Základy kryptografie IV.

Šifrovat?…..Rozhodně Ano!

Kryptosystémy s veřejným klíčem - Diffie-Hellmann

Jaroslav Pinkava

1. Úvod

Obsahem minulé části našeho seriálu byly základní vlastnosti systémů s veřejným klíčem. Pro tyto kryptosystémy existují dva různé typy klíčů. První z nich (veřejný klíč) slouží k šifrování, druhý (soukromý) má pak opačnou funkci - s jeho pomocí provádíme dešifrování. Ve veřejné literatuře se samotný pojem kryptosystému s veřejným klíčem objevil poprvé v roce 1976 v článku New Directions in Cryptography (autoři Whitfield Diffie a Martin E. Hellman).

V tomto článku se také objevil poprvé protokol k dohodě na klíči (pro symetrickou šifru) na bázi systému s veřejným klíčem. Tento protokol se dnes všeobecně nazývá Diffie-Hellmanovou dohodou na klíči (key agreement). Jeho průběh je následující.

I: Je zveřejněno dostatečně velké prvočíslo **p**. Dále pak je zveřejněno přirozené číslo **g** (**g < p**), které má tu vlastnost, že je generátorem grupy **Z(p),** tj. pro libovolné **y**, které je prvkem **Z(p)** existuje přirozené **w** tak, že

$$\mathbf{y = g^w \ mod \ p}.$$

Čísla **p** a **g** jsou tzv. základní parametry Diffie-Hellmanova kryptosystému.

II: Každý z účastníků si vygeneruje svůj soukromý klíč (např. soukromý klíč účastníka A označíme **a** a soukromý klíč účastníka B označíme **b**). Dále si pak každý z těchto účastníků spočte svůj veřejný klíč (veřejným klíčem účastníka A bude číslo $\mathbf{g^a \ mod \ p}$ a účastníka B pak číslo $\mathbf{g^b \ mod \ p}$).

III. K tomu, aby se účastníci A a B dohodli na tajném klíči (pro symetrickou šifru) provedou následující. Účastník A spočte **K** jako (pomocí veřejného klíče účastníka B a svého soukromého klíče)

$\mathbf{K = (g^b)^a \ mod \ p}$.

Účastník B spočte klíč **K** jako (pomocí veřejného klíče účastníka A soukromého klíče účastníka B)

$\mathbf{K = (g^a)^b \ mod \ p}$.

Klíč **K** je pak použit jako klíč pro symetrickou šifru. Současné implementace tohoto protokolu předpokládají, že takto spočtené **K** slouží jako tzv. sdílená tajná hodnota a konkrétní tajné klíče ($\mathbf{K_i}$ je např. tajný klíč pro den i) pro symetrickou šifru jsou z **K** odvozovány pomocí tzv. funkce pro odvození klíčů : $\mathbf{K_i = hash\ (z \ || \ h_i)}$. Symbolem hash je zde označena vhodně zvolená hashovací funkce (např. SHA-1). Hodnoty $\mathbf{h_i}$ jsou známé oběma stranám (např. časové údaje, hodnoty některých čítačů atd.).

2. Úloha diskrétního logaritmu

Bezpečnost Diffie-Hellmanova systému je založena na obtížnosti řešení úlohy tzv. diskrétního logaritmu. Tím rozumíme úlohu nalézt z rovnice $\mathbf{y = g^w \bmod p}$ při známé hodnotě **y** (a známých hodnotách parametrů **p** a **g**) hodnotu **w**. Pro tuto úlohu existují i efektivnější algoritmy než je útok hrubou silou (postupné ozkoušení všech možných hodnot **w**). Nejefektivnějším známým algoritmem je tzv. metoda síta číselného tělesa (number field sieve). Avšak i při použití této metody existují hranice její reálné využitelnosti. Současná výpočetní technika (pro obecné prvočíselné **p,** nikoli pro některá speciálně volená prvočísla - např. blízká mocnině dvojky, atd.) rozhodně není reálně schopná spočítat takovýto diskrétní logaritmus při hodnotách $\mathbf{p > 2^{1000}}$.

