UNIVERZITA PALACKÉHO V OLOMOUCI

PEDAGOGICKÁ FAKULTA

Katedra matematiky

Bakalářská práce

Lukáš Růžica

RSA – šifrovací metoda s veřejným klíčem

Olomouc 2019 **vedoucí práce: doc. RNDr. Tomáš Zdráhal, CSc.**

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci s názvem *RSA- šifrovací metoda s veřejným klíčem* vypracoval samostatně, a že veškerá použitá literatura je uvedena v závěru práce.

V Olomouci dne …….....

Lukáš Růžica

Poděkování

Rád bych na tomto místě poděkoval vedoucímu bakalářské práce doc. RNDr. Tomáši Zdráhalovi, Csc. za obětavou spolupráci i za čas, který mi věnoval při konzultacích.

Bibliografická identifikace

Jméno a příjmení autora	Lukáš Růžica
Název práce	RSA – šifrovací metoda s veřejným klíčem
Typ práce	Bakalářská
Pracoviště	Katedra matematiky
Vedoucí práce	doc. RNDr. Tomáš Zdráhal, CSc.
Rob obhajoby	2019
Abstrakt	Bakalářská práce seznamuje čtenáře s asymetrickým šifrováním RSA. V první kapitole se zaměříme na funkčnosti tohoto šifrování. V druhé kapitole si ukazujeme, jak probíhá šifrování RSA a ve třetí si pak představíme několik pokusů prolomit RSA. Celá práce je proložena příklady, které nám lépe ukáží, jak RSA funguje.
Klíčová slova	Kryptografie, asymetrická kryptografie, RSA šifrování, wMaxima, Euklidův algoritmus, Eulerova funkce
Počet stran	27
Počet příloh	0
Jazyk	český

Bibliographical identification

Autor´s first name and surname Lukáš Růžica

Title	RSA – cryptosystem using public key
Type of thesis	Bachelor
Department	Department of Mathematics
Supervisor	doc. RNDr. Tomáš Zdráhal, CSc.
The year of presentation	2019
Abstract	The bachelor thesis focuses on the asymmetric encryption RSA. In the first chapter we will focus on the functionality of this encryption. In the second chapter, we show how RSA encryption is in progress and in the third, we will try to break through. The whole work is interspersed with examples that will show us better how RSA works.
Keywords	cryptography, asymmetric cryptography, RSA encryption, wMaxima, Euclidean algorithm, Euler function
Number of pages	27
Number of appendices	0
Language	Czech

Obsah

Obsah 6

1. Úvod 7

2. Funkčnost principu RSA 8

2.1. Základní informace před samotným šifrováním RSA 8

2.2. Tvorba klíčového páru 12

2.3. Příklady na inverzní prvky: 15

3. Šifrování a dešifrování zprávy 19

3.1. Příklady na tvorbu klíčů a šifraci/dešifraci zprávy 20

4. Útoky na RSA 24

4.1. Příklady na hrubou sílu: 26

5. Závěr 31

6. Seznam použitých zdrojů: 32

1. Úvod

Tuto bakalářskou práci jsem si vybral proto, že RSA šifrovací systém je nejrozšířenějším kryptografickým algoritmem 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.

Účelem této práce je detailní pojednání o principu metody šifrování s veřejným klíčem RSA, tedy vysvětlení určitých pasáží modulární aritmetiky. Tyto pasáže jsou velmi nutné k pochopení matematického pozadí asymetrického šifrování RSA.

Dále se práce zaměří na algoritmus RSA a problematice faktorizace veřejných klíčů.

Následně bude pojednáváno o nutnosti použití sofistikovanějších matematických softwarů pro praktické šifrování. Jedním z volně šiřitelným softwarem je Maxima distribuovaný pod GNU General Public License.

Po přečtení celé této práce by měl každý mít přehled o šifrovacím systému RSA, a měl by mít taky základní znalost v matematickém softwaru Maxima, který jsme používali pro veškeré příklady, které jsou v práci uvedeny.

2. Funkčnost principu RSA

2.1. Základní informace před samotným šifrováním RSA

Dejme tomu, že dva lidi (Alice a Bob) spolu chtějí komunikovat tak, aby nejlépe nikdo nerozuměl jejím zprávám. Zvolí si pro způsob svojí komunikace kódování RSA, které je pojmenované po svých zakladatelích Rivest, Shamir a Adelman. Navíc si zvolí takovou metodu, která je pravděpodobně ta nejznámější, a to asymetrické šifrování. Co si ale pořádně představit vše pod asymetrickým šifrováním?

Základním rozdílem mezi asymetrickým a symetrickým šifrováním je jejich počet klíčů. Zatímco pro symetrické šifrování se používá jak u šifrování zprávy, tak i u jejího dešifrování jeden klíč, u asymetrického šifrování je to jinak. Asymetrické šifrování pracuje s dvěma klíči, kde jeden z klíčů slouží k zašifrování zprávy, no druhý zase k jejímu dešifrování. U asymetrického šifrování tedy není nutná výměna jakéhokoliv klíče, abychom byli schopni se domluvit. Každý totiž vlastní klíč veřejný, který je pro všechny volně přístupný, a klíč soukromý, který si každý z majitelů ponechává v tajnosti, takže jej nikde nezveřejňuje. Když už teď máme nějakou malou představu, s čím vlastně u šifrování RSA budeme pracovat, uveďme si nějaké základní definice a věty, které se nám budou hodit pro lepší pochopení tohoto typu šifrování (viz. lit. [1-2]).

Definice 1. Ať $m > 1$ je pevné přirozené číslo. Řekneme, že celá čísla a a b jsou kongruentní modulo n, (značíme $a \equiv b (\mathrm{mod}\, n)$), pokud existuje celé číslo k takové, že $a - b = k \cdot n$. Tedy kongruence modulo n je relací ekvivalence, která navíc respektuje operace sčítání a odčítání, tj. pro všechna celá čísla a, b, c, d platí:

$$a \equiv b (\mathrm{mod}\, n) \wedge c \equiv d (\mathrm{mod}\, n) \Longrightarrow a + c \equiv b + d (\mathrm{mod}\, n)$$

$$a \equiv b (\mathrm{mod}\, n) \wedge c \equiv d (\mathrm{mod}\, n) \Longrightarrow a \cdot c \equiv b \cdot d (\mathrm{mod}\, n)$$

Tuto definici lze chápat také tak, že čísla a, b jsou kongruentní právě tehdy, pokud dávají totožný zbytek po dělení číslem n.

