INFORMATIKA

Moderní šifry I

EDUARD BARTL

Přírodovědecká fakulta UP, Olomouc

Série článků o šifrování se snaží přiblížit problematiku moderních šifrovacích metod čtenáři se základními znalostmi středoškolské matematiky. První díl série vykládá základní principy asymetrického šifrování a bezpečné výměny tajného klíče. Text směřuje k vysvětlení šifry, které se říká RSA a která v současné době hraje důležitou roli při zabezpečení komunikace na Internetu i v dalších souvisejících oblastech, například v elektronickém podpisu. V této sérii tak nahlédneme pod pokličku objevům, které se podílely na prudkém rozvoji Internetu; jen těžko si lze totiž představit, že by byl Internet používaný v takové míře jako je tomu dnes, kdyby jeho uživatelé neměli solidní možnost ochránit svoje soukromé údaje a soukromou komunikaci.

Co se Eva nesmí dozvědět

Existuje mnoho způsobů, jak utajit citlivou informaci. Některé způsoby utajení jsou velmi jednoduché (například substituční nebo transpoziční šifra), jiné jsou naopak značně složité (například šifrovací stroj Enigma; ten byl dokonce kvůli své složitosti po nějakou dobu považován za nerozluštitelný). Přestože se tyto šifry zdají být rozdílné, scénář, jímž se řídí, je stále stejný. Zkusme si ho ve stručnosti popsat.

Na začátku jsou dva lidé, kteří si potřebují sdělit nějakou důvěrnou zprávu; tuto důvěrnou zprávu obyčejně nazýváme *otevřeným textem*. Odesilateli zprávy se v kryptografii zpravidla říká *Alice*, příjemce bývá pojmenován jako *Bob*. Aby Alice zajistila utajení této zprávy, tak ji zašifruje a pak pošle Bobovi. V tento okamžik nijak neřešíme, jestli je zpráva poslána

prostřednictvím pošty (ať už klasické nebo elektronické), telegrafu nebo nějakým jiným způsobem. Pouze předpokládáme, že způsob přenosu zprávy nijak nezaručuje její utajení (proto také Alice před odesláním zprávu zašifrovala). Do hry tak může vstoupit třetí osoba, která má možnost bez velkého úsilí zašifrovanou zprávu obdržet a na šifru takzvaně zaútočit; to znamená, může se pokusit ze zašifrované zprávy získat zprávu původní. Této třetí osobě se v knížkách o kryptografii často říká *Eva*.[1)] Bob v určitém okamžiku zašifrovanou zprávu přijme a dešifruje ji, čímž obdrží onu důvěrnou informaci od Alice. Všimněme si dobře, že ani Alice ani Bob nemají možnost zjistit, jestli skutečně došlo k Evině pokusu o útok. Protože jsou však paranoidní, tak útok předpokládají a snaží se použít natolik bezpečné šifrování, aby se Evě útok nezdařil.

V první polovině 20. století bylo konstruktérům šifer jasné, že by bezpečnost šifer neměli zakládat na utajení toho, jak šifry fungují.[2)] Princip fungování šifer[3)] se totiž utajuje jen velmi obtížně. Stačí, aby jeden z konstruktérů buď z vlastních pohnutek nebo proto, že byl nějakým způsobem donucen, princip Evě vyzradil a ta pak může nerušeně číst šifrovanou komunikaci, aniž by si toho byli Alice s Bobem vědomi.

Princip fungování šifry se proto zpravidla zveřejňuje. Je ovšem zřejmé, že musí existovat *něco*, co musí být drženo v tajnosti a co zajistí, že se Evě nepodaří zašifrovanou zprávu rozluštit. Čtenář se jistě dovtípí, že tím, co je potřeba držet v tajnosti, je nějaká podoba *tajného klíče*. Tento klíč musí být známý pouze Alici a Bobovi, Eva ho nesmí získat; pomocí něj totiž Alice provádí šifrování a Bob dešifrování.

Šifrování a dešifrování pod drobnohledem

Pokusme se nyní vše vysvětlit podrobněji. Šifrování a dešifrování se v kryptografii popisuje *matematickými funkcemi*. Matematickou funkci, která realizuje šifrování, budeme označovat písmenem e (využijeme prvního písmene anglického slova *encipher*, které znamená *šifrovat*) a budeme ji nazývat *šifrovací funkce*. Tato funkce „vyrobí“ z nějakého znaku x ote-

[1)] Patrně proto, že výslovnost anglické varianty tohoto jména – *Eve* – je [i:v]. Je tedy stejná jako výslovnost začátku anglického slova *eavesdrop* [i:vz.dra:p], což znamená *tajně naslouchat*.

