Ekonomická fakulta
Faculty of Economics
Jihočeská univerzita v Českých Budějovicích
University of South Bohemia in České Budějovice

Jihočeská univerzita v Českých Budějovicích
Ekonomická fakulta
Katedra aplikované matematiky a informatiky

Bakalářská práce

RSA algoritmus a jeho využití v elektronické komunikaci s orgány státní správy

Vypracoval: Stanislav Froula
Vedoucí práce: Mgr. Lenka Činčurová

České Budějovice 2016

JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH
Fakulta ekonomická
Akademický rok: **2014/2015**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Stanislav FROULA**
Osobní číslo:	**E13208**
Studijní program:	**B6208 Ekonomika a management**
Studijní obor:	**Obchodní podnikání**
Název tématu:	**RSA algoritmus a jeho využití v elektronické komunikaci s orgány státní správy**
Zadávající katedra:	**Katedra aplikované matematiky a informatiky**

Zásady pro vypracování:

Cílem práce je zhodnotit zabezpečení elektronické komunikace s využitím RSA algoritmu. Součástí práce je teoreticky popsat základní princip fungování algoritmu a šifrování s veřejným klíčem, předložit hlavní výhody a nevýhody jeho použití a uvést konkrétní seznam institucí, které používají elektronický podpis k ověření autenticity odesílatele.

Metodický postup:

1. Studium odborné literatury - literární přehled - základní princip fungování a využití RSA algoritmu a šifrování s veřejným klíčem.
2. Popis základního principu a fungování šifrovacího algoritmu, uvedení konkrétních příkladů na zjednodušeném modelu.
3. Zhodnocení praktické využitelnosti algoritmu, uvedení konkrétního seznamu institucí a odvětví, kde se využívá.
4. Vlastní dotazníkové šetření zjišťující informovanost různých skupin obyvatel z hlediska bezpečnosti odesílání důvěrných dat.
5. Závěry a obecná doporučení.

Rozsah grafických prací: **dle potřeby**

Rozsah pracovní zprávy: **40 - 50 stran**

Forma zpracování bakalářské práce: **tištěná**

Seznam odborné literatury:

1. **Gathen, J., & Gerhard, J. (2003).** *Modern Computer Algebra, Second Edition.* **Cambridge, United Kingdom: Cambridge University Press.**
2. **Křížek, M., Somer, L., & Šolcová, A. (2009).** *Kouzlo čísel. Od velkých objevů k aplikacím.* **Praha: Academia.**
3. **Tlustý, P. (2003).** *Lineární algebra a její aplikace.* **České Budějovice: Jihočeská univerzita v Českých Budějovicích.**
4. **Tlustý, P. (2006).** *Obecná algebra pro učitele.* **České Budějovice: Jihočeská univerzita v Českých Budějovicích.**

Vedoucí bakalářské práce: **Mgr. Lenka ČINČUROVÁ**
Katedra aplikované matematiky a informatiky

Datum zadání bakalářské práce: **9. ledna 2015**

Termín odevzdání bakalářské práce: **15. dubna 2016**

doc. Ing. Ladislav Rolínek, Ph.D.
děkan

L.S.

JIHOCESKÁ UNIVERZITA
V ČESKÝCH BUDĚJOVICÍCH
EKONOMICKÁ FAKULTA
Studentská 13 (26)
370 05 České Budějovice

prof. RNDr. Pavel Tlustý, CSc.
vedoucí katedry

V Českých Budějovicích dne 12. března 2015

Prohlášení:

Prohlašuji, že svoji bakalářskou práci jsem vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47 zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích dne …… …….....

Stanislav Froula

Poděkování

Tímto bych rád poděkoval Mgr. Lence Činčurové za odborné vedení, vstřícný přístup, ochotu a cenné rady při zpracování mé bakalářské práce. Dále bych chtěl poděkovat rodině za pochopení a obrovskou podporu během studia.