Příklad 1. Rovnice kongruence v Z_{21}

$$4 \equiv 25(\mathrm{mod}\ 21)$$

$$-21 \equiv 0(\mathrm{mod}\ 21)$$

$$0 \equiv 21(\mathrm{mod}\ 21)$$

$$19 \equiv 40(\mathrm{mod}\ 21)$$

Příklady ze zadání jsme vypočítali na papír a v programu wMaxima si naše výsledky ověřili pomocí funkce mod. Do programu jsme tedy zadali příkazy

$$mod(25,21)$$

$$mod(0,21)$$

$$mod(21,21)$$

$$mod(40,21)$$

Definice 2. Pro přirozené číslo n definujeme přirozené číslo $\varphi(n)$ jako počet čísel nesoudělných s n, větších než 0 a menších než n. Funcki $\varphi: N \to N$ nazýváme Eulerova funkce.

Příklad 2. Určete Eulerovy funkce pro hodnoty 7,9,70.

(i) $\varphi(7) = 6 \quad \to \quad hodnoty \quad \to \quad [1,2,3,4,5,6]$

(ii) $\varphi(9) = 6 \quad \to \quad hodnoty \quad \to \quad [1,2,4,5,7,8]$

(iii) $\varphi(70) = 24 \quad \to \quad hodnoty$

Tyto hodnoty jsme zjistili za pomocí programu Maxima (viz. lit. [8]), kde jsme využili funkci „*totient*“. Tento příkaz pro náš první příklad měl podobu $totient\ (7)$. U ostatních hodnot jsme tento postup opakovali a pro hodnotu $\varphi(70)$ jsme si to zkusili i ručně a zjistili jsme, že se jedná přesně o tyhle čísla:

$$3,9,11,13,17,19,23,27,29,31,33,37,39,41,43,47,51,53,57,59,61,63,67,69.$$

Definice 3. Nechť $p, q \in N$ jsou prvočísla. Pak platí $\varphi(n) = (p-1)(q-1)$.

Prvočíslo je takové číslo z množiny N, které je dělitelné beze zbytku jen samo sebou, a taky nejmenším přirozeným číslem 1. Mezi takové prvočísla patří např.: $(2, \dots 23, \dots 47, \dots 167, \dots)$.

Příklad 3. Vypište prvních 15 prvočísel.

Pomocí předchozí definice víme, co pro prvočísla platí, avšak pozor. Číslo 1 není považováno za prvočíslo, takže první prvočíslo a zároveň i jediné sudé číslo je číslo 2. Odpověď na otázku tedy zní, že prvních 15 prvočísel mají tvar 2,3,5,7,11,13,17,19,23,29,31,37,41,43,47.

Definice 4. Nechť p, q jsou prvočísla, $n = pq$. A nechť e, d jsou libovolná čísla splňující podmínku $[ed]_{\varphi(n)} = [1]_{\varphi(n)}$. Dále označme v, w čísla $0 \leq v \leq n-1$ a nechť platí $[v]_n = [v^{ed}]_n$. Potom platí $[v]_n = [w^d]_n$.

Příklad 4. Zvolíme-li si hodnoty $p = 5437$ a $q = 7331$, určeme poté $\varphi(n), n, e$ a d.

$$n = pq = 39858647$$

$$\varphi(n) = (p-1)(q-1) = 39845880$$

$$e = 25634761$$

$$d = 37458481$$

Z definice 4. si nyní vysvětlíme některé neznámé. Prvním náznakem k samotnému šifrování jsou neznámé v a w, kde v je číslo k zašifrování a w již číslo zašifrované. Jak tento průběh probíhá, si však ukážeme až později. Mnohem důležitější je pro nás ale z této definice rovnice $[ed]_{\varphi(n)} = [1]_{\varphi(n)}$, která nám říká, že roznásobíme-li mezi sebou čísla d a e, pak po vydělení $\varphi(n)$ nám vyjde zbytek 1. Takže hodnotu e jsme si zvolili, a následně vypočítali hodnotu d. V programu wMaxima jsme pracovali s obyčejným násobením a k nalezení hodnoty d jsme využili funkce

$$inv\_mod(e, n)$$

Věta 1. Nechť p, q jsou prvočísla, $n = pq$. Dále zvolme prvočíslo $2 \leq e \leq n-1$ nesoudělné s číslem $\varphi(n)$. Předpokládejme, že pro čísla e, d platí $[ed]_{\varphi(n)} = [1]_{\varphi(n)}$. Potom d je ve tvaru

$$d = \frac{1 + r\varphi(n)}{e}, \quad kde \quad [r]_e = [(e-1)\varphi(n)^{e-2}]_e.$$

Důkaz věty: Připomeňme si, že $[ed]_{\varphi(n)} = [1]_{\varphi(n)}$ platí právě tehdy když nám platí $ed = 1 + r\varphi(n)$. Takže nám opravdu stačí ověřit, že je-li číslo r voleno tak, aby platilo $e|1 + r\varphi(n)$. Pak lze stavit d, a platnost vztahů je tím dokázána.

Pro číslo e platí $e|1 + r\varphi(n)$ právě když $\langle 1 + r\varphi(n), 0\rangle \in \theta_e$, a to právě jen tehdy, kdy zbytek po dělní výrazu $1 + r\varphi(n)$ číslem e je nula. Tuto podmínku můžeme poté ekvivalentně vyjádřit ve tvaru $[1 + r\varphi(n)]_e = [0]_e$, nebo také jinak $[1]_e + [r]_e \cdot [\varphi(n)]_e = [0]_e$, dále třeba jako $[r]_e \cdot [\varphi(n)]_e = -[1]_e$. Opačný prvek k $[1]_e$ m tvar $[e-1]_e$. Pomocí inverse lze vyjádřit $[r]_e = [e-1]_e \cdot [\varphi(n)]_e^{-1}$. Vztah z věty 1. je platný právě jen tehdy, když je $[\varphi(n)]_e^{-1}$ roven $[\varphi(n)^{e-2}]_e$. Platí pak

$$[\varphi(n)]_e \cdot [\varphi(n)]_e^{-1} = [\varphi(n)]_e \cdot [\varphi(n)^{e-2}]_e = [\varphi(n)^{e-1}]_e = [\varphi(n)^{\varphi(e)}]_e = [1]_e.$$

Tento vtah nám plyne z předpokladu nesoudělnosti $\varphi(n)$ s e a užitím Fermatovy-Eulerovy věty. Samozřejmě platí $\varphi(e) = e - 1$, protože e bylo dáno jako prvočíslo. Tímto je důkaz hotový. Volba čísla r implikuje platnost $e|1 + r\varphi(n)$ a podmínka $ed = 1 + r\varphi(n)$ je splněna.

