Učitel matematiky

Petra Konečná

Zajímavosti z kryptologie (3) - vznik asymetrické šifry

Učitel matematiky, Vol. 23 (2015), No. 3, 129–140

Persistent URL: http://dml.cz/dmlcz/149421

ZAJÍMAVOSTI Z KRYPTOLOGIE (3)
VZNIK ASYMETRICKÉ ŠIFRY

Petra Konečná

Úvod

Historie kryptologie je několik tisíc let trvajícím příběhem o souboji kryptografů a kryptoanalytiků. Kryptografové se snaží vymyslet a používat bezpečné šifry a kryptoanalytici se snaží využít slabin používaných šifer a najít metody na jejich rychlé rozluštění. V průběhu let se střídavě misky vah přikláněly jednou na stranu kryptografů, podruhé na stranu kryptoanalytiků. Některé šifry rozluštěny byly, jiné nebyly, u některých to trvalo velice dlouho. Často za prolomením šifer stála nejen obrovská práce kryptoanalytiků, ale i špionážní činnost a štěstí. Od 2. poloviny 19. století začínají postupně kryptografické metody využívat i osoby mimo politiku a armádu[1]. To začíná klást na kryptologii nové nároky.

Článek navazuje na (Konečná, 2014) a (Konečná, 2015). Kapitola pojednávající o rozšíření použití kryptografie čerpá zejména z (Singh, 2003), (Adams, 2003) a (Piper & Murphy, 2006), podrobnější informace k DES a AES nalezneme např. v (Jiroušek, Ivánek, Máša, Toušek & Vaněk, 2006). Informace z oblasti teorie čísel pocházejí z (Knuth, 2010), (Skula, 2010), (Šolcová, 2001) a (Šolcová, 2010). Kapitoly pojednávající o využití jednosměrných funkcí a vzniku asymetrického šifrování čerpají z (Singh, 2003), (Adams, 2003), (Piper & Murphy, 2006), (Knuth, 2010), (Jiroušek, Ivánek, Máša, Toušek & Vaněk, 2006), (Berloquin, 2008) a (Konečná, Vavříčková & Wrublová, 2009).

[1] Přestože jsou zaznamenány historické případy použití šifer mezi běžnými lidmi, jedná se o výjimky. Šifrovaná komunikace probíhala zejména mezi politiky, náboženskými představiteli a ve vojenských kruzích.

Rozšíření kryptografie

Za zvýšením zájmu o kryptografii, ke kterému dochází od 2. poloviny 19. století, stojí zejména rozvoj telegrafu. Nejen obchodní společnosti, ale i širší veřejnost si začala uvědomovat, že je potřeba chránit zprávy obsahující citlivé informace. V té době většina používaných šifer byla profesionálním kryptoanalytikem prolomitelná, pro běžnou telegrafickou komunikaci však byla dostatečně bezpečná před náhodnými odposlouchávači.

Dalším zlomovým okamžikem, který vedl k masivnímu využívání kryptografie veřejností, byl vynález tranzistoru v roce 1947. Ten nahradil daleko nákladnější elektronky využívané v konstrukci počítačů, což vedlo k jejich zlevnění, a tedy dostupnosti nejen pro vládní a armádní kruhy, jak tomu do této doby bylo.

Moderní počítač vznikl v období II. světové války, kdy napomáhal zejména při luštění šifer vytvářených s pomocí šifrovacích strojů. Po konci II. světové války pokračoval rozvoj počítačové technologie. Počítač se stává pro kryptoanalýzu významný zejména tím, že umí rychleji zkoušet všechny možné klíče a tím výrazně urychluje útok hrubou silou. Je však užitečný i pro kryptografy; tvorba šifer již není limitována omezenými možnostmi konstrukce šifrovacího stroje a lze tedy vytvářet šifry čím dál složitější.

