MATEMATICKÁ PODSTATA METODY ASYMETRICKÉHO ŠIFROVÁNÍ

BÁRTEK Květoslav – ZDRÁHAL Tomáš, CZ

Resumé

RSA šifrovací systém je nejrozšířenější kryptografický algoritmus s veřejným klíčem na světě. Používá se k zašifrování zpráv bez nutnosti vzájemné výměny tajného klíče. Jeho bezpečnost je založena na obtížnosti rozkladu velkých celých čísel.

Klíčová slova: kryptografie, asymetrická kryptografie, RSA šifrování, CAS Maxima.

THE MATHEMATICS OF ASYMMETRIC CRYPTOGRAPHY

Abstract

The RSA cryptosystem is the most widely-used public-key cryptography algorithm in the world. It can be used to encrypt a message without the need to exchange a secret key separately. Its security is based on the difficulty of factoring large integers.

Key words: cryptography, asymmetric cryptography, RSA encryption, CAS Maxima.

Úvod

Teorie čísel byla až do 70. let 20. století považována za jedno z nejteoretičtějších odvětví matematiky. Právě v této době se však začalo ukazovat, že některé její teoretické výsledky se dají využít pro zabezpečení digitálních dat. V článku je popsáno matematické pozadí fungování šifrovací metody s veřejným klíčem známé pod zkratkou RSA. Je zde ukázáno, že bez použití matematických softwarů není prakticky možné metodu použít ani pro poměrně malá prvočísla. A je tím tak (mimo jiné) demonstrována skutečnost, že aktivní práce s některými ICT prostředky a jejich softwarovým vybavením je jediná možnost, jak může obyčejný člověk pochopit genialitu některých matematických výsledků známých již stovky let – princip metody RSA totiž vychází z tzv. malé Fermatovy věty (Pierre de Fermat, *1601 – †1665)) a z jejího zobecnění – věty Eulerovy (Leonhard Paul Euler, *1707 – †1783).

1 Problematika využití počítačů ve školské matematice

Použití či využití ICT v matematice, potažmo ve školské matematice je klišé již nejméně deset let. Zaměříme-li se pouze na počítače a jejich matematické softwary určené k nejrozumnějším výpočtům, tak to do jisté míry to připomíná situaci v (nejen) naší administrativě koncem sedmdesátých let 20. století, kdy do tehdejšího Československa přišly ze západu první počítače a „hledalo“ se jejich uplatnění. V čem byl tehdy (i teď ve školské matematice) základní problém?

První číslicové počítače byly vyrobeny ve 30. letech 20. století proto, aby umožnily řešit složité výpočty (toto potřeboval a do jisté míry realizoval už Charles Babbage koncem 19. století a je tak považován za vynálezce počítače). Byl tedy reálný problém, jeho řešení metodou „papír-tužka“ bylo neefektivní (prakticky nemožné) a proto byl vymyšlen „stroj“, aby tento problém vyřešil. Toto je naprosto přirozený postup. Pokud však jsme v situaci (a taková v úřednické práci byla tehdy a ve školské matematice je teď), že máme „stroj“, ale žádný problém, který by nešel vyřešit „ručně“, je snaha použít počítač za každou cenu absurdní. Konkrétně ve školské matematice: Devět učitelů základní školy z deseti se zeptá:

„Proč máme používat matematické softwary k řešení úloh, které umíme vypočítat na papíře? Protože je to „cool“? Ukažte mi takový problém (ale musí být pro žáky alespoň trochu zajímavý) a pak se o tom můžeme bavit dál!“

Nuže, v dalším takový problém uvedeme – budeme se bavit o asymetrickém šifrování. Bavit tak, abychom ve smyslu shora uvedeného uspokojili DESET z DESETI učitelů a tito pak začali používat se svými žáky alespoň nějaký sofistikovanější matematický software, protože bez něj se rozumně šifrovat prostě nedá. No a když už se žáci (a jejich učitelé) s aktivním používáním matematického softwaru při řešení některých úloh setkají, bude to začátek k tomu, aby se mohlo mluvit o „využití počítačů (obecněji ICT) ve výuce matematiky“. Jinak řečeno, budou se řídit schématem:

PROBLÉM – POČÍTAČ – VYŘEŠENÍ PROBLÉMU

a nikoliv

VYŘEŠENÝ PROBLÉM – POČÍTAČ – CO S POČÍTAČEM?