2.2. Tvorba klíčového páru

Jak už je tedy zřejmé z předchozí kapitoly, pracujeme zde s dvěma klíči. Tyto klíče jsou zvoleny tak, aby výpočet jednoho klíče z druhého byl algoritmicky řešitelný, avšak neúnosný z hlediska výpočetního výkonu soudobých i budoucích počítačů. Jejich využití je takové, že jedním klíčem zprávu zašifrujeme, tomuto klíči se říká klíč veřejný, a tím druhým ji budeme dešifrovat, to je zase klíč soukromý. Než si však ukážeme tvorbu obou klíčů, musíme stanovit, s jakými čísly zde smíme pracovat. Celé šifrování RSA je definované na množině přirozených čísel a využívá jak platnosti Eulerovy věty, tak i nesoudělnost určenou Euklidovým algoritmem.

Když už tedy víme, jaké čísla můžeme pro kódování používat a s jakými pravidly budeme pracovat, zaměřme se na založení dvou hlavních faktorů, tedy oněch klíčů. Jedná se o dvojici čísel, které podléhají určitým pravidlům.

Než si však ukážeme tyto dvojice, zvolme si dvě od sebe různá prvočísla, které si označíme jako p a q. Samozřejmě čím větší čísla si zvolíme, tím bude kódování bezpečnější a pro někoho, kdo touží znát šifrovanou komunikaci složitější si ji přečíst. Jakmile jsme si tedy určili p a q, vynásobíme tyto dvě prvočísla mezi sebou a získáme n, jinak řečeno modulo. To získáme za pomoci vztahu

$$n = p \cdot q.$$

Původ tohoto čísla by měl znát pouze jeho majitel, nikomu by tedy neměl prozradit dvě prvočísla, díky kterým získal hodnotu n. Důvod, proč by hodnoty obou prvočísel neměl nikomu prozradit je hlavně ten, aby nikdo nemohl zjistit majitelův $\varphi(n)$, aby tedy nikdo kromě majitele nemohl zjistit, kolik existuje nesoudělných čísel čísla n. Zná-li by někdo totiž hodnotu nesoudělnosti, bylo by pro něj už mnohem jednodušší zjistit majitelův soukromý klíč tudíž by mohl útočník cizí konverzace číst zprávy, které mu nejsou určeny. Tímto tématem se však budeme zabývat až později.

Po získání modula využijeme naší znalosti Eulerovy funkce $\varphi(n)$, která je předepsaná v def.3 rovnicí

$$\varphi(n) = (p-1) \cdot (q-1).$$

Po tomto výpočtu si už jen zvolíme hodnotu e tak, aby číslo e bylo menší než číslo n $(e < n)$ a platilo také to, že námi zvolená hodnota e musí být s hodnotou $\varphi(n)$ nesoudělná $(\nexists h \in N;\ \varphi(n) \neq h \cdot e)$. Toto číslo je označováno jako *„šifrovací/veřejný exponent“*, tedy číslo, pomocí kterého naši zprávu později zakódujeme, aby ji nikdo nebyl schopný přečíst kromě přijímatele. Po těchto krocích jsme docílili znalosti veřejného klíče. Ten má kombinaci dvou cifer, a to ve tvaru (n, e). Když už jsme si teď ukázali, jak přijít na klíč veřejný, pojďme se zaměřit na klíč soukromý, pomocí kterého budeme zprávu moci rozšifrovat neboli dešifrovat. I tento klíč se skládá ze dvou hodnot a to n, které již z dřívější rovnice známe a hodnoty d. Tato hodnota je označována jako *„dešifrovací/soukromý exponent“* a její hodnotu můžeme vypočítat z následujícího vztahu

$$e \cdot d - k \cdot \varphi(n) = 1,$$

kde k je právě taková hodnota, že vyjádříme-li z předchozí rovnice neznámou d, k musí být takové celé číslo, aby nám rovnice platila vždy pro celé číslo d

$$d = \frac{[k \cdot \varphi(n) + 1]}{e}.$$

Zde si jen můžeme opět připomenout, jak důležité je uchovávat si nesoudělnost čísla n v tajnosti. Kdyby jej totiž někdo znal, nedělalo by mu vůbec problém pracovat tímto postupem a zjistit si tak cizí soukromý klíč. Bohužel i bohudík tato metoda určení d nám bude příjemná jen v případě, že jsme si zvolili poměrně nízká neboli malá prvočísla p a q. Jakmile si zvolíme totiž prvočísla, které mají klidně až pět set míst, je až skoro nemožné s touto rovnicí pracovat. V takovém případě se obracíme na inverzní prvek čísla e. Důležitým faktorem je zde však to, že zde již pracujeme ve $\varphi(n)$, nikoliv v N $(e \cdot d \equiv 1\varphi(n))$. V programu Maxima využijeme následující funkce a získáme tak soukromý klíč, který je dán tvarem (n, d).

$$d\text{: } inv\_mod(e, \varphi(n)).$$

A zde je skvěle vidět, proč bychom nikomu neměli prozrazovat ona dvě prvočísla, pomocí kterých jsme si určili i číslo $\varphi(n)$. Bude-li mít totiž někdo cizí přístup k našemu $\varphi(n)$ a opravdu základní přehled o šifrování RSA, je následně schopen si přečíst veškerou zašifrovanou zprávu, která nám přijde a bude tak schopen pracovat naším jménem/klíčem.

Při určení soukromého klíče, přesněji *„dešifrovacího/soukromého exponent“* jsme využili inverzního prvku. Ukažme si tedy, jak přesně tato vlastnost funguje.

Mějme definovanou množinu Z_9. Budeme-li chtít znát inverzní prvek pro číslo x z této množiny, musí nám platit, že roznásobíme-li tyto dvě čísla, dostaneme výsledek 1. Jinak řečeno multiplikativní inverze pro číslo x je právě takové číslo, které když se vynásobí s x je rovno 1. Tuto podmínku můžeme zapsat vztahem

$$x \cdot x^{-1} = 1.$$

Avšak pozor, ne pro každé číslo x existuje inverzní prvek. Musíme si totiž uvědomit, že nám stále platí podmínka $\gcd(x, Z_9) = 1$, a jak můžeme vidět v tab. 1, jsou to právě čísla 3 a 6, pro které neexistuje inverzní prvek. Pro zjednodušení bychom mohli říct, že nejsou-li všechny hodnoty v množině Z_9 obsazeny v každém řádku i sloupci, tak dané číslo nemá inverzní prvek v dané množině.

