UNIVERZITA PALACKÉHO V OLOMOUCI

PEDAGOGICKÁ FAKULTA

Katedra matematiky

Diplomová práce

Lukáš Růžica

Eulerova věta a RSA šifrování s veřejným klíčem

Olomouc 2022

vedoucí práce: doc. RNDr. Tomáš Zdráhal, CSc.

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracoval zcela samostatně pod vedením doc. RNDr. Tomáše Zdráhala, CSc. a že jsem uvedl veškerou použitou literaturu.

V Olomouci dne .....

Bc. Lukáš Růžica

Poděkování

Děkuji mému vedoucímu bakalářské i diplomové práce panu doc. RNDr. Tomáši Zdráhalovi, CSc. za odborné vedení, trpělivost a ochotu, kterou mi při vypracování každé z prací věnoval. Dále děkuji i škole, na níž jsem mohl výzkum provádět a i žákům, že byli ochotní a spolupracovali.

Bibliografická identifikace

Jméno a příjmení autora	Bc. Lukáš Růžica
Název práce	Eulerova věta a RSA šifrování s veřejným klíčem
Typ práce	Diplomová
Pracoviště	Katedra matematiky
Vedoucí práce	doc. RNDr. Tomáš Zdráhal, CSc.
Rob obhajoby	2023
Abstrakt	Diplomová práce se věnuje algoritmu RSA, kde se v teoretické části popisuje princip samotného šifrování. Vysvětleny jsou zde základy srozumitelné i těm, kteří o tomto systému doposud neslyšeli. Praktická část je věnována dotazníkovému šetření na základní škole. Cílem diplomové práce je porovnat matematické znalosti s úrovní algoritmu RSA a dále sledovat využití ICT na základě obtížných matematických operací při algoritmu RSA.
Klíčová slova	Algoritmus RSA, šifrování, dešifrování, Euklidés, Malá Fermatova věta, Eulerova funkce, Wolfram Cloud
Jazyk	Český

Bibliographical identification

Autor´s first name and surname	Bc. Lukáš Růžica
Title	Euler's Theorem and RSA Public Key Cryptography
Type of thesis	Master
Department	Department of Mathematics
Supervisor	doc. RNDr. Tomáš Zdráhal, CSc.
The year of presentation	2023
Abstract	The thesis is devoted to the RSA algorithm, where the theoretical part describes the principle of encryption itself. It explains the basics, which can be understood even by those who have never heard of the RSA algorithm before. The practical part is devoted to a questionnaire survey in a primary school. The aim of the thesis is to compare the mathematical knowledge with the level of the RSA algorithm and furthermore to observe the use of ICT based on difficult mathematical operations in the RSA algorithm.
Keywords	RSA algorithm, encryption, decryption, Euclid, Fermat's little theorem, Euler's function, Wolfram Cloud
Language	Czech

Obsah

Obsah

Úvod

RSA šifrovací systém nese název po těch, kteří se podíleli na jeho vzniku. Na začátek si však uveďme fakt, že tento nejrozšířenější kryptografický algoritmus nevznikl během chvilky. Jeho základní pilíře vytvořili matematici Euklidés (325 př.n.l. – 260 př.n.l.) a Pierre de Fermat (1601–1665), kterým se nechal inspirovat o několik let později Leonhard Paul Euler (1707–1783). Všechny poznatky těchto tří matematiků dali pak dohromady v 70.letech 20.st. tři profesoři z MIT (Massachusetts Institute of Technology) Rivest, Shamir a Adleman (proto také zkratka RSA – jako jejich počáteční písmena).

V této práci si detailně projdeme systém asymetrického šifrování RSA (pokud někteří neznají ještě rozdíl mezi symetrickým a antisymetrickým šifrováním, doporučujeme prostudovat [5]). Nejprve si ukážeme teoretickou stránku celého šifrování, kde si vše definujeme a následně dokážeme. Nemusíte se však nikterak bát složitého matematického počítání, neboť ke všemu budeme používat ICT (informační a komunikační technologie). Přesněji budeme pracovat s volně přístupným softwarem Wolfram Cloud.

Záměrem této práce totiž není vás jen informovat o RSA jako takovém, ale poukázat na fakt, jak lze efektně využít počítač ve výuce matematiky, nehledě na náročnost početních operací. Přesně o tom taky vypovídá praktická část této práce. Chceme přiblížit ICT do klasické výuky matematiky na ZŠ, a jelikož samotná matematika šifrovacího systému RSA je poměrně jednoduchá, je zcela přívětivé právě algoritmus RSA takhle využít.

V teoretické části této práce si předvedeme šifrování a dešifrování, které si následně všichni společně budeme moci vyzkoušet. Postupně si zde objasníme všechny podstatné matematické kroky vedoucí k úspěšnému algoritmu RSA, a pokud vše správně pochopíme, měli bychom dostát úspěchu. O tomto úspěchu se poté přesvědčíme sami tak, že si mezi sebou zkusíme zprávu zašifrovat/dešifrovat a zjistíme, co jsme si chtěli, nebo co nám někdo chtěl říct.

1. Teoretická část

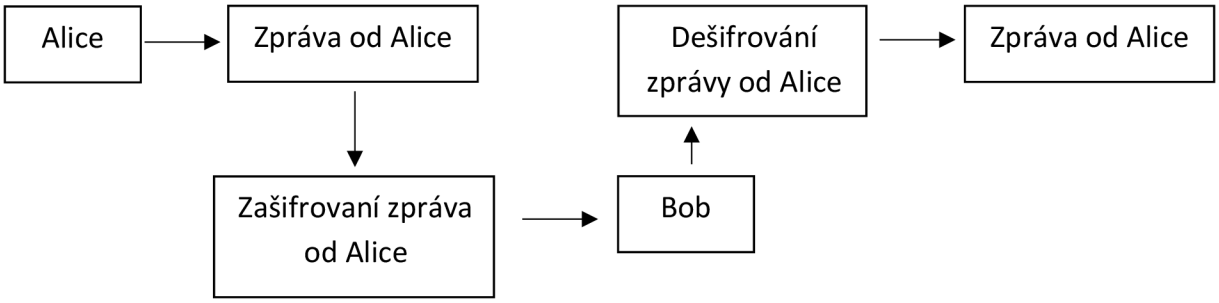
1.1. Asymetrické šifrování

Asymetrické šifrování vzniklo až v druhé polovině 20. století. Přesněji se první zmínka o tomto šifrovacím algoritmu objevila v roce 1978 v článku [7], který publikovali autoři Rivest, Shamir a Adleman, jejichž iniciály také tvoří samotný název kryptosystému. I když se to nezdá, tak na základě této šifry je dnes založeno mnoho šifrovacích systémů, a to z důvodu, že jeho bezpečnost je založena na složitosti výpočtu rozkladu čísla na prvočinitele. Avšak systém je bezpečný pouze tehdy, jsou-li správně zvoleny parametry ovlivňující samotnou bezpečnost. Než začneme o těchto parametrech mluvit, zmiňme, že každý uživatel disponuje dvěma klíči, kde jeden z nich je soukromý (*„private“*) a druhý veřejný (*„public“*). Právě tvorba těchto klíčů razantně ovlivňuje bezpečnost systému, aby nikdo nemohl narušit skrytou (zašifrovanou) zprávu. Pro začátek si ale hned prozraďme, že se jedná o opravdu dvě velká prvočísla, u kterých není takový problém zjistit jejich součin, nýbrž ze součinu určit prvočísla, ze kterých byl složen. Momentálně totiž není znám žádný algoritmus, který by dokázal efektivně tento problém, přesněji řečeno rozklad, řešit. Pro zjednodušení si přiznejme, že součin dvou velkých prvočísel dokážeme pomocí softwaru opravdu rychle určit (vypočítat), ale opačně by nám to dělalo značné potíže. Takový rozklad by mohl trvat i s tím nejvýkonnějším softwarem několik let. Znovu si totiž dovolím připomenout, že šifrovací algoritmus pracuje s velkými prvočísly, například s takovými, že uděláme-li jejich součin, dostane číslo o velikosti 309 cifer, a to už opravdu nejsou malá čísla.

Jak už bylo zmíněno dříve, jedná se o poměrně nové rozšíření samotné kryptografie. Do 70. let 20 století se pracovalo pouze se šifrováním symetrickým, kde se pracuje pouze s jedním klíčem. Avšak asymetrické šifrování přineslo pro společnost neuvěřitelné možnosti. Pomocí tohoto principu šifrování/dešifrování dnes dokáže fungovat několik, pro nás v životě nepostradatelných věcí, jakož jsou platební karty, platební portály, posílání SMS, MMS a mnoho dalších.

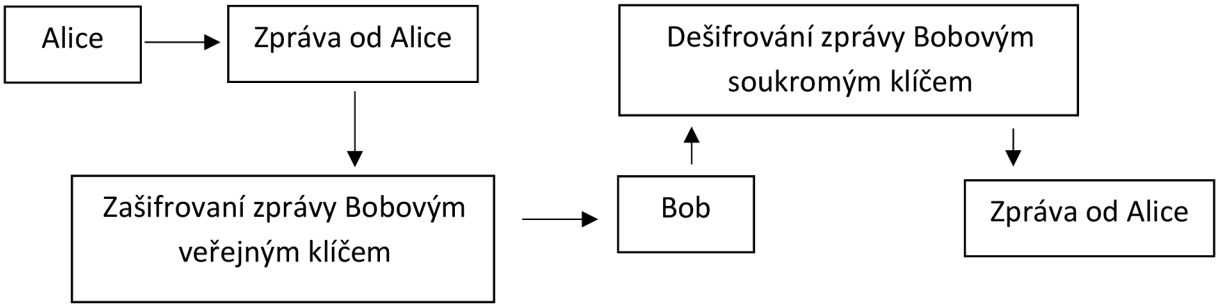
Jak celý tento princip šifrování funguje, je na pochopení poměrně jednoduché, ale pro jeho dokázání už tomu tak zcela není. Každopádně i k tomu se v pozdějších částech diplomové práce dostaneme, prozatím nám bude bohatě stačit schéma, které nám předvede, jak takový

algoritmus RSA vlastně probíhá. Co se děje se zprávou, kterou chceme poslat, a jak vypadá zpráva, kterou nám chce poslat někdo jiný. Pro lehčí orientaci budeme používat fiktivní jména Alice a Bob, která se v odborných literaturách používají pro vysvětlení asymetrického šifrování.

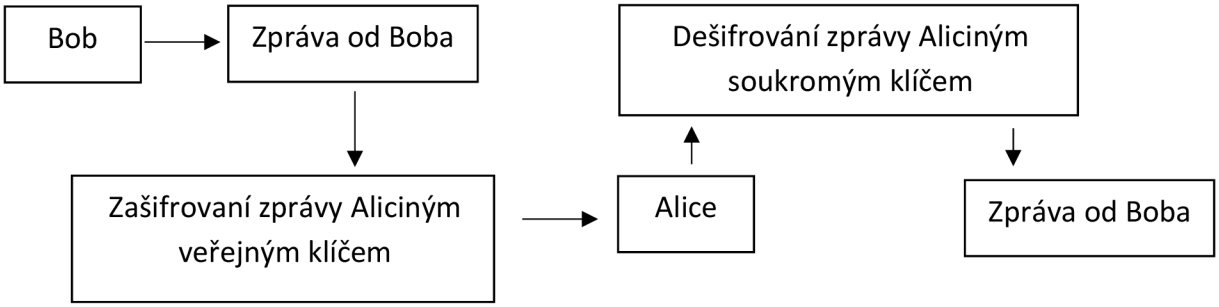


Obrázek 1: Schéma pro představu fungování asymetrického šifrování

Pro některé z vás to může být jasné, ale samotné schéma Obrázku 1 nám stále nic neříká o tom, jak se klíče generují, jaké pro ně platí podmínky, zda je mezi nimi nějaká souvislost, a ani kdy se vlastně používají. Upravme si tedy toto schéma do takového tvaru, že si aspoň ukážeme, kdy se jaký klíč používá a čí klíč vlastně použit je. Nyní si ale už znázorníme obě zprávy, tedy jak zprávu od Alice Bobovi (Obrázek 2), tak i Bobovu zprávu pro Alici (Obrázek 3).



Obrázek 2: Schéma zprávy od Alice pro Boba



Obrázek 3: Schéma zprávy od Boba pro Alici

Z obou posledních schémat znázorňujících oboustrannou diskusi lze vidět, že chce-li jeden z nich napsat tomu druhému, musí použít příjemcům veřejný klíč (*„public key“*) a chce-li příjemce tuto zprávu přečíst, použije svůj soukromý klíč (*„private key“*). Nyní už víme, jak takové šifrování vypadá, ale neznáme podmínky a parametry ovlivňující jeho bezpečnost, a to je chyba. Proto se v dalších kapitolách zaměříme na samotnou tvorbu autorských klíčů, u nichž si vysvětlíme, proč právě musí splňovat všechny ty podmínky, které si řekneme [9].

1.1.1. Generování klíčů

Tvorba *„public key“* a *„private key“* jsou nejpodstatnějším a nejzávažnějším krokem pro plnohodnotně správné šifrování RSA. Jak už samotné názvy napovídají, tak jeden klíč bude přístupný všem, můžeme si jej pro zjednodušení představit jako datum našeho narození, které může kdokoliv znát nebo si jej nějak zjistit. Druhý klíč však bude zcela soukromý a ten nesmí znát nikdo jiný než my sami. Ten si zase můžeme představit jako PIN od naší platební karty nebo telefonu, který by nikdo kromě nás (jakožto majitele) neměl znát. Pomineme-li tyto představy, tak oba klíče (veřejný i soukromý) jsou spolu nějak provázány, tudíž jeden se neobejde bez druhého a zase obráceně.

Prvně si stanovme *„public key“*, který je poměrně jednoduše zadán. Jelikož se zde celou dobu bavíme o algoritmu RSA, který si zakládá na složitosti rozkladu součinu dvou prvočísel, stanovme si tyto prvočísla a určeme jejich součin. Navíc si můžeme zrovna ujasnit, proč právě prvočísla. Kdyby se nám totiž nejednalo o prvočísla, ale například o čísla sudá, mohli bychom udělat jejich číselný rozklad, a to stejně tak i u čísel lichých (nedosáhli bychom tak jedinečnosti čísel, neboť by se jednalo o čísla složená). Číselný rozklad však nedokážeme udělat u prvočísel, a právě proto jsou pro nás tak zajímavá a svůj potenciál zde zcela využijí. Mějme tedy jedno prvočíslo $[\,p\,]$ a druhé prvočíslo $[\,q\,]$ takové, že $[\,q\,] \neq [\,p\,]$ (důvod podmínky $[\,q\,] \neq [\,p\,]$ jsme si rozepsali v pozdější fázi této práce). Chceme-li určit jejich součin, není nic jednoduššího, než mezi sebou tato dvě prvočísla vynásobit a získat součin $[\,n\,]$. Právě součin těchto prvočísel je jedním ze stavebních pilířů obou klíčů a říká se mu *„modul“* nebo také modulo. Tento název se odvíjí od toho, co s touto hodnotou budeme v budoucnu dělat. Přesněji řečeno je to početní operace související s operací celočíselného dělení, zkrátka zbytek

po dělení. Konkrétně půjde o zbytek, který se pro nás stane zašifrovanou zprávou, ale o tom více až v dalších kapitolách.