2 Šifrování čísel umocňováním

Dejme žákům praktický matematický problém na tolik zajímavý, že jej budou chtít řešit, i když se k tomu budou muset naučit pracovat s nějakým matematickým softwarem:

Na sdíleném excelovském listě (viz Tabulka 1 níže) má žák „svě“ jednociferné (kvůli jednoduchosti) číslo „zašifrovat“ tak, že jej umocní na čtvrtou – viz instrukce adresáta (v tomto případě učitele) a výsledek má zapsat do sloupce „Veřejná instrukce adresáta: Umocnit na 4.“ Učitel potom vypočítá čtvrtou odmocninu z tohoto čísla a výsledek zapíše do sloupce „Dešifrováno adresátem“. Následně žák výsledek překontroluje a má odpovědět na to, zda učitel jeho zašifrované číslo správně dešifroval.

Tabulka 1 – Šifrování umocňováním

Jméno	Příjmení	Mysli si jednociferné číslo	Veřejná instrukce adresáta: Umocnit na 4.	Dešifrováno adresátem	Měl adresát pravdu?	Jak adresát údaj dešifroval?
Adam	Adámek		16	2	ANO	?
Bohdan	Bělík		4096	8	ANO	Udělal 4. odmocninu
...	...		...	...	...	...
...	...		...	...	...	...
...	...		...	...	...	...

Jistě nebude trvat dlouho, kdy žáci nebudou chtít své „tajné“ číslo takto šifrovat, protože tento sdílený sešit přece vidí každý a vypočítat 4. odmocninu není žádný problém. Takže každý, ne jenom učitel – jediná osoba, které své číslo chtěl žák „svěřit“, je schopen žákovo tajné číslo „odhalit“. A má pravdu, jak plyne z následujícího:

Šifrujeme pomocí vztahu $y = x^e$. To znamená, že šifrované číslo x se umocní na číslo e a adresátovi se sdělí výsledek y . Tuto instrukci zadá veřejně adresát, tj. zadá tzv. šifrovací „exponent“ e (encrypt); zde $e = 4$ a pokud např. odesílatel Adam šifroval číslo $x = 2$, jedná se o výraz $y = 2^4 = 16$.

A dešifrujeme pomocí $x = y^d$. To znamená, že zašifrované číslo y se umocní na číslo d a dostane se tak původní číslo x . Jde tedy o to najít tento dešifrovací „exponent“ d (decrypt); zde je zřejmě $d = 1/e$ – musí totiž platit $e \cdot d = 1$; tedy $d = 1/4$ a v našem případě dostáváme $x = 16^{1/4} = 2$.

Jak již bylo řečeno, toto d najde snadno **každý**: Pokud se číslo zašifrovalo např. tak, že se umocnilo na čtvrtou, dešifruje se jednoduše tak, že se zašifrované číslo umocní na jednu čtvrtinu – tedy vypočítá se jeho čtvrtá odmocnina. Tedy takové šifrování žádný význam nemá. Vše vyplývá z následujících rovností

$y^d = (x^e)^d = x^{e \cdot d} = x^1 = x$, v našem případě Adama to vypadá takto

$$16^{1/4} = (2^4)^{1/4} = 2^{4 \cdot 1/4} = 2^1 = 2.$$

3 Šifrování umocňováním a zbytkem při dělení

Zkusme nyní „nepatrně“ adresátovu instrukci pro šifrování čísla změnit. A sice tak, že šifrované číslo se sice opět umocní, ale tentokrát se nesdělí (veřejně – opět budeme pracovat se sdíleným excelovským listem) výsledek tohoto umocnění, ale zbytek při dělení tohoto výsledku nějakým konkrétním číslem. Vše je jasné z následující Tabulky 2:

Jméno	Příjmení	Mysli si přirozené číslo menší než 91	Veřejná instrukce adresáta: Umocni na 5., vyděl číslem 91 a sděl zbytek	Dešifrováno adresátem	Měl adresát pravdu?	Jak adresát údaj dešifroval?
Adam	Adámek		23	4	ANO	?
Bohdan	Bělík		85	50	ANO	?
...	...		...	...	...	...
...	...		...	...	...	...
...	...		...	...	...	...