V tab.1 jsme barevně rozlišili, jak hlavní poloosu, podle které jsou data symetrické (červeně), tak i všechny čísla, které v námi zvolené množině nemají inverzní prvek (zeleně).

$Z_9(\cdot)$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	4	6	8	1	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	6	1	5
5	0	5	1	6	2	7	3	8	4
6	0	6	3	0	6	3	0	6	3
7	0	7	5	3	1	8	6	4	2
8	0	8	7	6	5	4	3	2	1

Tabulka 1: Zbytkové třídy množiny Z_9 s operací násobení

Pomocí tab. 1 jsme si tedy již vědomi, co musí platit pro to, aby prvek z dané množiny měl inverzní prvek. Pro více ukázek jsou k práci přiloženy příklady, které naši znalost prohloubí a ukáží, jak za pomocí funkce mod určit inverzní prvky/čísla. V příkladech se také setkáme i s maticí 3x3, u které je nutné si uvědomit, v jaké množině pracujeme. Dále je to totiž stále jen, a jen to samé.

2.3. Příklady na inverzní prvky:

<u>Příklad 5:</u> 3.7.1. Pokud existují, nalezněte inverse (viz. lit. [3])

a) **Čísla 6 v Z_{14}**
b) **Čísla 6 v Z_{41}**
c) **Čísla 160 v Z_{841}**

Řešení:

a) $6 \equiv 1(\mathrm{mod}14)$ $\qquad 14 = 6 \cdot 2 + 2$

$6x \equiv 1(\mathrm{mod}14)$ $\qquad 6 = 2 \cdot 3 + 0$

$x \equiv \frac{1}{6}(\mathrm{mod}14)$

$x \equiv 6^{-1}(\mathrm{mod}14)$

Číslo 6 v Z_{14} nemá inverzní prvek

b)

$6 \equiv 1(\mathrm{mod}41)$ $\qquad 41 = 6 \cdot 6 + 5$

$6x \equiv 1(\mathrm{mod}41)$ $\qquad 6 = 5 \cdot 1 + 1$

$x \equiv \frac{1}{6}(\mathrm{mod}41)$

$x \equiv 6^{-1}(\mathrm{mod}41)$

$1 = 6 - 5$

$1 = 6 - (41 - 6 \cdot 6)$

$1 = 6 - 41 + 6 \cdot 6$

$1 = -41 + 7 \cdot 6$

$7 \equiv 6^{-1}(\mathrm{mod}41)$

Číslo 6 v Z_{41} má inverzní prvek 7

c)

$$160 \equiv 1(\mathrm{mod}841) \qquad 841 = 160 \cdot 5 + 41$$

$$160x \equiv 1(\mathrm{mod}841) \qquad 160 = 41 \cdot 3 + 37$$

$$x \equiv \frac{1}{160}(\mathrm{mod}841) \qquad 41 = 37 \cdot 1 + 4$$

$$x \equiv 160^{-1}(\mathrm{mod}841) \qquad 37 = 4 \cdot 9 + 1$$

$$37 - 4 \cdot 9 = 1$$

$$37 - (41 - 37) \cdot 9 = 1$$

$$10 \cdot 37 - 9 \cdot 41 = 1$$

$$10 \cdot (160 - 41 \cdot 3) - 9 \cdot 41 = 1$$

$$10 \cdot 160 - 39 \cdot (841 - 160 \cdot 5) = 1$$

$$205 \cdot 160 - 39 \cdot 841 = 1$$

$$160^{-1}(\mathrm{mod}841)x \equiv 205$$

Všechny 3 příklady jsme si počítali na papír, avšak jejich správnost jsme si ověřili v programu mod.

<u>Příklad 6:</u> 3.7.8. Pokud existují, nalezněte inversní matice (viz. lit. [3])

1) **V Z_6:** $\begin{pmatrix} \mathbf{7} & \mathbf{8} & \mathbf{9} \\ \mathbf{6} & \mathbf{5} & \mathbf{3} \\ \mathbf{2} & \mathbf{2} & \mathbf{1} \end{pmatrix}$

2) **V Z_{15}, kde $t \in Z_{15}$ je parametr :** $\begin{pmatrix} \mathbf{7} & \mathbf{8} & \mathbf{9} \\ \mathbf{6} & \mathbf{5} & \mathbf{3} \\ \mathbf{2} & \mathbf{2} & \mathbf{1} \end{pmatrix}$

Řešení:

1) Abychom zjistili inversní matici, musíme zadanou matici vynásobit maticí jednotkovou

$$\left(\begin{array}{ccc|ccc} 7 & 8 & 9 & 1 & 0 & 0 \\ 6 & 5 & 3 & 0 & 1 & 0 \\ 2 & 2 & 1 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 5 & 3 & 0 & 1 & 0 \\ 2 & 2 & 1 & 0 & 0 & 1 \end{array}\right) \begin{matrix} \cdot 4 \\ \\ \cdot 1 \end{matrix} \sim \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 5 & 3 & 0 & 1 & 0 \\ 0 & 4 & 1 & 4 & 0 & 1 \end{array}\right) \begin{matrix} \\ \\ \cdot 4 \end{matrix} \sim$$

$$\sim \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 5 & 3 & 0 & 1 & 0 \\ 0 & 0 & 1 & 4 & 4 & 1 \end{array}\right) \cdot 5 \sim \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & 3 & 0 & 5 & 0 \\ 0 & 0 & 1 & 4 & 4 & 1 \end{array}\right) \begin{matrix} \\ \cdot 1 \\ \cdot 3 \end{matrix} \sim \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 5 & 3 \\ 0 & 0 & 1 & 4 & 4 & 1 \end{array}\right) \begin{matrix} \cdot 1 \\ \\ \cdot 3 \end{matrix} \sim$$

$$\sim \left(\begin{array}{ccc|ccc} 1 & 2 & 0 & 1 & 0 & 3 \\ 0 & 1 & 0 & 0 & 5 & 3 \\ 0 & 0 & 1 & 4 & 4 & 1 \end{array}\right) \cdot 1 \cdot 4 \sim \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 2 & 3 \\ 0 & 1 & 0 & 0 & 5 & 3 \\ 0 & 0 & 1 & 4 & 4 & 1 \end{array}\right)$$