[2)] Je historicky doloženo memorandum německých kryptografů pracujících na zlepšování šifrovacího stroje Enigma, které říká, že „při posuzování bezpečnosti šifry se předpokládá, že nepřítel má šifrovací stroj k dispozici“ [4].

[3)] Principem fungování šifry rozumíme postup, jakým tato šifra „vyrobí“ z otevřeného textu zašifrovanou zprávu a naopak.

vřeného textu a nějakého tajného klíče k určitý znak y zašifrovaného textu, což stručně zapisujeme jako

$$y = e(x, k).$$

Matematickou funkci, která popisuje dešifrování, budeme označovat písmenkem d (opět zde využijeme prvního písmene anglického slova: *decipher* znamená *dešifrovat*) a budeme ji nazývat *dešifrovací funkce*. Funkce d, jak můžeme čekat, z nějakého znaku y zašifrovaného textu a nějakého tajného klíče k „vyrobí“ příslušný znak x otevřeného textu. To může být opět stručně zapsáno jako

$$x = d(y, k).$$

Funkce e a d jsou přitom navrženy tak, že pokud Alice použije funkci e k zašifrování znaku x pomocí klíče k a získá tak znak y, pak Bob dešifrováním y pomocí téhož klíče k musí získat původní znak x. Musí tedy platit

$$d(e(x, k), k) = x.$$

Funkcím, které splňují tuto podmínku, se říká *inverzní*.[4)]

Dobře si všimněme, že co se šifrování a dešifrování týče, mají Alice a Bob stejné schopnosti. To znamená, že stejně jako Alice může šifrovat zprávu a Bob ji pak dešifrovat, může naopak Bob nějakou zprávu zašifrovat a Alice ji dešifrovat. Z tohoto pohledu je tedy vztah Alice a Boba symetrický a každému šifrování, které se vyznačuje touto vlastností, se proto říká *symetrické šifrování*.

Pro lepší pochopení si vše ukážeme na jednoduchém příkladu. Znaky otevřeného textu musí být nejprve vhodným způsobem kódovány, to znamená, převedeny na čísla, se kterými funkce e a d (a potažmo i počítač) umějí pracovat. Vhodné by bylo použít známé ASCII kódování,[5)] pro naše účely však bude bohatě stačit následující jednoduché kódování: písmeno `a` budeme kódovat číslem 0, písmeno `b` číslem 1, písmeno `c` číslem 2 atd. Nebudeme přitom uvažovat českou diakritiku (písmena s háčky, čárkami nebo kroužky) ani interpunkční znaménka (čárky, tečky, středníky,

[4)] S tímto pojmem se setkáváme na střední škole při výuce reálných funkcí jedné reálné proměnné – například na intervalu $\langle 0, \infty)$ je kvadratická funkce inverzní k funkci druhá odmocnina.

[5)] ASCII je zkratkou z American Standard Code for Information Interchange, což znamená „americký standardní kód pro výměnu informací“. ASCII umožňuje kódovat 128 znaků, například mezera je kódována číslem 32, malé písmeno `a` je kódováno číslem 97 a tak podobně.

závorky, uvozovky apod.); potřebovat budeme pouze (viditelnou) mezeru ␣, kterou budeme kódovat číslem 26. Kódování je přehledně znázorněno v tab. 1.

znak	`a`	`b`	`c`	`d`	...	`y`	`z`	␣
kódové číslo	0	1	2	3	...	24	25	26

Tab. 1 Jednoduché kódování písmen abecedy a mezery ␣.

Uvažovat budeme jednoduchou posouvací šifru; tajným klíčem k je číslo určující posunutí abecedy zašifrovaného textu vůči abecedě otevřeného textu. Šifrovací funkce e je pak definována následujícím způsobem:

$$e(x, k) = x + k, \tag{1}$$

kde x je jedno z čísel od 0 do 26 kódující znak otevřeného textu. Předpokládejme, že se Alice s Bobem shodnou na tajném klíči $k = 5$ a že Alice bude chtít zašifrovat písmeno `b`. Nejprve si z tab. 1 zjistí kód tohoto písmene (číslo 1) a pak již může vypočítat hodnotu funkce e:

$$e(x, k) = e(1, 5) = 1 + 5 = 6.$$

Z téže tabulky pak Alice zjistí, jaké písmeno se kóduje číslem 6. Dojde tedy k závěru, že písmeno otevřeného textu `b` se šifruje písmenem `G` (v literatuře o kryptografii bývá zvykem psát otevřený text malými písmeny, kdežto zašifrovaný text velkými písmeny). Pozornému čtenáři jistě neunikne, že takto definovaná šifrovací funkce nepracuje zcela správně. Pokud by totiž Alice potřebovala šifrovat znak, jenž se kóduje číslem 22 nebo vyšším, pak by se přičtením čísla 5 dostala mimo rozsah tab. 1. Toto „přetečení“ se dá naštěstí snadno odstranit tak, že se začne počítat od začátku.[6)] Například písmeno `y` kódované číslem 24 se tak bude šifrovat písmenem `C` kódovaným číslem 2.

Jak již dobře víme, dešifrovací funkce d je inverzní k šifrovací funkci e, platí tedy

$$d(y, k) = y - k, \tag{2}$$

kde y je jedno z čísel od 0 do 26 kódující znak zašifrovaného textu. Samozřejmě zde musíme vyřešit „podtečení“ v případě, že dešifrujeme písmena kódovaná číslem 4 nebo menším. To se však dělá podobným trikem jako v případě „přetečení“. Můžeme tak snadno ověřit, že písmena `G` a `C` se pomocí funkce d dešifrují zpět na písmena `b` a `y`.

[6)] Využijeme takzvanou *modulární aritmetiku*. Podrobně se k tomuto „kruhovému počítání“ vrátíme v příštím díle.

Nejde-li to silou, pak to půjde ještě větší silou

Jednoduché symetrické šifry, o kterých byla doposud řeč, se v dnešní době nedají k praktickému šifrování použít – jsou nevhodné k šifrování e-mailových zpráv, k zabezpečení komunikace mezi bankou a klientem a podobně. Důvod je nasnadě. Ve chvíli, kdy na scénu vstoupily moderní počítače, zmíněné šifry přestaly být bezpečné. Pokud totiž Eva zachytí zašifrovanou zprávu, může rychle pomocí počítače zkoušet různé klíče a skončit ve chvíli, kdy obdrží nějaký smysluplný text. Pokud je zašifrovaná zpráva dostatečně dlouhá, tak si může být jistá, že je tento smysluplný text hledanou zprávou. Tomuto způsobu získání tajného klíče se říká *útok hrubou silou*. Pojmenování je to vskutku příhodné; Eva nemusí vymýšlet nic složitého, stačí hrubou silou „kácet“ jeden klíč za druhým.

Čtenáře jistě napadne, že by pro zajištění bezpečnosti stačilo zvětšit počet klíčů natolik, že by Evě i nejrychlejším počítačem trvalo příliš dlouho projít všechny možné kombinace klíčů. Dostatečná délka tajných klíčů a potažmo i dostatečně velký počet různých klíčů je skutečně jedním ze základních požadavků, které musí moderní šifry splňovat.[7)] Například šifra AES[8)] používá klíče, které mají, pokud je zapíšeme v binární podobě, délku až 256 bitů (to znamená, že tajným klíčem je posloupnost nul a jedniček a délka této posloupnosti je až 256). Počet všech klíčů je tedy $2^{256} \doteq 1{,}158 \cdot 10^{77}$, což je skutečně obrovské číslo.[9)]

Mohlo by se zdát, že bezpečné moderní šifry s dlouhým klíčem vyřešily problém se zabezpečením komunikace. Zdaleka tomu tak není. Dokonce i šifra AES trpí jedním zásadním nedostatkem. Představme si následující situaci: Alice, Bob a Charlie spolu potřebují (každý s každým) zabezpečeně komunikovat. Například tedy Alice si potřebuje posílat zprávy s Charliem tak, aby je Bob (a kdokoliv jiný) nemohl číst. Použijí k tomu šifru AES nebo jinou dostatečně bezpečnou šifru. Kolik tajných klíčů si musí mezi

[7)] Zdůrazněme, že dostatečně velký počet klíčů nezaručuje, že je daná šifra skutečně bezpečná. K šifrám, jako je substituční šifra nebo Vigenèrova šifra, existují velmi chytré metody, jak rychle najít tajný klíč bez použití hrubé síly (v případě substituční šifry stačí použít frekvenční analýzu, u Vigenèrovy šifry je nejprve potřeba zjistit délku bloku). Moderní bezpečné šifry musí být odolné i vůči těmto metodám.