Obsah

1 Úvod

Rozšíření internetu a elektronického obchodování s sebou přineslo problém v podobě zabezpečení přenášených informací a zajištění soukromí uživatelů elektronické komunikace. Každý den je elektronicky přenášeno a skladováno velké množství osobních a citlivých informací. Za účelem jejich ochrany před nežádoucím přístupem či zneužitím se používají různé kryptografické metody. Jednou z těchto kryptografických metod je i RSA algoritmus, jehož princip a využití je hlavním tématem této bakalářské práce.

V první části práce je čtenář seznámen se základními pojmy kryptografie, elektronického podpisu a samotného RSA algoritmu. Je vysvětlen matematický princip algoritmu, který je následně demonstrován na konkrétním zjednodušeném příkladu. Součástí teoretické části je mimo jiné i zhodnocení bezpečnosti RSA a uvedení jeho hlavních výhod a nevýhod. Praktická část se zabývá dotazníkovým šetřením zjišťujícím informovanost uživatelů internetového bankovnictví ohledně zásad jeho bezpečného využívání. Byla stanovena následující výzkumná otázka: „Jaká je všeobecná informovanost uživatelů iternetového bankovnictví o bankami doporučených bezpečnostních zásadách užívání internetového bankovnictví?“. Na základě této výzkumné otázky byly stanoveny čtyři hypotézy, jejichž potvrzení nebo vyvrácení je uvedeno v závěru práce.

Hypotéza č. 1: Minimálně 2/3 respondentů nečetlo bezpečnostní zásady svých bank.

Hypotéza č. 2: Pohlaví nemá vliv na informovanost o bezpečnostních zásadách (rozdíl míry informovanosti nepřesahuje 5 %).

Hypotéza č. 3: Se zvyšujícím se vzděláním roste míra informovanosti o bezpečnostních zásadách.

Hypotéza č. 4: Se zvyšujícím se věkem klesá míra informovanosti o bezpečnostních zásadách.

2 Literární rešerše

2.1 Základní pojmy

Kryptologie je věda, která se zabývá šifrováním ze všech úhlů pohledu. Jejími hlavními disciplínami jsou kryptografie a kryptoanalýza.

Kryptografie je nauka o metodách utajování obsahu zpráv převodem do podoby, která je čitelná jen se speciální znalostí. Někdy je pojem obecněji používán pro vědu o čemkoli spojeném se šiframi jako alternativa k pojmu kryptologie.

Kryptoanalýza je věda zabývající se metodami získávání obsahu šifrovaných zpráv bez přístupu k tajným informacím, především k získávání tajného klíče, který je za normálních okolnostní potřeba. V netechnickém kontextu je používán tento termín obecně pro prolamování kódu. Je vlastně opakem kryptografie, která šifry vytváří.

Šifrování je proces transformace informace do tvaru, který je nesrozumitelný pro kohokoliv kromě určeného příjemce.

Dešifrování je proces transformace šifrované informace do původního tvaru srozumitelného pro kohokoliv.

K šifrování a dešifrování je obvykle potřeba použít specifickou tajnou informaci – tzv. **klíč**. Některé kryptografické mechanismy používají jeden stejný klíč pro šifrování i dešifrování zároveň, jiné mechanismy používají pro šifrování jeden klíč a pro dešifrování jiný. Tato problematika bude upřesněna v následujícím textu.

Kryptografický algoritmus je matematická funkce používaná pro šifrování a dešifrování.

Plaintext, neboli čistý text, je původní informace/zpráva, která je obecně srozumitelná.

Cipher, neboli šifra je srozumitelná informace transformovaná do informace srozumitelné pouze určitému subjektu.