Inversní matice k matici $\begin{pmatrix} 7 & 8 & 9 \\ 6 & 5 & 3 \\ 2 & 2 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 \\ 0 & 5 & 3 \\ 2 & 2 & 1 \end{pmatrix}$ je $\begin{pmatrix} 1 & 2 & 3 \\ 0 & 5 & 3 \\ 4 & 4 & 1 \end{pmatrix}$ v Z_6

2) K určení parametru t a nalezení zároveň inverzní matice k matici zadané, musíme pracovat s determinantem. Všechny možné determinanty si tedy rozepíšeme

$$\det A = 16t + 8 - 12 - 8t = 8t + 11$$

$$\det A_{11} = 4t - 0 \cdot 4 = 4t \qquad a_{11} = (-1)^{1+1} A_{11} = 4t$$

$$\det A_{12} = 2 \cdot t - 0 \cdot 3 = 2t \qquad a_{12} = (-1)^{1+2} A_{12} = -2t$$

$$\det A_{13} = 2 \cdot 4 - 4 \cdot 3 = 11 \qquad a_{13} = (-1)^{1+3} A_{13} = 11$$

$$\det A_{21} = 4 \cdot t - 1 \cdot 4 = 4t - 4 \qquad a_{21} = (-1)^{2+1} A_{21} = -4t + 4$$

$$\det A_{22} = 4 \cdot t - 1 \cdot 3 = 4t - 3 \qquad a_{22} = (-1)^{2+2} A_{22} = 4t - 3$$

$$\det A_{23} = 4 \cdot 4 - 4 \cdot 3 = 4 \qquad a_{23} = (-1)^{2+3} A_{23} = 11$$

$$\det A_{31} = 4 \cdot 0 - 1 \cdot 4 = 11 \qquad a_{31} = (-1)^{3+1} A_{31} = 11$$

$$\det A_{32} = 4 \cdot 0 - 1 \cdot 2 = 13 \qquad a_{32} = (-1)^{3+2} A_{32} = 2$$

$$\det A_{33} = 4 \cdot 4 - 4 \cdot 2 = 8 \qquad a_{33} = (-1)^{3+3} A_{33} = 8$$

$$\frac{4 - 4t}{8t + 11} = 0 \rightarrow 4 - 4t = 0 \rightarrow t = 1$$

$$\frac{1}{8t + 11} \cdot \begin{pmatrix} 4t & -2t & 11 \\ -4t + 4 & 4t - 3 & 11 \\ 11 & 2 & 8 \end{pmatrix} = 4 \cdot \begin{pmatrix} 4 & 0 & 11 \\ 13 & 1 & 2 \\ 11 & 11 & 8 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 14 \\ 7 & 4 & 8 \\ 14 & 14 & 2 \end{pmatrix}$$

3. Šifrování a dešifrování zprávy

Z předchozí kapitoly víme, jak vypadá klíč veřejný (n, e), tak i klíč soukromý (n, d). Jejich vznik jsme si dokonce také již předvedli dříve, proto ani ten tady již zmiňovat nebudeme. Zaměříme se pouze na samotné šifrování zprávy a následně její dešifrování.

Předveďme si obdobnou situaci jako je zmíněna v našem zdroji (viz. lit. [5]). Zákeřná macecha zakazuje popelce se účastnit jakýchkoliv veřejných akcí. Jak však všichni z pohádky víme, tak se ale popelka zúčastní královského bálu, kde následně ztratí svůj střevíček, pomocí kterého si ji poté princ najde. Jak to souvisí s naším tématem? Představme si, že všichni z pohádky vlastní svoje dva klíče, tedy klíč veřejný a soukromý. Střevíc si představme, jako číslo a berme v úvahu i to, že jej popelka neztratila omylem, ale nechala jej tam právě z důvodu, aby jej princ našel. Jak to chápat? Popelka si zjistila princův veřejný klíč a nechala za sebou při svém odchodu z bálu střevíc, který znázorňoval šifrovanou zprávu, kterou mohl jen princ přeložit se svým soukromým klíčem.

Teď máme uvedený příběh, nyní se podívejme, jak by tato komunikace probíhala. Zprávu, kterou by popelka do střevíčku zašifrovala, by měla tvar

$$t = mod\left(r^{e_p}; n_p\right),$$

kde t je zašifrovaná zpráva, r je původní zpráva před dešifrováním, e_p je princův *veřejný exponent* a n_p jeho modul z princova veřejného klíče. Nyní stačilo jen popelce svou zašifrovanou zprávu dostat k princi. Ten, až ji příjme ji bude dešifrovat pomocí svého soukromého klíče pomocí vztahu

$$r = mod\left(t^{d_p}, n_p\right),$$

kde r je již dešifrovaná zpráva od popelky, t je zašifrovaná zpráva určená k dešifrování, d_p je princův *soukromý exponent* a n_p stejně jako u šifrování modul princova soukromého klíče. Po této rovnici dešifroval princ zprávu od popelky. Věděl tedy již, kde bydlí právě ta žena, která ho celý večer tak přitahovala a má se stát jeho paní.

3.1. Příklady na tvorbu klíčů a šifraci/dešifraci zprávy

<u>Příklad 7:</u> Křičí-li na sebe dva rybáři po měsíci na moři s dvěma loděmi čísla 6901 a 725, byli bychom schopni určit, kolik vylovili za svou cestu ryb?