Tabulka 2 – Šifrování umocňováním a zbytkem při dělení

Tentokrát se asi nesetkáme s tím, že by nějaký žák „odhalil“, jak mohl učitel číslo správně dešifrovat. Podívejme se, proč tomu tak je.

Nejprve běžně používané označení: Pokud je číslo a zbytek při dělení čísla b číslem N , tak to zapisujeme takto $a \equiv b \pmod{N}$, případně jednodušeji $a \equiv_N b$ a říkáme, že „ a je kongruentní b modulo N – nebo „ b je kongruentní a modulo N – tato relace je evidentně symetrická. (Tedy např. $3 \equiv_{12} 15$, či $9 \equiv_{91} 100$.)

Šifrujeme pomocí kongruence $y \equiv_N x^e$. To znamená, že šifrované číslo x se umocní na číslo e , následně vydělí číslem N a vzniklý zbytek se sdělí adresátovi jako číslo y . Tuto instrukci zadá veřejně adresát, tj. zadá tzv. veřejný klíč, kterým je dvojice čísel (N, e) (e opět z anglického encrypt); zde $e = 5$ a pokud např. odesílatel Adam šifroval číslo $x = 4$, jedná se o výraz $y \equiv_{91} 4^5 = 23$. (O správnosti tohoto výsledku se lze lehce přesvědčit písemným dělením – právě z tohoto důvodu se zabýváme čísly poměrně malými (do 91).)

A dešifrujeme pomocí kongruence $x \equiv_N y^d$. Jak bude vypadat dešifrovací exponent d (decrypt) tentokrát? Vše poznáme z následujících úvah:

Aby metoda fungovala, muselo by platit něco podobného jako $d \cdot e = 1$ v předchozím případě šifrování pouhým umocňováním, tedy tedy $d \cdot e \equiv_N 1$. Tato kongruence neznamena nic jiného, než že číslo N dělí rozdíl $d \cdot e - 1$, což zapisujeme $N \mid d \cdot e - 1$ a je to ekvivalentní s tvrzením, že existuje takové celé číslo k , že $d \cdot e = 1 + k \cdot N$ (např. $5 \cdot 3 \equiv_{14} 1$, tedy $14 \mid 5 \cdot 3 - 1$ a platí, že existuje celé číslo k takové, že $5 \cdot 3 = 1 + k \cdot 14$).

Po ujasnění předchozích zápisů už můžeme psát

$$y^d \equiv_N (x^e)^d \equiv_N x^{e \cdot d} \equiv_N x^{l + k \cdot N} \equiv_N x \cdot (x^N)^k$$

POKUD by PLATILO $x^N \equiv_N 1$, pak by $(x^N)^k \equiv_N 1^k \equiv_N 1$ a bylo by proto $y^d \equiv_N x$ neboli dešifrovali bychom zašifrovaný text. Bohužel $x^N \equiv_N 1$ pochopitelně NEPLATÍ (např. $4^2 = 16$ a 16 při dělení 2 dává zbytek 0 a ne 1).

Platí však (za předpokladu, že čísla x a N jsou nesoudělná; v případě našeho šifrování nás však tento předpoklad nijak neomezí), že

$x^{\phi(N)} \equiv_N 1$, kde $\phi(N)$ je počet čísel nesoudělných a menších než N ($\phi(N)$ se nazývá Eulerova funkce čísla N).

Toto je znění Eulerovy věty – jedná se o zobecnění malé Fermatovy věty. Teprve v roce 1977 (do té doby nemělo toto čistě teoretické tvrzení žádný aplikační význam) publikovali pánové Revert, Shamir a Adleman, pracovníci z Massachusetts Institute of Technology (MIT), nesmírně užitečnou aplikaci těchto vět, nyní známou jako RSA asymetrické šifrování. V dalším, v souvislosti s hledáním dešifrovacího exponentu d , se o RSA dovíme více. Hledejme tedy d nejprve pro konkrétní číselné hodnoty:

Adresát si zvolí číslo, kterým se bude umocněné číslo dělit – zvolí tedy N – např. 91. (Potom číslo, které se bude šifrovat, musí být z intervalu $<1, N>$. Poznamenejme přímo zde, že můžeme pochopitelně šifrovat i text. A sice tak, že jej zakódujeme právě nějakým číslem – např. písmeno po písmenu jejich ASCII kódem.)