Druhým základním prvkem *„public key“* je [e], kterému se říká *„encrypt“*. Ve volném překladu bychom použili *„šifrovací exponent“*. Ten, než si ale správně určíme, je třeba znát Eulerovu funkci pro *„modulo.“* Cože to ta Eulerova funkce vlastně je, si hned ukážeme. Jedná se o počet nesoudělných čísel s číslem, ke kterému danou funkci stanovíme. Jelikož ji přikládáme k *„modulo“*, tedy k hodnotě [n], pak hledáme Eulerovu funkci [$\varphi(n)$]. Její výpočet není příliš složitý (pokud znáte prvočísla, ze kterých je *„modulo“* složeno) a dosáhneme jí vzorcem

$$\boldsymbol{\varphi(n) = (p - 1) \cdot (q - 1)}. \qquad (1)$$

Výpočet této funkce je pro bezpečnost šifrovacího algoritmu RSA klíčový (viz 1.1.2.) a odvíjí se od ní i další klíčové vlastnosti pro správnost šifrování než jen *„šifrovací exponent“*. Nyní je pro nás ale podstatné zjistit, jakou hodnotu bude mít právě onen *„šifrovací exponent“*. Hodnota [e] musí být s hodnotou [$\varphi(n)$] nesoudělná, neboť byla by s ní soudělná (tedy bylo by možné hodnotu Eulerovy funkce vyjádřit šifrovacím exponentem), neplatila by nám rovnice

$$\boldsymbol{e \cdot d \equiv 1 \; mod \; \varphi(n)}, \qquad (2)$$

kde [d] je *„dešifrovací exponent“* z anglického *„decrypt“*. A proč nám tato rovnice musí vlastně platit, je zcela jednoduché. Celý šifrovací systém RSA pracuje se složitostí rozložení prvočísel (to už víme), logicky tedy i s nesoudělnými čísly. Musíme tedy najít takovou číselnou kombinaci šifrovacího a dešifrovacího exponentu, která nám bude vytvářet v [$\mathrm{mod}\; n$] zbytek 1. Hledáme pro šifrovací exponent inverzní hodnotu dešifrovacího exponentu v modulo $\varphi(n)$. V případě komunikace bychom mohli napsat rovnici ve tvaru

$$\boldsymbol{m^{ed} \equiv m \; mod \; n}, \qquad (3)$$

kde [m] je zpráva k šifrování/dešifrování, [e] je šifrovací exponent, [d] je dešifrovací exponent a [n] je modulo, ve kterém pracujeme. Z rovnice je totiž zřejmé, že umocníme-li zprávu na součin exponentů (šifrovacího a dešifrovacího), získáme opět stejnou zprávu.

K čemu toto vlastně všechno vedlo, je zcela prosté. Našim úkolem je vytvořit si naše oba klíče. Jeden klíč, přesněji klíč veřejný, jsme si již schopni vytvořit a má tvar

$$(\boldsymbol{n}, \boldsymbol{e}). \tag{4}$$

Druhý klíč bude vypadat dost podobně, jen místo šifrovacího exponentu dosadíme dešifrovací exponent

$$(\boldsymbol{n}, \boldsymbol{d}), \tag{5}$$

avšak ten prozatím ještě neznáme. Díky bohu pro nás (autory klíče) není těžké tenhle dešifrovací exponent získat a využijeme k tomu již předešlé rovnice, které jsme si zde sdělili.

Využijme pro začátek rovnici (3). Tato rovnice je platná pouze tehdy, pokud násobek exponentů je roven násobku Eulerovy funkce plus jedna, a právě z tohoto důvodu se zjišťovala nesoudělnost exponentů s Eulerovou funkcí. Byl by totiž exponent soudělným s touhle funkcí, nemohla by nám platit tato rovnice a systém by nám přestal fungovat, tudíž máme rovnici

$$\boldsymbol{e} \cdot \boldsymbol{d} = \boldsymbol{k} \cdot \boldsymbol{\varphi}(\boldsymbol{n}) + \mathbf{1}, \tag{6}$$

kde k je celé číslo. Z této rovnice lze vidět, že šifrovací exponent je opravdu multiplikativní inverzí dešifrovacího exponentu (samozřejmě to platí i obráceně), jenže pozor! Algoritmus RSA pracuje v modulo, takže musíme zohlednit obor čísel, ve kterém se veškeré matematické operace dějí. Pro správné nalezení inverzního prvku (pokud existuje) se využívá rozšíření Euklidova algoritmu (pro ukázku výpočtu takového algoritmu doporučuji bakalářkou práci od autora Lukáš Růžica).

Z rovnice (3) a (6) si teď řekněme, jak nalézt dešifrovací exponent, který nám chybí k vytvoření soukromého klíče v podobě (5). Dáme-li obě rovnice dohromady, dostáváme rovnici o tvaru

$$\boldsymbol{m}^{\boldsymbol{e}\cdot\boldsymbol{d}} = \boldsymbol{m}^{\boldsymbol{k}\cdot\boldsymbol{\varphi}(\boldsymbol{n})+\mathbf{1}} \equiv \boldsymbol{m} \; \boldsymbol{mod} \; \boldsymbol{n}, \tag{7}$$

ze které můžeme vyvodit rovnice

$$\boldsymbol{e} \cdot \boldsymbol{d} = \boldsymbol{k} \cdot \boldsymbol{\varphi}(\boldsymbol{n}) + \mathbf{1} \tag{8}$$

$$\boldsymbol{m}^{\boldsymbol{e}\cdot\boldsymbol{d}} = \boldsymbol{m}^{\boldsymbol{k}\cdot\boldsymbol{\varphi}(\boldsymbol{n})+\mathbf{1}} \equiv \boldsymbol{m} \; \boldsymbol{mod} \; \boldsymbol{p}, \tag{9}$$

$$\boldsymbol{m}^{\boldsymbol{e}\cdot\boldsymbol{d}} = \boldsymbol{m}^{\boldsymbol{k}\cdot\boldsymbol{\varphi}(\boldsymbol{n})+\mathbf{1}} \equiv \boldsymbol{m} \; \boldsymbol{mod} \; \boldsymbol{q}, \tag{10}$$

a to právě díky rovnici (1). Z rovnice (8) si vyjádříme výpočet dešifrovacího exponentu a zároveň si z rovnic (9) a (10) ukážeme důležitost různých i nesoudělných prvočísel p a q.

$$\boldsymbol{d = \frac{k \cdot \varphi(n) + 1}{e}} \qquad (11)$$

$$\boldsymbol{a \cdot [k \cdot \varphi(n) + 1] = p} \qquad (12)$$

$$\boldsymbol{b \cdot [k \cdot \varphi(n) + 1] = q,} \qquad (13)$$

kde a a b jsou přirozená čísla. Budeme-li nyní chtít jednu neznámou (jedno z prvočísel) vyjádřit v podobě druhého, spojením rovnic (12) a (13) nám vzniká rovnice v podobě

$$\boldsymbol{\frac{p}{q} = \frac{a}{b}}. \qquad (14)$$

Přesně toto je právě důkaz i důvod toho, proč máme dvě prvočísla, která si nejsou rovna a jsou spolu nesoudělná. Jedním z důvodů je fakt, že zjistit druhou odmocninu z nějakého čísla je opravdu primitivní a pokud by nám rovnice (14) vycházela jako celé číslo, bylo by po celém složitém počítáním, neboť bychom hledali pouze takovou kombinaci, kdy jedno číslo je násobkem druhého [8]. Chtěli bychom důkazy početní, stačí si připomenout důkaz rozšířeného Euklidova algoritmu, malé Fermatovy věty a Eulerovy funkce.

1.1.2. Důkaz správnosti algoritmu RSA

Během studia o algoritmu RSA jsme zjistili, že veškerou komunikaci mezi odesílatelem a příjemcem, kterou zašifrujeme pomocí veřejného klíče, můžeme dešifrovat pouze jemu příslušným soukromým klíčem a samozřejmě i naopak. Neřekli jsme si však žádné další podmínky, které musí systém RSA splňovat. Pojďme tento nedostatek napravit a říct si vlastně kdy, proč a jak nám tento algoritmus funguje.

Tvorbu klíčů máme za sebou a nyní se podívejme na takové tři základní pilíře, díky nímž můžeme algoritmus RSA považovat za bezpečný. Vezmeme-li to podle stáří těchto znalostí, prvně si řekneme něco o Euklidově algoritmu, následně zmíníme Malou Fermatovu větu, a nakonec se zaměříme na Eulerovu funkci, která je defacto zjednodušením Malé Fermatovy věty.

Jak bylo zmíněno, prvně si něco řekneme o Euklidově algoritmu. Jedná se o algoritmus, pomocí kterého lze najít největšího společného dělitele (v pozdější části se setkáme se zkratkou "GCD" z anglického „Great Common Division“ – největší společný dělitel). Nejde však jen o to, že pomocí něj nalezneme tohoto dělitele, ale v modulární aritmetice, a s tou my pracujeme, dokážeme nalézt i inverzní prvek. Právě tuto vlastnost jsme již využili v předešlé kapitole generování klíčů, a to přesně v rovnici (2) [10]. Než však přejdeme na inverzní prvky, zobrazme si postup nalezení největšího společného dělitele na ukázkových příkladech [12].

a) $GCD\,(300, 816)$

$$816 = 2 \cdot 300 + 216$$

$$300 = 1 \cdot 216 + 84$$

$$216 = 2 \cdot 84 + 48$$

$$84 = 1 \cdot 48 + 36$$

$$48 = 1 \cdot 36 + 12$$

$$36 = 3 \cdot 12 + 0$$

b) $GCD\,(358, 217)$

$$358 = 1 \cdot 217 + 141$$

$$217 = 1 \cdot 141 + 76$$

$$141 = 1 \cdot 76 + 65$$

$$76 = 1 \cdot 65 + 11$$

$$65 = 5 \cdot 11 + 10$$

$$11 = 1 \cdot 10 + 1$$

$$10 = 1 \cdot 10 + 0$$

Druhý základním poznatkem je Malá Fermatova věta. Jedná se o větu z teorie čísel, která nám říká, že pro každé prvočíslo p nesoudělné s číslem a platí rovnice

$$\boldsymbol{a^p \equiv a \bmod p}, \qquad (15)$$

nebo je taky znám přepis rovnice do tvaru

$$\boldsymbol{a^{p-1} \equiv 1 \bmod p}. \qquad (16)$$

Tohoto tvrzení se později chytil Leonhard Euler a Malou Fermatovu větu zobecnil. To si však ukážeme až za chvíli. Nejprve si dokažme, že tato rovnice vůbec platí a využijeme matematické indukce [15].

Zvolme si libovolné $k < p - 1$ a víme, že nám platí rovnice $a^{p-1} \equiv 1 \bmod p$. V oblasti přirozených čísel, což je množina obsahující kladná celá čísla, označující se $\mathbb{N}$, platí nerovnice $1 \leq a \leq k$. Dále $(k+1)^p \equiv k^p + 1^p \bmod p$.

Pro důkaz bychom zvolili $[13]$.

1. $\boldsymbol{a = 1 \rightarrow 1^p \equiv 1 \bmod p}$
2. Indukční předpoklad $\boldsymbol{k^{p-1} \equiv 1 \bmod p}$
3. $\boldsymbol{a = k + 1 \rightarrow (k+1)^{p-1} \equiv 1 \bmod p}$
4. $\boldsymbol{(k+1)^p \equiv k^p + 1 \bmod p}$
5. $\boldsymbol{k^p = k \bmod p}$

Když už jsme si důkaz Malé Fermatovy věty ukázali, pojďme si zkusit nějaké příklady propočítat a ověřit si, zda danému tématu dostatečně rozumíme.

a) Kolik je 7^{35} v Z_{17}

V dnešní době bychom použili ICT (například Wolfram Cloud), zadali funkci "$PowerMod$" a měli výsledek. My si však zde ukážeme i metodu, jak vypočítat tento typ příkladů bez využití ICT. Dejte si pozor, že pracujeme v oboru celých čísel v $\bmod 17$, proto někdy v rovnici máme rovná se a někdy znaménko kongruence (aby bylo rozpoznat, co jsme prováděli s čísly) $[14]$.

$$7^{35} = 7^{16} \cdot 7^{16} \cdot 7^3 \equiv 1 \cdot 1 \cdot 7^2 \cdot 7 = 49 \cdot 7 \equiv 15 \cdot 7 = 105 \equiv 3$$

$$7^{35} \equiv 3 \bmod 17$$

b) Vypočtěte inverzi k šifrovacímu exponentu $e = 5$ v $\bmod \varphi(n)$, kde $\varphi(n) = 5\,412$.

Víme, že chceme-li vypočítat inverzi (neboli inverzní prvek) k hodnotě 5, musíme sestrojit rovnici s neznámou d ($e^{-1} = d$ v $\bmod n$), která bude mít tvar

$$e \cdot e^{-1} \equiv 1 \bmod \varphi(n)$$

$$5 \cdot d \equiv 1 \bmod 5\,412$$

$$d \equiv 5^{-1} \bmod 5\,412$$

Nyní jsme si vyjádřili rovnici, pomocí které dokážeme vypočítat dešifrovací exponent (prvek inverzní k šifrovacímu exponentu e). Dalším našim krokem bude číselný rozklad.

$$5\,412 = 5 \cdot 1\,082 + 2$$

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

Po číselném rozkladu vyjádříme zbytek 1 jako rozdíl dvou čísel. Pokračujeme až tak dlouho, dokud rozdíl nebude tvořen násobkem čísla 5 a jiným násobkem čísla $5\,412$. Přesně těch dvou čísel, která máme určená v zadání.

$$1 = 5 - 2 \cdot 2$$

$$1 = 5 - 2 \cdot (5\,412 - 5 \cdot 1\,082)$$

$$1 = 2\,165 \cdot 5 - 2 \cdot 5\,412$$

Zde již vidíme rozklad čísla 1 do výše zmíněného tvaru. Kdybychom tuto rovnici chtěli následně přepsat do původního zadání, dostaneme tvar

$$5 \cdot 2\,165 - 2 \cdot 5\,412 \equiv 1 \bmod 5\,412$$

$$5 \cdot 2\,165 \equiv 1 \bmod 5\,412$$

$$e = 5;\ d = 2\,165.$$

Zjistili jsme tedy, že inverzní prvek k šifrovacímu exponentu e je dešifrovací exponent $d = 2\,165$, pro zkoušku můžeme v prostředí Wolfram Cloud zadat příkaz v podobně $PowerMod[e, -1, \varphi(n)]$ a přesvědčit se, zda je opravdu náš výsledek správný či nikoliv.