Řešení:

1) Označíme-li si jejich vyřčená čísla jako čísla veřejně šiřitelná, můžeme si je označit jako veřejný klíč. Číslo $6901 = n$ a $725 = e$.
2) Z předchozích kapitol bychom si mohli klást otázku, že známe-li veřejný klíč, pusťme se do šifrování zprávy, ale pozor, zde tu zprávu neznáme. Půjdeme tedy na to obráceně. Nebudeme se tedy snažit zprávu (označme si ji jako m) zašifrovat, ale nejprve ji vůbec určit. K tomu budeme potřebovat znát *dešifrovací exponent* d. Ten získáme z tvaru
$$d = \frac{[k \cdot \varphi(n) + 1]}{e}.$$
3) Abychom však získali *dešifrovací exponent*, musíme určit hodnotu $\varphi(n)$. Její hodnotu vypočítáme ze vztahu
$$\varphi(6901) = (67 - 1) \cdot (103 - 1) = 66 \cdot 103 = 6732.$$
4) Nyní se vrátíme k bodu 2 a budeme hledat takové k, aby nám při jeho dosazení vycházelo číslo d jak celé číslo.

$$k\colon 1 \qquad d = \frac{[1 \cdot 6732 + 1]}{725} = 9{,}2869 \qquad k\colon 2 \qquad d = \frac{[2 \cdot 6732 + 1]}{725} = 18{,}572$$
$$k\colon 3 \qquad d = \frac{[3 \cdot 6732 + 1]}{725} = 27{,}858 \qquad k\colon 4 \qquad d = \frac{[4 \cdot 6732 + 1]}{725} = 37{,}143$$
$$k\colon 5 \qquad d = \frac{[5 \cdot 6732 + 1]}{725} = 46{,}429 \qquad k\colon 6 \qquad d = \frac{[6 \cdot 6732 + 1]}{725} = 52{,}735$$
$$k\colon 7 \qquad d = \frac{[7 \cdot 6732 + 1]}{725} = 65$$

Nyní jsme již zjistili dešifrovací klíč (65) a můžeme tak zjistit nezašifrovanou zprávu.

5) Když už známe soukromý i veřejný klíč, zaměřme se na samotnou zprávu. Pro její zjištění využijeme rovnice

$$m^d \equiv x \cdot mod\ 6901$$

$$42^{65} \equiv x \cdot mod\ 6901$$

$$x = 2688$$

Nyní již víme, že rybáři na svém pobytu na moři za měsíc vylovili 2688 ryb.

K přesnějšímu vypočítání nám sloužil program wMaxima, nebo pokud to stačilo, tak i obyčejná kalkulačka na stole.

<u>Příklad 8:</u> Vytvořte jak veřejný, tak i soukromý klíč, pokud znáte obě prvočísla.

$\boldsymbol{p = 5; q = 17}$

Řešení:

Nejdříve si určíme modulus n, který je dán součinem obou prvočísel.

$$n = p \cdot q = 5 \cdot 17 = 85$$

Dále si určíme $\varphi(n)$, které z teorie víme, jakým vztahem je definované.

$$\varphi(n) = (p-1)(q-1) = 4 \cdot 16 = 64$$

Teď si musíme určit takové e, které bude nesoudělné s $\varphi(n)$. Dejme tomu, že

$$e = 19.$$

Nyní si vypočítáme soukromý exponent za pomoci Euklidova algoritmu

$$64 = 3 \cdot 19 + 7 \rightarrow 7 = 64 + (-3 \cdot 19)$$

$$19 = 2 \cdot 7 + 5 \rightarrow 5 = 19 + (-2 \cdot 7) \rightarrow 5 = 7 \cdot 19 + (-2 \cdot 64)$$

$$7 = 1 \cdot 5 + 2 \rightarrow 2 = 7 + (-1 \cdot 5) \rightarrow 2 = 3 \cdot 64 + (-10 \cdot 19)$$

$$5 = 2 \cdot 2 + 1 \rightarrow 1 = 5 + (-2 \cdot 2) \rightarrow 1 = 27 \cdot 19 + (-8 \cdot 64)$$

Poněvadž se snažíme najít inverzní prvek v Z_{64}, musí nám tedy platit rovnice

$$1 = (-8) \cdot 64 \bmod 64.$$

Je nám tedy poté jasné, že hodnota d bude 56. A teď už jsme našli jak soukromý klíč, tak i klíč veřejný.

Veřejný klíč: $(e, n) = (19{,}85)$

Soukromý klíč: $(d, n) = (56{,}85)$

<u>Příklad 9:</u> Mějme Lukáše, který by Jacobovi rád napsal zprávu. Lukáš však nechce, aby obsah zprávy byl schopen zjistit i někdo jiný než Jacob a tak ji zašifruje. Jak bude vypadat zašifrovaná zpráva o obsahu 206 a jak ji Jacob vlastně přečte?

Řešení:

Nejprve si Lukáš musí najít Jacobův veřejný klíč, pomocí kterého mu zašifruje obsah zprávy 206. Když už najde jeho volně přístupný klíč, který má tvar $(391; 7)$, může se pustit do zašifrování.

$$mod\ (206^{7}; 391) = 298$$

Nyní zašifrovanou zprávu 298 pošle Jacobovi a ten pomocí svého soukromého klíče $(391; 151)$, jenž zná pouze a jen on, může zprávu dešifrovat. Tato rovnice bude mít tvar

$$mod\ (298^{151}; 391) = 206$$

K výsledkům jsme docílili pomocí programu wMaxima, kde bylo využito opět funkce mod.

4. Útoky na RSA

Jak už to ale tak bývá, vše má svůj háček. U šifrování RSA je to možnost útoku, neboli narušení konverzace mezi lidmi, kteří si píší. Tyto útoky můžeme rozdělit do několika typů, které si zde vypíšeme. Avšak pozor, i přes pokusy narušit RSA, je při správném používání a dodržování pravidel zcela prozatím nemožné nabourat komunikaci, a tak nám stále RSA zaručuje naprostou bezpečnost v digitální komunikaci. Takže si pojďme říct, na co si při RSA dát pozor, aby vše fungovalo, jak má.

Nejznámější, avšak už ne tak zcela aktuálním způsobem je hrubá síla, aneb pokusit se faktorizovat číslo n. Spočívá v tom, že známe-li uživatelův veřejný klíč, snažíme se jeho modul n rozložit na dvě prvočísla p a q. Tento způsob je poměrně primitivní a dá se předním lehce ubránit. Stačí nám totiž, když budeme pracovat s velkými prvočísly a nikomu nesdělovat naše soukromé hodnoty, neboť čím větší p a q zvolíme, tím bude pro útočníka obtížnější určit rozklad modulu n, viz. př.9. Avšak hrubá síla spočívá nejen ve snaze faktorizovat modul n, ale pracuje i se znalostí kvadratické rovnice. Jak? Udělejme si předpoklad, že n je sudé/liché číslo. V případě, že n bude sudé číslo, můžeme tvrdit, že platí-li nám rovnost

$$n = p \cdot q$$

získáme hodnoty p, q tak, že $p = 2$ a $q = \frac{n}{2}$ (případně obráceně). Budeme-li vycházet z předpokladu, že je n liché a dosadíme rovnici $n = p \cdot q$ do rovnice $\varphi(n) = (p-1) \cdot (q-1)$, získáme tvar v podobě

$$p + q = n + 1 - \varphi(n).$$

Jelikož by n mohlo být liché, tak $\varphi(n)$ by bylo liché taky. Z toho můžeme usoudit, že hodnota $p + q$ bude muset být sudá. Vyjádříme-li si to teď pomocí kvadratické rovnice, dostaneme tvar

$$x^2 - 2bx + n = 0,$$

kde $2b$ je rovno $(p + q)$. Dále pomocí diskriminantu jsme schopní vypočítat hodnoty p, q. Tedy již vše potřebné k zjištění si soukromého klíče [4]. Detailní postup vidíme v př.11.

