Základy kryptografie III.

Šifrovat?…..Rozhodně Ano!

Asymetrické šifry

Jaroslav Pinkava

V úvodní části našeho seriálu jsme hovořili o základních vlastnostech šifrovacích algoritmů . V druhé části jsme se věnovali symetrickým šifrám, tj. šifrám, kde příslušný tajný klíč je použit jak k zašifrování, tak i k dešifraci příslušných textů. V dnešní již třetí části se blíže podíváme na tzv. **asymetrické šifry.** V předešlých pokračováních jsme se o nich již zmínili. Jejich základní vlastností je existence dvou klíčů. Jeden klíč je určen k zašifrování vysílaných zpráv, druhý klíč je určen k dešifrování těchto zpráv. Klíč, který je určen k šifrování nazýváme **veřejným klíčem**, klíč určený k dešifrování se nazývá **soukromý klíč.** Veřejný klíč může být učiněn přístupný široké veřejnosti. S jeho pomocí může zprávy šifrovat vlastně kdokoliv. Avšak pouze majitel příslušného soukromého klíče může tyto zprávy dešifrovat. Soukromý klíč je tedy nezbytné chránit stejně jako tajné klíče pro symetrickou šifru. Kryptosystémy s veřejným klíčem proto také musí být konstruovány tak, aby ze znalosti veřejného klíče nebylo možné odvodit soukromý klíč. Tato význačná vlastnost vede ve svých důsledcích k tomu, že je podstatně složitější konstruovat systémy s veřejným klíčem (asymetrické šifry) než tomu je pro symetrické šifry.

Veřejnost se s pojmem systému s veřejným klíčem setkává teprve od roku 1976, kdy byla opublikována stať autorů Diffie a Hellmana New Directions in Cryptography. Existují však dnes již podložené názory, že tyto systémy byly vynalezeny dříve. Například Angličané oznámili, že systémy s veřejným klíčem byly zde objeveny již na začátku 70-tých let. James Ellis ukázal v roce 1970 teoretickou uskutečnitelnost myšlenky a Clifford Cocks v roce 1973 nalezl určitou variantu RSA. O pár měsíců později Malcolm Williamson vynalezl analog dnešního systému Diffie-Hellmana. Američané (NSA) oznámili, že měli k dispozici systémy s veřejným klíčem o deset let dříve než se objevil revoluční vynález W.Diffie a M.Hellmana. Konkrétně se o něm objevuje zmínka již v NSAM 160 (National Section Action Memorandum 16) z června 1962, dnes odtajněném. Tyto systémy použili při zabezpečení jaderných hlavic.

Systémy s veřejným klíčem byly přivedeny na svět původně proto, aby s jejich pomocí byl vyřešen problém klíčového hospodářství pro symetrické šifry. V síti účastníků, kde potenciálně chce komunikovat každý účastník s každým - utajeně, pomocí symetrické šifry - vzrůstá množství potřebných tajných klíčů. Tyto tajné klíče je třeba samozřejmě předat tak, aby byly k dispozici vždy pouze příslušným dvěma účastníkům. Pokud však v této síti jsou využívany šifry s veřejným klíčem, pak celá situace se stává podstatně jednodušší. Každý účastník získá (vhodným způsobem) dvojicí klíčů - veřejný a soukromý. Veřejné klíče jsou následovně vhodným způsobem "opublikovány" - např. prostřednictvím certifikačních autorit (zmíníme se o nich podrobněji v některém z dalších pokračování našeho seriálu). Nyní každý může zaslat důvěrnou zprávu při užití pouze veřejně dostupné informace. Tuto zprávu může dešifrovat pouze zamýšlený příjemce. Pouze on je majitelem příslušného soukromého klíče.

Uvedeme následující jednoduchý příklad použití systému s veřejným klíčem. Účastník A (budeme mu říkat např. Alenka) chce vytvořit bezpečný kanál zašifrovaný symetrickou šifrou tak, aby jeho prostřednictvím mohl účastníkovi B (můžeme mu říkat třeba Béďa) zasílat své informace. Alenka chce, aby s těmito informacemi se mohl seznámit pouze Béďa a nikdo jiný. Nejprve Alenka získá veřejný klíč Bédi. Prostřednictvím tohoto klíče zašifruje tajný klíč **K** a zašle ho Béďovi. Béďa použije svůj soukromý klíč a dešifruje obdrženou zprávu. Získá tak příslušný klíč pro symetrickou šifru. Nyní Alenka může Béďovi zasílat libovolné množství zpráv zašifrovaných tímto tajným klíčem **K** symetrické šifry. Alenka ví, že pouze Béďa má možnost dešifrovat informace, které mu zasílá pomocí klíče **K**. Pouze Béďa je totiž vlastníkem potřebného soukromého klíče a pouze on mohl správně dešifrovat úvodní zprávu obsahující tajný klíč pro symetrickou šifru.