V průběhu 60. let 20. století ceny počítačů klesaly a jejich výkon narůstal. Počítače začaly hojně využívat zejména banky, obchodní společnosti a firmy. Aby bylo možné efektivně využívat šifrovanou komunikaci mezi větším množstvím institucí, bylo nezbytné používat stejný šifrovací systém. Úkolem tedy bylo najít a zavést bezpečný šifrovací standard. Tím se stal v roce 1976 *DES (Data Encryption System)*, který vycházel ze systému *Lucifer* vyvinutého na počátku 70. let H. Feistelem. Jedná se o velice složitou šifru. Zjednodušeně můžeme proces popsat tak, že se zpráva rozdělí na dvě poloviny, přičemž se postupně na tyto části aplikuje šestnáct kol složitých mechanismů. Ty zprávu postupně mění tak, až je zcela promíchaná. Proto se také tomuto procesu říká „hnětení těsta“ nebo „mandl“. Dešifrovaní se poté provádí aplikací inverzních šifrovacích mechanismů. Oproti původnímu systému Lucifer

měl DES omezený počet klíčů na 2^{56}. Toto omezení si prosadila americká NSA tak, aby snížila bezpečnost šifry na tu úroveň, kterou sama svými nejvýkonnějšími počítači byla schopna prolomit. Od roku 2002 nahradil DES šifrovací standard *AES (Advanced Encryption System)* s 2^{112} možnostmi klíče, jelikož DES byl v letech 1998–1999 prolomen.

I přes obrovskou složitost jsou výše uvedené šifry teoreticky prolomitelné[2]. Jejich bezpečnost je založena zejména na tom, že doba potřebná pro jejich prolomení je natolik dlouhá, že je dostačující pro utajení obsahu zprávy. Největší slabinou těchto šifer je klíč. U všech šifer používaných do 70. let 20. století se pro šifrování i dešifrování používal shodný klíč, proto se tyto typy šifer nazývají *symetrické*. Tímto se kryptografové dostávali do problému, jak bezpečně doručit klíč druhé straně – příjemci. Jediným zaručeně spolehlivým způsobem je osobní předání, toto však z časových důvodů nebylo pro všechny komunikující strany reálné. Proto se klíče distribuovaly prostřednictvím speciálních zaměstnanců těchto institucí, kteří jezdili po celém světě a osobně předávali klíče příjemcům zpráv od dané instituce. Z rozmachem obchodní sítě a nárůstem komunikujících stran neúměrně rostly náklady na distribuci tajných klíčů. Situace se stávala neudržitelnou.

O několik staletí zpět

Prvočísla jsou přirozená čísla dělitelná pouze jedničkou nebo sama sebou. Tato vybraná přirozená čísla byla pravděpodobně známa už starověkým civilizacím. První podrobné studie prvočísel a jejich vlastností byly uskutečněny v antickém Řecku. Ve svém díle *Základy* řecký matematik Eukleides (asi 325–260 př. n. l.) dokázal nejen to, že prvočísel je nekonečně mnoho, ale také to, že každé přirozené číslo je možné rozložit na součin prvočísel. Dnes této vlastnosti říkáme *Základní věta aritmetiky*. Vlastnostem prvočísel se v průběhu let věnovalo velké množství matematiků. Vzpomeneme tři z nich, na jejichž výsledcích stojí moderní metody šifrování.

[2]V článku (Konečná, 2015) jsme si uvedli, že jedinou skutečně bezpečnou šifrou je Vernamova šifra, nazývaná také jednorázová tabulková šifra.

Pierre de Fermat (1601–1665) byl povoláním právník – advokát, který se matematice věnoval z pouhého zaujetí jako „amatér“. Proslavil se zejména díky svým objevům a hypotézám v teorii čísel, přestože se věnoval i dalším oblastem matematiky. Jeho nejznámější hypotézou je Velká Fermatova věta[3]. Pro teorii čísel a samotnou kryptografii je však daleko významnější *Malá Fermatova věta*:

Nechť p je prvočíslo, a je přirozené číslo takové, že a, p jsou nesoudělná. Potom platí, že a^{p-1} po dělení dává zbytek 1.

Malou Fermatovu větu lze užít například k důkazu toho, že číslo je složené, aniž bychom znali některého z netriviálních dělitelů, dá se tedy použít pro test prvočíselnosti.