Jako poslední nám zůstává Eulerova funkce φ, kterou jsme si již několikrát v předchozích stránkách zmínili. Tato funkce je definována jako počet kladných celých čísel, která jsou nižší než číslo, pro kterou funkci hledáme, a jsou s tímto číslem nesoudělná. Obecně se tato funkce zapisuje jako $\varphi(n)$, kde $n \geq 2$. Pro přesnější představu si uveďme jednoduché příklady.

$$\varphi(6) = 2 \qquad \dots \qquad \{1; 5\}$$

$$\varphi(10) = 4 \qquad \dots \qquad \{1; 3; 7; 9\}$$

$$\varphi(15) = 8 \qquad \dots \qquad \{1; 2; 4; 7; 8; 11; 12; 13; 14\}$$

Z předešlých příkladů už máme snad lehkou představu, co to ta Eulerova funkce je, avšak jakou to vlastně hraje roli u nás v systému RSA jsme si neřekli. Prvně se zaměřme, co nám vlastně Eulerova funkce říká. Jsou-li p a q prvočísla, poté

$$\boldsymbol{\varphi(p) = p - 1} \qquad (17)$$

$$\boldsymbol{\varphi(q) = q - 1} \qquad (18)$$

a uděláme součin těchto dvou prvočísel stejně, jako děláme při tvorbě modulo v systému RSA, dostaneme tvar

$$\boldsymbol{n = p \cdot q} \qquad (19)$$

$$\boldsymbol{\varphi(n) = \varphi(p) \cdot \varphi(q)} \qquad (20)$$

$$\boldsymbol{\varphi(n) = (p - 1) \cdot (q - 1)}, \qquad (1)$$

kde jsme si vlastně vyjádřili počet nesoudělných čísel se součinem dvou od sebe různých prvočísel $[4]$. Avšak Eulerova věta říká ještě něco, u čeho se chvilku pozastavíme.

$$\boldsymbol{x^{\varphi(n)} \equiv 1 \bmod n}, \qquad (21)$$

právě tehdy když x a n jsou nesoudělná čísla, to znamená $GCD(x, n) = 1$. Na této větě staví i systém RSA, přesto se může stát, že x a n budou čísla soudělná, tedy budou mít nějakého společného dělitele. Pojďme si takový případ zrovna ukázat $[2]$.

a) Je dána zpráva $x = 5$, Eulerova funkce $\varphi(n) = 312$ a hodnota $n = 395$.

Kdybychom se drželi předešlé rovnice (21), získáme tvar

$$5^{312} \equiv 1 \bmod 395,$$

Jenže pokud příklad vyřešíme, například v prostředí Wolfram Cloud, získáme zcela jiný výsledek

$$5^{312} \equiv 80 \bmod 395.$$

Jak je tedy možné, že i přes tuto nejasnost je systém RSA tak bezpečný? Důvod je zcela prostý, neboť zpráva je násobkem daného modulo. Stačí nám tedy rovnici upravit do příslušného tvaru, a to tak, že modulo již nebude násobkem dané zprávy.

$$395 : 5 = 79$$

Tímto získáme nové modulo a rovnici (21) můžeme přepsat do tvaru

$$5^{312} \equiv 1 \bmod 79,$$

který již souhlasí s definicí.

Tímto příkladem jsme si nedokázali jen pravost Eulerovy věty, ale i důvod, proč je důležité volit příliš velká prvočísla k vytvoření modulo. Je dost možné, že některé zprávy určené k šifrování mohou být násobkem funkce modulo stejně, jak tomu bylo tady, ale pokud neznáme Eulerovu funkci φ, nejsme schopni rozhodnout, že tomu tak opravdu je. Kdybychom totiž prozradili naši velikost oné funkce, mohlo by se nám někdy stát, že naše tajná konverzace bude prolomena a my tak „ztratíme“ náš soukromý klíč.

1.1.3. Vyhodnocení RSA

V předešlé kapitole jsme si vysvětlili, jak nám vše v systému RSA spolu funguje, a kde platí jaké podmínky. Aby nám to však dávalo celé smysl trochu víc, než jen v obecné rovině a důkazech, pojďme si načrtnout celý průběh komunikace.

Mějme dva kamarády $ALICI$ a $BOBA$, kteří si spolu budou chtít psát tak, aniž by kdokoli zjistil obsah jejich komunikace. $ALICE$ bude chtít tedy poslat soukromou zprávu $BOBOVI$. Bude tedy muset vzít $BOBŮV$ veřejný klíč $(viz$ rovnice 15 a 16$)$ a pomocí něj zašifrovat zprávu Z ve tvaru $K_{VB} = (n_B, e_B)$. Nyní je schopen jen BOB tuto zprávu dešifrovat, neboť jen on zná příslušný soukromý klíč $K_{SB} = (n_B, d_B)$. Situaci si můžeme představit následovně:

$ALICE$ zašifruje zprávu $BOBOVI \rightarrow Z_{\check{S}} = Z^{e_b} \bmod(n_B)$

BOB dešifruje zprávu od $ALICE \rightarrow Z_D = Z_{\check{S}}^{d_M} \bmod(\mathrm{n_B}) = Z$

Pro přesnější interpretaci a pochopení vytvořme oběma těmto uživatelům jejich klíče

BOB:

$$K_{VB} = (n_B, e_B) = (50\,381, 487)$$

$$K_{SB} = (n_B, d_B) = (50\,381, 2\,755)$$

ALICE:

$$K_{VA} = (n_A, e_A) = (22\,327, 669)$$

$$K_{SA} = (n_A, d_A) = (22\,327, 1\,741)$$

Představme si, že zprávu, kterou chce $ALICE$ napsat, má tvar $Z = 1\,977$, budeme postupovat následovně.

1. $ALICE$ zašifruje zprávu pomocí $BOBOVA$ veřejného klíče

$$\mathrm{Z} \rightarrow \mathrm{Z_Š} = \mathrm{mod}(Z^{\mathrm{e_B}}, n_B)$$

$$\mathrm{Z_Š} = \mathrm{mod}(1977^{487}, 50\,381)$$

$$Z_{\mathrm{Š}} = 14\,805$$

a pošle mu zprávu v podobě $Z_{\mathrm{Š}} = 14\,805$.

2. BOB dešifruje zprávu od $ALICE$ pomocí svého veřejného klíče

$$\mathrm{Z_Š} \rightarrow \mathrm{Z_D} = \mathrm{mod}\left(Z_{\mathrm{Š}}^{\mathrm{d_B}}, n_{\mathrm{B}}\right) = Z$$

$$\mathrm{Z_D} = \mathrm{mod}(14\,805^{2\,755}, 50\,381)$$

$$Z_{\mathrm{D}} = Z = 1\,977$$

pomocí svého soukromého tak dokázal dešifrovat zašifrovanou zprávu a zjistil její obsah.

1.1.4. Útoky na RSA

Útoků na narušení komunikace pomocí algoritmu RSA již bylo nespočet. My si zde zmíníme pouze nějaký přehled. Řekneme si, kdy mohou být tyto způsoby útoků úspěšné, ale hlavně si tím dokážeme i to, že pokud dodržujeme vždy správné podmínky a volíme vhodné parametry, nikdy tento šifrovací systém nemůže být nabourán cizí osobou (pokud budeme časem vždy volit větší a větší prvočísla k tvorbě našich klíčů).

Mezi takové jednoduché útoky můžeme řadit například útok hrubou silou. Jednoduchý je však pouze v tom, jaké matematické znalosti může útočník mít, neboť se zde snažíme rozložit $\mathrm{modulo}\ n$. Zjistit tedy prvočísla p a q, ze kterých je modulo složeno. Tato metoda je poměrně účinná, pokud autor klíčů nezvolil příliš velká prvočísla. K detailnějšímu prostudování této metody bychom doporučili prostudovat bakalářskou práci $[11]$.

Dalším poměrně primitivním způsobem, jak by šel systém RSA prolomit, je sdílení jednotného modulo. Zkrátka bude-li mít skupinka přátel stejné modulo (které jim bude přiděleno nějakým správcem) a každý z nich má svůj vlastní šifrovací (logicky i dešifrovací) exponent, není příliš těžké jejich zprávy prolomit, a to i na základě velikost šifrovacího exponentu ve skupině lidí využívající jednotné modulo. Pro více informací doporučujeme prostudovat $[6]$.

1.2. Cvičné šifrování

Po veškeré teorii si zde zkusme, jak šifrování RSA rozumíme. Naším úkolem je si pouze ověřit fakt, že teorii zvládáme a danému šifrování již dostatečně rozumíme. Veškeré postupy, jak správně zprávu zašifrovat, jsme si již ukázali, nyní tak máme možnost si to procvičit a nebojte, v následující kapitole se zase podíváme na dešifrování.

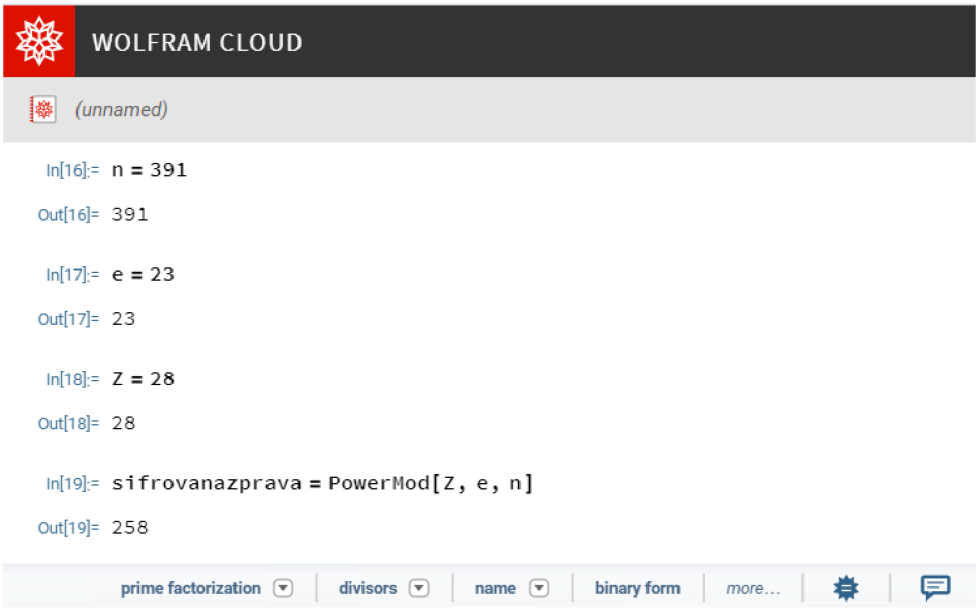
1.2.1. Příklad 1. - Šifrování

Pan Jan chce poslat svou zprávu "28" svému příteli Jirkovi, který má veřejný klíč $(n; e) = (391; 23)$. Jak bude vypadat zašifrovaná zpráva?

I když se nám zadání jeví poměrně složité, pojďme si jej předvést a dokázat si, že zase tak složité není. Neboť vše, co potřebujeme znát, již víme ze zadání. Víme totiž, co budeme šifrovat a víme i klíč, podle kterého šifrování proběhne. Abychom tedy docílili správného šifrování, využijme rovnici (17)

$$28^{23}\mathrm{mod}(391).$$

Pro první ukázku šifrování použijeme volně přístupný software Wolfram Cloud a pomocí funkce "$PowerMod$" získáme zašifrovanou zprávu v podobě "258" viz Obrázek 4 níže, kterou Jan pošle Jiřímu.



Obrázek 4: Ukázka průběhu šifrování k příkladu 1.

1.2.2. Příklad 2. – Šifrování

Jaký tvar by měla zpráva "$1\ 934$", pokud bychom ji chtěli poslat příjemci, jehož veřejný klíč má tvar $(n; e) = (430\ 271;\ 877)$?

Z předešlého příkladu již víme, že lze využít příkazu "$PowerMod$" v zdarma přístupném softwaru Wolfram Cloud a průběh tohoto šifrování by vypadal obdobně, jako v Tabulce 1. Zjistili bychom tedy, že zprávu "$1\ 934$" zašifrujeme pomoci daného klíče do tvaru "$229\ 297$".

Pro znázornění průběhu šifrování a následně i dalších operací v prostředí Wolfram Cloud jsme zvolili metodu zobrazení v tabulce, neboť obrázky nebyly vždy dobře čitelné a zabíraly více místa. Proto u pozdějších příkladů bude vždy obrázek jen u úvodního příkladu (ukázky) a u dalších příkladů si veškerý průběh zobrazíme v tabulkách.

In („vstup“)	Out („výstup“)
$\mathrm{n} = 430271$	430271
$\mathrm{e} = 877$	877
$\mathrm{Z} = 1934$	1 934
$\mathrm{sifrovanazprava} = \mathrm{PowerMod}[\mathrm{Z}, \mathrm{e}, \mathrm{n}]$	229 297

Tabulka 1: Ukázka průběhu šifrování k příkladu 2.

