Kryptografie

Anna Bernáthová*, Jan Hudeček**, Jiří Syrový***

* Gymnázium Bernarda Bolzana, P-8 (anicka@matfyz.cz)
** Gymnázium Voděradská, P-10 (hudecekjan@volny.cz)
*** Gymnázium J. K. Tyla, HK (syrovy.jiri@quick.cz)

Abstrakt:

Už jste někdy zkoušeli vykrást banku? Zajímalo by vás, proš se vám to nepovedlo? Píšete milostný dopis a chcete ho skrýt před zvědavým bratrem?

Naše práce se zabývá kryptografií – transformováním textu do podoby, kterou je možno dešifrovat pouze se znalostí patřičného klíče. Dozvíte se zde např. o principu elektronického podpisu a o tom, že není zcela bezpečný. Tento problém ale řeší kvantová kryptografie, které je věnována závěrečná část práce.

1. Úvod

Již od dávnověku lidé touží předávat si zprávy tak, aby si je nemohl přečíst nikdo nepovolaný. Kryptografie tedy existuje už dávno, primitivní šifrovací tabulku používal už César. S jednoduchými šiframi se často setkáváme např. ve hrách na táborech – každé písmenko zprávy zaměníme za nějaký symbol a jsme hotoví. Tomu se říká substituční šifra. Její rozluštění je však celkem snadné – pokud máme dostatečně dlouhý text, budou se v něm některé symboly vyskytovat se stejnou četností jako v přirozeném jazyce. Mezi další jednoduché šifry patří např. šifry translační nebo transpoziční.

My se budeme věnovat nejen klasickým moderním, ale i kvantovým šifrám. První se dnes používají např. v bankovní komunikaci a s nimi stojí a padá tolik diskutovaný elektronický podpis. Fungují na principu veřejného klíče. A druhé zmíněné jsou stále ještě ve stadiu vývoje.

2.1 Klasická moderní kryptografie

Ačkoliv princip kryptografie s veřejným klíčem je velice jednoduchý, objeven byl teprve před pětadvaceti lety. Do té doby platilo ve světě šifrování pravidlo, že šifrovací klíč je jeden a jeho znalost slouží k rozšifrování i zašifrování zprávy. Systémy s veřejným klíčem uvedly do kryptografie existenci klíčů dvou, jednoho veřejně známého a druhého tajného, a umožnily tím zjednodušit řadu problémů, týkající se komunikace zejména vzdálených osob. Ukážeme si nyní, na čem je asymetrická kryptografie založena.

Zprávu jakýmkoliv standartním způsobem převedeme na číslo a poté zašifrujeme pomocí veřejného klíče – provedeme s ní jistou operaci a dostaneme zašifrovaný text. Její podstatnou vlastností je, že provedení opačné operace (rozšifrování) musí být velmi obtížné, pokud kromě

veřejného klíče neznáme ještě další informaci, klíč soukromý. Bez znalosti tohoto klíče to dnešnímu počítači při použití nejlepších z dosud známých algoritmů trvá řádově miliardy let.

První z úspěšných šifer tohoto typu je RSA, pojmenovaná podle prvních písmen příjmení svých tvůrců Rivest, Shamir, Adleman. Uvedeme si ji jako příklad.

Nejdříve zavedeme operaci modulo, kterou budeme potřebovat. *A* modulo *M* je celočíselné zbytek po dělení čísla *A* číslem *M*. Modulo *M* lze provádět i aritmetické operace jako je sčítání a násobení. To uděláme tak, že operandy nejdříve sečteme nebo vynásobíme a výsledek této operace modulo *A* je pak výsledkem celého příkladu. Tak například $15^2 = 1 \pmod{16}$. Už z uvedeného příkladu je patrné, že například umocňování modulo *A* se bude chovat jinak, než jsme na to zvyklí z reálných čísel. Přesněji řečeno, vlastnosti takových funkcí, jako je k-tá mocnina závisejí na tom, jaký je prvočíselný rozklad modulu *M*. Podobně jako umocňování lze na aritmetice modulo *A* zavést i odmocňování. Zatímco však spočítat *x* na *k*-tou mod *M* je jednoduché a stačí k tomu znát *M*, *x* a *k*, spočítat *k*-tou odmocninu z *x* mod *M* bez znalosti prvočíselného rozkladu modulu *M* nedokážeme. Na tom je právě založen systém RSA. Každý člověk má určen svůj modul *M*, který je součinem dvou velkých prvočísel a tato prvočísla zná jenom on sám.