Větu v 18. století zobecnil a dokázal L. Euler (1707–1783). Pro zobecněné tvrzení využil funkci $\varphi(n)$, která udává počet čísel menších než n takových, že jsou s n nesoudělná[4]. *Eulerova věta* známá také jako *Eulerova-Fermatova věta* poté zní takto:

Nechť a, m jsou nesoudělná přirozená čísla. Potom platí, že $a^{\varphi(m)}$ po dělení m dává zbytek 1.

V roce 1801 ve svém díle *Aritmetické výklady* zavedl J. C. F. Gauss tzv. *modulární aritmetiku*[5], kde využívá pojmu *kongruence modulo přirozené číslo m na množině celých čísel*. Jedná se o binární relaci na množině celých čísel danou následujícím vztahem

$$a \equiv b \pmod{m} \text{ právě tehdy, když } m \mid (a - b).$$

S využitím této relace můžeme Eulerovu-Fermatovu větu zapsat ve tvaru, která je používaná dnes:

[3] Jedná se o větu zabývající se celočíselnými řešeními rovnice $x^n + y^n = z^n$, kterou napsal na okraj stránky latinského překladu Diofantova díla *Aritmetika* bez uvedení důkazu. Důkaz se snažilo najít velké množství matematiků i dalších nadšenců. Podařilo se to až v roce 1994 britskému matematikovi A. Wilesovi.

[4] Dnes je tato funkce nazývána *Eulerova funkce*. Pokud $n = p_1^{k_1} \cdots p_r^{k_r}$ je prvočíselný rozklad přirozeného čísla n , potom $\varphi(n) = (p_1 - 1) \cdot p_1^{k_1 - 1} \cdots (p_r - 1) \cdot p_r^{k_r - 1}$.

[5] Někdy také nazývána aritmetika zbytkových tříd.

Nechť a, m jsou nesoudělná přirozená čísla. Potom platí
$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Ani jeden ze zmiňovaných matematiků netušil, jaký význam bude mít tato věta za několik století.

Kouzlo jednosměrné funkce

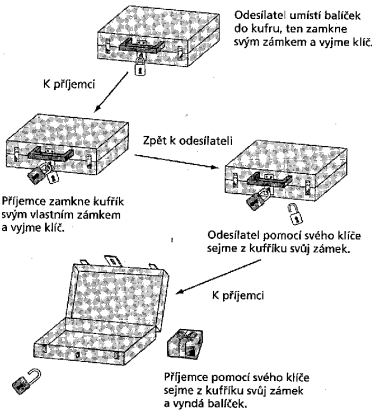
Kryptografové vždy snili o nalezení mechanismu šifrování tak, aby nebylo zapotřebí vyměňování tajných klíčů, které mohou snadno padnout do nevhodných rukou. Problém s distribucí klíčů se stával o to palčivější, o co se rozšiřovala skupina uživatelů šifer. Až do 70. let 20. st. se zdálo, že tento problém je neřešitelný. S brilantním řešením přišel tým matematiků, jejichž objev je považován za jeden z největších kryptografických úspěchů.

Samotný princip výměny tajného klíče lze popsat následovně. Předpokládejme, že Alice a Bob[6] si potřebují poslat tajné heslo (klíč pro tajnou komunikaci). Nemohou se však setkat a neznají nikoho spolehlivého, po kom by heslo mohli poslat. Provedou tedy následující postup. Alice vezme kufřík, vloží do něj tajné heslo a zamkne kufřík svým klíčkem, který si důkladně uschová. Následně kufřík pošle standardní cestou Bobovi. Ten jej nemá čím odemknout (klíček má jen Alice). Proto vezme vlastní zámek a kufřík s pomocí něj zamkne ještě jednou, přitom svůj klíček si také uschová. Kufr vrátí Alici. A potom to je již jednoduché, Alice odstraní svůj zámek, kufřík je však stále zabezpečen zámkem od Boba, může jej tedy opět poslat. Bob odstraní svůj zámek a tím se dostane k tajnému obsahu kufříku.