(Kunderová, n.d.; Jančařík, 2009b)

2.2 Kryptografie

Kryptografie je věda, která se zabývá psaním „tajným kódem“. Využívá matematické metody pro potřeby ochrany dat před jejich zneužitím. Jedná se o starobylé umění –

první doložené písemné použití kryptografie sahá až do roku 1900 př. n. l., kdy egyptský písař použil v nápisu nestandardní hieroglyfy. Někteří odborníci tvrdí, že kryptografie vznikla spontánně ve stejné době jako samotné psaní. Využití kryptografie je opravdu široké, od diplomatických misí až po bitevní plány v období válek. Není proto překvapující že po rozsáhlém rozvoji informačních technologií vznikly zcela nové formy kryptografie. Posíláme-li data přes nedůvěryhodné médium, například internet, je nezbytné tato data chránit – je nutné využít kryptografických metod. (Kessle, 2016; Oborová zdravotní pojišťovna, n.d.)

2.2.1 Hlavní cíle kryptografie

Mezi hlavní cíle moderní kryptografie patří zajištění:

- **Autentizace** – Proces prokazování totožnosti. Autentizace může probíhat na základě znalosti (heslo), vlastnictví (klíč, kreditní karta) nebo charakteristických vlastností (biometrické informace − např. otisky prstů).
- **Důvěrnosti** – Udržení obsahu zprávy v tajnosti. Zabezpečení této služby je nejdůležitějším cílem kryptografie.
- **Integrity** – Zamezení neoprávněné modifikaci dat. Modifikací se rozumí např. smazání části dat, vložení nových dat nebo substituce části stávajících dat jinými daty. Se zamezením neoprávněné modifikaci souvisí i schopnost tuto modifikaci detekovat.
- **Autorizace** – Potvrzení původu dat, tedy prokázání, že data vytvořil (je jejich autorem) skutečně ten, o němž se domníváme, že je autorem.
- **Nepopiratelnosti** – Jedná se o jistotu, že autor dat nemůže své autorství popřít.

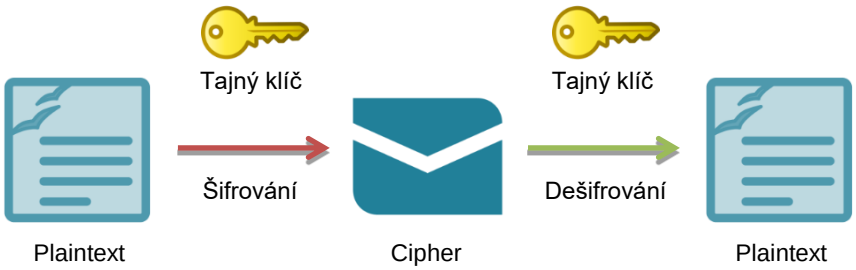
(Mendelova univerzita v Brně, n.d.)

2.2.2 Symetrická kryptografie

Symetrická kryptografie využívá jednoho tajného klíče pro šifrování i dešifrování. Jak můžeme vidět na Obrázek 1, odesílatel zprávy použije klíč k zašifrování zprávy (plaintext) a odešle šifru (cipher) příjemci. Aby příjemce získal původní plaintext, použije k dešifrování zprávy naprosto stejného klíče. Hlavní výhodou symetrických algoritmů je jejich rychlost a nízká výpočetní náročnost. (Kessle, 2016; Earchivace, 2014)

Největší nevýhodou je problém distribuce klíče neboli fakt, že tajný klíč musí být sdílen s každým, kdo má zprávu šifrovat či dešifrovat. Musí tedy již předem proběhnout určitá forma komunikace ke sdílení klíče. Mezi nejpoužívanější symetrické šifrovací algoritmy současnosti patří algoritmus AES (Advanced Encryption Standard), který vytlačil předchozí oblíbený 3DES (Digital Encryption Standard), jako další příklady lze uvést IDEA, Twofish, Blowfish, CAST a další. (Kessle, 2016; Earchivace, 2014)