[8)] AES je zkratkou z anglického názvu Advanced Encryption Standard. Jedná se o takzvanou blokovou šifru, která byla zavedena roku 2001 a dnes je využívaná zejména v protokolu WPA2 definujícím komunikaci a zabezpečení v bezdrátových Wi-Fi sítích. Tuto šifru také využívá známý program pro internetovou telefonii – Skype.

[9)] Pro srovnání: počet atomů ve viditelném vesmíru se odhaduje na 10^{80}.

sebou vyměnit?[10] Snadno se dopočítáme, že pouze 3 – jeden tajný klíč si musí vyměnit Alice s Bobem, jeden Alice s Charliem a jeden Charlie s Bobem. Pokud do své skupiny přiberou ještě jednoho účastníka, řekněme kupříkladu Davida, pak již budou potřebovat 6 klíčů. Jak bude vypadat situace, pokud skupina bude mít obecně n účastníků? Protože každé dvojici ze skupiny přiřazujeme jiný klíč (přičemž nezáleží na pořadí účastníků v dané dvojici), můžeme počet klíčů v závislosti na počtu účastníků vyjádřit kombinačním číslem

$$\binom{n}{2} = \frac{n!}{(n-2)! \cdot 2!} = \frac{n \cdot (n-1)}{2}.$$

Například pro skupinu o tisíci účastnících tedy celkem potřebujeme

$$\frac{1\,000 \cdot 999}{2} = 499\,500 \text{ klíčů.}$$

Vidíme tedy, že počet tajných klíčů roste s počtem účastníků dosti rychle. To klade velké nároky na *správu klíčů*: klíče je nejprve potřeba vytvořit, účastníci si je musí vyměnit a poté bezpečným způsobem uložit. A právě ve výměně tajných klíčů tkví hlavní nevýhoda symetrických šifer (tedy i šifry AES). Tato výměna totiž musí probíhat opět zabezpečeně. Jestliže by se Evě podařilo během výměny tajný klíč získat, tak by mohla nerušeně číst jakoukoliv zprávu tímto klíčem zašifrovanou.

Jakým způsobem bezpečnou výměnu klíčů vyřešit? Lákavá možnost by mohla být následující: pokud se chce Alice domluvit s Bobem na nějakém tajném klíči, tak ho může jednoduše zašifrovat (třeba s využitím téže šifry, kterou se chystají zabezpečit samotnou komunikaci). Tím se ale zjevně problém nevyřeší, pouze odsune na jinou úroveň; pro zašifrování tajného klíče se totiž Alice a Bob musí bezpečně domluvit na dalším tajném klíči.

Přibližně do 60. let 20. století, tedy v dobách, kdy šifrování zpráv používala především armáda nebo vládní organizace dané země, se výměna klíčů řešila celkem jednoduše. Komunikující strany se buď osobně setkaly a klíč si vyměnily nebo si zajistily nějakého důvěryhodného kurýra a ten jim výměnu tajného klíče zprostředkoval. Přestože není toto řešení zrovna ideální, v minulosti fungovalo celkem uspokojivě. Situace se však zcela zásadně změnila v okamžiku, kdy se začaly ve větší míře používat počítače

[10] V anglicky psané literatuře se často používá termín *key exchange*, proto budeme také mluvit o *výměně klíče*. Víme však, že klíč pro šifrování i dešifrování je tentýž, takže bychom měli tuto výměnu spíše chápat jako *vzájemné sdělení klíče*. Proto se také můžeme setkat s příhodným označením *key distribution – distribuce klíče*.

v soukromé sféře a pro firmy i běžné uživatele vyvstala nutnost zabezpečit svoji vlastní komunikaci. Osobní setkání komunikujících stran za účelem výměny klíče se stalo prakticky neproveditelné a použití důvěryhodného kurýra příliš zdlouhavé a finančně nákladné. Bylo tedy nezbytně nutné najít nějaký jiný způsob bezpečné výměny tajných klíčů, který by obstál i v nových podmínkách nebo vymyslet zásadně jiný způsob šifrování, který by výměnu klíčů vůbec nevyžadoval.