Tento postup je geniálně jednoduchý. Má však háček. Na rozdíl od používání visacích zámků není postupné aplikování šifrovacích mechanismů obecně komutativní. Co tedy s tím? Řešení poskytla mnoho let stará modulární aritmetika.

V podstatě to vypadá jako matematické kouzlo. Postavme Alici a Boba každého do jednoho rohu velké místnosti tak, že na sebe nevidí a mohou se dorozumívat jen hlasitým voláním, přitom

[6] Pro popis komunikace se od začátku v literatuře standardně volí tato dvě jména, v článku je tento zvyk zachován.



Obr. 1: Princip výměny tajného klíče (Piper & Murphy, 2006)

je v místnosti spousta dalších osob. Úkolem Alice a Boba je vyměnit si tajné číslo tak, aby nikdo z přítomných toto heslo nezjistil. Alice na Boba zakřičí, že budou pro výpočet používat čísla 7 a 71. Poté každý chvilku tiše počítá a Alice zakřičí číslo 45 a Bob číslo 58. Poté zase oba chvilku počítají a oběma vyjde tajné číslo 20. Jak je to možné?

Oba využili pro výpočet funkci $f(x) \equiv g^x \pmod m$, $g < m$, kde za prvočíslo m vybrali 71 a g volili tak, aby jeho mocniny $g^k \pmod m$ pro různá k nabývaly všech hodnot $1, \ldots, m-1$. Zvolili tedy číslo 7, které podmínku splňuje[7]. Tato čísla mohou být veřejně známá. Poté aplikovali následující postup:

1. Alice si zvolila tajné číslo $A = 10$, Bob si zvolil tajné číslo $B = 4$. Toto číslo nikomu neprozradí.
2. Každý dosadil své tajné číslo za x do funkce $f(x) \equiv 7^x \pmod{71}$ a vypočítal funkční hodnotu. Alice tedy vypočítala hodnotu $\alpha \equiv 7^A \pmod{71} \equiv 7^{10} \pmod{71} \equiv 45 \pmod{71}$. Bob vypočítal hodnotu $\beta \equiv 7^B \pmod{71} \equiv 7^4 \pmod{71} \equiv \equiv 58 \pmod{71}$.
3. Hodnoty α, β si sdělí veřejně.

[7]Prvek g je generátorem multiplikativní grupy $(\mathbb{Z}_m \setminus \{0\}, \cdot)$.

4. Opět počítají:
   - Alice $k_A \equiv \beta^A \pmod m \equiv 58^{10} \pmod{71} \equiv 20 \pmod{71}$,
   - Bob $k_B \equiv \alpha^B \pmod m \equiv 45^4 \pmod{71} \equiv 20 \pmod{71}$.

   Oběma vychází stejné číslo, které je požadovaným tajným klíčem. Jak je možné, že vychází stejný výsledek, si můžeme ověřit jednoduchým důkazem.
   $k_B \equiv \alpha^B \pmod m \equiv \left(g^A\right)^B \pmod m \equiv g^{BA} \pmod m \equiv$
   $\equiv \left(g^B\right)^A \pmod m \equiv \beta^A \pmod m \equiv k_A$.

Výše uvedenou metodu objevili v roce 1976 W. Diffie, M. Hellman a R. Merkle a našli tak způsob předávání tajného klíče. Přitom ono „matematické kouzlo“ stojí na „tricích“, které lze zvládnout se znalostmi středoškolské matematiky.

Bezpečnost metody zajišťuje právě užití modulární aritmetiky. Funkce $f(x) \equiv g^x \pmod m$ je totiž *jednosměrnou funkcí*. To znamená, že funkční hodnotu lze dosazením argumentu vypočítat jednoduše. Ovšem zpětné zjištění hodnoty z pouhé znalosti funkce a funkční hodnoty je nepoměrně složité.

x	32	102	172	242	312	382
$g^x \pmod m$	6	6	6	6	6	6

Tab. 1: Nejednoznačnost určení argumentu ze znalosti funkční hodnoty funkce

Jednosměrnou funkci lze pochopit na příkladech z běžného života – míchaná vajíčka připravíme jednoduše, zpětná separace bílku a žloutku je však nemožná. Jiným příkladem je vhození dopisu do schránky či míchání barev.