2.2 Matematický princip šifrování s veřejným klíčem

Máme číslo $n = pq$, kde *p* a *q* jsou různá velká prvočísla (minimálně padesát cifer). Dále máme exponent *s*. Dvojice čísel *n* a *s* tvoří veřejný klíč – může ji tedy znát kdokoliv a použít ji k zašifrování zprávy. Zprávu převede na číslo *M* a zašifruje operací $E=(M^s \pmod{n})$. *E* je šifrovaná zpráva (encrypted), *M* je původní zpráva (message). Jak převést daný text na čísla? Můžeme například k A přiřadit 10, B = 11, C=12 atd. Mezera mezi písmeny bude 99. Napíšeme takto celý text (např. 202324329929173428142115) za sebe a rozdělíme jej na bloky, které jsou menší než *n*. Tedy pokud *n* = 23 393, můžeme text rozdělit na bloky 20 232 –4 329 –9291 –7342 –8142 –115. Moc na tom nezáleží, ale kvůli dešifrování by žádný blok neměl začínat nulou. Zároveň nesmíme reprezentovat jednotlivé znaky různě dlouhými čísly – pokud se rozhodneme písmenu A přiřadit číslo 1, nebude vědět, jestli 12 znamená L (dvanácté písmeno abecedy) nebo AB. S takto upraveným textem provedeme výše zmíněnou operaci. Nyní může text rozluštit pouze příjemce, který umí *n* faktorizovat – nám se to už nikdy nepodaří.

Než si budeme povídat o dešifrování, je nutno se zmínit o Eulerově funkci, kterou budeme potřebovat. Funkce $\phi(n)$ přiřadí číslu *n* hodnotu rovnou počtu čísel, která jsou menší než *n* a jsou s ním nesoudělná. Tedy pro prvočíslo *p* platí, že $(p) = p-1$. Pro součin dvou prvočísel platí, že $(pq)=(p-1)(q-1)$. Poznamenejme, že pro účely šifrování je nutné, aby čísla *n* a *s* byla nesoudělná, tedy $(n,s)=1$.

Mějme b, jeden blok zprávy, potom je $0 \leq b \leq n - 1$. Je zašifrován operací $E \equiv M^s \pmod{n}$.

Pokud si zvolíme jako příklad $b = 20232$, $p=149$ a $q=157$, takže $n=23393$ a $\phi(n) = 23088$. Musíme si zvolit exponent *s*, nesoudělný s $\phi(n)$. Nejmenší takové číslo je 5. Takže zprávu zakódujeme tak, že spočítáme zbytek z 20232^5 modulo 2 393. To je 20036, takže $E = 20036$. Stejným způsobem zašifrujeme zbytek zprávy.

Nyní se konečně dostáváme k dešifrování. Kromě informací obsaženým ve veřejném klíči musíme znát ještě exponent inverzní k *s* modulo $\phi(n)$, říkáme mu klíč soukromý. Nazvěme jej exponent *d*. Spočítáme jej takto: $ds \equiv 1 \pmod{\phi(n)}$. Pokud známe faktorizaci čísla *n*, známe i $\phi(n)=(p-1)(q-1)$. Exponent *d* tedy můžeme spočítat takto:

$d \equiv s^{\phi(\phi(n)) - 1} \pmod{\phi(n)}$, protože $ds \equiv s^{\phi(\phi(n))} \pmod{\phi(n)}$.

Pokud šifrovaná zpráva je $E \equiv M^s \pmod{n}$, můžeme ji dešifrovat $E^s \equiv M^{sd} = M^{\phi(n)k} + 1 \pmod{n}$.

$M^{\phi(n)} \equiv 1 \pmod{n}$ a *tedy* $E^d \equiv M \pmod{n}$. Aby celý proces fungoval jak má, je nutné, aby M bylo nesoudělné s n. Tím se ale nemusíme příliš trápit, protože šance, že tomu tak nebude je v řádu 10^{-50}.

Zájemce o tuto problematiku tedy odkazujeme na seznam literatury na konci příspěvku.

2.3 Bezpečnost

Šifra, kterou jsme představili, není v principu bezpečná. To, že neznáme algoritmus, jak rychle faktorizovat (rozkládat na prvočísla) neznamená, že žádný neexistuje. Americké tajné služby zaměstnávají největší matematické mozky planety, aby tento problém vyřešily a vůbec není jisté, jestli už toto tajemství dávno neodhalily. Navíc, se zdokonalováním výpočetní techniky jednou přijde okamžik, kdy i použití současného algoritmu nebude trvat příliš dlouho (z toho existují některé výjimky, například algoritmy, jež by k úspěšnému běhu potřebovaly více paměti, než kolik je ve vesmíru atomů). Pokud se podaří sestrojit kvantové počítače, bude klasické kryptografii definitivně odzvoněno. Již nyní se podařilo faktorizovat číslo 15 pomocí kvantového počítače a vývoj pokračuje.

3.1 Kvantová kryptografie

Impuls k vývoji kvantové kryptografie dala obava o bezpečnost klasické kryptografie, která by se mohla již za několik let stát téměř nepoužitelná. Základní myšlenkou kvantové kryptografie je generování „stejných“ náhodných čísel pro obě strany (odesilatele i příjemce), které se poté použijí pro zašifrování textu například pomocí funkce **xor**. Pokud použijeme k zašifrování klíč stejně dlouhý jako je vlastní text, znemožníme útok. Tento způsob se samozřejmě dá použít i bez kvantového přenosového kanálu, ale je nutné doručit klíč jinak, což není tak bezpečné jako při použití KPK. Při využití KPK je náhodnost těchto čísel zaručena použitím náhodného fyzikálního děje, jehož bezpečnost zaručuje sama příroda.