Obrázek 1: Symetrické šifrování



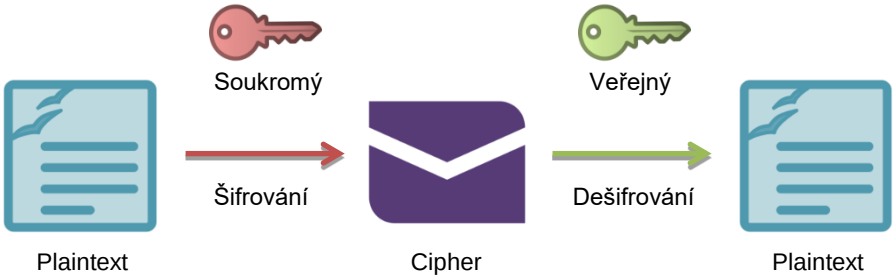
Zdroj: Vlastní zpracování

2.2.3 Asymetrická kryptografie

Asymetrická kryptografie je jedním z nejvýznamnějších objevů v kryptografii za posledních 300–400 let. Využívá totiž dva klíče – veřejný a soukromý. Tyto klíče dohromady tvoří klíčový pár a jsou matematicky příbuzné, ovšem znalost jednoho klíče nedovoluje snadné vypočítání klíče druhého. Veřejný klíč je dostupný každému, zato soukromý klíč musí majitel udržovat v tajnosti. V zásadě platí, že při generování klíčového páru se nejprve generuje soukromý klíč a až poté klíč veřejný. Důležité je, že nezáleží na tom, který klíč je aplikován jako první. Pro to, aby proces fungoval správně, jsou zapotřebí oba dva. (Kessle, 2016; Earchivace, 2014)

Asymetrické šifry v kombinaci s dalšími technologiemi jsou používány zejména pro šifrování, digitální podepisování a ověřování digitálních podpisů či časových razítek. Nevýhodou asymetrické kryptografie ve srovnání se symetrickou je však rychlost šifrování. Mezi nejvyužívanější asymetrické algoritmy patří **RSA** (Rivest, Shamir, Adleman), dále ECC (Elliptic Curve Cryptography) nebo DSA (Digital Signature Algorithm). (Kessle, 2016; Earchivace, 2014)

Obrázek 2: Asymetrické šifrování

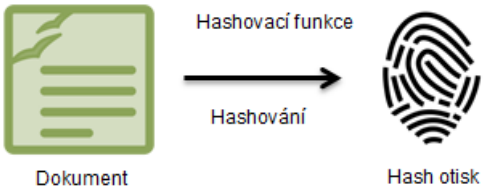


Zdroj: Vlastní zpracování

2.2.4 Hashovací funkce

Hashovací funkce, nazývaná také „jednosměrné šifrování“, je speciální matematicko-kryptografickou funkcí, která v jistém smyslu nepoužívá žádné klíče. Místo toho vypočítá jednoznačný hash otisk zprávy (při aplikaci např. na soubor či email), který nelze použít reverzně – tzn., že z hashe nelze vytvořit původní zprávu. Hash otisk má podle použité funkce konstantní délku v bitech (např. 160 bitů). Další klíčovou vlastností otisku je zajištění neměnnosti (integrity) dokumentu. Pokud změníme byť jeden znak, dostaneme na výstupu úplně jiný hash otisk. Srovnáním původního a nového hashe lze jednoznačně dokázat, že byl dokument modifikován. V současné době je nejpoužívanější hashovací funkcí SHA, dále stojí za zmínku HMAC, RIPEMD a MD. (Jančařík, 2009a; Kessle, 2016; Earchivace, 2014)

Obrázek 3: Hashovací funkce



Zdroj: Vlastní zpracování

2.3 Elektronický podpis

Elektronický podpis je matematická metoda používaná k ověření pravosti a integrity zprávy, softwaru nebo elektronického dokumentu.

Zákon č. 227/2000 Sb. o elektronickém podpisu[1] definuje elektronický podpis jako „*údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě.*“ (ustanovení § 2 zákona o elektronickém podpisu)

Zákon mimo jiné upřesňuje používanou terminologii a definuje příslušné pojmy tak, aby byl odlišen stupeň důvěryhodnosti a bezpečnosti jednotlivých elektronických podpisů.