Přestože schéma výměny klíčů Diffie-Hellman-Merkle nebylo zcela dokonalé[8], uvedený systém konečně vyřešil problém distribuce klíčů. A s využitím jednosměrné funkce pro šifrování šli matematici ještě dále.

[8] Problém vstupu třetí osoby do komunikace či nutnost výměny klíče ve stejný čas.

Kryptografie s veřejným klíčem

Doposud známé a používané šifry byly symetrické, tzn. pro šifrování a dešifrování se používal tentýž klíč. Problém s výměnou tajného klíče sice již byl vyřešen, ale stále se používal pro symetrické šifrovací systémy.

S myšlenkou *asymetrické šifry* přišel v roce 1975 W. Diffie. Princip spočívá v tom, že existují klíče dva – jeden *veřejný*, který může znát kdokoli a slouží pro zašifrování zprávy, a druhý *soukromý*, který zná jen příjemce a pouze on může zprávu dešifrovat. Výhodou takové šifry, na rozdíl od tajné výměny klíče a použití symetrické šifry, by bylo to, že odesílatel může zašifrovanou zprávu odeslat kdykoliv, bez nutnosti spojení v daném čase s příjemcem.

W. Diffie předpokládal, že by se dalo využít nějaké vhodné jednosměrné funkce. Můžeme si to představit např. tak, že každý je schopen na základě jména a adresy najít v telefonním seznamu číslo a zavolat příjemci. Opačně však z telefonního čísla dohledat v seznamu identitu volané osoby je komplikované, v případě velmi obsáhlého seznamu v podstatě časově nereálné.

Do hledání vhodné funkce se pustili další vědci. Úspěchu bylo dosaženo v roce 1977, kdy R. Rivest, A. Shamir a L. Adleman představili *systém RSA*. Šifra se tvoří následujícím způsobem:

1. Najdeme náhodně dvě velká prvočísla p, q a položíme $m = p \cdot q$.
2. Zvolíme přirozená čísla i, j tak, aby $i \cdot j \equiv 1 \pmod{(p-1) \cdot (q-1)}$.
3. Zveřejníme m, i pro šifrování a utajíme p, q, j. Veřejným klíčem je dvojice přirozených čísel m, i, kterým říkáme modul a šifrovací exponent, j je tajný klíč a současně dešifrovací exponent.

Pokud nám bude chtít někdo poslat zprávu, převede ji do čísla x tak, aby $x < m$. Tím, že se v praxi používají více než 100-ciferná prvočísla, není příliš pravděpodobné, že by zpráva přesáhla jejich součin. Následně vypočítá šifrové číslo y tak, že $y \equiv x^i \pmod{m}$, pro digitální přenos převede šifrové číslo y na binární zápis, tím dostane šifrovou zprávu a pošle nám ji.

Poté, co bychom šifrovou zprávu obdrželi, převedeme ji na šifrové číslo y. Následně bychom vypočetli číslo $x < m$ podle vztahu $x \equiv y^j \pmod{m}$ a převedli je na zdrojovou zprávu.

Představme si, že chceme vytvořit náš konkrétní systém RSA. Pro ilustraci použijeme malá prvočísla:

1. Určíme si libovolná prvočísla p, q, např. $p = 71$, $q = 43$. Určíme $m = p \cdot q = 71 \cdot 43 = 3053$.
2. Určíme $\varphi(m) = (p-1)(q-1) = 70 \cdot 42 = 2940$.
3. Určíme i, j tak, aby platilo $i \cdot j \equiv 1 \pmod{(p-1)\cdot(q-1)}$. Víme, že číslo $2941 \equiv 1 \pmod{2940}$ a platí $2941 = 173 \cdot 17$. Odtud $i = 173$, $j = 17$.

Nyní máme vytvořen systém. Hodnoty čísel p, q zničíme, hodnotu j si uschováme (bude tajná, pouze pro nás) a hodnoty m, i zveřejníme. Každý, kdo nám bude chtít poslat šifrovou zprávu, musí tyto hodnoty použít.