Pokud parametry systému jsou generovány jako v normě pro podpis DSA (Digital Signature Algorithm - viz dále), resp. v připravované normě ANSI X9.42, je třeba řešit úlohu diskrétního logaritmu v podgrupách grupy **Z(p)**. Jestliže **q** je největší prvočíslo prvočíselného rozkladu čísla **p-1** a **g** je generátor podgrupy řádu **q**, pak např. při využití Pollardova **ρ**-algoritmu je složitost úlohy diskrétního logaritmu v této podgrupě řádově srovnatelná s druhou odmocninou z **q**.

3. Některé modifikace

Diffie-Hellmanův systém lze přímo použít pouze k výměně klíčů. Pro šifrování resp. digitální podpis však existují varianty tohoto kryptosystému.

3.1. El-Gamalův systém s veřejným klíčem (šifrovací algoritmus).

Účastník B chce zašifrovat zprávu m pro účastníka A. Východiskem je stejné rozvržení parametrů systému a klíčů jako u Diffie-Helmanovy dohody na klíči (platí výše uvedené body I. a II.). Účastník B provádí dále následující.

III (G). a) zvolí náhodné číslo **r**, $\mathbf{0 < r < p-1}$.

b) spočte $\mathbf{c = g^r \bmod p}$ a také $\mathbf{d = m.\,(g^a)^r \bmod p}$

c) šifrovým textem je dvojice **(c,d)**, tuto zašle straně A.

Při dešifraci pak účastník A musí učinit toto.

IV. (G) a) pomocí svého soukromého klíče **a** spočte $\mathbf{c^{p-1-a} \bmod p\ (= c^{-a} = g^{-ar})}$

b) otevřený text získá výpočtem jako $\mathbf{m = d\,c^{-a} \bmod p}$

3.2. Digital Signature Standard (americká norma pro digitální podpis).

V DSS se poprvé objevil následující modifikovaný přístup ke generování parametrů kryptosystému na bázi diskrétního logaritmu. Nejprve je náhodně generováno menší prvočíslo **q** (mající řádově délku 160 bitů). Prvočíslo **p** je pak odvozováno jako náhodné prvočíslo potřebné délky (tj. např. 1024 bitů) avšak takové, že prvočíslo **q** je dělitelem čísla **p-1**. Generátor **g** je volen tak, aby jeho řád byl roven číslu **q** (takovýto postup je v současné době volen i v draftu P1363 a draftu ANSI X9.42).

Generování digitálního podpisu (zprávy m libovolné délky) dle DSA probíhá následovně.

Podepisující strana A

a) vygeneruje náhodné (utajované) přirozené číslo **r**, $\mathbf{0 < r < q}$.
b) spočte: $\mathbf{c = (g^r \bmod p) \bmod q}$, $\mathbf{d = r^{-1} (hash(m) + ac)}$
c) podpisem strany A je dvojice **(c,d)**.

Při verifikaci podpisu strany A provádí strana B následující:

a) spočte $\mathbf{w = d^{-1} \bmod q}$ a spočte **hash (m).**
b) spočte **u = w. hash(m) mod q** a také **v= c.w mod q**
c) spočte $\mathbf{t = (g^u (g^a)^v \bmod p) \bmod q}$
d) akceptuje podpis tehdy a jen tehdy, když **t = c**.

4. Cramer-Shoup

Bezpečnost kompletního kryptografického systému v praxi závisí nejen na bezpečnosti použitých šifrovacích algoritmů, ale i na bezpečnosti použitých kryptografických protokolů. Tato bezpečnost závisí rovněž na konkrétní aplikaci, ve které je daný kryptografický protokol použit.

V srpnu tohoto roku na konferenci Crypto´98 v Santa Barbaře byl opublikován nový kryptosystém vycházející z myšlenek Diffie-Hellmanova systému. Tento kryptosystém (dle autorů je nazýván Cramer-Shoupův) je bezpečný i proti velice sofistikovaným metodám. Zejména pro komunikace na Internetu, při aplikacích elektronického obchodu (elektronické aukce, manipulace s kreditními kartami, ochrana soukromých informací) přináší nový systém výrazně vyšší bezpečnost.