Elektronický podpis je svou podstatou elektronický ekvivalent vlastnoručního podpisu či razítka, nabízí ovšem větší vnitřní bezpečnost. Funguje na principu šifrování s veřejným klíčem, tedy asymetrického šifrování, které již bylo zmíněno výše. Cílem elektronického podpisu je vyřešit problém s manipulací a zosobňováním v elektronické komunikaci. (BusinessInfo, 2002)

Elektronický podpis umožňuje příjemci ověřit identitu podepisujícího – příjemce tedy bezpečně ví, kdo je autorem či odesílatelem zprávy. Příjemce má také jistotu, že zprávu nikdo v průběhu transportu nemodifikoval (tzn., ověřuje integritu zprávy), což ruční podpis může zajistit pouze s obtížemi. Mezi další výhody elektronického podpisu patří zaručení nepopiratelnosti zprávy – odesílatel nemůže popřít, že opravdu odeslal příslušnou zprávu s daným obsahem. (BusinessInfo, 2002)

V mnoha zemích, včetně České republiky, jsou elektronické podpisy připojené k datové zprávě rovnoprávným ekvivalentem vlastnoručního podpisu na písemném dokumentu. (I.CA, 2015)

2.3.1 Přehled právních předpisů a standardů pro elektronický podpis

- Směrnice 1999/93/EC Evropského parlamentu a Rady Evropské unie o zásadách Společenství pro elektronické podpisy;
- Zákon č. 227/2000 Sb. o elektronickém podpisu;
- Zákon č. 226/2002 Sb. (novela zákona č. 227/2000 Sb.);

[1] V České republice vstoupil zákon o elektronickém podpisu v platnost 1. října roku 2000. Zákon vychází ze Směrnice Evropského parlamentu a Rady 1999/93/ES. (Vondruška, 2004)

- Vyhláška č. 366/2001 Sb., o upřesnění podmínek stanovených v § 6 a 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu.

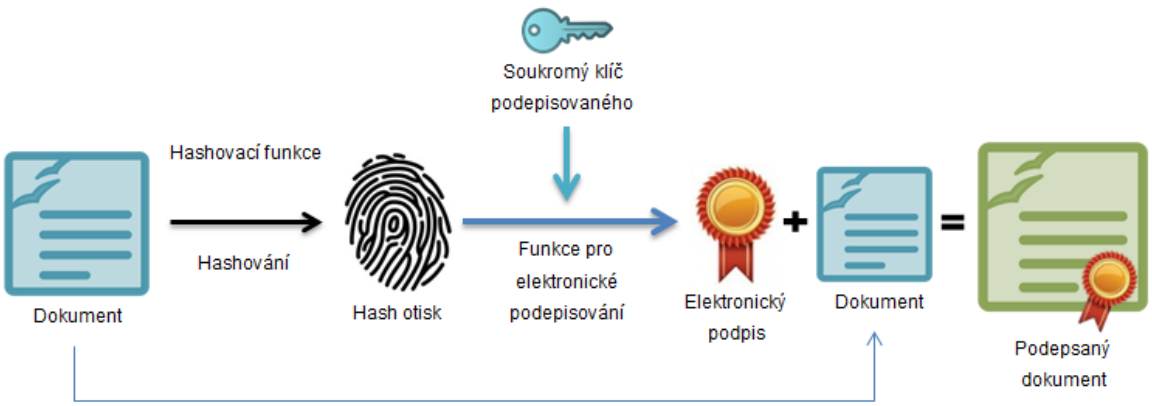
(BusinessInfo, 2002)

2.3.2 Vytvoření elektronického podpisu

Elektronický podpis si můžeme představit jako číselnou hodnotu zastoupenou sledem znaků a vypočtenou pomocí matematického vzorce. Vzorec závisí na dvou vstupech: na posloupnosti znaků, které zastupují podepisovaný elektronický dokument, a na tajném číslu – tzv. soukromém klíči odesílatele. (Entrust, 2001; BusinessInfo, 2002)