Bezpečná výměna klíče

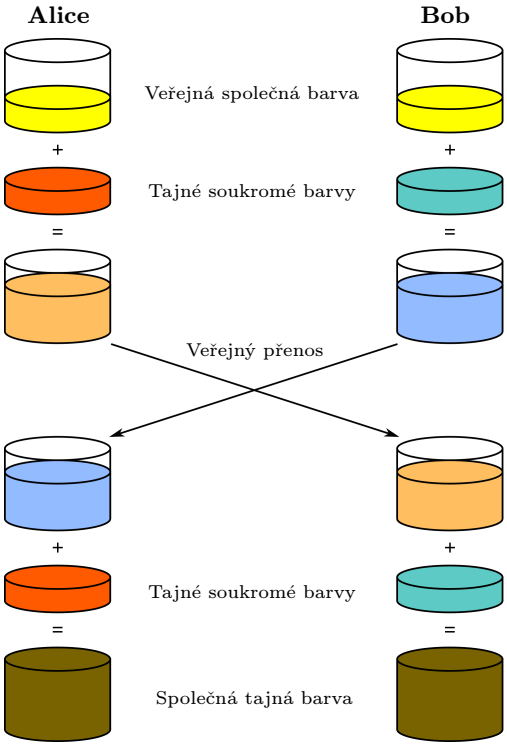
Povězme si nejprve něco o první možnosti – o bezpečné výměně tajného klíče. S velmi zajímavým řešením přišli američtí informatici Ralph Merkle, Whitfield Diffie a Martin Hellman. Tato metoda byla publikována roku 1976 [1], o dvacet let později však vyšlo najevo, že byla objevena již na začátku sedmdesátých let Jamesem Ellisem, Cliffordem Cocksem a Malcolmem Williamsonem. Tito kryptografové ovšem na svůj objev přišli v rámci své práce v britské vládní zpravodajské a špionážní organizaci GCHQ (Government Communications Headquarters) a nemohli tak svůj objev zveřejnit.

Pokusíme se Diffieho–Hellmanovu–Merklovu výměnu klíče (jak je často nazývána) vysvětlit na příkladu, který by byl sice v praxi těžko použitelný, dobře však demonstruje popisovaný princip. Představíme si totiž, že tajným klíčem nebude nějaké číslo, jak tomu bylo doposud, ale bude jím plechovka s barvou určitého odstínu. Bezpečnost šifrování tedy bude založena na obtížnosti uhádnout odstín této barvy.

Postup výměny tajné barvy je znázorněn na obr. 1. Tento obrázek je rozdělen do dvou sloupců, v levém jsou zobrazeny barvy, jež má k dispozici Alice v jednotlivých krocích výměny, v pravém sloupci jsou pak uvedeny barvy, které získává v jednotlivých krocích Bob. Barva, na které se Alice a Bob potřebují dohodnout, je hnědá, zobrazená vespod obrázku.

Proces výměny začne tím, že se Alice a Bob dohodnou na nějaké společné barvě; na obrázku je tato barva zobrazena na prvním řádku, jedná se tedy o žlutou barvu. Tato společná barva může být zvolena náhodně a Alice a Bob se na ní mohou dohodnout nezabezpečeně. Je tedy lhostejno, zdali se Eva dozví, že se jedná o žlutou barvu či nikoliv. V dalším kroku (zachyceném na druhém řádku obrázku) si Alice i Bob zvolí svoji vlastní tajnou barvu. V našem případě si Alice zvolila červenou barvu, Bob zelenou barvu. Svoji vlastní tajnou barvu si Alice i Bob mohou zvolit náhodně, je však nezbytně nutné, aby obě tyto tajné barvy zůstaly utajené. Poté

Alice smíchá společnou žlutou barvu se svojí tajnou barvou (červenou) a stejně tak Bob smíchá společnou barvu se svojí tajnou barvou (zelenou). Smícháním získají novou barvu – Alice béžovou, Bob modrou.



Obr. 1 Diffieho–Hellmanova–Merklova výměna tajného klíče (zdroj: Wikipedia https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange)

V dalším kroku si Alice a Bob tyto smíchané barvy vymění (výměna může proběhnout nezabezpečeně). Alice tedy obdrží modrou barvu, Bob béžovou; na obrázku je tento moment zachycen na čtvrtém řádku. Posledním krokem je přidání tajné barvy do takto vyměněné barvy: Alice smíchá červenou barvu s modrou, získá tak hnědou barvu, Bob smíchá zelenou barvu s béžovou a získá také hnědou barvu.

Jak je možné, že Alice i Bob získají na konci výměny stejnou barvu? Zdůvodnění je snadné a pozorný čtenář je jistě uviděl v průběhu čtení předchozích dvou odstavců. Stačí sledovat, jakým způsobem „cestuje“ schéma-

tem společná barva zvolená na začátku:

1. společná (žlutá) barva na straně Boba byla nejprve smíchána s Bobovou tajnou barvou (zelenou), pak byla poslána na stranu Alice, kde byla smíchána s její tajnou barvou (červenou);
2. společná (žlutá) barva na straně Alice byla smíchána s její tajnou barvou (červenou), poslána Bobovi, který ji smíchal se svojí tajnou barvou (zelenou).