1.2.3. Zašifrujte správně zprávu s příslušným veřejným klíčem.

a) Zašifrujte číslo 49 pomocí

Veřejný klíč: $\mathrm{K_V} = (54\,104\,537;\ 1\,703)$

$$Z = 49$$

$$Z_{\check{\mathrm{S}}} = \mathrm{mod}\,(49^{1\,703}, 54\,104\,537)$$

$$Z_{\check{\mathrm{S}}} = 18\,283\,177$$

In („vstup“)	Out („výstup“)
$\mathrm{n} = 54104537$	54 104 537
$\mathrm{e} = 1703$	1 703
$\mathrm{Z} = 49$	49
$\mathrm{sifrovanazprava} = \mathrm{PowerMod}[\mathrm{Z}, \mathrm{e}, \mathrm{n}]$	18 283 177

Tabulka 2: Ukázka průběhu šifrování k příkladu 1.2.3 a)

b) Zašifrujte číslo 167 pomocí

Veřejný klíč: $\mathrm{K_V} = (679\,027;\ 559)$

$$Z = 167$$

$$Z_{\check{S}} = \mathrm{mod}\,(167^{559}, 679\,027)$$

$$Z_{\check{S}} = 190\,009$$

In („vstup“)	Out („výstup“)
$\mathrm{n} = 679027$	679 027
$\mathrm{e} = 559$	559
$\mathrm{Z} = 167$	167
$\mathrm{sifrovanazprava} = \mathrm{PowerMod[Z, e, n]}$	190 009

Tabulka 3: Ukázka průběhu šifrování k příkladu 1.2.3 b)

c) Zašifrujte číslo 8 105 pomocí

Veřejný klíč: $\mathrm{K_V} = (1\,501\,144\,452\,391\,851\,539;\ 593\,401)$

$$Z = 8\,105$$

$$Z_{\check{S}} = \mathrm{mod}\,(8\,105^{593\,401}, 1\,501\,144\,452\,391\,851\,539)$$

$$Z_{\check{S}} = 1\,277\,841\,198\,579\,671\,933$$

In („vstup“)	Out („výstup“)
$\mathrm{n} = 1501144452391851539$	1 501 144 452 391 851 539
$\mathrm{e} = 593401$	593 401
$\mathrm{Z} = 8105$	8 105
$\mathrm{sifrovanazprava} = \mathrm{PowerMod[Z, e, n]}$	1 277 841 198 579 671 933

Tabulka 4: Ukázka průběhu šifrování k příkladu 1.2.3 c)

d) Zašifrujte číslo 25 613 pomocí

Veřejný klíč: $\mathrm{K_V} = (1\,007, 26)$

$$Z = 25\,613$$

$$Z_{\check{S}} = \mathrm{mod}\,(25\,613^{26}, 1\,007)$$

$$Z_{\check{S}} = 476$$

In („vstup“)	Out („výstup“)
$\mathrm{n} = 1007$	1 007
$\mathrm{e} = 26$	26
$\mathrm{Z} = 25613$	25 613
$\mathrm{sifrovanazprava} = \mathrm{PowerMod[Z, e, n]}$	476

Tabulka 5: Ukázka průběhu šifrování k příkladu 1.2.3 d)

Avšak pozor, dovolujeme si vás upozornit na fakt, že kombinace těchto klíčů nemusí nikterak existovat. Když si sami totiž budete chtít vytvořit takovýto klíč, zjistíte, že k nim nelze najít jejich dešifrovací exponent d. Proto se zde bavíme o pouhém šifrování a nikoliv dešifrování, neboť to by zde nebylo ani možné.

1.3. Cvičné dešifrování

Jak tomu bylo u kapitoly cvičné šifrování, tak zde tomu nebude jinak. Pomocí soukromého klíče si procvičíme, jak zprávu určenou pro nás dešifrovat a zjistit tak, co nám autor zprávy chtěl sdělit.

1.3.1. Příklad 1. - Dešifrování

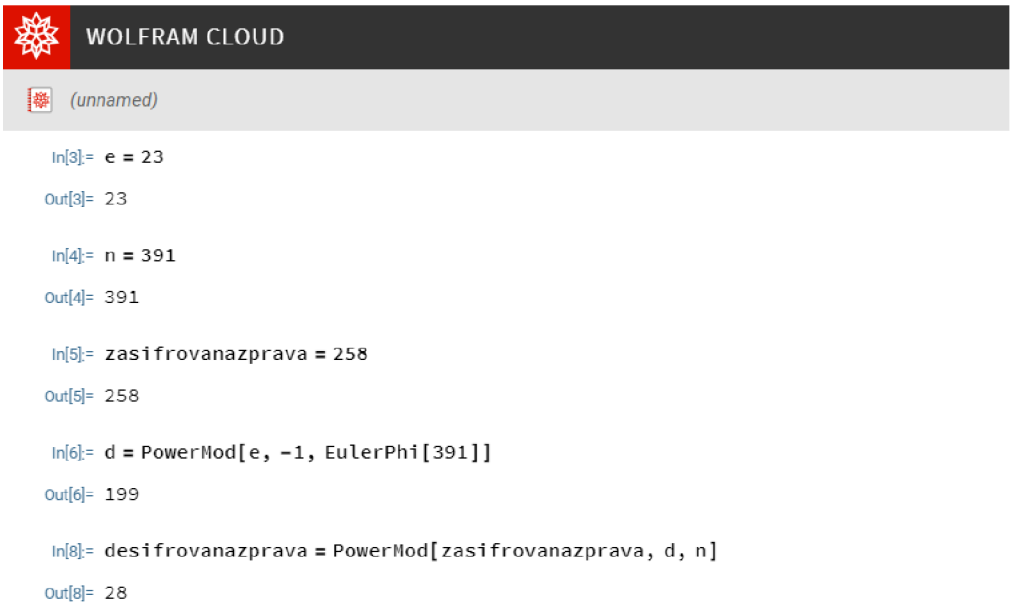
Pan Jiří dostal zprávu od svého přítele Jana, ve které je napsáno "258". Co se ukrývá pod touto zašifrovanou zprávou určenou právě Jiřímu?

Bystřejším čtenářům jistě došlu, že je to navazování na příklad "1.2.1.", a tak mnozí jistě již ví, co se pod zašifrovanou zprávou skrývá. Pan Jiří však ne, a proto si ukážeme, jak takovou zprávu je třeba správně dešifrovat.

Pan Jiří k tomu bude potřebovat svůj vlastní soukromý klíč $(n; d) = (391;\ 199)$, kde hodnotu "d" zjistil pomocí softwaru Wolfram Cloud, a to za pomoci příkazu "$PowerMod[23, -1, EulerPhi[391]]$". Následně se zašifrovanou zprávou udělá dost podobný krok jako pan Jan, když zprávu šifroval

$$258^{199} \mathrm{mod} 391.$$

Stejně tak i zde si přiložíme Obrázek 5 s celým postupem a dešifrovanou zprávu máme v původní podobě "28".



Obrázek 5: Ukázka průběhu dešifrování k příkladu 1

1.3.2. Příklad 2. – Dešifrování

Co by se skrývalo za zprávou "80 168", pokud by byla určena někomu, jehož veřejný klíč má tvar $(n; e) = (667\ 726;\ 409)$?

I zde se odkážeme již na dřívější příklad, a to příklad "1.2.2.". Avšak v tuto chvíli nebudeme příjemci skryté zprávy, nýbrž útočníci, kteří chtějí tuto zprávu získat a zjistit, co se

v ní skrývá. Abychom něco takového dokázali, musíme zjistit soukromý klíč příjemce, a vzhledem k jeho malému modulo, to nebude až tak obtížné. Ve všech početních operacích nám opět poslouží WolframCloud.

Ze všeho nejdříve si určíme dešifrovací exponent d a následně zprávu jen dešifrujeme. Z předchozího příkladu známe příkaz "$PowerMod[e, -1, EulerPhi[n]]$", který nám nalezne právě dešifrovací exponent. Avšak pozor, tohoto příkazu lze využít opravdu jen tehdy, pokud bude funkce "$modulo$" malé číslo, neboť faktorizace čísel větších již ani výpočetní technika nezvládne (doposud). Veškerý postup lze vidět v Tabulce 6.

In („vstup“)	Out („výstup“)
$\mathrm{zasifrovanazprava} = 80168$	80 168
$\mathrm{e} = 409$	409
$\mathrm{n} = 667726$	667 726
$\mathrm{d} = \mathrm{PowerMod}[\mathrm{e}, -1, \mathrm{EulerPhi}[\mathrm{n}]]$	280 489
$\mathrm{Zprava} = \mathrm{PowerMod}[\mathrm{zasifrovanazprava}, \mathrm{d}, \mathrm{n}]$	1 934

Tabulka 6: Ukázka průběhu dešifrování k příkladu 2

1.3.3. Dešifrujte správně zprávu s příslušným soukromým klíčem.

a) Dešifrujte číslo $5\,933$ pomocí

Soukromého klíče: $\mathrm{K_S} = (14\,587\ ;\ 12\,793\ )$

$$Z_{\check{\mathrm{S}}} = 5933$$

$$Z_{\mathrm{D}} = \mathrm{mod}\,(5933^{\,12\,793}\,; 14\,587\,)$$

$$Z_{\mathrm{D}} = \ 336$$

In („vstup“)	Out („výstup“)
$\text{zasifrovanazprava} = 5933$	5 933
$\text{e} = 12793$	12 793
$\text{n} = 14587$	14 587
$\text{Zprava} = \text{PowerMod}[\text{zasifrovanazprava}, \text{d}, \text{n}]$	336

Tabulka 7: Ukázka průběhu dešifrování k příkladu 1.3.3. a)

b) Dešifrujte číslo $234\,921$ pomocí

Soukromého klíče: $\text{K}_\text{S} = (523\,423;\ 192\,799\ )$

$$Z_{\check{\text{S}}} = 234\,921$$

$$Z_\text{D} = \text{mod}\,(234\,921^{\,192\,799};\ 523\,423)$$

$$Z_\text{D} = 29\,328$$

In („vstup“)	Out („výstup“)
$\text{zasifrovanazprava} = 234921$	234 921
$\text{e} = 192799$	192 799
$\text{n} = 523423$	523 423
$\text{Zprava} = \text{PowerMod}[\text{zasifrovanazprava}, \text{d}, \text{n}]$	29 328

Tabulka 8: Ukázka průběhu dešifrování k příkladu 1.3.3. b)

c) Dešifrujte číslo $57\,692$ pomocí

Soukromého klíče: $\text{K}_\text{S} = (635\,963;\ 361\,717\ )$

$$Z_{\check{\text{S}}} = 57\,692$$

$$Z_\text{D} = \text{mod}\,(57\,692^{361\,717}, 635\,963)$$

$$Z_\text{D} = 123\,552$$

In („vstup“)	Out („výstup“)
$\text{zasifrovanazprava} = 57692$	57 692
$\text{e} = 361717$	361 717
$\text{n} = 635963$	635 963
$\text{Zprava} = \text{PowerMod}[\text{zasifrovanazprava}, \text{d}, \text{n}]$	123 552

Tabulka 9: Ukázka průběhu dešifrování k příkladu 1.3.3. c)

d) Dešifrujte číslo 2 622 082 325 pomocí

Soukromého klíče: $\text{K}_\text{S} = (3\ 043\ 729\ 299,\ 1\ 408\ 425\ 139)$

$$Z_{\check{\text{S}}} = 2\ 622\ 082\ 325$$

$$Z_\text{D} = \text{mod}\ (2622082325^{1408425139}, 3043729299)$$

$$Z_\text{D} = 2\ 891\ 540\ 737$$

In („vstup“)	Out („výstup“)
$\text{zasifrovanazprava} = 2622082325$	2 622 082 325
$\text{e} = 1408425139$	1 408 425 139
$\text{n} = 3043729299$	3 043 729 299
$\text{Zprava} = \text{PowerMod}[\text{zasifrovanazprava}, \text{d}, \text{n}]$	2 891 540 737

Tabulka 10: Ukázka průběhu dešifrování k příkladu 1.3.3. d)

2. Praktická část

2.1. Úvod k praktické části

K výzkumu bylo zapotřebí vybrat žáky, kteří dostatečně ovládají matematické operace, které jsou k šifrování/dešifrování zapotřebí. Proto jsme zvolili 8. a 9. ročník ze Základní školy Hodonín, Očovská 1, příspěvková organizace. Z těchto ročníků byli i tak vybráni - pod vedením kantorů matematiky této základní školy (spolu se mnou, jakožto jedním

z kantorů a tvůrcem diplomové práce) - pouze ti, kteří by na pochopení algoritmu RSA měli dostačující předpoklady.

Tuto početní skupinu 71 žáků, tvořenou dvěma ročníky základní školy, jsem osobně učil několik hodin a všichni se mnou absolvovali výuku, která byla zaměřena na algoritmus RSA a jeho správné používání (s tím související i tvorba klíčů). Výuka probíhala dle rozvrhu třídy, vždy podle jejich odpoledního vyučování (bylo domluveno s vyučujícími i vedením školy, že žáky budu učit já a připravovat je na výzkum diplomové práce). Níže v Tabulce 11 je rozpis, které dny jsem učil v jaké třídě.

Třídy	Den	Čas
8.A	Sudý týden – pondělí	14:00 – 15:30
8.B	Sudý týden - čtvrtek	14:00 – 15:30
8.C	Lichý týden – čtvrtek	14:00 – 15:30
9.A	Sudý týden – středa	14:00 – 15:30
9.B	Lichý týden – středa	14:00 – 15:30
9.C	Lichý týden – pondělí	14:00 – 15:30

Tabulka 11: Rozpis tříd určený k blokové výuce

V každé ze zmíněných tříd jsem měl tři dvouhodinové bloky konané vždy v jedné ze dvou počítačových učeben, a jelikož učebna občas svým vybavením dostatečně nepokryla počet všech žáků, využil jsem nových Ipadů ve škole (upřímně jsem toho trošku následně litoval, neboť psaní v prostředí Wolfram Cloud bylo těžší a zdlouhavější). Výuku v těchto blocích jsem rozdělil do tří pomyslných kapitol:

1) Základní matematika v prostředí Wolfram Cloud
2) Komunikace pomocí RSA
3) Opakování algoritmu a výzkumná část

V prvním dvouhodinovém bloku, který jsem nazval *„Základní matematika v prostředí Wolfram Cloud,“* jsem se se žáky věnoval registraci do webového prostředí Wolfram Cloud (někdy to zabralo více času, než jsem čekal). Následně jsme si zde zkoušeli základní

matematické znalosti a operace, tedy jak se čísla sčítají, odčítají, násobí, dělí, umocňují, odmocňují a dělí se zbytkem (tak, abychom znali zbytek po vydělení daným číslem). Pro ukotvení kódů, které se museli žáci naučit, jsem vždy volil 12 příkladů a kontroloval, zda jsou všichni schopni ovládat prostředí Wolfram Cloud v této základní oblasti matematiky. Veškerá čísla, se kterými jsme pracovali, jsem žákům předem předepsal a nahrál na sdílený disk školy, aby nenastala situace, že někdo číslo špatně opíše. Ke všem matematickým operacím byly použity textové dokumenty s názvem matematické operace a s příklady, které si měli žáci vyřešit v prostředí Wolfram Cloud. Veškeré příklady zde přikládám spolu s řešením.

