnou cyklickou konečnou multiplikativní grupu G *s generátorem* g.

Výpočet diskrétního logaritmu

- Zatímco spočíst $Y = g^k \mod m$ při znalosti k, g, m je snadné, spočíst diskrétní logaritmus k je velmi obtížné.
- **Naivní algoritmus** *(trial multiplication)*: umocňování g na vyšší a vyšší mocniny k, dokud se $Y \equiv g^k$. Časová složitost naivního algoritmus je lineární v počtu prvků grupy, tzn. exponenciální v počtu cifer ve velikosti grupy.
- Existují lepší algoritmy (např. Baby-step giant-step, Index calculus algorithm) ale žádné nedosahují polynomiální složitosti v počtu cifer ve velikosti grupy.
- Účinný kvantový algoritmus (Peter Shor).

Osnova

ElGamal – Základní fakta

- Algoritmus asymetrické kryptografie (šifrování s veřejným klíčem).
- 1985, Taher ElGamal (Egypt/USA).
- Nevýhoda: Šifrovaná data jsou dvakrát delší než data nešifrovaná.
- Nasazení není tak velké jako u RSA algoritmu.
- ElGamal algoritmus může být definován nad libovolnou cyklickou grupou G (typicky to bývá multiplikativní grupa $\mathbb{Z}_p^*$ modulo $p \in \mathbb{P}$).
- Bezpečnost spočívá na volbě této grupy a na problému vyřešení diskrétního logaritmu.
- Existuje ještě ElGamal podpisové schéma (a jeho vylepšení DSA), o něm se zmíníme pouze krátce.

Generování klíče:

- **Veřejné parametry:** Generátor g multiplikativní cyklické grupy G řádu q.
- **Tajný klíč:** Náhodné číslo x z $\{0, 1, \ldots, q-1\}$.
- **Veřejný klíč:** $h = g^x$.
- Zveřejněn bude veřejný klíč h a také informace o grupě (tzn. G,g,q).
- Tajný klíč x je třeba ponechat v tajnosti.

Šifrování:

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

- Vybereme náhodné y z $\{0, 1, \ldots, q-1\}$.
- Spočteme $c_1 = g^y$.
- Spočteme $s = h^y$ (tzv. ephemeral key = *jepičí klíč*).
- Pozn. Tyto kroky bylo možné provést před samotným šifrováním.
- Převedeme zprávu m do zprávy $m' \in G$ (např. pomocí OAEP).
- Spočítáme $c_2 = s \cdot m' (= h^y \cdot m')$.
- Odešleme šifrový text (c_1, c_2).
- Pozn. Dále je nutné dobře utajit(popř. zničit) ephemeral key s.

Dešifrování:

- Obdržíme šifrový text (c_1, c_2)
- Spočteme $m' = c_2 \cdot ((c_1)^x)^{-1}$.
- Převedeme na původní zprávu m.
- Postup funguje, protože

$$c_2 \cdot (c_1^x)^{-1} = s \cdot m' \cdot ((g^y)^x)^{-1} =$$
$$= h^y \cdot m' \cdot (g^{xy})^{-1} = g^{xy} \cdot m' \cdot (g^{xy})^{-1} = m'$$

Příklad

- Jako grupa G se nejčastěji volí multiplikativní grupa $\mathbb{Z}_p^*$ s nějakým svým generátorem.
- Dále je možno zvolit vhodnou aditivní grupu bodů rovinné eliptické křivky.
- Z hlediska bezpečnosti ekvivalentní.

Příklad

Zkusme si postup ElGamalova algoritmu pro zašifrování zprávy $m = 6$ v multiplikativní grupě $\mathbb{Z}_{11}^*$ s generátorem 7. Příjemce zvolí svůj tajný klíč $x = 3$, příjemce zvolí svůj empheral key $y = 5$.

Hledání generátoru cyklické grupy

Poznámka

Algoritmus hledání generátoru cyklické grupy Mějme cyklickou grupu G řádu n, kde n má prvočíselný rozklad: $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$.