Předpokládejme, že nám chce odesílatel poslat zdrojovou zprávu, která bude v binárním zápisu 1011111:

1. Odesílatel převede binární zprávu do čísla v desítkové soustavě, tedy $x = 1\cdot2^6+0\cdot2^5+1\cdot2^4+1\cdot2^3+1\cdot2^2+\cdot2^1+1\cdot2^0 = 95$.
2. Ověří, zda platí $x < m$. Platí, že $95 < 3053$.
3. Určí šifrové číslo y tak, že vypočítá $y \equiv 95^{173} \pmod{3053}$. Pro výpočet využije metody postupného výpočtu čtverců čísel modulo m. Rozepíše si číslo 95^{173} takto:

$$95^{173} = 95^{128+32+8+4+1}$$

$$y_0 = 95^1 \equiv 95 \pmod{3053}$$

$$y_1 = 95^2 = 9025 \equiv 2919 \pmod{3053}$$

$$y_2 = 95^4 = \left(95^2\right)^2 \equiv 2919^2 \equiv 2691 \pmod{3053}$$

$$y_3 = 95^8 = \left(95^4\right)^2 \equiv 2691^2 \equiv 2818 \pmod{3053}$$

$$y_4 = 95^{16} = \left(95^8\right)^2 \equiv 2818^2 \equiv 271 \pmod{3053}$$

$$y_5 = 95^{32} = \left(95^{16}\right)^2 \equiv 271^2 \equiv 169 \pmod{3053}$$

$$y_6 = 95^{64} = \left(95^{32}\right)^2 \equiv 169^2 \equiv 1084 \pmod{3053}$$

$$y_7 = 95^{128} = \left(95^{64}\right)^2 \equiv 1084^2 \equiv 2704 \pmod{3053}$$
$$y = 95^{173} = 95^{128+32+8+4+1} \equiv$$
$$\equiv 2704 \cdot 169 \cdot 2818 \cdot 2691 \cdot 95 \equiv 1429 \pmod{3053}.$$

Šifrové číslo $y = 1429$ by pro digitální přenos musel ještě převést do binárního zápisu, toto číslo zde není díky své délce vypsáno. Poté, co obdržíme šifrovou zprávu, použijeme svůj tajný klíč $j = 17$. Využijeme metody postupného výpočtu čtverců modulo m:

$$x \equiv 1429^{17} \equiv 1429^{16+1} \equiv 547 \cdot 1429 \equiv 95 \pmod{3053}.$$

Dostáváme $x = 95$, což v binárním zápisu odpovídá zprávě od odesílatele 1011111.

Tento systém asymetrického šifrování stojí na následující větě:

Nechť i, j, m jsou přirozená čísla taková, že i je nesoudělné s $\varphi(m)$ a $i \cdot j \equiv 1 \pmod{\varphi(m)}$. Potom pro libovolné přirozené číslo x nesoudělné s m platí

$$\left(x^i\right)^j \equiv x \pmod{m}.$$

Důkaz této věty je velmi jednoduchý a využívá Eulerovu-Fermatovu větu. Jestliže $i \cdot j \equiv 1 \pmod{\varphi(m)}$ potom z definice kongruence plyne $\varphi(m) \mid (i \cdot j - 1)$ a tedy existuje přirozené číslo k takové, že $i \cdot j = k \cdot \varphi(m) + 1$.
Odtud $\left(x^i\right)^j = x^{ij} = x^{k \cdot \varphi(m)+1}$ a s užitím Eulerovy-Fermatovy věty dostáváme $x^{k \cdot \varphi(m)+1} = x^{k \cdot \varphi(m)} \cdot x \equiv 1 \cdot x \pmod{m}$.