Jak můžeme vidět, v obou dvou případech byla společná (žlutá) barva smíchána s oběma tajnými barvami (červenou a zelenou). Jediný rozdíl mezi body 1 a 2 je v tom, že jsou tajné barvy přidány v opačném pořadí. Výsledek smíchání však musí být totožný, v našem příkladě je jím hnědá barva.

Můžeme si také všimnout, že pokud bude Eva odposlouchávat komunikaci mezi Alicí a Bobem, pak získá společnou (žlutou) barvu a barvy, které vznikly přidáním tajných barev do této společné barvy (modrou a béžovou). Bez znalosti aspoň jedné z tajných barev však nikdy nedospěje k výsledné (hnědé) barvě, která představuje tajný klíč.

Jak bylo řečeno v úvodu této sekce, zvolený příklad s mícháním barev by byl v praxi nepoužitelný. Ve skutečné Diffieho–Hellmanově–Merklově výměně klíče se proto nemíchají barvy, ale jistým způsobem se „míchají“ čísla. V tento okamžik je nad naše znalosti vysvětlit toto „míchání“ čísel podrobně, v příštím díle ovšem požadované znalosti získáme a k Diffieho–Hellmanově–Merklově výměně klíče se ještě krátce vrátíme.

Zámek, který se zamyká jedním a odemyká jiným klíčem

Přejděme nyní k šifrování, které výměnu tajného klíče vůbec nepotřebuje. Začneme tím, že se zkusíme podívat na symetrické šifrování trochu jinýma očima: Alice chce poslat zprávu Bobovi, napíše ji tedy na papír a zamkne ji do skříňky. Zamčení zprávy do skříňky odpovídá jejímu zašifrování. Pro jednoduchost předpokládáme, že skříňka je nerozbitná, a že je možné ji otevřít pouze použitím (jediného) správného klíče. Tento klíč je vlastně tajným klíčem, o kterém jsme se bavili doposud. Alice po uzamčení pošle skříňku Bobovi třeba obyčejnou poštou. Pro Evu nemusí být obtížné skříňku během její cesty od Alice k Bobovi získat, pokud ji však získá, tak ji bez klíče neotevře (leda, že by vyráběla klíče různých tvarů a zkoušela, jestli jeden z nich zámek neodemkne). Naopak Bob, jakožto právoplatný příjemce, musí mít možnost skříňku otevřít (tedy zprávu dešifrovat). Musí

mít proto k dispozici kopii stejného klíče, jako má Alice. Na podobě tajného klíče se však Alice s Bobem musí nějak domluvit, čímž se vracíme k problému výměny klíče.

Otázka tedy zní: nebylo by možné zkonstruovat skříňku s naprosto novým typem zámku, který by se zamykal jedním, ale odemykal zcela jiným klíčem? Bob by byl jediným vlastníkem klíče pro odemykání zámku (dešifrování zprávy), proto se tomuto klíči říká *soukromý*. Klíč určený pro zamykání zámku (šifrování zpráv) by mohl Bob komukoliv poskytnout, třeba tak, že by na svých webových stránkách zveřejnil detailní popis jeho tvaru. Alice (nebo kdokoliv jiný, kdo by chtěl Bobovi poslat zprávu) by si podle návodu klíč vyrobila o mohla ho použít pro uzamčení zprávy. Tento klíč se proto nazývá *veřejný*.

Celý vtip tkví v tom, že rozdělením tajného klíče na klíč soukromý a veřejný tak naprosto odpadá nepohodlná, nákladná a nebezpečná[11)] správa tajných klíčů.

Tomuto způsobu šifrování se často říká *šifrování s veřejným klíčem* nebo také *asymetrické šifrování*. U zrodu asymetrických šifer opět stáli, nám už známí, Whitfield Diffie a Martin Hellman.

Zbývá tedy nějakou konkrétní šifru s veřejným klíčem zkonstruovat. Pokud bychom zůstali u našeho mechanického příměru se skříňkou uzamykatelnou jedním klíčem a odemykatelnou druhým (jiným) klíčem, tak taková konstrukce překvapivě existuje a je velmi jednoduchá. Jedná se o skříňku, která se sama uzamkne pouhým zaklapnutím dvířek. Veřejný klíč sice nemá fyzickou podobu – v tomto případě je jím znalost toho, jak dvířka zaklapnout – to však na podstatě věci nic nemění. Klíč, který skříňku odemyká, musí být vlastněn pouze zamýšleným příjemcem skříňky, a je tedy výše zmíněným soukromým klíčem.[12)]

Tímto jednoduchým nápadem jsme však problém zdaleka nevyřešili. Přenést ho do světa počítačového šifrování (to znamená, najít vhodnou šifrovací a dešifrovací funkci) totiž není vůbec snadné a informatikům trvalo poměrně dlouhou dobu, než se jim to podařilo.