Vytvoření elektronického podpisu je proces, jenž probíhá ve dvou krocích. V prvním kroku vytvoříme hash otisk zasílaného elektronického dokumentu, který v druhém kroku zašifrujeme soukromým klíčem podepisovaného uživatele. Takto vytvořený elektronický podpis připojíme k odesílanému souboru, jehož je součástí. Software, který umí pracovat s funkcionalitou digitálního podpisu, dokáže rozeznat, že je daný soubor podepsaný. (Entrust, 2001; BusinessInfo, 2002)

Obrázek 4: Vytvoření elektronického podpisu



Zdroj: Vlastní zpracování

Při ověřování postupuje příjemce tak, že k dokumentu sám znovu vypočítá hash otisk a pomocí veřejného klíče odesílatele dešifruje elektronický podpis, čímž získá původní

otisk. Oba otisky porovná a zjistí, zda nebyl dokument pozměněn, tj. zda se skutečně jedná o dokument, který odesílatel napsal a podepsal. (Entrust, 2001; BusinessInfo, 2002)

2.3.3 Elektronický podpis a zaručený elektronický podpis

Elektronický podpis a zaručený elektronický podpis se z technického pohledu neliší způsobem vytvoření či ověřování, nýbrž svou úrovní bezpečnosti. Důvěryhodnost podpisu se skládá ze spolehlivosti zařízení a metod, které byly při jeho vytvoření použity. V případě zaručeného elektronického podpisu jsou požadavky na bezpečnost vyšší. To se odráží v akreditaci – posuzování provozních podmínek certifikačních autorit, a zároveň při certifikaci produktů – posuzování bezpečnosti provozních zařízení pro vytváření podpisu. Podle zákona je zaručeným elektronickým podpisem ten elektronický podpis, který splňuje následující požadavky:

- *je jednoznačně spojen s podepisující osobou,*
- *umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,*
- *byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,*
- *je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat.*

(ustanovení § 2 zákona o elektronickém podpisu)

Pro nezaručený elektronický podpis jsou bezpečnostní požadavky podstatně nižší. (Národný bezpečnostný úrad, 2015)

V České republice jsou celkem 3 certifikační autority, které mohou vydat certifikát k elektronickému podpisu (viz tabulka 1).

Tabulka 1: Certifikační autority v ČR

	Poskytoval certifikačních služeb	Kvalifikované služby
1.	**První certifikační autorita, a. s.**	Vydávání kvalifikovaných certifikátů
	IČO 26439395, Podvinný mlýn 2178/6, PSČ 190 00 Praha 9	Vydávání kvalifikovaných systémových certifikátů;
		Vydávání kvalifikovaných časových razítek;

		Vydávání prostředků pro bezpečné vytváření elektronických podpisů.
2.	**Česká pošta, s. p.**	Vydávání kvalifikovaných certifikátů;
	IČO 47114983, Olšanská 38/9, PSČ 225 99 Praha 3	Vydávání kvalifikovaných systémových certifikátů;
		Vydávání kvalifikovaných časových razítek.
3.	**eIdentity a. s.**	Vydávání kvalifikovaných certifikátů;
	IČO 27112489, Vinohradská 184/2396, PSČ 130 00 Praha 3	Vydávání kvalifikovaných systémových certifikátů;
		Vydávání kvalifikovaných časových razítek.

Zdroj: Vlastní zpracování podle MVCR (2015)

Úkolem Certifikační autority je ověřit totožnost žadatele o certifikát a jednoznačně svázat jeho identifikaci s daty pro tvorbu elektronického podpisu prostřednictvím certifikátu, který žadateli vydává. Tyto autority tudíž plní dvě základní funkce:

- certifikační – zaručující, že deklarovaný veřejný klíč přísluší dané osobě,
- validační – potvrzující platnost certifikátu. (I.CA, 2015)

Obdobně jako v případě občanských průkazů mají také certifikáty určitou platnost, zpravidla 1 rok. Před uplynutím této doby je možné elektronickou cestou požádat o vydání certifikátu následného v případě, že nedošlo ke změně údajů, na základě kterých byl vydán prvotní certifikát. Certifikát obsahuje informace týkající se uživatele, doby platnosti klíče, informace o používání klíče a informace o certifikační autoritě. (I.CA, 2015)