Mnohem zajímavější způsobem narušení, ale zároveň i funkčnost šifrování je čínská věta o zbytcích. Místo aby se zabývala aritmetickými operacemi velkých čísel, stačí když se zaměříme na jejich zbytky. Jak může tahle čínská věta o zbytcích vlastně fungovat? Uveďme

si jednoduchý příklad a důkladně si jej rozepišme. Mějme žáky, které když postavíme do 5 řad, zbydou nám 3, kteří si nemají kam stoupnout [6]. Když se je pokusíme postavit do 11 řad, zůstanou nám zase žáci 2. Jsme nyní schopni určit, kolik je žáků? Samozřejmě, a to pomocí čínské větě o zbytcích. Zapišme si získané informace do dvou základních rovnic

$$5 \cdot k + 3 = a,$$

$$11 \cdot l + 2 = a,$$

kde l a k jsou takové hodnoty, aby nám platila rovnost postavíme-li tyto rovnice k sobě. Vyjádříme-li si však neznámou pomocí funkce modulo, dostaneme tvary:

$$a = 3 \pmod 5$$

$$a = 2 \pmod{11}$$

Zde si uvědomme, že roznásobíme-li mezi sebou obě hodnoty u funkce modulo, získáme maximální počet žáků. Je tedy jasné, že ve třídě je v rozmezí 1 až 55 žáků. Nyní udělejme substituci v podobě

$$5 \cdot k + 3 = 2 \pmod{11}.$$

Abychom se zbavili čísla 3, přičtem k celé rovnici 8, neboť nám platí $(3 + 8)\ \mathrm{mod} 11 = 0$.

$$5 \cdot k = 10 \pmod{11}$$

Dále bychom se rádi zbavili 5, a proto rovnici vynásobíme inverzním prvkem čísla 5, tedy 9.

$$9 \cdot 5 \cdot k = 9 \cdot 10 \pmod{11}$$

$$45 \cdot k = 90 \pmod{11}$$

$$1 \cdot k = 2 \pmod{11}$$

Vyšlo nám, že $k = 2$, takže dosadíme-li do první rovnice, dostaneme výsledek, že máme 13 žáků.

$$5 \cdot 2 + 3 = 13$$

4.1. Příklady na hrubou sílu:

<u>Příklad 10:</u> O Bobovi víme, že jeho veřejný klíč má tvar $(n; e) = (253; 7)$. Pokuste se určit jeho soukromý klíč.

Řešení:

Z předchozí kapitoly jsme si probrali několik případů, jak zjistit cizí soukromý klíč. U tohoto příkladu si ukážeme metodu hrubou silou a názorně si předvedeme, proč se tomu říká hrubou silou. Nezbyde nám totiž nic jiného, než vzít modul n a snažit se jej faktorizovat, zjistit jeho prvočíselný rozklad. Takže si pojďme ukázat, jak náš postup bude vypadat.

$$\frac{253}{2} = 126{,}5 \qquad \frac{253}{7} = 36,\overline{142857}$$

$$\frac{253}{3} = 84,\bar{3} \qquad \frac{253}{8} = 31{,}625$$

$$\frac{253}{4} = 63{,}25 \qquad \frac{253}{9} = 28,\bar{1}$$

$$\frac{253}{5} = 50{,}6 \qquad \frac{253}{10} = 25{,}3$$

$$\frac{253}{6} = 42{,}1\bar{6} \qquad \frac{253}{11} = 23$$

Když už jsme našli celé hodnoty, ze kterých majitelův modul n byl složen, jsme schopni určit i majitelův dešifrovací exponent. Pokud tedy $p = 11$ a $q = 23$, tak $\varphi(n) = 220$. Následně budeme pracovat již se vzorcem, který z teorie známe a to

$$d = \frac{[k \cdot \varphi(n) + 1]}{e},$$

který jsme detailněji využili u př. 7. Zde si již však ukážeme jen výsledek, kde $d = 63$.

Nyní již víme, proč musíme používat veliká čísla. Při použití poměrně malých čísel není tak těžké faktorizovat modul n a zjistit si tak něčí soukromý klíč.

Pro ověření jsme pracovali s programem wMaxima, kde jsme si prvně určili přesnější hodnoty zlomků, abychom zjistili, zda nám vychází celá část, nebo zlomková. Zde jsme mohli využít funkce $factor$, která nám faktorizuje číslo n. Jinak řečeno nám zařídí rozklad číslo n na prvočísla. Jakmile jsme zjistili tyto 2 prvočísla, řešili jsme výpočet $\varphi(n)$ a následně d. Následně jsme pracovali tzv. s metodou pokus omyl a snažili se najít takové k, aby číslo d byla celá část, tedy celé číslo, nikoliv zlomkové číslo.

<u>Příklad 11:</u> O čísle Alice $n = 6\,457\,037$ víme, že je součinem dvou různých prvočísel p, q. Navíc ještě víme, že platí $\varphi(n) = 6\,451\,776$. Nalezněte prvočísla p, q.

Řešení:

U předešlého příkladu jsme se snažili faktorizovat n, avšak zde je modul příliš velké číslo, a proto zvolíme druhý způsob zmíněný v teorii. Prvně si vypišme rovnice, které známe.

$$n = p \cdot q = 6\,457\,037$$

$$\varphi(n) = (p-1) \cdot (q-1) = n + 1 - (p+q) = 6\,457\,038 - (p+q)$$

Po vypsání obou rovnic je nám zřejmé, že známe jak součet, tak i součin obou prvočísel p a q. Součet jsme si pouze vyjádřili z předchozí rovnice, jako

$$p + q = 6\,457\,038 - 6\,451\,776 = 5\,262.$$

Teď již víme, čemu se rovná součin i součet námi hledaných dvou prvočísel. Stačí nám tedy, když do obecného zápisu kvadratické rovnice dosadíme hodnoty součtu a součinu. Následně vypočítáme kořeny kvadratické rovnice a získáme tak hodnoty prvočísel p a q. Tato kvadratická rovnice bude mít tvar

$$x^2 - 5\,262x + 6\,457\,037 = 0.$$

Při upravení zjistíme, že diskriminant je roven $1\,860\,496$ a jeho odmocnina je $1\,364$. Proto již můžeme psát, že pro kvadratické kořeny platí

$$p = \frac{5\,262 + 1\,364}{2} = 3\,313$$

$$q = \frac{5\,262 - 1\,364}{2} = 1\,949.$$

Nyní jsme získali prvočíselný rozklad (hodnoty p, q) a to jen za předpokladu, že jsme si zjistili Alice číslo n a znali jsme její $\varphi(n)$.