Dále adresát najde $\phi(N)$ – tedy $\phi(91)$:

Nesoudělná čísla s 91 jsou: 1, 2, 3, 4, 5, 6, 8, 9, 10, 11, 12, 15, 16, 17, 18, 19, 20, 22, 23, 24, 25, 27, 29, 30, 31, 32, 33, 34, 36, 37, 38, 40, ... 90 (celkem 72 čísel), proto $\phi(91) = 72$.

Teprve nyní určí adresát šifrovací exponent e – ten musí být nesoudělný s $\phi(N)$ – např. 5.

Tedy adresátův veřejný klíč je dvojice $(N, e) = (91, 5)$ – tímto bude odesílatel svůj text (číslo) šifrovat. Adam šifroval číslo 4 podle adresátovy instrukce „Umocni na 5., vyděl číslem 91 a sděl zbytek“, tedy podle veřejného klíče $(91, 5)$

Pro tak malá čísla to může udělat „ručně“ – najde tak zašifrované číslo $y = 23 \equiv_{91} 4^5$.

Pomocí rovností, kterými došel adresát k tomu, že čísla e a $\phi(N)$ jsou nesoudělná, tedy pomocí

$$72 = 5 \cdot 14 + 2$$

$$5 = 2 \cdot 2 + 1$$

$$2 = 1 \cdot 2 + 0$$

najde adresát dešifrovací exponent d . Tudíž číslo, pro které musí platit $d \cdot e \equiv_N 1$:

$$1 = 5 - 2 \cdot (72 - 5 \cdot 14) = (-2) \cdot 72 + 29 \cdot 5 \text{ (např. } 29 \cdot 5 \text{ znamená } 29 \text{ krát } 5\text{)}. \text{ Odtud}$$

$$29 \cdot 5 - 1 = 2 \cdot 72, \text{ tj. } 72 / (29 \cdot 5 - 1), \text{ tj. } 29 \cdot 5 \equiv_{72} 1 \text{ a tedy } d = 29.$$

Můžeme proto konstatovat, že adresátův soukromý klíč je dvojice $(N, d) = (91, 29)$ – tímto bude adresát zašifrovaný text dešifrovat.

Připomeňme, že dešifrujeme pomocí kongruence $x \equiv_N y^d$ – sem dosadíme tedy příslušná čísla

$$x \equiv_{91} 23^{29}$$

$$23^{29} \equiv_{91} x.$$

Číslo 23^{29} je už poměrně veliké, takže nám k nalezení x nepomůže ani MS Excel a jeho funkce MOD. Dá se to však udělat opět „ručně“, jak je patrné z následujícího (pokud by tento postup připadal někomu nečitelný, vůbec to nevadí, neboť stejně bude tuto rovnici řešit pomocí nějakého matematického softwaru – viz dále v textu):

$$(29)_{10} = (11101)_2 = 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$$

$$23^{29} = 23^{(1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0)} = 23^{2^4} \cdot 23^{2^3} \cdot 23^{2^2} \cdot 23^{2^0}$$

$$23^{2^0} \equiv_{91} 23, 23^{2^1} \equiv_{91} 74, 23^{2^2} \equiv_{91} 74^2 \equiv_{91} 16, 23^{2^3} \equiv_{91} 16^2 \equiv_{91} 74, 23^{2^4} \equiv_{91} 74^2 \equiv_{91} 16,$$

$$23^{29} \equiv_{91} 23 \cdot 16 \cdot 74 \cdot 16 = 435712 \equiv_{91} 4, \text{ tedy } x = 4 \text{ (což je odeslaná zpráva)}$$

Je vidět, že tento výpočet byl pracný. Čili se nemůžeme divit, že pro velká N a e je metodou “papír-
tužka” prakticky neproveditelný.

Proto potřebujeme POČÍTAČ a nějaký sofistikovanější matematický software. Např. program CAS
Maxima distribuovaný pod GNU General Public License. I jeho on-line verze pro android je pro
potřeby asymetrického šifrování RSA naprosto dostačující. Syntaxe potřebných funkcí je intuitivní a
je tedy po krátké instruktáži přístupná prakticky každému žákovi vyššího stupně základní školy,
nemluvě o středoškolském studentovi.