Druhý blok s názvem „*Komunikace pomocí RSA*“ už se týkala všech náležitostí, které jsou k porozumění asymetrické šifrování algoritmu RSA zapotřebí. To znamená, že jsme si zde zkoušeli funkce na náhodné prvočíslo ("$RandomPrime$") a stejně tak i náhodné celé číslo („$RandomInteger$“). Neopomenuli jsme ani funkci na nejmenšího společného dělitele ("GCD"). Pro jistotu jsme si vyzkoušeli i funkci na ověření prvočísla ("$PrimeQ$"). Opět jsem vyžadoval od žáků 12 ukázkových příkladů, ve kterých měli měnit velikost výsledných čísel a vždy ověřit, zda se jedná o prvočíslo či nikoliv. Zhruba v polovině této dvouhodinové sekce jsme si vytvořili hlavně naše klíče, tedy klíč veřejný (n, e) a klíč soukromý (n, d). Nakonec jsme si ke konci zkusili zašifrovat a následně dešifrovat i nějakou zprávu, podle vlastních klíčů (některé skupiny bohužel stihly jen jednu zprávu, no jiné měly možnost si zašifrovat zpráv víc). Všechny kroky provedené ve dvou hodinových blocích, které žáci pod mou kontrolou museli vykonat, lze vidět na Obrázku 6 a Obrázku 7.

V posledním bloku nesoucí název „*Opakování algoritmu a výzkumná část*“ jsem si pro žáky na začátek hodiny připravil aktivizační hru, ve které měli za úkol dešifrovat jim určenou zprávu. Tato zpráva byla pro každého individuální, neboť jsem vzal vždy datum narození žáka (to jsem si zjistil ze školního systému) a zašifroval jej podle jeho veřejného klíče. Tohle jsem opakoval u všech žáků a následně čísla rozeslal. Žáci měli za úkol zprávu dešifrovat a zjistit, co číselná kombinace znamená. Tato aktivita se poměrně chytila a žáci z ní byli nadšení (a krapet vyděšení, jak to vše vlastně funguje). Po této krátké aktivitě jsem žákům rozeslal dotazník, kde jsem je již nechal samostatně pracovat a sledoval, jak se jim daří otázky plnit. Čas určený k vyplnění dotazníku jsem původně cílil na 45 min, ale po usouzení a sledování situace jsem jej navýšil na 60 min.

Všechny z bloků byly podloženy prezentací, kterou přikládám k této práci jako přílohu, a zde ji aspoň v jednoduchosti zmíním spolu se zkušenostmi, kterých jsem nabyl při jejím prezentování. Zprvu jsem chtěl žákům přiblížit, co to vlastně zkratka RSA znamená a zobrazit si nějaké jednoduché schéma samotného šifrování. Této „kapitole“ jsem příliš času nevěnoval a snažil se žáky spíše jen v rychlosti namotivovat, že kryptografie, jako taková, je již mezi námi delší dobu (viz Caesarova šifra). Pro nadšence jsem měl připravenou literaturu $[3]$, která mě samotného motivovala se o dané téma zajímat (avšak dovoluji si upozornit, že knížka není určena jen pro jedno přečtení).

V prezentaci následoval první z větších problémů, a to byla samotná registrace do prostředí Wolfram Cloud, neboť někteří si nepamatovali svůj osobní mail (nedej bože jej vůbec neměli) a jiní, a že jich bylo dost, si nebyli schopni zapamatovat své přihlašovací údaje do dalších dvouhodinových bloků. I přes tato úskalí byli žáci však vždy v následujících blocích připraveni a schopni si nějak poradit (použitím jednoho účtu pro více uživatelů). Po všech těchto strastích jsme se mohli vrhnout na samotné prostředí Wolfram Cloud, posunout se v prezentaci a vyzkoušet si, jak se v tomhle prostředí pracuje. Celé toto bylo otázkou jednoho slidu, ale zhruba $15 - 20$ min.

Po registraci jsme si v prezentaci a současně na svých zařízení vyzkoušeli operaci sčítání, která byla rozdělena do dvou slidů (stejně jako všechny následující matematické operace). Žáci měli možnost si příklady okopírovat z jednotlivých textových dokumentů (přiložených na školním serveru) a vkládat do systému Wolfram Cloud (opět někteří nezklamali a neznali zkratky pro zkopírovat a vložit). Po matematické operaci sčítání následovalo odčítání, násobení, dělení, dělení se zbytkem, umocňování a odmocňování (všechny zmíněné operace i příklady k nim vidíme na následujících stránkách a opět je žáci měli v textových dokumentech na školním serveru).

Když už jsme společně zvládali příkazy pro všech 7 zmíněných matematických operací, posunuli jsme se dál a zaměřili se na složitější příkazy, díky nimž jsme dokázali nalézt prvočíslo, ověřit pravost tohoto prvočísla, určit nejmenšího společného dělitele a vygenerovat si náhodné celé číslo z daného intervalu. Pro nalezení prvočísla byl využít příkaz

$$RandomPrime[\text{interval od; interval do}],$$

pro jeho ověření jsme následně psali

$$PrimeQ[\text{hodnota prvočísla}],$$

pro určení nejmenšího společného dělitele jsme využili příkazu

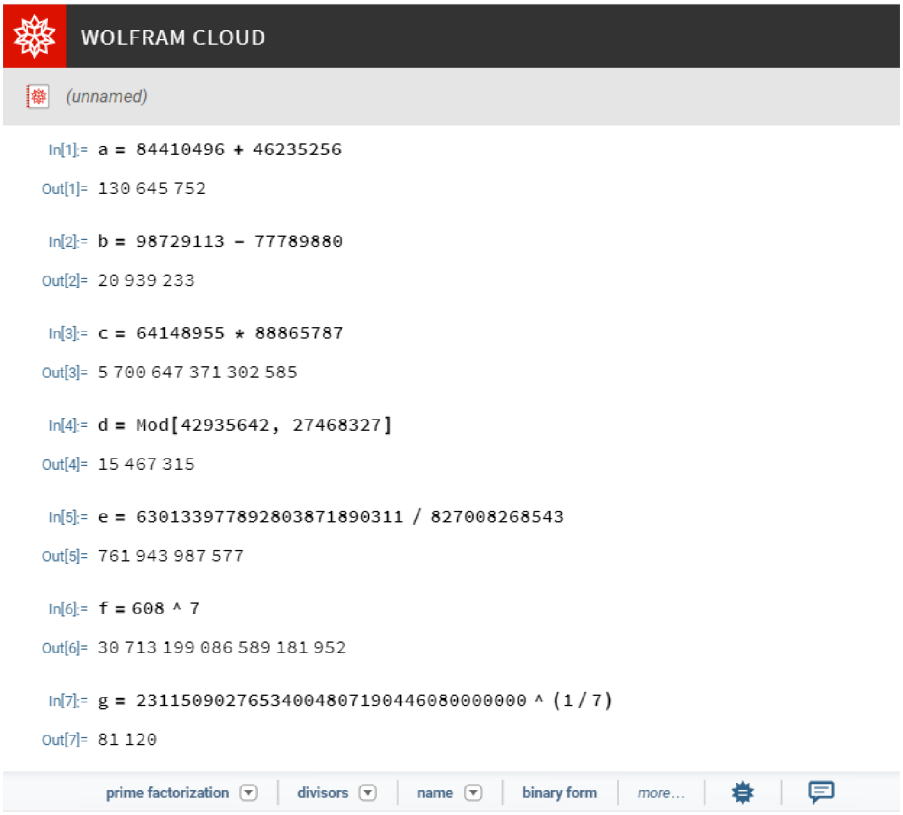
$$GCD[\text{číslo 1, číslo 2, ...}]$$

a k nalezení reálného čísla poté sloužil příkaz

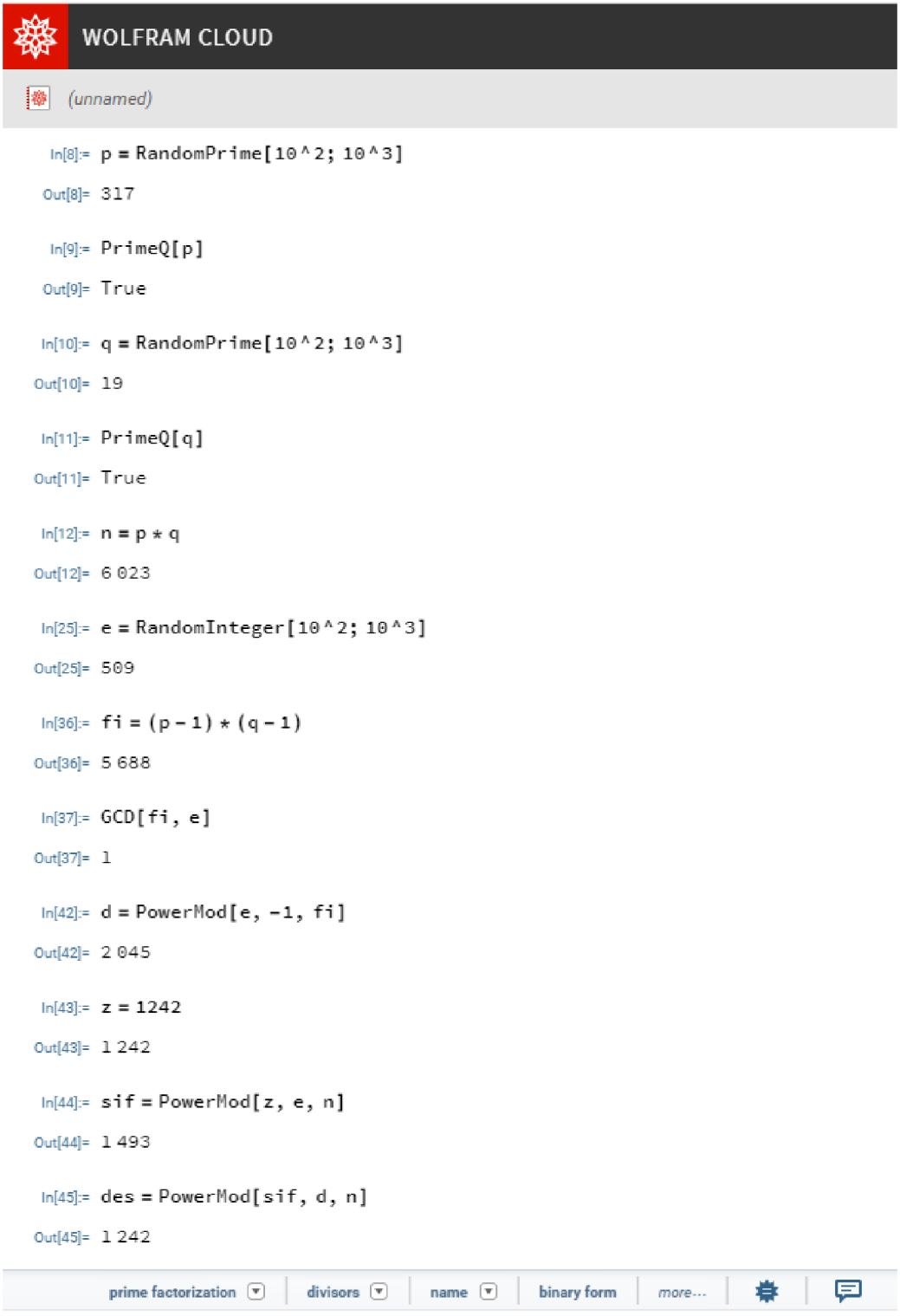
$$RandomInteger[\text{interval od; interval do}].$$

Dovoluji si upozornit (protože někteří ze žáků to bohužel nepochopili), že hodnotu interval od a interval do určujeme sami v podobě numerických hodnot.

Poté už nám chybělo jediné, a to zkusit si vytvořit nějaký veřejný klíč, k tomu klíč soukromý, a poté vymyslet zprávu, kterou bychom mohli zašifrovat (následně dešifrovat). V prezentaci jsem měl zvolené „ukázkové“ klíče, které jsme si všichni nejprve opsali a zkusili si pomocí nich zašifrovat zprávu a následně tuto zprávu i dešifrovat. Některé ze žáků to zajímalo a chtěli si vytvořit svoje vlastní klíče, tak jsem přepnul na další slidy v prezentaci, kde byla ukázka příkazů, pomocí kterých si byli schopni všichni vytvořit své klíče. Ukázku těchto příkazů (a nejen jich) přikládám stejně jako onu prezentaci mezi přílohy, aby bylo vidět, jaké všechny příkazy žáci poznali a které využili pro algoritmus RSA.