<u>Příklad 12:</u> Spočítejte zbytek čísla 12^{147369} po dělení číslem 79781.

Řešení:

Nejprve musíme určit prvočíselný rozklad čísla $79781 = 13 \cdot 17 \cdot 19^2$. Protože čísla prvočíselného rozkladu $13, 17$ a 19^2 jsou navzájem nesoudělná je podle čínské věty o zbytcích číslo 12^{147369} v Z_{79781} určeno jednoznačně svými zbytky po dělení prvočíselného rozkladu. Nyní využijeme faktu Eulerovi funkce $a^{\varphi(n)} = 1$ v Z_n a vypočítáme si zbytky:

$$12^{147369} = 12^{12 \cdot 12280 + 9} = 12^9 = 12 \text{ v } Z_{13}$$

$$12^{147369} = 12^{16 \cdot 9210 + 9} = 12^9 = 5 \text{ v } Z_{17}$$

$$12^{147369} = 12^{342 \cdot 430 + 309} = 12^{309} = 113 \text{ v } Z_{361}$$

Nyní využijeme čínskou větu o zbytcích a bude nám tedy platit

$$12^{147369} = (12 \cdot \mathrm{M}_1 \cdot \mathrm{N}_1) + (5 \cdot \mathrm{M}_2 \cdot \mathrm{N}_2) + (113 \cdot \mathrm{M}_3 \cdot \mathrm{N}_3) \text{ v } Z_{79781}$$

Dále jsme schopni určit velikosti hodnot M a hodnot N

$$\mathrm{M}_1 = 17 \cdot 19^2 = 6137$$

$$\mathrm{M}_2 = 13 \cdot 19^2 = 4693$$

$$\mathrm{M}_3 = 13 \cdot 17 = 221$$

$$\mathrm{N}_1 = \mathrm{M}_1^{-1} = 1^{-1} = 1 \text{ v } Z_{13}$$

$$\mathrm{N}_2 = \mathrm{M}_3^{-1} = 1^{-1} = 1 \text{ v } Z_{17}$$

$$\mathrm{N}_3 = \mathrm{M}_3^{-1} = 221^{-1} = 312 \text{ v } Z_{361}$$

Tudíž získáme rovnici

$$12^{147369} = (12 \cdot 6137 \cdot 10) + (5 \cdot 4693 \cdot 13) + (113 \cdot 221 \cdot 312) = 70147 \text{ v } Z_{79781}$$

Pro přesnější počítání jsme pracovali s programem wMaxima, který nám u tohoto příkladu hlavně sloužil svou funkcí mod. Avšak i když jsme si výsledek mohli zapsat ihned a veškerý postup vynechat, snažili jsme se zde celý postup znázornit. Takže i když jsme výsledek našeho zadání znali, chtěli jsme ukázat, jak na něj přijít v případě, že hodnoty budou moc velké na to, aby je software wMaxima zvládnul zpracovat. Právě proto jsme zde uvedli veškerý postup, neboť i funkce některých softwarů jsou omezené a někdy nám hold nezbyde nic jiného, než vzít papír a vše si vypočítat sám, nebo aspoň upravit do takové míry, aby to software se kterým pracujeme zvládnul.

5. Závěr

Práce čtenáře provede funkčností asymetrického šifrování RSA. Ze začátku mu předvede základní definice a kritéria, která pro tenhle systém platí. Po zvládnutí úvodní kapitoly čtenář získá přehled, jak se vytváří šifrovací a dešifrovací klíč, které slouží k samotnému šifrování RSA. Tyto nabyté znalosti si pak může procvičit v příkladech, které jsou za každou kapitolou, případně přímo v ní přiloženy. Když už bude schopen sám všechny příklady vypočítat, přejde k další kapitole, kde se setká se samotným šifrování a dešifrováním pomocí obou klíčů. Stejně jako u předešlých kapitol i zde si bude moci své znalosti následně procvičit a zjistit tak, zda dané téma dostatečně chápe. Ke konci práce se dozví, jak šifrovací systém RSA zaručuje svoji bezpečnost proti nežádoucím útočníkům. A přesně tohle bylo hlavním cílem této práce. Ukázat, že šifrovací systém RSA je stále bezpečný, a i přes události, které se stali ve Finsku, kde šifrování RSA selhalo lidskou chybou. Můžeme tedy bez problému věřit tomuto systému, pokud samozřejmě budeme dodržovat veškerá jeho pravidla a kritéria.

Tento text by mohl sloužit jako podpůrný text pro studium asymetrického šifrování a dále chceme dodat, že veškeré výpočty jsme provedli za pomoci wMaxima [8], který nám poměrně hodně zjednodušil všechny příklady.

6. Seznam použitých zdrojů:

[1] BLAŽEK, Jaroslav a spol. *Algebra a teoretická aritmetika.* Státní pedagogické nakladatelství. Praha, 1985.

[2] BALKOVÁ, Ľ. *RSA* (*Úvod do kryptologie),* FJFI ČVUTI, Praha, 2011.

[3] BURDA, Karel. *Úvod do kryptografie.* Akademické nakladatelství CERM. Brno, 2015.

[4] HALAŠ, Radomír. *Úvod do teorie čísel.* UPOL. Olomouc, 2014.

[5] MENEZES, Alfred, VAN OORSCHOT, Paul, VANSTONE, Scott. *Handbook of applied cryptography.* Boca Raton. CRC Press, 1997.

[6] VELEBIL, Jiří. *Diskrétní matematika.* ČVUT Praha, 2007.

[7] SINGH, Simon: *The Code Book, Fourth Estate.* London, 2000.

[8] Maxima, a Computer Algebra Systém [online]. [cit. 2014-02-07]. Dostupné z: http://maxima.sourceforge.net/