Tzv. aktivní útoky obchází složitost řešení příslušných matematických problémů kryptoanalýzy jinou cestou. Veřejně dostupnému serveru je zasílána posloupnost kvalifikovaně konstruovaných zpráv. Následující analýzou příslušných odpovědí tohoto serveru může útočník rozkrýt obsah šifrovaných zpráv procházejících touto sítí. V roce 1991 tři odborníci IBM (Danny Dolev, Cynthia Dwork a Moni Naor) ukázali, že obvyklé dnešní kryptosystémy (s veřejným klíčem) jsou potenciálně "poddajné" (malleable). To znamená, že narušitel může (potenciálně) i bez znalosti dešifrovacího klíče převést šifrový text jedné zprávy na šifrový text jiné "blízké" zprávy. Například se to může ukázat nebezpečné v situacích, kdy šifrovaná zpráva obsahuje výši nabídky pro smlouvu. Narušitel tuto zprávu zachytí a zamění ji za zprávu s výrazně nižší nabídkou a to vše bez znalosti konkrétního znění původní zprávy.

"Nepoddajné" systémy (mezi které patří i Cramer-Shoupův kryptosystém) neutralizují aktivní útoky přidáním další posloupnosti výpočtů a zajistí tak, že server nevydá žádnou podstatnou informaci v případě, že odpovídá na falešný text. Cramer-Shoupův systém navíc umožňuje i efektivní implementaci (vyžaduje zhruba dvojnásobný čas zpracování oproti současným obdobným kryptosystémům - "poddajným"). Matematici ukázali, že vlastnost nepoddajnosti je ekvivalentní bezpečnosti systému oproti tzv. útokům s volitelným šifrovým textem (adaptive chosen ciphertext attack). To odpovídá situaci, kdy narušitel může předkládat k dešifraci libovolné šifrové texty (s vyjímkou toho "pravého").

Nyní popíšeme, jak vypadá samotné Cramer-Shoupovo kryptoschema. Předpokládáme opět, že máme k dispozici grupu **Z(p)**, kde **p** je prvočíslo.

A. Generování klíče: Nejprve získáme generátory grupy **Z(p)** čísla g_1 a g_2. Dále jsou náhodně vygenerována čísla

$$x(1), x(2), y(1), y(2), z \in Z(p).$$

Následovně jsou spočtena čísla

$$c = g_1^{x(1)} g_2^{x(2)}, \quad d = g_1^{y(1)} g_2^{y(2)}, \quad h = g_1^{z}.$$

Pevně zvolíme hashovací funkci **H**.
Veřejným klíčem je potom vektor (g_1, g_2, c, d, h, **H**) a soukromým klíčem je vektor (**x(1), x(2), y(1), y(2), z**).

B. Šifrování: Jestliže **m** je příslušný otevřený text (**m** $\in$ **Z(p)**), pak jeho zašifrování probíhá následovně. Nejprve je náhodně vygenerováno číslo **r** $\in$ **Z(p)**. Posléze spočteme

$$u_1 = g_1^{r}, \quad u_2 = g_2^{r}, \quad e = h^{r} m, \quad s = H(u_1, u_2, e), \quad v = c^{r} d^{rs}.$$

Šifrovým textem je čtveřice (u_1, u_2, **e, v**).

C. Dešifrování: Jestliže máme dán šifrový text v podobě čtveřice (u_1, u_2, **e, v**), pak jeho dešifrování provedeme následovně. Nejprve je spočtena hodnota $s = H(u_1, u_2, e)$, a ověřeno zda platí

$$u_1^{x(1) + s.y(1)} u_2^{x(2) + s.y(2)} = v.$$

Pokud tato podmínka není splněna, výstupem dešifrovacího algoritmu je "zamítnutí". V opačném případě je jeho výstupem

$$m = e / u_1^{z}.$$

Výstupem popsaného schematu je skutečně výchozí otevřený text. O tom se lze přesvědčit postupným dosazením jednotlivých hodnot.