Obrázek 6: Souhrn ukázkových příkladů k pochopení základních matematických operací



Obrázek 7: Souhrn všech základních příkazů k algoritmu RSA v prostředí Wolfram Cloud

Sčítání

In („vstup“)	Out („výstup“)
a = 84410496 + 46235256	130 645 752
b = 98729113 + 77789880	176 518 993
c = 64148955 + 88865787	153 014 742
d = 42935642 + 27468327	70 403 969
e = 4347363466 + 8 018771648	12 366 135 114
f = 5040908913 + 4518749354	9 559 658 267
g = 7401865584 + 8263262620	15 665 128 204
h = 9299501028 + 2605971129	11 905 472 157
i = 382670363963 + 937271081629	1 319 941 445 592
j = 19359512855 + 473015498651	492 375 011 506
k = 220606701593 + 376865885067	597 472 586 660
l = 135902611536 + 386649917780	522 552 529 316

Tabulka 12: Seznam příkladů pro žáky na operaci sčítání

Odčítání

In („vstup“)	Out („výstup“)
a = 84410496 − 46235256	38 175 240
b = 98729113 − 77789880	20 939 233
c = 64148955 − 88865787	−24 716 832
d = 42935642 − 27468327	15 467 315
e = 4347363466 − 8 018771648	−3 671 408 182
f = 5040908913 − 4518749354	522 159 559
g = 7401865584 − 8263262620	−861 397 036
h = 9299501028 − 2605971129	6 693 529 899
i = 382670363963 − 937271081629	−554 600 717 666
j = 19359512855 − 473015498651	−453 655 985 796
k = 220606701593 − 376865885067	−156 259 183 474
l = 135902611536 − 386649917780	−250 747 306 244

Tabulka 13: Seznam příkladů pro žáky na operaci odčítání

Násobení

In („vstup“)	Out („výstup“)
a = 84410496 ∗ 46235256	3 902 740 891 646 976
b = 98729113 ∗ 77789880	7 680 125 852 776 440
c = 64148955 ∗ 88865787	5 700 647 371 302 585
d = 42935642 ∗ 27468327	1 179 370 254 410 934
e = 4347363466 ∗ 8 018771648	34 860 514 904 711 811 968
f = 5040908913 ∗ 4518749354	22 778 603 894 191 592 202
g = 7401865584 ∗ 8263262620	61 163 559 198 531 670 080
h = 9299501028 ∗ 2605971129	24 234 231 193 073 820 612
i = 382670363963 ∗ 937271081629	358 665 865 938 964 112 935 727
j = 19359512855 ∗ 473015498651	9 157 349 626 748 269 658 605
k = 220606701593 ∗ 376865885067	83 139 139 847 557 503 811 731
l = 135902611536 ∗ 386649917780	52 546 733 576 481 679 510 080

Tabulka 14: Seznam příkladů pro žáky na operaci násobení

Dělení se zbytkem

In („vstup“)	Out („výstup“)
a = Mod[84410496, 46235256]	38 175 240
b = Mod[98729113, 77789880]	20 939 233
c = Mod[64148955, 88865787]	64 148 955
d = Mod[42935642, 27468327]	15 467 315
e = Mod[4347363466, 8018771648]	4 347 363 466
f = Mod[5040908913, 4518 49354]	135 318 729
g = Mod[7401865584, 8263262620]	7 401 865 584
h = Mod[9299501028, 2605971129]	1 481 587 641
i = Mod[382670363963, 937271081629]	382 670 363 963
j = Mod[19359512855, 473015498651]	19 359 512 855
k = Mod[220606701593, 376865885067]	220 606 701 593
l = Mod[135902611536, 386649917780]	135 902 611 536

Tabulka 15: Seznam příkladů pro žáky na operaci dělení se zbytkem

Dělení

In:	a = 81238029080808165233892 / 573733780739
Out:	141 595 338 828
In:	b = 100745042992358580073980 / 295695829606
Out:	340 704 984 330
In:	c = 252455521015073703100840 / 955484318632
Out:	264 217 335 745
In:	d = 376066937890279356679525 / 980994576841
Out:	383 352 718 525
In:	e = 630133977892803871890311 / 827008268543
Out:	761 943 987 577
In:	f = 55098202968219914062351608 / 7225109866167
Out:	7 625 932 890 824
In:	g = 17362153588209679317338240 / 1780244530678
Out:	9 752 679 078 080
In:	h = 45418808533456744479389720 / 6984654899416
Out:	6 502 656 063 545
In:	i = 44409196834194130617336 45 / 1514173766755
Out:	2 932 899 632 079
In:	j = 21891765415092672579142080 / 2574366156709
Out:	8 503 749 693 120
In:	k = 40934704652874541372785097 / 8197761113501
Out:	4 993 400 525 597
In:	l = 403099400003651037473852 80 / 6201837135361
Out:	6 499 677 292 480

Tabulka 16: Seznam příkladů pro žáky na operaci dělení

Umocňování

In:	a = 892 ^ 5
Out:	564 708 431 199 232
In:	b = 980 ^ 2
Out:	960 400
In:	c = 840 ^ 9
Out:	208 215 748 530 929 664 000 000 000
In:	d = 525 ^ 9
Out:	302 993 792 183 303 833 007 8125
In:	e = 311 ^ 8
Out:	87 515 123 947 429 289 281
In:	f = 608 ^ 7
Out:	30 713 199 086 589 181 952
In:	g = 240 ^ 7
Out:	45 864 714 240 000 000
In:	h = 720 ^ 9
Out:	51 998 697 814 228 992 000 000 000
In:	i = 645 ^ 5
Out:	111 634 536 403 125
In:	j = 80 ^ 5
Out:	3 276 800 000
In:	k = 97 ^ 8
Out:	7 837 433 594 376 961
In:	l = 280 ^ 6
Out:	481 890 304 000 000

Tabulka 17: Seznam příkladů pro žáky na operaci umocňování

Odmocňování

In:	$a = 387796492777052919811890176 \text{ ^ } (1/5)$
Out:	207 836
In:	$b = 5117971600 \text{ ^ } (1/2)$
Out:	71 540
In:	$c = 208215748530929664000000000000000000000000000 \text{ ^ } (1/9)$
Out:	84 000
In:	$d = 16147909647923656640625 \text{ ^ } (1/4)$
Out:	356 475
In:	$e = 344511057261080254448826202052693761000000000 \text{ ^ } (1/8)$
Out:	276 790
In:	$f = 201592731853360017485125893393764843 52 \text{ ^ } (1/7)$
Out:	213 408
In:	$g = 231150902765340048071904460800000 00 \text{ ^ } (1/7)$
Out:	81 120
In:	$h = 236220968830733592020767406 25 \text{ ^ } (1/5)$
Out:	472 785
In:	$i = 189187159595417600000 \text{ ^ } (1/5)$
Out:	11 360
In:	$j = 48271699195859665446528614400000 0 \text{ ^ } (1/6)$
Out:	280 080
In:	$k = 113013708951260875751239590043256289062 5 \text{ ^ } (1/8)$
Out:	76 145
In:	$l = 156932381408580870400000000000 0 \text{ ^ } (1/6)$
Out:	107 800

Tabulka 18: Seznam příkladů pro žáky na operaci odmocňování

2.2. Organizace a metody výzkumu

Dotazník byl vypracován pro žáky základních škol 8. a 9. ročníku. K jeho vypracování mohli žáci pracovat s jakoukoliv výpočetní technikou, ať už se jednalo o školní počítače, školní Ipady nebo jejich soukromé telefony. Volba, pomocí jakého typu VT test vypracují, byla zcela na nich a stejně tak i využití softwarů či různých webových portálů.

Byl zde stanoven jediný vstupní parametr. Ze všech žáků, kteří se mnou prošli všechny tři dvouhodinové bloky, byli následně vybráni pouze ti, kteří by nemuseli výzkum této práce dehonestovat. Na tomto sítu se podíleli spolu se mnou dva ze tří matematických kantorů dané základní školy. Důvodem, proč jsme zvolili tohle kritérium, je fakt, že někteří ze žáků by byli schopni pouze odpovědi tipovat za účelem vidiny volné vyučovací hodiny (bohužel ani tomu jsme však u některých z vybraných nezabránili).

2.2.1. Cíle a hypotézy výzkumu

Základní i nejpodstatnější částí praktické práce je stanovení si cílů, hypotéz a výzkumných otázek nebo úkolů. Práce by měla dokázat, jak moc jsou žáci znalí svých prostředků VT a zda ji umí ovládat k matematickým operací pro algoritmus RSA. Porovnávat zde ale nebudeme pouze jejich znalosti se systémem RSA, nýbrž i jejich znalosti ICT využité v prospěch matematiky. Na tomto základě jsme taky stanovili tyto cíle:

1. *Porovnat znalosti základních matematických operací použitých při systému RSA*

Porovnání kvalit matematických základů k používání systému RSA nám může odhalit znalosti, které žáci základních škol nabyli za dobu svého studia. Zjistit, zda mají vůbec matematické základy k pochopení složitějších matematických operací a souvislostí, které jsou k dostatečnému pochopení RSA zapotřebí. Na základě tohoto cíle byl taky výzkumný test zcela ovlivněn a prvních 15 otázek je směřováno k tomuhle cíli.

Dále chceme poukázat na rozdílné nároky jednotlivých učitelů, kteří po svých žácích nemusí vždy vyžadovat znalosti do stejné hloubky a v neposlední řadě taky poukázat na rozdílné vědomosti v oblasti matematiky u algoritmu RSA mezi ročníky, i když při využívání ICT

bychom zde velké rozdíly vidět neměli (tyto rozdíly jsme ve výzkumu nezapočítali, neboť získaná data od všech žáků se nám sjednotila, a tak není možné vytáhnout jen data žáků z 8. a 9. ročníku zvlášť). Z posledního dvouhodinového bloku, kdy se však psal výzkumný test, jsem si nejen já, ale i někteří z mých kolegů kantorů (které zajímal formát diplomové práce) všimli, že žáci z nižšího ročníku se orientovali mnohem víc (to připisujeme s kolegy tomu, že například umocňování bylo právě jejich probíranou látkou v klasické hodině matematiky).

2. *Porovnat využití výpočetní techniky při algoritmu RSA*

Na využívání výpočetní techniky ve školství existuje mnoho názorů i přístupů, které se však nikdy neshodnou. Naším cílem je předvést, jak moc jsou žáci schopni využívat výpočetní techniku pro matematické účely, zda ovládají nějaký software, případně webový portál.

Tento cíl je stanoven především z důvodu ověření, zda si žáci z dvouhodinových bloků něco pamatují, a dokáží přijat více informací než ročníky před nimi. Navíc předpokládáme, že část žáků (ti s lepším průměrem a větší aktivitou v klasické hodině matematiky) budou ve větší míře využívat výpočetní techniku a nebudou spoléhat jen na kalkulačku (která navíc nedokáže všechny příklady v dotazníku správně vyřešit).

Hypotézy jsme si poté stanovili na základě našich cílů. Vzhledem k možnostem tohoto výzkumu a nějakých osobních předpokladů jsme stanovili tyto hypotézy:

H1. Žáci s lepšími znalostmi v matematice se ve větší míře mnohem lépe orientovali v početních operací systému RSA než žáci, kteří nemají tak dobré znalosti.

Hlavní myšlenkou je přesvědčit se o tom, že i když všichni žáci, kteří se podíleli na výzkumu, měli z dvouhodinových bloků stejné informace o algoritmu RSA, a i stejnou práci v prostředí Wolfram Cloud, budou úspěšnější právě ti, kteří jsou v normálních hodinách matematiky rychlejší a mají lepší průměr známek než druzí. Avšak si dovolujeme zdůraznit, že známka nic nemusí vypovídat o znalostech jedince, tudíž zde nebudeme zohledňovat jen průměr jedince, nýbrž i jeho aktivitu v hodině a celkový přehled v učivu matematiky (osobně konzultováno vždy s daným vyučujícím matematiky v příslušné třídě). Proto je dotazník tvořen i několika otázky, zaměřenými čistě na početní bázi, která právě rozhodne o tom, zda má přehlednost matematických operací vliv na pochopení algoritmu RSA.

H2. Aktivnější žáci na všech dvouhodinových blocích s panem učitelem měli větší přehled o dílčích krocích při správné tvorbě klíče a posílání zpráv než žáci, kteří byli ve dvouhodinových blocích pasivní.

Zaměřujeme se zde na fakt, že ti, kteří byli ve dvouhodinových blocích aktivnější a občas se na něco zeptali, měli méně problémů v druhé polovině dotazníku, který vyplňovali. Nešlo však jen o tvorbu klíče, nýbrž i o šifrování, dešifrování a případně i nějakou souvislost mezi dílčími faktory systému RSA. Zkrátka zda aktivita v blocích s panem učitelem je přímo úměrná úspěšnosti při vyplňování dotazníku.

H3. Žáci po dvouhodinových blocích s panem učitelem využili ve větší míře mnohem lépe výpočetní techniku než žáci, kteří se odmítali naučit pracovat s ICT s využitím v matematice.

Převážně tuto hypotézu stavíme do roviny, kde větší využití výpočetní techniky znamená větší šance na správné pochopení matematického pozadí algoritmu RSA. V dotazníku totiž záměrně byly vybrány i příklady, při kterých nám rozhodně papír vzhledem k času stačit nebude a využití klasické kalkulačky je v některých případech nedostatečné. Proto jsme k vypracování dotazníku zvolili volně přístupný Wolfram Cloud, ve kterém jsme žáky také proškolili a ukázali jim základní příkazy.

2.2.2. Metody

S ohledem na modernizaci škol a nutnosti využití softwaru Wolfram Cloud jsme zvolili metodu dotazníků. Respondenti zde odpovídali na celkem 30 otázek. Ze všech těchto otázek bylo 17 otázek, kde měli možnost výběru jedné správné odpovědi, a 13 otázek, kde museli správnou odpověď napsat. Všechny tyto otázky v dotazníku jsou zde přiloženy.

Úvodem bývá u mnoha dotazníků demografické rozložení, ale to jsme v našem případě vynechali. Všichni respondenti chodí na Základní školu Očovská, Hodonín, příspěvková organizace a rozlišit u nich jen pohlaví a to, zda bydlí přímo ve městě Hodonín nebo v okolí nám přišlo nepodstatné. Proto jsou všechny otázky v dotazníku směřovány už

k matematickým znalostem, které vypovídají i o jejich dovednostech s ICT a znalostech algoritmu RSA.

Prvních 15 otázek, přesně polovina dotazníku, je zaměřených čistě na matematické znalosti, nikoliv na systém RSA. Chtěli jsme si pomocí těchto otázek ověřit, jak žáci zvládají ICT v oblasti matematiky. Zda si pamatují z dvouhodinových bloků všechny příkazy v prostředí Wolfram Cloud a pokud ne, zda jsou schopni si nějak s možností ICT poradit. Jedná se nám o všeobecný přehled, který si žáci mohli právě na těchto 15 otázkách vyzkoušet. V této první polovině dotazníku jsou 2 otázky na principu rozhodnutí, zda číslo je či není prvočíslo, 4 otázky na násobení, 4 otázky na umocnění a 5 otázek na dělení se zbytkem. Nejvíce je tam právě otázek na dělení se zbytkem, neboť jsme očekávali, že právě zde budou žáci konat nejvíce chyb a tyto otázky jim dají nejvíce zabrat, neboť si neuvědomí, že se vlastně ptáme na zbytek po dělení, nikoliv na výsledek podílu.

Druhá polovina dotazníku je tvořena už čistě otázkami týkajících se samotného systému RSA. Přesněji řečeno z těchto zbývajících 15 otázek je právě 5 otázek zaměřených na šifrování zprávy, 5 otázek na dešifrování zprávy, 2 otázky na tvorbu klíčů a zbývající 3 otázky se týkají obecných vlastností, které bychom měli pro správné pochopení algoritmu RSA znát.