2.3.4 Využití elektronického podpisu

Využitím zaručeného elektronického podpisu lze elektronicky komunikovat nejen s orgány veřejné správy, tedy zdravotními pojišťovnami, s krajskými, městskými a obecními úřady i soudy, ale také v komerční sféře. (iPodnikatel.cz, 2011)

Možnosti využití elektronického podpisu:

- **Veřejná správa:**
  - při zasílání datové zprávy prostřednictvím datových schránek;
  - při zasílání elektronických podání úřadům prostřednictvím e-podatelen;

- při podávání daňových přiznání prostřednictvím aplikace EPO (Daňový portál);
- při povinném kontrolním hlášení DPH;
- při zasílání dokumentů České správě sociálního zabezpečení;
- při zasílání dokumentů v rámci projektu e-Customs[2];
- při žádostech o dotace EU podávaných prostřednictvím aplikace eAccount CzechInvest;
- při žádostech o výpisy z Rejstříku trestů;
- při podávání hlášení prostřednictvím ISPOP[3];
- při vyřizování jednotlivých agend na Magistrátu hl. m. Prahy a úřadech městských částí prostřednictvím portálu praha.eu;
- při odesílání jednotných registračních formulářů (JRF) pro podání Živnostenskému rejstříku;
- při podávání návrhů na zápis nebo změnu zapsaných údajů do Obchodního rejstříku;
- při odesílání formulářů resortu MPSV;
- při elektronickém podávání přihlášek Úřadu průmyslového vlastnictví;
- při odesílání formulářů prostřednictvím Portálu farmáře – Ministerstvo zemědělství;
- při elektronické komunikaci s VZP.

(I.CA, 2015)

- **Komerční sféra:**
  - při obchodování na trhu s elektřinou a plynem;
    - ČEPS, a.s. prostřednictvím elektronického portálu Damas;
    - JAO - Joint Allocation Office[4];
    - Operátor trhu (OTE, a.s.);
    - Organizátor krátkodobého trhu s elektřinou (OKTE, a.s., portál ISOT, ISZO);

[2] Bezpapírové celní prostředí napříč celou Evropou (NCTS – elektronická komunikace mezi deklaranty, Celní správou ČR a zeměmi EU a ESVO, eDovoz, vývoz). (I.CA, 2015)
[3] Integrovaný systém plnění ohlašovacích povinností, tj. ohlašovacích povinností z oblasti životního prostředí. (I.CA, 2015)
[4] Pro usnadnění vnitřního trhu s elektřinou v Evropské unii byl fúzí společností CAO a CASC.EU vytvořen společný úřad pro alokaci přeshraničních přenosů kapacit. (I.CA, 2015)

- CASC.EU, CAO;
- MAVIR Hungarian Independant Transmission Operator Company Ltd., Hungary;
- SEPS Slovenská elektrizačná sústava, a.s., Slovak Republic;

➢ při elektronické komunikaci se zdravotními pojišťovnami;
➢ pro komunikaci s ČNB (cenné papíry);
➢ pro elektronické tržiště Gemin.cz.

(I.CA, 2015)

- **Další použití elektronického podpisu:**
  - ➢ při ukládání dokumentů v systémech elektronické spisové služby a v elektronických archivech (PDF);
  - ➢ při zasílání elektronických faktur, dodacích listů a jiných účetních dokladů;
  - ➢ při podepisování e-mailových zpráv;

(I.CA, 2015)

Institucí využívající elektronický podpis je velké množství, příklady těchto institucí jsou k dispozici v následující tabulce. Jedná se o příklady bank, finančních úřadů a zdravotních pojišťoven v České republice.