Další velmi důležitou vlastností systémů s veřejným klíčem je fakt, že poskytují velmi užitečný nástroj pro prostředky autentizace a jsou základem při vytváření digitálních podpisů. V předešlém odstavci vlastně byla popsána určitá nejjednodušší verze autentizačního protokolu, jehož prostřednictvím si Alenka zabezpečila autentizaci příjemce zpráv. V praxi bývají tyto protokoly o něco složitější. Totiž také příjemce chce vědět od koho mu jsou příslušné šifrované zprávy zasílány, tj. chce autentizovat příslušného odesilatele. Tento požadavek přijímajíci strany lze zabezpečit např. následovně. Alenka klíč **K** ze všeho nejdříve zašifruje svým soukromým klíčem. Dále pak postupuje stejně jako v minulém odstavci. K dalšímu šifrování použije veřejný klíč Bédi. Tedy Béďovi zašle klíč **K** nejpve zašifrovaný svým soukromým klíčem a pak zašifrovaný veřejným klíčem Bédi. Na druhé straně Béďa nyní obdrženou zprávu nejprve dešifruje svým soukromým klíčem a potom veřejným klíčem Alenky. Získá tak klíč **K** pro symetrickou šifru. Oproti předešlé situaci však nyní Béďa ví, že tento klíč mu mohla poslat pouze Alenka. Pouze Alenka totiž je vlastníkem příslušného soukromého klíče, nikdo jiný nemohl dospět ke stejnému výsledku bez znalosti Alenčina soukromého klíče.

Tím jsme zároveň ukázali jednoduchou verzi digitálního podpisu. Alenka zasílanou zprávu (klíč) nejprve podepsala svýn soukromým klíčem a teprve pak ji šifrovaně poslala Béďovi. Béďa si po dešifraci svým soukromým klíčem ověřil Alenčin podpis, využil k tomu Alenčin veřejný klíč.

Dnes existuje celá řada konkrétních systémů s veřejným klíčem. Jedním z nejpopulárnějších je stále RSA.
Tento kryptosystém je založen na skutečnosti, že matematici neumí dosti dobře faktorizovat velká čísla. Např. číslo 3239 bylo získáno jako součin dvou menších čísel (dále již nerozložitelných, tedy tzv. prvočísel). Jak lze zjistit, která dvě prvočísla bylo použita? V našem příkladu lze metodou postupných pokusů poměrně snadno dospět k závěru, že 3239=41x79. Jakmile začneme však používat dostatečně velká čísla, záhy zjistíme, že potřebujeme k provedení příslušného rozkladu nějaký výrazně efektivnější algoritmus. Počet potřebných pokusů totiž velmi rychle narůstá. Jak tedy vlastně funguje samotné RSA?

Předpokládejme tedy, že jsem Béďa a chci si nejprve vygenerovat dvojici veřejný klíč a soukromý klíč. Zvolím dvě dostatečně velká prvočísla **p** a **q** (tzn. například každé z těchto prvočísel má délku 512 bitů). Tato prvočísla zvolím náhodně tak, aby nikdo jiný nemohl tyto čísla získat. Spočtu číslo **n=pq**, tj. součin těchto prvočísel. Číslo **n** (parametr kryptosystému RSA) je veřejné a je publikováno spolu s veřejným klíčem.

Dále předpokládejme, že zprávu **z**, kterou chceme zašifrovat máme vyjádřenu v číselné formě, tj. jako jedno číslo, které je menší než **n**, resp. jako posloupnost čísel, z nichž každé je menší než číslo **n**. Označme veřejný klíč symbolem **e**. Vlastní šifrování probíhá dle formule

$$z^e \bmod n = s.$$

Dešifrování soukromým klíčem **d** probíhá analogicky:

$$s^d \bmod n = z.$$

Důležitou otázkou, kterou zbývá vyřešit, je jak získat dvojici klíčů **e** a **d** tak, aby výše uvedené vztahy platily.
Pokud známe rozklad čísla **n** na příslušné prvočinitele **p** a **q**, pak odpověď dává vztah:

$$de \equiv 1 \bmod \phi(n),$$

kde $\phi(n)$ je tzv. Eulerova funkce, která je v našem případě rovna součinu $(p-1)(q-1)$. Fakticky výpočet probíhá tak, že **e** je obvykle pevně zvoleno jako nějaké poměrně malé číslo. Příslušné šifrování proběhne s menším počtem potřebných operací a tedy i rychleji. Číslo **d** je pak dopočteno z výše uvedeného vztahu. Toto mohu provést však pouze tehdy, pokud znám číslo $\phi(n)$, tedy čísla **p** a **q**.