1. *Zvol náhodné $g \in G$.*
2. *For $i = 1$ to k:*
   i. *Spočti $b = g^{n/p_i}$.*
   ii. *Pokud $b == 1$, vrať se na krok 1.*
3. *Vrať generátor g.*

Příklad

V našem případě $\mathbb{Z}_{11}^*$ je řád $10 = 2 \cdot 5$. Pokud vybereme např. $g = 4$ dostaneme pro $b = 4^5 \equiv 1 \mod 11$ a tedy algoritmus se vrátí na krok 1. Naopak v případě $g = 7$ nalezneme generátor.

Common System-Wide parameters

- Obě zúčastněné strany se mohou předem domluvit na používané grupě $\mathbb{Z}_p^*$ a jejím generátoru g. Poté se tyto informace nemusí posílat jako součást veřejného klíče. Úspora místa.
- **Výhoda:** Umocňování při šifrování může být urychleno díky předpočítání.
- **Nevýhoda:** Menší bezpečnost $\Longrightarrow$ je třeba volit větší modul p.

ElGamal – Bezpečnost

- Problém prolomení ElGamalova šifrování: tj. při daném p, g, $h = g^x$, $c_1 = g^y$, $c_2 = h^y$ spočítat $m = c_2 \cdot (g^{xy})^{-1}$.
- Je ekvivalentní řešení Diffie-Helmann problému(DHP): Víme g^x, g^y, chceme nalézt g^{xy}.
- Pokud bychom uměli vyřešit problém diskrétního logaritmu: spočetli bychom x a y a pak pouze dosadili.
- Prolomení ElGamalovy šifry je tedy založeno na diskrétním logaritmu.
- Je nezbytně nutné, aby se pro zašifrování různých zpráv volili různé klíče y. Pokud by totiž zprávy m a $\tilde{m}$ byly šifrovány pomocí stejného empheral key y na šifrové texty (c_1, c_2) a $(\tilde{c}_1, \tilde{c}_2)$. Pak $c_2/\tilde{c}_2 = m/\tilde{m}$ a tudíž bychom ze znalosti m mohli jednoduše získat i $\tilde{m}$.

ElGamal – Doporučená délka parametrů

- S vývojem řešení diskrétního logaritmu a s rostoucí výpočetní silou je třeba volit stále větší klíče.
- V roce 1996: alespoň modul p o 768 bitech a 1024 bitů pro dlouhodobé šifry.
- V roce 2003: Pro dlouhodobě bezpečné šifry je třeba volit alepsoň 2000 bitů, tzn. $p > 2^2000 \approx 0.115 \cdot 10^6 03$.
- Pro Common System-Wide parameters musí být voleny ještě větší p. Je to proto, že stěžejní část Index-calculus algoritmu pro výpočet diskrétního logaritmu tvoří předpočítání faktorové databáze. To je ovšem pro předem známé p možno udělat dopředu.

Podpisové schéma ElGamal

- Taher ElGamal, 1984
- Založeno také na obtížnosti řešení problému diskrétního logaritmu.
- Dnes se již téměř nepoužívá, protože existuje vylepšení DSA (Digital Signature Algorithm).