Na začátku stálo jedno důležité pozorování. Zamknutí skříňky pomocí veřejného klíče (zaklapnutí dvířek) a odemknutí skříňky pomocí soukro-

[11)] Nebezpečná v tom smyslu, že kurýr nemusí být tak důvěryhodný, jak se Alice s Bobem domnívali a že tedy může tajný klíč vyzradit.

[12)] Ještě jednodušším příkladem takového systému je obyčejná poštovní schránka. Kdokoliv do ní může vhodit dopis, ale pouze pověřený zaměstnanec pošty má (soukromý) klíč, kterým se schránka odemyká. Poštovní schránka tak realizuje bezpečný přesun dopisu mezi odesilatelem a poštou.

mého klíče je snadno a rychle proveditelnou akcí. Odemknutí skříňky pouze se znalostí veřejného klíče (se znalostí, jak zaklapnout dvířka) je však velmi obtížné. Stejně tak šifra, kterou se snažíme zkonstruovat, by měla vypadat tak, že šifrování pomocí veřejného klíče a dešifrování pomocí soukromého klíče by mělo být jednoduché a rychlé; dešifrování se znalostí veřejného klíče by však mělo být obtížné, v ideálním případě nemožné.

Převedeno do řeči matematických funkcí, které takovou šifru popisují, to znamená, že:

1. pro zvolené číslo x a veřejný klíč k_e[13)] musí být výpočet hodnoty šifrovací funkce $y = e(x, k_e)$ snadný;
2. pokud budeme znát zašifrované číslo y a soukromý klíč k_d, tak výpočet původní hodnoty $x = d(y, k_d)$ musí být také snadný;
3. výpočet čísla x pouze ze znalosti zašifrovaného čísla y a veřejného klíče k_e – jinými slovy, výpočet takového x, aby platilo $y = e(x, k_e)$ – musí být obtížný.

Protože je výpočet hodnoty šifrovací funkce e „v jednom směru“ (bod 1) snadný a „v opačném směru“ (bod 3) obtížný, je taková šifrovací funkce nazývána *jednosměrnou funkcí*. K původní hodnotě x se tak můžeme dostat pouze s využitím soukromého klíče (bod 2), kterému se proto někdy říká *zadní vrátka*.

Dokážeme najít vhodného kandidáta jednosměrné funkce se zadními vrátky? Pokusme se nejprve zamyslet třeba nad funkcí

$$e(x, k_e) = k_e \cdot x.$$

Veřejným klíčem k_e bude například číslo 2. Ptáme se tedy, jestli funkce, která danému x přiřadí číslo $2x$, splňuje podmínky kladené na jednosměrnou funkci. Výpočet v jednom směru (tedy výpočet dvojnásobku zadaného čísla) je jistě snadný a rychlý. Výpočet v opačném směru (tedy vydělení zadaného čísla dvěma) je ovšem také rychlý. Čtenář by mohl namítnout, že pro obrovská čísla násobení a dělení rychlé není. Zde však *rychlost výpočtu* chápeme následujícím způsobem: pro násobení a dělení máme k dispozici

[13)] Zopakujme si, že uvažujeme dva klíče – jeden veřejný určený pro šifrování, druhý soukromý určený pro dešifrování. Tyto klíče je potřeba ve výpočtech nějakým způsobem odlišit, proto již nemůžeme používat jediný symbol k. Index e v symbolu k_e je opět odvozen od slova *encipher*, česky *šifrovat*. Čtenář se jistě dovtípí, že soukromý klíč budeme značit symbolem k_d.

postup, pomocí kterého jsme schopni daný výpočet úspěšně provést v několika krocích tak, že zvětšováním zadaných čísel počet těchto kroků *nebude dramaticky růst*. Tímto postupem[14)] je známé násobení a dělení „v ruce“, jak jsme se mu naučili na základní škole. Zmíněná funkce tedy není jednosměrná a pro konstrukci šifry s veřejný klíčem je tedy nepoužitelná.