O takto popsaném schematu dokázali jeho autoři, že je bezpečné proti útoku s volitelným šifrovým textem. Schema lze samozřejmě modifikovat tak, že parametry jsou generovány stejně jako pro DSA, tj. nejprve je vygenerováno menší prvočíslo **q** a teprve posléze prvočíslo **p** takové, že **q** je dělitelem čísla **p-1.**

5. Systémy na bázi diskrétního logaritmu a současné kryptografické normy

Oproti RSA, kde platnost patentu ještě stále trvá, je situace při použití Diffie-Hellmanova schematu jiná. Platnost patentu již totiž vypršela v roce 1997. Tato skutečnost vedla i autory některých připravovaných norem (např. S/MIME) ke snaze použít zde právě schema Diffie-Hellmana. Napomáhá tomu také skutečnost, že díky řadě nových výsledků (stačí zmínit právě Cramer-Shoupovo schema) jsou kryptosystémy na bázi diskrétního logaritmu flexibilnější - např. systém RSA neumožňuje výpočet sdílené tajné hodnoty.

V současné době kromě již zmíněného DSS (Digital Signature Standard, americká norma pro digitální podpisy) jsou systémy na bázi diskrétního logaritmu (mezi které patří všechna námi zmíněná schemata) základem při vytváření několika norem pro šifrování s veřejným klíčem. Zejména se to týká normy připravované skupinou P1363. Tato norma je nyní ve finální fázi, připravuje se její předložení NIST. Je založena na dokonalém popisu tří základních kryptosystémů s veřejným klíčem. Jsou to systémy založené:

a) na úloze faktorizace (RSA a Rabin-Williamsův systém),
b) na úloze diskrétního logaritmu
c) na úloze diskrétního logaritmu pro eliptické křivky.

Speciálně pro finanční instituce je připravována norma ANSI X9.42, která konkrétně rozpracovává dvě varianty systémů pro dohodu na klíči na bázi diskrétního logaritmu. Jsou to klasický Diffie-Hellmanův systém a tzv. MQV systém (Menezes, A.; Qu, M.; Vanstone, S.). Obě schemata jsou zde koncipována tak, aby sloužila k výpočtu sdílené tajné hodnoty. Přitom mezi oběma stranami není nutná žádná další komunikace, k výpočtu jsou použity veřejné klíče opačné strany a vlastní soukromé klíče. MQV systém se při této výměně navíc opírá o existenci dvou dvojic klíčů (pro každou stranu). Jedna z těchto dvojic je tzv. statická (klíče mají dlouhodobou platnost), druhá je tzv. efemerální (klíče mají relativně krátkou dobu platnosti).

Příkladem užití systému na bázi diskrétního logaritmu v rámci celé řady protokolů rozpracovaných pro internet je draft S/MIME (poslední je verze draft-ietf-smime-x942-03.txt). Autoři vychází z připravované normy ANSI X9.42, a navazují na rozpracování normy X.509 pracovní skupinou pkix (podoba certifikátů veřejných klíčů).

Slovník kryptologických pojmů:

Schema pro dohodu na klíči: Je to způsob, kterým se dvě či více entit dohodne na společném klíči, který znají pouze tyto entity. Využijí k tomu veřejné klíče druhé strany a své vlastní tajné klíče. Dohodnutý společný klíč pak spolu sdílí při užití nějakého symetrického šifrovacího algoritmu (key agreement scheme).

Tajná hodnota:
Hodnota, která je používána k odvození tajného klíče, sama však jako tajný klíč nesmí být používána (secret value).

Sdílený tajný klíč:
Tajný klíč sdílený dvěma či více stranami, obvykle je výsledkem dohody na klíči (shared secret key).

Sdílená tajná hodnota:
Tajná hodnota sdílená dvěma či více stranami - obvykle v průběhu dohody na klíči (shared secret value).

Funkce pro odvození klíčů:
Funkce s jejíž pomocí je na základě sdílené tajné hodnoty odvozován tajný klíč (key derivation function).

Některé zajímavé WWW stránky:

http://www.cs.wisc.edu/~shoup/papers/
webovská stránka jednoho z autorů nového kryptoschematu
http://www.cryptosoft.com/html/secpub.htm
přehled některých odborných článků z kryptologie, které lze nalézt na webu.
http://www.counterpane.com/biblio/
obdobný přehled
http://security.isu.edu/publications.html
on-line publikace tentokrát šířeji zaměřené na problematiku bezpečnosti
http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm
přehled zákonů týkajících se použití kryptografických metod
v jednotlivých zemích světa