Bezpečnost celého systému je, jak jsme již uvedli, založena na obtížnosti úloze faktorizace. Existují algoritmy, které v dnešní době si dokáží poradit s faktorizací čísla v délce řádově 400 možná 500 bitů. Pokud číslo n má délku 1024 bitů, tak je předpoklad, že v nejbližším desetiletí takovýto kryptosystém nebude prolomen. Variantou RSA je Rabin-Williamsův systém. O tomto kryptosystému bylo dokázáno, že jeho prolomení je ekvivalentní úloze faktorizace.

Dalším důležitým systémem s veřejným klíčem je Diffie-Hellmanův kryptosystém a celá řada kryptosystémů z něj odvozených (např. El Gamalův kryptosystém a Cramer-Shoupův kryptosystém, objevený v letošním roce, dále schéma pro digitální podpisy DSA). Bezpečnost těchto kryptosystémů je založena na složitosti úlohy výpočtu diskrétního logaritmu, tj. stanovení čísla x ze vztahu (čísla **a**, **b** a **p** jsou známa, **p** je prvočíslo):

$$a^x \bmod p = b$$

Stejně jako pro RSA jsou dnes za bezpečné považovány Diffie-Hellmanovy kryptosystémy, kde p má délku 1024 bitů a více.

Třetí důležitou skupinu kryptosystémů s veřejným klíčem tvoří kryptosystémy na bázi eliptických křivek. Jejich bezpečnost je založena opět na úloze diskrétního logaritmu, tentokrát eliptického. Tyto tři kryptosystémy tvoří také základ připravované normy pro systémy s veřejným klíčem pracovní skupinou P1363.

Existuje ještě celá řada dalších konkrétních kryptosystémů s veřejným klíčem. Praktický význam má zejména kryptosystém na bazi Lucasových funkcí. Zajímavý je rovněž nový kryptosystém (1997) vzniklý v laboratořích IBM autorů M. Ajtai and C. Dwork.

V příští části našeho seriálu se budeme věnovat Diffie-Hellmanově kryptosystému, dále pak letošním objevu, novému kryptosystému, jehož autory jsou R.Cramér a V.Shoup. O tomto kryptosystému jejich autoři dokázali, že je bezpečný i proti poměrně sofistikovaným útokům (adaptive chosen ciphertext attack). Následující pokračování bude věnováno eliptickým křivkám.

Slovník kryptologických pojmů:

Asymetrická šifra: kryptografický algoritmus, který používá jiný klíč pro šifrování a jiný klíč pro dešifrování (oproti tomu symetrické šifry používají pro šifrování a dešifrování tentýž klíč).

Veřejný klíč: veřejná část dvojice klíčů v asymetrické kryptografii (public key). Veřejný klíč bývá široce dostupný a může být používán k šifrování zpráv a verifikaci digitálních podpisů.

Soukromý klíč: utajovaná část dvojice klíčů v asymetrické kryptografii (private key). Soukromý klíč je výhradním vlastnictvím jedné entity a není nikomu jinému sdělován. Je používán k dešifraci zpráv zašifrovaných veřejným klíčem a k vytváření digitálních podpisů (které lze verifikovat veřejným klíčem).

Kryptosystémy s veřejným klíčem:

RSA: první praktický kryptosystém s veřejným klíčem založený na složitosti úlohy faktorizace

Rabin-Williams: varianta RSA, je součástí připravované normy skupinou P1363

Diffie-Hellman: první algoritmus s veřejným klíčem, 1976, využívá diskrétní logaritmus v konečných polích

DSA: algoritmus pro digitální podpisy navržený NIST (USA)

El-Gamal: varianta Diffie-Hellmana určená k šifrování

eliptické kryptosystémy: kryptosystémy na bázi eliptických křivek, mají nejkratší klíče z existujících kryptosystémů

Lucasův systém: systém na bázi Lucasových funkcí

Některé zajímavé WWW stránky:

http://csrc.ncsl.nist.gov/publications.html
NIST (National Institute of Standarts and Technology), řada kryptografických norem

http://www.io.com/%7Eritter/NETLINKS.HTM
Ritter's Net Links, další řada adres na webu týkajících se problematiky kryptologie

http://www.rsa.com/
webovské stránky firmy RSA, obsahují řadu užitečných informací

http://grouper.ieee.org/groups/1363/
P1363, pracovní skupina připravující novou normu pro systémy s veřejným klíčem

http://www.maths.uq.oz.au/~krm/listi.html
široký seznam adres k problematice teorie čísel, včetně teorie čísel v kryptologii, v systémech s veřejným klíčem