2.2.3. Test – Dotazník

1. Rozhodni, které z nabízených čísel je prvočíslo
    a. $3\,587$
    b. $7\,919$
    c. $9\,889$
    d. $6\,293$

2. Rozhodni, které z nabízených čísel není prvočíslo
    a. $7\,489$
    b. $5\,113$
    c. $8\,429$
    d. $6\,697$

3. Jaký je výsledek příkladu $37 \cdot 865 =$

4. Jaký je výsledek příkladu $41 \cdot 572 =$

5. Jaký je výsledek příkladu $17 \cdot 923 =$

6. Jaký je výsledek příkladu $61 \cdot 376 =$

7. Jaké číslo získáme, umocníme-li číslo 52 na 7?

8. Jaké číslo získáme, umocníme-li číslo 72 na 13?

9. Jaké číslo získáme, umocníme-li číslo 59 na 22?

10. Jaké číslo získáme, umocníme-li číslo 38 na 35?

11. Napiš celočíselný zbytek u příkladu $179 : 13 =$

12. Napiš celočíselný zbytek u příkladu $579 : 27 =$

13. Napiš celočíselný zbytek u příkladu $3\,712 : 76 =$

14. Napiš celočíselný zbytek u příkladu $8\,712 : 106 =$

15. Napiš celočíselný zbytek u příkladu $17\,434 : 1\,937 =$

16. Zašifruj zprávu 457 podle veřejného klíče $(n, e) = (2881{,}23)$

    a. 389
    b. 379
    c. 489
    d. 479

17. Zašifruj zprávu 27 podle veřejného klíče $(n, e) = (1147{,}79)$

    a. 767
    b. 667
    c. 567
    d. 467

18. Zašifruj zprávu 8 podle veřejného klíče $(n, e) = (21{,}73)$

    a. 8
    b. 7
    c. 9
    d. 6

19. Zašifruj zprávu 2 podle veřejného klíče $(n, e) = (365{,}17)$

    a. 37
    b. 47
    c. 57
    d. 27

20. Zašifruj zprávu 5 podle veřejného klíče $(n, e) = (215,23)$

    a. 180
    b. 190
    c. 200
    d. 210

21. Dešifruj zprávu 69 podle svého soukromého klíče $(n, d) = (215,95)$

    a. 19
    b. 20
    c. 21
    d. 22

22. Dešifruj zprávu 164 podle svého soukromého klíče $(n, d) = (166,35)$

    a. 48
    b. 58
    c. 68
    d. 38

23. Dešifruj zprávu 20590888 podle svého soukromého klíče $(n, d) = (27580367,9980047)$

    a. 1
    b. 4
    c. 2
    d. 3

24. Dešifruj zprávu 41145 podle svého soukromého klíče $(n, d) = (58847,19939)$

    a. 2
    b. 22
    c. 222
    d. 2222

25. Dešifruj zprávu 16 podle svého soukromého klíče $(n, d) = (287,181)$

    a. 16
    b. 32
    c. 48
    d. 64

26. Znáte-li prvočísla (p) a (q) spolu s hodnotou (e). Napište tvar soukromého klíče (n, d)

    $p = 7$

    $q = 71$

    $e = 73$

    a. $(497,397)$
    b. $(497,497)$
    c. $(497,511)$
    d. $(497,5183)$

27. Znáte-li prvočísla (p) a (q) spolu s hodnotou (e). Napište tvar veřejného klíče (n, e)

    $p = 31$

    $q = 11$

    $e = 79$

    a. $(2449,79)$
    b. $(341,79)$
    c. $(42,79)$
    d. $(121,79)$

28. Znáte-li prvočísla (p) a (q) napište, jakou hodnotu má Eulerova funkce fi(n)

    $p = 1789$

    $q = 3533$

    a. 6315216
    b. 6320537
    c. 5322
    d. 1744

29. Co musí platit mezi šifrovacím exponentem (e) a Eulerovou funkcí fi(n).

a. Jsou nesoudělné $=$ nejmenší společný násobek je 1
b. Jedno číslo je násobkem čísla druhého
c. Mezi nimi není žádné pravidlo
d. Jejich násobek je roven součtu prvočísel (p) a (q)

30. Co znamená mod? $(modulo)$

a. Násobení čísel se zaokrouhlením v řádu jednotek
b. Dělení čísel s celočíselným zbytkem
c. Hledání největšího společného dělitele více než dvou čísel
d. Hledání nejmenší společného násobku více než dvou čísel

2.2.4. Výsledky dotazníku

Než se vrhneme na samotné vyhodnocování dotazníků, usoudil jsem společně s vedoucím diplomové práce, že by bylo záhodno se pozastavit nad tím, jak dlouho by trvalo například vypočítat příklad 16 bez výpomoci ICT (zvolil jsem jeden z těžších příkladů, který se týkal dělení se zbytkem). Dovoluji se považovat za poměrně zdatného matematika v této oblasti, a přesto mi příklad dal zabrat a strávil jsem nad ním necelých 19 min. Nedovoluji si ani odhadnout, kolik času by to zabralo žákům, kteří se podíleli na výzkumu (už jen z toho principu, že nemají takové znalosti jako já) kdyby nevyužili pomoci ICT, a už vůbec si netroufám odhadnout, kolik času by jim teoreticky pak dal zabrat celý dotazník bez možnosti ICT.

Před samotným vyhodnocováním našich hypotéz si ještě ukažme jednotlivá řešení. Na následujících stránkách bude tedy vidět jeden dotazník z 8. a jeden z 9. ročníku Základní školy Očovská, Hodonín, příspěvková organizace, spolu se správným řešením celého dotazníku (zobrazen jako první). Dovolujeme si upozornit na otázku 10, u které je numerická chyba způsobena kapacitou znaků, která byla v dotazníku nastavena. Bohužel této chyby jsme si všimli až při vyhodnocování výsledků. Správná odpověď k této otázce je

19 607 665 147 616 160 921 060 454 382 127 930 075 730 561 467 240 415 232,

to nám ale dotazník nevzal, a tak jsme uznávali za správnou odpověď výsledek, ve kterém chybí posledních 6 číslic a výsledek je tak v podobě

19 607 665 147 616 160 921 060 454 382 127 930 075 730 561 467 240.

Otázky	Správné řešení
1.	7 919
2.	6 697
3.	32 005
4.	23 452
5.	15 691
6.	22 936
7.	1 028 071 702 528
8.	1 397 405 517 247 104 682 033 152
9.	909 377 607 891 473 342 964 601 076 981 440 190 281
10.	19 607 665 147 616 160 921 060 454 382 127 930 075 730 561 467 240
11.	10
12.	12
13.	64
14.	20
15.	1
16.	389
17.	767
18.	8
19.	37
20.	190
21.	19
22.	48
23.	3
24.	16
25.	64
26.	$(497, 397)$
27.	$(341, 79)$
28.	6 315 216
29.	Jsou nesoudělné = nejmenší společný dělitel je 1
30.	Dělení čísel s celočíselným zbytkem

Tabulka 19: Správné výsledky dotazníku k diplomové práci

Otázky	8. Ročník
1.	7 919
2.	6 697
3.	32 005
4.	23 452
5.	15 691
6.	22 936
7.	1 028 071 702 528
8.	1 397 405 517 247 104 682 033 152
9.	909 377 607 891 473 342 964 601 076 981 440 190 281
10.	19 607 665 147 616 160 921 060 454 382 127 930 075 730 561 467 240
11.	13.769
12.	21.444
13.	48.842
14.	82.189
15.	9.001
16.	379
17.	767
18.	7
19.	57
20.	190
21.	20
22.	58
23.	4
24.	2 222
25.	32
26.	$(497, 397)$
27.	$(121, 79)$
28.	5 322
29.	Jedno číslo je násobkem čísla druhého
30.	Násobení čísel se zaokrouhlením v řádu jednotek

Tabulka 20: Výsledky studenta 8. ročníku za čas 47 min a 9 s

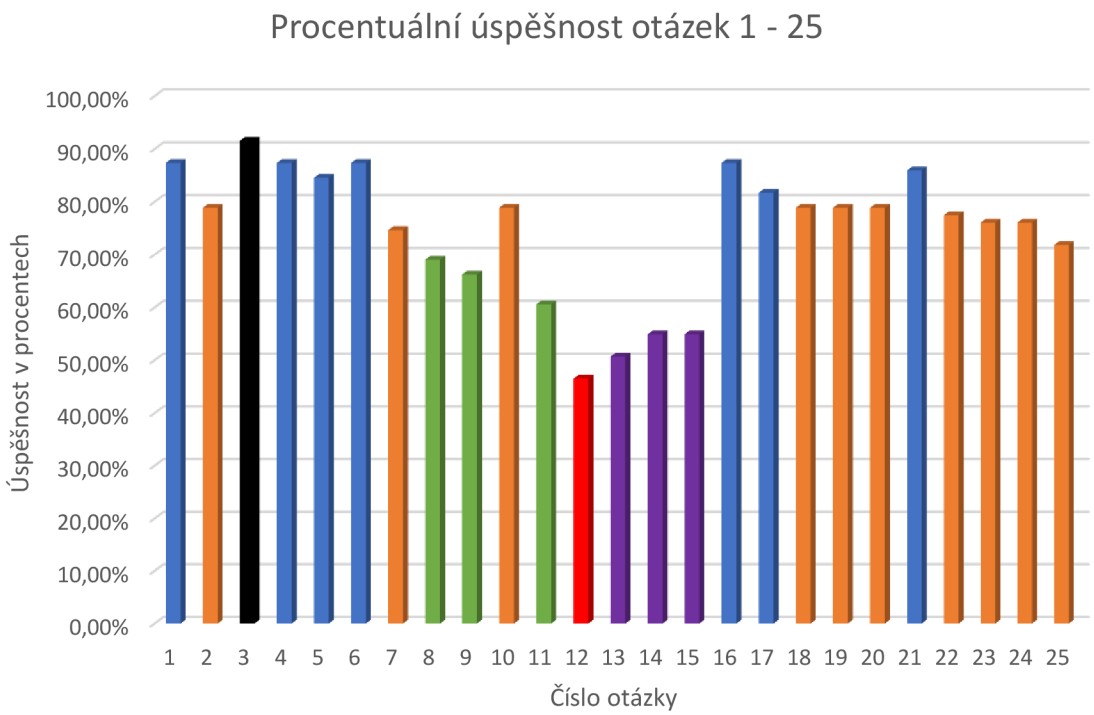
Otázky	9. Ročník
1.	7 919
2.	6 697
3.	32 005
4.	23 452
5.	15 691
6.	22 936
7.	1 028 071 702 528
8.	1 397 405 517 247 104 682 033 152
9.	909 377 607 891 473 342 964 601 076 981 440 190 281
10.	19 607 665 147 616 160 921 060 454 382 127 930 075 730 561 467 240
11.	10
12.	12
13.	64
14.	20
15.	1
16.	389
17.	667
18.	9
19.	27
20.	180
21.	22
22.	58
23.	2
24.	2
25.	64
26.	$(497, 497)$
27.	$(42, 79)$
28.	6 320 537
29.	Jejich násobek je roven součtu prvočísel (p) a (q)
30.	Násobení čísel se zaokrouhlením v řádu jednotek

Tabulka 21: Výsledky studenta 9. ročníku za čas 60 min a 19 s

Jak již bylo dříve zmíněno, dotazník je zformován do dvou částí, kde jednu z nich můžeme považovat čistě za početní bez znalostí algoritmu RSA, a právě druhou část založenou pouze na znalostech algoritmu RSA. K První části tohoto dotazníku náleží i naše první hypotéza.

H1. Žáci s lepšími znalostmi v matematice se ve větší míře mnohem lépe orientovali v početních operací systému RSA než žáci, kteří nemají tak dobré znalosti.

Abychom potvrdili nebo vyvrátili danou hypotézu, tak jsme získané výsledky z dotazníků vynesli do sloupcového grafu s tím, že jsme si vypočítali procentuální úspěšnost všech zúčastněných $\left(\frac{počet\ těch, kteří\ správně\ odpověděli}{počet\ všech, kteří\ psali\ výzkumný\ dotazník} \cdot 100\%\right)$. Graf jsme si barevně rozdělili do 6 barev, kde černá barva je úspěšnost nad 90%, modrá nad 80%, oranžová nad 70%, zelená nad 60%, fialová nad 50% a červená nad 40%. Z těchto dat lze poté vidět, že nejobtížnější otázkou pro žáky byla otázka 12 (v této otázce mimochodem zaznělo až 24 různých odpovědí).

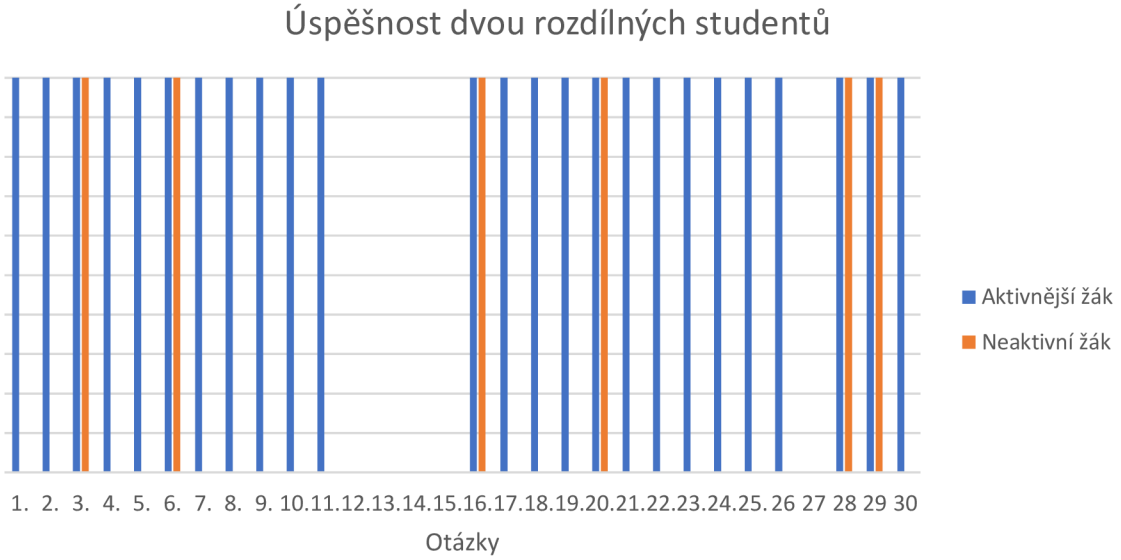


Tabulka 22: Procentuální úspěšnost otázek u dotazníku

Domnívali jsme se, že žáci s lepšími výsledky a větší aktivitou v klasické hodině matematiky budou mít i lepší výsledky při vypracovávání dotazníku na algoritmus RSA. V této fázi je zapotřebí zmínit, že z obou ročníků byl udělán výběr za pomoci pedagogů matematiky na Základní škole Hodonín, Očovská 1, příspěvková organizace a výzkumu se tak zúčastnili

nejhůře ti, jejichž průměr z matematiky byl maximálně 3,3 (nemohli jsme zvolit přísnější kritérium, neboť bychom nezískali dostatečný počet respondentů do našeho výzkumu – i tak pracujeme poměrně s malou skupinou).