Osnova

Diffie-Hellman výměna klíčů

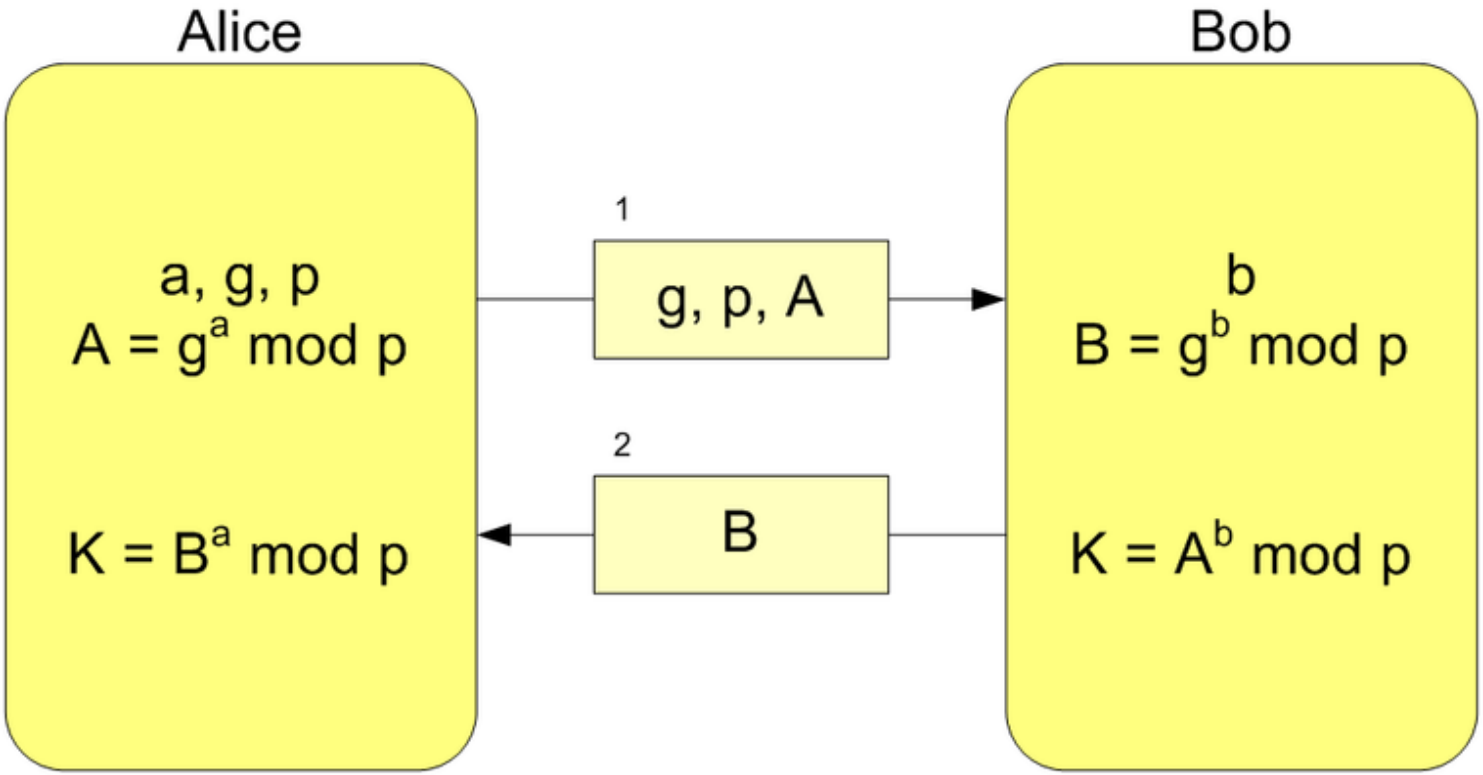
- Whitfield Diffie a Martin Hellman v roce 1976 (třetí spoluautor Ralph Merkle).
- Kryptografický protokol, který umožňuje přes nezabezpečený kanál vytvořit mezi komunikujícími stranami šifrované spojení bez předchozího dohodnutí šifrovacího klíče.
- Výsledkem výměny informací je utvoření společného *symetrického klíče*, který může být použit pro další komunikaci.
- Výhoda: Klíč nikdy není kanálem posílán v otevřené formě (jsou posílány jen dílčí informace k utvoření klíče).
- Nevýhoda: Bezbrannost proti útoku Man in the Middle, D-H protokol neumožňuje autentizaci účastníků. Tento protokol bez kombinace z jinými metodami je možný použít pouze tam, kde případný útočník nemůže aktivně zasahovat do komunikace.
- Počet účastníků není omezen. Demonstrujeme pro 2.

Diffie-Hellman – Obecný postup

1. Alice a Bob se domluví na společné multiplikativní cyklické konečné grupě G s generátorem g. (Toto je obvykle provedeno mnohem dřív než zbytek protokolu).
2. Alice si zvolí náhodné číslo $a \in \mathbb{N}$ a odešle g^a Bobovi.
3. Bob si zvolí náhodné číslo $b \in \mathbb{N}$ a odešle g^b Alici.
4. Alice si vypočte $(g^b)^a$.
5. Bob si vypočte $(g^a)^b$.