Bezpečnost šifry je založena na tom, že číslo – modul lze jednoduše vypočítat ze zadaných hodnot prvočísel, zpětné nalezení původních hodnot nutných k rozluštění textu je však při správné volbě hodnot prakticky nemožné. Správnou volbou se míní dostatečně velká prvočísla[9], v současnosti se používají prvočísla v řádech 10^{250}. Jelikož doposud není známa efektivní metoda rozkladu přirozeného čísla na prvočísla, i ty nejvýkonnější počítače by pro faktorizaci potřebovaly miliardy let.

[9]Další podmínky pro volená čísla lze najít např. (Knuth, 2010).

Závěr

V současnosti se miska vah přiklonila na stranu kryptografů. Stávajícími algoritmy je prvočíselný rozklad součinů čísel řádově 10^{250} nemyslitelný. I kdybychom použili nejvýkonnější typy počítačů, potřebovali bychom pro rozklad $3 \cdot 10^{11}$ let. Hledáním výkonnějších počítačů, které by byly schopny úlohy řešit s mnohem větší rychlostí, bychom si nepomohli, protože tyto počítače by se daly využít i pro zdokonalení šifer.

Díky mnoho let staré modulární aritmetice, která ve své době nesloužila k aplikaci v reálném životě[10], můžeme dnes žít životem, na který jsme zvyklí, můžeme využívat prostředky, bez kterých si již možná neumíme život představit. A v neposlední řadě na objevech v této oblasti matematiky je dnes postavena bezpečnost civilizace.

Literatura

[1] Adams, S. (2003). *Šifry a kódy*. Banská Bystrica: Slovart, s. r. o.

[2] Berloquin, P. (2008). *Skryté kódy a velkolepé projekty*. Banská Bystrica: Euromedia Group, k. s.

[3] Jiroušek, R., Ivánek, J., Máša, P., Toušek, J. & Vaněk, N. (2006). *Principy digitální komunikace*. Voznice: Leda.

[4] Knuth, D. E. (2010). *Umění programování 2. díl*. Brno: Computer Press, a. s.

[5] Konečná, P. (2014). Zajímavosti z kryptologie (1) – od prvopočátků až po frekvenční kryptoanalýzu. *Učitel matematiky*, 23(1).

[6] Konečná, P. (2015). Zajímavosti z kryptologie (2) – obrana před frekvenční kryptoanalýzou. *Učitel matematiky*, 23(2).

[7] Konečná, P., Vavříčková, L. & Wrublová, M. (2009). *Kódy a šifry – jejich matematický základ a historie*. Ostrava: OU.

[8] Pickover, C. A. (2012). *Matematická kniha*. Praha: Dokořán.

[10] P. Fermat neprojevoval zájem o aplikace matematiky v reálném životě.

[9] Piper, F. & Murphy, S. (2006). *Kryptografie*. Praha: Dokořán.

[10] Singh, S. (2003). *Kniha kódů a šifer*. Praha: Dokořán a Argo.

[11] Skula, L. (2010). *Malá Fermatova věta*. Praha: CEFRES USR 3138 CNRS-MAEE. Dostupné z `http://www.cefres.cz/pdf/c28/skula_2002_mala_fermatova_veta.pdf`

[12] Šolcová, A. (2001). *D'Artagnan mezi matematiky – pocta Pierru Fermatovi k 400. výročí narození*. Pokroky matematiky, fyziky a astronomie, 46(4), 286–298.

[13] Šolcová, A. (2010). *Fermatův odkaz*. Praha: CEFRES USR 3138 CNRS-MAEE. Dostupné z `http://www.cefres.cz/pdf/c28/solcova_2002_fermatuv_odkaz.pdf`

Abstract

Cryptology is the science of encryption, decryption and deciphering. The ability to use secret means of communication and the ability to decipher secret messages were behind many historical events. This article – by means of selected historical events – will represent cryptology as an interesting scientific discipline that has been accompanying the mankind since antient times and has been permeating our daily lives up to the present times. The text also points at intermingling of many branches and disciplines which can be used in teaching. The third part deals with expansion of cryptography which resulted in formation of the assymetric cipher.

RNDr. Petra Konečná, Ph.D.
Přírodovědecká fakulta OU
30. dubna 22
701 03 Ostrava
e-mail: Petra.Konecna@osu.cz