K potvrzení, nebo vyvrácení této hypotézy bylo však zapotřebí vyhodnotit žáky nejen dle výsledků dotazníku, ale i podle jejich znalostí z hodin matematiky (založeno na subjektivním vnímání vyučujícího) a porovnat to právě s výsledky těch, jejichž aktivita a ohodnocení v hodinách matematiky není na takové úrovni, jako ostatních spolužáků podílejících se na výzkumu. Pro názorné srovnání jsem vybral 2 respondenty, kde právě jeden je aktivnější a „úspěšnější“ v matematice než druhý. Výsledky tohoto porovnání můžete vidět v grafu níže.



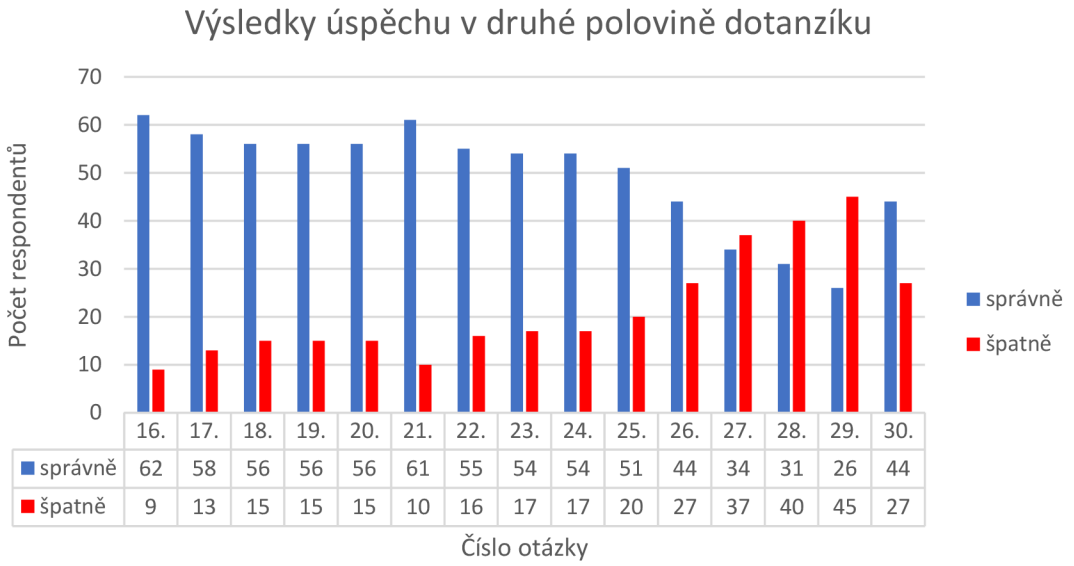
Tabulka 23: Úspěšnost dvou studentů v celém dotazníku

Z tohoto grafu lze pěkně zcela vidět, že hypotézu **H1** můžeme přijat a potvrdit, neboť aktivnější žák byl úspěšnější v dotazníku přesně u 19 otázek (dovolujeme si poukázat na fakt, že jsme srovnávali spolužáky, nikoliv žáky z jiných ročníků) a nejednalo se však jistě pouze o jeho znalosti, ale i aktivní přístup během dvouhodinových bloků. Takto jsme si namátkou vždy vybrali 2 respondenty a porovnali jejich odpovědi. Ve všech případech byl úspěšnější aktivní žák s lepším průměrem než žák pasivní.

Další z našich hypotéz pojednávala o dílčích krocích algoritmu RSA, neboli o druhé polovině výzkumného dotazníku, který respondenti vyplňovali.

H2. Aktivnější žáci na všech dvouhodinových blocích s panem učitelem měli větší přehled o dílčích krocích při správné tvorbě klíče a posílání zpráv než žáci, kteří byli ve dvouhodinových blocích pasivní.

Prvně si zde vysvětleme, že se opět jedná o subjektivní pohled toho, kdo je z žáků aktivní a kdo nikterak (pasivní). Opět si zde znázorníme úspěšnost otázek k celku všech respondentů. Tentokrát však nebudeme volit procentuální závislost, nýbrž si jen pro přehled znázorníme úspěšnost a neúspěšnost v jednotlivých otázkách v druhé polovině dotazníku.



	16.	17.	18.	19.	20.	21.	22.	23.	24.	25.	26.	27.	28.	29.	30.
správně	62	58	56	56	56	61	55	54	54	51	44	34	31	26	44
špatně	9	13	15	15	15	10	16	17	17	20	27	37	40	45	27

Tabulka 24: Počet správných a špatných odpovědí v druhé polovině dotazníku

Zde lze vidět, že žáci nejvíce chybovali právě v samotných otázkách na teorii, která byla v posledních 5 otázkách. Avšak zde chybovali všichni žáci, neboť samotné teorii a vlastně principu RSA už nevěnovali pozornost a mám pocit, i ze samotných bloků, že jí rozumět ani nechtěli.

Když se ale zaměříme na naši hypotézu **H2**, je zcela nutné ji vyvrátit a nepřijmout. Důvodem je nevhodně vytvořený dotazník, který měl v této fázi být vytvořen otázkami otevřenými, neboť při vyplňování dotazníků mnoho žáků zkoušelo neustále nějaké varianty příkazů, dokud jim nevycházel aspoň jeden z možných nabízených výsledků (bohužel tohoto problému jsme si všimli pozdě). Nelze tedy z dotazníku rozhodnout, zda opravdu aktivnější

žáci měli větší přehled o funkčnosti algoritmu RSA, pokud více jak polovina neodpověděla správně na posledních pár otázek a snažili spíše vylučovací metodou určit správnou odpověď u zbývajících otázek. Navíc si dovolujeme zmínit, že u otevřených otázek byl ze žákovských odpovědí mnohokrát vidět nezájem a otrávenost, že se vůbec na nějakém výzkumu musí podílet.

Poslední hypotézou jsme si chtěli ověřit, jak moc využívají žáci podílející se na výzkumu ICT, proto byla hypotéza stanovena jako

H3. Žáci po dvouhodinových blocích s panem učitelem využili ve větší míře mnohem lépe výpočetní techniku než žáci, kteří se odmítali naučit pracovat s ICT s využitím v matematice.

Základním faktorem je zde to, že žáci byli poměrně nuceni využívat ICT, neboť bez této možnosti by dotazník v požadovaném čase nestihli vyplnit. Bohužel musím dodat, že mnozí se i tak obraceli na možnost kalkulačky než na Wolfram Cloud, ve kterém jsme ve dvouhodinových blocích pracovali. Tomu přisuzujeme i výsledky, které někteří byli schopni napsat, nebo dokonce čas, za který to někteří z dotazovaných zvládli „vyřešit“. Důležité je zde zdůraznit, že Wolfram Cloud byl pro žáky jen momentální záležitostí a jeho využití našli jen při vyplňování dotazníku, nikoliv už však při klasické výuce matematiky (dokonce někteří z kantorů si připomenuli práci v tomto softwarovém prostředí a jiný platformách k obohacení výuky). Je tedy na místě se ptát, zda hypotézu přijat a akceptovat na základě složitosti dotazníku, nebo hypotézu nepřijat a odmítnout s tím, že po dotazníku nikdo již nevyužíval ICT o nic víc, než využíval do té doby. Na základě získaných dat a dojmů, které panovaly při dvouhodinových blocích a vyplňování dotazníku, bych si dovolil hypotézu **H3** vyvrátit a nepřijat.

2.3. Využité programy

K vypracování dotazníku byly žáky využity softwary jako Wolfram Cloud a klasická kalkulačka (kterou nabízí operační systém). U kalkulačky nabízené operačním systémem se žáci potýkali s problémy, jako jsou mocnina, odmocnina a dělení se zbytkem. I když jsme si všechny z těchto 3 matematických operací ukazovali v blocích, tak je zřejmě žáci zapomněli, a při vypracovávání dotazníku jim dělali značné problémy. Na rozdíl od těch, kteří volili mnou doporučovaný Wolfram Cloud, kde se naučili základní příkazy, a hlavně nezapomněli přihlašovací údaje ke svému účtu.

V prostředí Wolfram Cloud žáci využili pro samotné šifrování/dešifrování následujících příkazů (příkazy pro samotné matematické operace jsme si již zobrazili v tabulkách u ukázkových 12 příkladů).

Příkaz	**Význam**
$p = RandomPrime[10^2; 10^3]$ $q = RandomPrime[10^2; 10^3]$	Generování náhodně velkého prvočísla v daném rozsahu
$PrimeQ[p]$ $PrimeQ[q]$	Ověření určeného prvočísla
$n = p * q$	Součin dvou předem zjištěných prvočísel (modulo)
$e = RandomInteger[10^2; 10^3]$	Generování náhodně velkého celého čísla v daném rozsahu
$fi = (p-1) * (q-1)$	Nalezení Eulerovy funkce (počet nesoudělných čísel)
$GCD[e, fi]$	Nejmenší společný násobek čísla e a čísla fi
$d = PowerMod[e, -1, fi]$ $d = ModularInverse[e, fi]$	Nalezení dešifrovacího exponentu d
$Z =$	Naše zpráva skrytá v arabských číslech
$sif = PowerMod[Z, e_p, n_p]$	Naše zpráva zašifrovaná pomocí příjemcova veřejného klíče
$des = PowerMod[sif, d_s, n_s]$	Dešifrovaná zpráva pomocí našeho soukromého klíče

2.4. Závěr praktické části

Přínosem této diplomové práce je rozhodně její teoretická část, která pojednává o zjednodušení vysokoškolského učiva algoritmu RSA do úrovně ZŠ, a uchopení učiva do takové míry, aby mu rozuměli i mladší žáci. Snažíme se zde poukázat na to, že základní matematické dovednosti nabyté na ZŠ mají větší rozsah, než si žáci mohou myslet, a opravdu je důležité, aby neopomíjeli matematiku jako takovou. Bavíme se tu o základech asymetrického šifrování a důkazech, které systém RSA musí splňovat, aby správně fungoval.

Navíc jsme práci koncipovali tak, aby sloužila jako průvodní text těm, kteří by se o systém RSA mohli někdy zajímat. Snažili jsme se tedy práci psát v tom duchu, aby vše bylo srozumitelné a nikterak složité pro čtenáře, proto jsme se často vyhýbali složitým důkazům, velkým početním operacím a složitým definicím, které bychom museli zdlouhavě vysvětlovat (na to jsou psány již jiné práce). Dovoluji si říct, že práce je zcela srozumitelná pro šikovnějšího žáka střední školy.

Po teoretické části jsme se dali na část praktickou, kde jsme zkoumali dva poslední ročníky základní školy. Cílem této praktické části bylo porovnat znalosti základních matematických operací použitých při systému RSA a porovnat využití výpočetní techniky při algoritmu RSA. Oba tyto cíle jsme v práci naplnili. K porovnání matematických znalostí nám slouží dotazník, který žáci vyplňovali, a veškeré hodnocení jsme zmínili v kapitole „Výsledky dotazníku“. Co se týče porovnání výpočetní techniky při algoritmu RSA, tak jsme zde bohužel narazili na problém, neboť dotazník byl vytvořen tak, že vlastně nutil žáky pracovat s výpočetní technikou, neboť by jinak nestihli dotazník včas vyřešit. Možná právě proto některé z respondentů dotazník spíše obtěžoval, a celý výzkum tak „sabotovali“ svými náhodnými výsledky. I přes tento nezdar však žáci pracovali s ICT, ať už s volně přístupným softwarem Wolfram Cloud, nebo jen se systémovou kalkulačkou ve školní technice.

3. Seznam použitých zdrojů:

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

[2] BÁLKOVÁ, Ľubomíra *RSA (Úvod do kryptologie)* [online]. FJFI ČVUTI, Praha, 15. dubna 2010 [cit. 2023-03-25] https://kmlinux.fjfi.cvut.cz/~balkolub/Vyuka/slajdy_RSA.pdf

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

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

[5] DURČÁK, Pavel. *Symetrické a asymetrické šifrování* [online]. 18.9.2018 [cit. 2023-03-26]. Dostupné z: https://www.napocitaci.cz/33/symetricke-a-asymetricke-sifrovani-uniqueidgOkE4NvrWuNY54vrLeM677jX7sp3Lu-ZpLpGVMy1prA

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

[7] RIVEST, R. L., SHAMIR, A., ADLEMAN, L.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM 21, 1978 , str. 120 – 126.

[8] OPRŠAL, Jakub. *RSA a teorie čísel* [online]. In: . s. 29-31 [cit. 2023-03-25]. Dostupné z: https://prase.cz/library/RSAJO/RSAJO.pdf

[9] AMIROVÁ, Kamilla. *Asymetrické algoritmy: RSA* [online]. 2007 [cit. 2023-03-26]. Dostupné z: https://sifrovani.fd.cvut.cz/asym_algo.html

[10] POKORNÝ, Michal a Martin MAREŠ. Teorie čísel. In: *Korespondeční seminář z programování* [online]. [cit. 2023-04-12]. Dostupné z: https://ksp.mff.cuni.cz/kucharky/teorie-cisel/

[11] RŮŽICA, Lukáš. *RSA – Šifrovací metoda s veřejným klíček* [online]. Olomouc, 2019 [cit. 2023-02-21]. Bakalářská práce. Univerzita Palackého, Pedagogická fakulta. Doc. RNDr. Tomáš Zdráhal, CSc. Dostupné z: https://library.upol.cz/arl-upol/cs/csg/?repo=upolrepo&key=61868618051

[12] Příklad na Euklidův algoritmus. In: *Euklidův algoritmus* [online]. Ostrava: Vysoká škola Báňská [cit. 2023-03-26]. Dostupné z: https://mi21.vsb.cz/sites/mi21.vsb.cz/files/unit/eukliduv_algoritmus.pdf

[13] Malá Fermatova věta. *Wikidot* [online]. [cit. 2023-03-23]. Dostupné z: http://hariprasad-mathematics.wikidot.com/

[14] Malá Fermatova věta. In: *Algoritmy* [online]. [cit. 2023-03-23]. Dostupné z: https://www.algoritmy.net/article/59/Mala-Fermatova-veta

[15] Modulární aritmetika, Malá Fermatova věta*.: s účinností od 10. listopadu 2014* [online]. Ústav aplikované matematiky ČVUT v Praze, Fakulta dopravní, [cit. 2023-03-25]. Dostupné z: https://zolotarev.fd.cvut.cz/static/mag/mag-2014-04-slides.pdf