Řekněme, že Alice a Bob si chtějí poslat šifrovanou zprávu. Jsou dva způsoby jak to mohou udělat. První a starší z nich je protokol BB84, který navrhli v roce 1984 Charles Bennett a Gilles Brassard. Jejich protokol (BB84) využívá v zásadě dvou kvantových poznatků: teorému o *klonování kvantových stavů* a nemožnosti měření určitých párů veličin současně. Je nutné uvést, že protokol řeší pouze nejcitlivější místo utajené komunikace. A sice výměnu klíčů bez použití důvěryhodné osoby, která by klíče oběma stranám doručila. Pokud jsme totiž schopni (kvantově-) bezpečně distribuovat klíč, pak nám nic nebrání v tom, abychom jako komunikační schéma použili některý z klasických algoritmů (nenapadnutelných kvantovým počítačem), jako je například dříve zmíněný **xor**.

Toto schéma funguje relativně jednoduše. Dva účastníci (Alice a Bob) se nejdříve domluví na tom, které dvě roviny polarizace použijí. Alice použije laser na vysílání jednotlivých fotonů, které poté zachytává jak Alice tak i Bob. Alice i Bob si náhodně zvolí rovinu polarizace pro přijmutí každého fotonu. Informaci o tom, jakou si zvolili rovinu polarizace si po skončení komunikace vymění po veřejném kanálu. Pro šifrování mohou použít pouze ta náhodná data, která se shodují v polarizaci. Pokud by někdo „poslouchal“ a zvolil si špatnou rovinu polarizace bude ovlivňovat posílaná data, čímž zvýší chybovost na úroveň, podle které jasně zjistíme zda někdo poslouchá.

Dále existuje druhá, novější (1991) metoda, která se od první liší hlavně složitostí, a také zdrojem fotonů. Tato metoda používá dva fotony v tzv. provázaném stavu. Fotony jsou v tomto

stavu silně korelovány. Každý z účastníků obdrží svůj foton a změří jeho polarizaci. Když zvolí stejnou polarizaci, získají sobě si jednoznačně odpovídající hodnoty.

Obě metody jsou silně citlivé na jakékoliv vnější změny, a proto také pokud někdo bude poslouchat, ovlivní konečnou statistiku přijatých hodnot, která se vyhodnotí, a případný odposlech prozradí.

3.2 Výhody a nevýhody kvantové kryptografie

Hlavní výhodou je principiální neprolomitelnost. Skutečná neprolomitelnost záleží na implementaci. Například je problém přesně zjistit, zda je chybovost kanálu je způsobena "odchytáváním" či skutečnou chybovostí přenosového kanálu. Další možnost útoku je na veřejný kanál (A--E--B - Eva mění přenesené informace).

Mezi nevýhody patří zatím malá přenosová vzdálenost (zatím max. 30 km), malá přenosová rychlost, drahá implementace a nutnost "pevného" přenosového kanálu. Některé nevýhody by se daly samozřejmě částečně odstranit. Například znásobení počtu přenosových kanálů, ...

Pro praktické použití tato kryptografie sice příliš nehodí, ale zvyšuje bezpečnost například u bank, státních a vojenských institucí, ...

4. Závěr

Dnes, kdy většina písemné komunikace probíhá elektronicky, se bez kryptografie neobejdeme. Aplikace kvantové kryptografie je velmi nákladná, ale myslíme, že v nejbližších letech se nemusíme bát používat podstatně méně náročnou kryptografii klasickou.

Poděkování

Děkujeme Doc. Ing. Igoru Jexovi DrSc. za uvedení do problematiky a za poskytnutí literatury. FJFI ČVUT za zajištění materiálního zázemí. Marianovi Kechlibarovi za konzultace. Organizátorům Fyzikálního týdne za jejich úsilí o to, aby tato akce proběhla ke spokojenosti všech zúčastněných.

Reference:

[1] HOI-KWONG-LO - POPESCU, S. - SPILLER, T.: *Introduction to Quantum Computation and information,* World Scientific, Singapore, 1998, 79-113

[2] SCHROEDER, M.R.: *Number Theory in Science and Communication,* Springer-Verlag, Heidelberg, 1986, 26-38

[3] COUTINHO, S.C.: *Mathematics of ciphers*, A K Peters Ltd., Natilk, Massachusetts, 1998

[4] BOUWMEESTER, D.-EKERT, A.-ZEILINGER,A.: *The Physics of Quantum Computation,* Springer-Verlag, Heidelberg, 2000, 26-45

[5] MACCHIAVELLO, C.- PALMA, G.M.-ZEILINGER, A.: *Quantumcomputation and quantum information theory,* World Scientific, Singapore, 1999, **235**

[6] WILLIAMS, C.-CLEARWATER, S.H.: *Explorations in quantum computing,* Springer-Verlag, New York, 1998, 163-183

[7] KUPČA, V.: http://cml.fsv.cvut.cz/~kupca/qc/qc.html, 2001