Uveďme bez bližšího vysvětlování ty funkce softwaru CAS Maxima, které jsou pro RSA potřeba:

Funkce mod N ($\equiv_N$):

mod(x, N)

(%i1) mod(14,5);

4

Funkce power_mod(a, n, m), která řeší rovnici $a^n \equiv_m x$:

(%i2) power_mod(2,4,5);

1

Funkce inv_mod(x, p), kde x je číslo ke kterému hledáme inverzi a p je modulo, ve kterém inverzi
počítáme:

(%i3) inv_mod(40,127);

54

Největší společný dělitel gcd(a, b);

(%i4) gcd(20,8);

4

Prvočísla:

(%i5) primep(3);

true

(%i6) primep(4);

false

(%i7) next_prime(10);

11

Výpočet hodnoty Eulerovy funkce provedeme pomocí funkce totient(n):

(%i8) totient(5);

4

(%i9) totient(8);

4

(%i10) totient(13);

12

Podívejme se tedy, jak by se řešil Adamův problém šifrování čísla 4 metodou „umocni, vyděl
nějakým číslem a zapiš zbytek pomocí příslušných funkcí v Maximě:

Adresátův veřejný klíč je dvojice $(N, e) = (91, 5)$

Šifruje se číslo 4:

power_mod(4,5,91);

23

totient(91);

72

inv_mod(5,72);

29

Proto adresátův soukromý klíč je dvojice $(N, d) = (91, 29)$

power_mod(23,29,91);

4

Dešifrované, a tedy původní šifrované číslo, bylo číslo 4.

Shrňme si, co jsme doposud udělali:

Každý žák ví, jak své číslo šifroval (zná veřejný klíč (N, e) a navíc zná metodu, jak bylo jeho číslo dešifrováno. (Pokud metodu nezná, zeptá se na ní adresáta a ten mu ji klidně přesně popíše – viz popis nahoře). Protože žáci svá tajná čísla šifrují do sdíleného sešitu, zcela jistě si uvědomí, že jejich zašifrované číslo může (podobně jako v předchozím příkladu šifrování umocňováním) dešifrovat úplně každý, kdo má k sešitu přístup, tedy především všichni jeho spolužáci. Takže jak to vlastně jejich učitel myslel, když jim řekl, že jedině on bude moci jejich zašifrované číslo dešifrovat a nikdo jiný už to nedokáže? Přece, pokud jeho spolužák vidí ve sdíleném excelovském jeho číslo $y \equiv_N x^e$, tak vzhledem k tomu, že zná také N , najde $\phi(N)$ – např. v CAS Maximě funkcí `totient( $\phi(N)$ )`. A odsud už je jenom krůček k „SOUKROMÉMU“ dešifrovacímu exponentu d :

`inv_mod(e,  $\phi(N)$ )`.

Nyní už zbývá jenom zachycené číslo vložit jako jeden z argumentů funkce `power_mod(y, d, N)` a najde tak původní x .

V čem je tedy podstata tohoto šifrování RSA?

Že jeho spolužák (potažmo tak nějaký „špión“) nenajde $\phi(N)$. Jak to? Má přece k dispozici funkci `totient( $\phi(N)$ )`? Protože nalezení $\phi(N)$ trvá pro velká čísla N MOC dlouho:

Například pro tak „malinké“ číslo jako $N =$

128243199501723361359275202929838997632567303002512

našla Maxima $\phi(N) =$

54958233971390812604410282746984514727812532196864

Za asi 30 vteřin. Ve skutečnosti se však volí N MNOHEM a MNOHEM VĚTŠÍ...

Jak ale potom najde $\phi(N)$ adresát?

Jednoduše: N zadá jako součin dvou prvočísel a využije toho, že pro Eulerovu funkci $\phi(N)$ platí:

1. Je-li p prvočíslo, pak $\phi(p) = p - 1$.

2. $\phi(p \cdot q) = \phi(p) \cdot \phi(q)$

Jsou-li tedy p i q prvočísla, je pro $N = p \cdot q$

$\phi(N) = \phi(p \cdot q) = (p - 1) \cdot (q - 1)$

Protože

1. prvočísel je nekonečně mnoho (a můžeme tak teoreticky volit stále větší a větší (dvě) prvočísla)

2. neexistuje efektivní algoritmus k rozkladu součinu na dva činitele (v podstatě se postupuje způsobem pokus – omyl

nemohou ani nejrychlejší počítače v „reálném“ čase najít $\phi(N)$ a tedy žádný „špión“ nedešifruje zašifrovanou zprávu.