Alice i Bob nyní vlastní společně sdílený tajný klíč g^{ab} (díky asociativitě umocňování), který může sloužit k dalšímu šifrování. Obvykle se volí multiplikativní grupa $\mathbb{Z}_p^*$, kde p je prvočíslo.

Diffie-Hellman – Princip



$$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$$

Obrázek: Diffie-Hellman výměna klíčů

Příklad:

Alice		Bob		Eva	
zná	nezná	zná	nezná	zná	nezná
$p = 11$	$b = ?$	$p = 11$	$a = ?$	$p = 11$	$a = ?$
$g = 2$		$g = 2$		$g = 2$	$b = ?$
$a = 4$		$b = 7$			$K = ?$
$A = 2^4 \equiv 5 \mod 11$		$B = 2^b \equiv 7$		$A = g^a \equiv 5$	
$B = g^b \equiv 7 \mod 11$		$A = g^a \equiv 5$		$B = g^b \equiv 7$	
$K = B^a \equiv 3 \mod 11$		$K = A^b \equiv 3$		$K = B^a \equiv 3$	

Tabulka: Bezpečnost vůči odposlouchávači (eavesdropper)

Poznámka

Pro Alici by mělo být těžké zjistit Bobův tajný klíč (a obráceně). Pokud by tomu tak nebylo, mohla by Eva rovněž rozluštit Bobův tajný klíč.

Bezpečnost

- K získání společného sdíleného klíče K je třeba řešit DHP: při známém g^a, g^b, ale neznámém a, b, nalézt g^{ab}.
- Problém řešení diskrétního logaritmu — nejsou známy příliš účinné algoritmy.
- D-H protokol je bezpečný pokud se zvolí p alespoň o 300 cifrách, a a b o alespoň 100 cifrách. Naproti tomu generátor g se volí malý — v praxi 2 nebo 5.
- Pro modul $p \in P$ se často volí $p = 2q + 1$ kde q je také prvočíslo (tzv. Sophie Germain prvočíslo). Je to proto, že řád grupy $\mathbb{Z}_p^*$ má poté v prvočíselném rozkladu jen 2 a q, kde q je velké prvočíslo. Toto znesnadňuje použití Pohlig–Hellmanova algoritmu na řešení diskrétního logaritmu.
- Pro generování tajných klíčů a a b je třeba užít dobrý generátor náhodných čísel.

Autentizace

- D-H protokol je náchylný k útoku Man-in-the-Middle. Carl zachytí $A = g^a \mod p$ od Alice a podvrhne jí svoji hodnotu $C = g^c \mod p$. Alice a Carl vypočítají sdílený tajný klíč $K_{ac} = K_{ca}$. Carl pošle svou hodnotu $C = g^c \mod p$ Bobovi, který se domnívá, že je to hodnota od Alice a zašle mu svou hodnotu $B = g^b \mod p$. Bob a Carl vypočítají sdílený tajný klíč $K_{bc} = K_{cb}$. Veškerá komunikace mezi Alicí a Bobem je tak odposlouchávána Carlem, který může také přenášená data modifikovat.
- Proto je většinou v praxi nutná autentizace účastníků.
- **Password-authenticated key agreement (PAKE):** autentizace pomocí hesla.

Užití

- **Šifrování s veřejným klíčem:** Alice zveřejní veřejný klíč (p, g, g^a). Bob zvolí náhodné b a odešle Alici svůj veřejný klíč g^b a zprávu zašifrovanou pomocí symetrického klíče g^{ab}. Pouze Alice je schopna tuto zprávu rozluštit. V praxi se příliš neužívá (v této oblasti spíše RSA).
- V praxi jako součást **IPSec (Internet Protocol Security)**.
- **SSH (Secure Shell)** — bezpečná výměna dat.
- **SSL (Secure Sockets Layer).**

Děkuji za pozornost.