Zkusme jinou funkci, řekněme

$$e(x, k_e) = x^{k_e}.$$

Za veřejný klíč opět zvolíme číslo 2. Pokud tedy šifrujeme nějaké konkrétní číslo x, pak pouze vypočítáme hodnotu druhé mocniny čísla x, čímž získáme zašifrované číslo y. Výpočet druhé mocniny (to znamená, násobení čísla sebou samým) je – jak už dobře víme – rychle proveditelné. Jestliže naopak chceme získat ze zadaného zašifrovaného čísla y jemu odpovídající číslo x, musíme vypočítat druhou odmocninu čísla y. Výpočet druhé odmocniny je však opět možné provést poměrně rychle například s pomocí *metody bisekce*.[15)]

Nalezení vhodného kandidáta jednosměrné funkce se zadními vrátky se zdá být obtížné. Ve skutečnosti jsme se však druhým, výše uvedeným příkladem k tomuto kandidátovi přiblížili – je jím opravdu funkce $e(x, k_e) = x^{k_e}$, na umocnění se ovšem musíme podívat pohledem takzvané *modulární aritmetiky*, které jsme se lehce dotkli při vysvětlování „přetečení“ při sčítání v rovnici (1). Zmíněná funkce se často nazývá RSA funkcí, protože stojí v samotném základu asymetrického šifrování RSA.

Stručné zdůvodnění, proč je RSA funkce vhodným kandidátem je takové, že modulární aritmetika se chová oproti běžně používané aritmetice velmi nepravidelně. Abychom však tomuto zdůvodnění byli schopni lépe porozumět, bude nutné podrobněji si vysvětlit, jak vlastně modulární aritmetika funguje. Příští díl tedy začneme vysvětlením modulární aritmetiky; poté budeme moci přejít k vysvětlení šifrování RSA a k některým jeho aplikacím (například v elektronickém podpisu).

[14)] V informatice takovému postupu říkáme *algoritmus*.

[15)] Této metodě se také někdy říká *metoda půlení intervalu*. V rychlosti (a značně zjednodušeně) si ji popíšeme na následujícím příkladu. Chceme vypočítat $\sqrt{576}$. Začneme tím, že výsledek odhadneme, řekněme, že jím bude číslo 21. Druhá mocnina z 21 je 441, což je méně než požadovaných 576. Odhad proto zvětšíme, třeba na číslo 26. To je však příliš, protože 26^2 je 676. Odhad tedy zmenšíme, například na číslo 24, což už je správný výsledek. Poznamenejme, že ve skutečnosti se čísla nehádají, ale stanovují jako prostředek intervalu daného hodnotami vypočtenými v předchozím kroku. Zvídavého čtenáře odkážeme na knihu od Donalda Knutha [2].

Literatura

[1] *Diffie, W., Hellman, M.*: New directions in cryptography. IEEE Transactions on Information Theory, roč. 22 (1976), č. 6, s. 644–654.

[2] *Knuth, D. E.*: The Art of Computer Programming, Volume 3: Sorting and Searching. Addison-Wesley, 1998.

[3] *Levy, S.*: Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age. Penguin Books, 2001.

[4] *Singh, S.*: Kniha kódů a šifer: Tajná komunikace od starého Egypta po kvantovou kryptografii. Argo, Dokořán, 2003.

Dva základní šifrovací principy

MIROSLAV KOLAŘÍK

Přírodovědecká fakulta UP, Olomouc

Ukážeme si základní principy ze zajímavé a stále se rozvíjející oblasti informatiky – z kryptologie.[1)] Kryptologie zahrnuje kryptografii a kryptoanalýzu. Kryptografie se zabývá metodami utajení (říkáme také šifrováním) obsahu zpráv; toto utajení se provádí tak, že se zpráva převede do podoby, která je srozumitelná pouze zamýšlenému příjemci. Kryptoanalýza se zabývá luštěním zašifrovaných zpráv (dešifrováním).

První kryptografické metody se objevily už ve starověkém Řecku a až do začátku 20. století byly založené na jednoduchých principech. Představíme si dva základní šifrovací principy: substituci a transpozici. Jedná se o jednoduché a přitom zásadní šifrovací metody, které se využívají i u moderních kryptografických metod, jako jsou například DES nebo AES. Šifrovací principy demonstrujeme na několika jednoduchých příkladech, které mohou být použity při výuce na základních a středních školách.

Substituční šifry

Jako první se budeme věnovat substituci, neboli záměně (náhradě). Začneme pěkně zvolna jednoduchým příkladem. Představme si situaci, že

[1)] Kryptologie je naukou o metodách utajování zpráv i o tom, jak zašifrované zprávy luštit (dešifrovat).