Co je myšleno tím „reálným“ časem? Zatímco nejrychlejším současným počítačům trvá vynásobit dvě čísla velikosti 2^{350} asi 2,5 sekundy, rozložit tak velké číslo na součin dvou čísel trvá asi 250 000 roků. Pokud se jedná o čísla velikosti 2^{1000} , tak jejich součin zabere asi 12 sekund, zatímco faktorizace by trvala asi 2 biliony let.

Není snad třeba dodávat, že pro plazmové počítače a případně rychlejší algoritmy (zatím je ale nikdo nenašel) se jednoduše ta dvě prvočísla zvětší...

Pokud někdo četl o „prolomitelnosti“ RSA neuronovými sítěmi, tak se jedná o něco úplně jiného. Tyto sítě sice dokážou do jisté míry faktorizovat velká čísla, ale potřebují (velmi zhruba řečeno) ještě něco, co se v případě RSA nemají šanci dovědět.

Jaké aktivity v oblasti RSA může učitel s žáky dělat? Vzhledem k GDPR (General Data Protection Regulation) by zřejmě neměl chtít po svých žácích, aby mu do sdíleného sešitu napsali třeba poslední čtyřčíslí svých rodných čísel. Pokud však zvolí metodu RSA a bezpečný (tedy především hodně velké N) veřejný klíč (N, e) , mohou žáci svá poslední čtyřciferná čísla bezpečně zašifrovat.

Nebo i jinak: I přesto, že žáci nechtějí, aby jejich známku z písemné práce viděli ostatní spolužáci, může jim učitel ve sdíleném sešitě jejich známky zašifrovat, a to na základě instrukcí toho kterého žáka – tyto instrukce mohou být přímo „součástí“ jeho jména.

Závěr

V práci bylo explicitně pojednáno o nutnosti použití sofistikovanějších matematických softwarů pro praktické šifrování. Bylo nastíněno, že jedině systematictější vzdělávání učitelů v problematice asymetrického šifrování a finanční matematiky vůbec může napomoci k tomu, aby jejich žáci ztratili nedůvěru k finančním operacím založených na veřejném zasílání privátních dat. V neposlední řadě bylo v práci ukázáno, že i ve školské matematice existují zajímavé problémy, jejichž řešení se bez počítače nedá realizovat.

Literatura

- Burda, K. (2015). Úvod do kryptografie. Akademické nakladatelství CERM. Brno
- Monterde, J. & Vallejo, J. (2012). Implementing the RSA Cryptosystem with Maxima CAS. *The Electronic Journal of Mathematics and Technology*. Vol. 6, No. 1, pp. 34-53.
- Ribenboim, P. (1996). The New Book of Prime Number Records. New York: Springer-Verlag.
- Rosen, K. (2005). Elementary Number Theory and Its Applications. New York: Addison-Wesley.
- Singh, S. (2000). The Code Book. Fourth Estate. London.
- Smart, N. (2003). Cryptography: An Introduction. London: McGraw-Hill.
- Tlustý, P. (2006). Obecná algebra pro učitele. Jihočeská univerzita. České Budějovice.
- Velebil, J. (2007). Diskrétní matematika: Text k přednášce. [online] Praha: [s.n.], 193 s. Dostupné z <ftp://math.feld.cvut.cz/pub/velebil/y01dma/dma-notes.pdf>.

Kontaktní adresa:

Květoslav Bártek, Mgr. Ph.D.,
Katedra matematiky, Pedagogická fakulta UP, Žižkovo nám. 5, 771 40 Olomouc, ČR, tel.: +420 585 635 5714, e-mail: kvetoslav.bartek@upol.cz

Tomáš Zdrahal, doc. RNDr. CSc.,
Katedra matematiky, Pedagogická fakulta UP, Žižkovo nám. 5, 771 40 Olomouc, ČR, tel.: +420 585 635 5710, e-mail: tomas.zdrahal@upol.cz