Tabulka 2: Instituce používající elektronický podpis

Banky	
Air Bank	Hráského 2231/25
	Praha 11
Citibank	Bucharova 2641/14
	158 02 Praha 5
Česká spořitelna	Olbrachtova 1929/62
	140 00 Praha 4
Equa bank	Amazon Court, Karolinská 661/4
	186 00 Praha 8
Fio banka	V Celnici 1028/10
	117 21 Praha 1
GE Money Bank	Vyskočilova 1422/1a
	140 28 Praha 4
Komerční banka	Na Příkopě 33 čp. 969
	114 07 Praha 1

mBank	Jugoslávská 1
	120 00 Praha 2
Raiffeisenbank	Hvězdova 1716/2b
	140 78 Praha 4
Sberbank CZ	Na Pankráci 1724/129
	140 00 Praha 4
UniCredit Bank	Na Příkopě 858/20
	111 21 Praha 1
Česká národní banka	Na Příkopě 28
	115 03 Praha 1
Finanční úřady	
Finanční úřad pro hlavní město Prahu	Štěpánská 619/28
	111 21 Praha 1
Finanční úřad pro Středočeský kraj	Žitná 12
	120 00 Praha 2
Finanční úřad pro Jihočeský kraj	Mánesova 1803/3a
	371 87 České Budějovice
Finanční úřad pro Plzeňský kraj	Hálkova 14
	305 72 Plzeň 3
Finanční úřad pro Karlovarský kraj	Krymská 2a
	360 01 Karlovy Vary
Finanční úřad pro Ústecký kraj	Velká Hradební 61
	400 21 Ústí nad Labem-Město
Finanční úřad pro Liberecký kraj	1. máje 97
	460 02 Liberec
Finanční úřad pro Královéhradecký kraj	Horova 17
	500 02 Hradec Králové
Finanční úřad pro Pardubický kraj	Boženy Němcové 2625
	530 02 Pardubice I
Finanční úřad pro Kraj Vysočina	Tolstého 2
	586 01 Jihlava
Finanční úřad pro Jihomoravský kraj	náměstí Svobody 4
	602 00 Brno
Finanční úřad pro Olomoucký kraj	Lazecká 545/22
	779 11 Olomouc
Finanční úřad pro Moravskoslezský kraj	Na Jízdárně 3162/3
	709 00 Ostrava
Finanční úřad pro Zlínský kraj	třída Tomáše Bati 21
	761 86 Zlín
Zdravotní pojišťovny	
Všeobecná zdravotní pojišťovna	Orlická 4/2020
	130 00 Praha 3
Vojenská zdravotní pojišťovna České	Drahobejlova 1404/4

republiky	190 03 Praha 9
Česká průmyslová zdravotní pojišťovna	Jeremenkova 11
	703 00 Ostrava
Oborová zdravotní pojišťovna zaměstnanců bank, pojišťoven a stavebnictví	Roškotova 1225/1
	140 21 Praha 4
Zaměstnanecká pojišťovna Škoda	Husova 302
	293 01 Mladá Boleslav
Zdravotní pojišťovna ministerstva vnitra České republiky	Kodaňská 1441/46
	101 00 Praha 10
Revírní bratrská pokladna	Michálkovická 108
	710 15 Slezská Ostrava

Zdroj: Vlastní zpracování podle www.banky.cz, www.finance.cz a www.financnisprava.cz

3 RSA

RSA algoritmus je v současnosti jedním z nejpoužívanějších asymetrických šifrovacích algoritmů. V roce 1977 jej navrhli matematici Ron **R**ivest, Adi **S**hamir a Leonard **A**delman z Massachusetts Institute of Technology[5]. Jedná se o první algoritmus, který je vhodný jak pro elektronické podepisování, tak i šifrování s veřejným klíčem. (Matějová, 2005; Tlustý, 2006)

3.1 Historie

Myšlenka asymetrického kryptografického systému využívající soukromého a veřejného klíče je přisuzována autorům Whitfieldu Diffieovi a Martinu Hellmanovi, kteří koncept publikovali v roce 1976. Tito autoři také představili digitální podpis. Jejich formulace využívala sdílený tajný klíč vytvořený umocněním určitého čísla, nicméně nechali otevřený problém realizace jednosměrné funkce (tzv. one-way function), zřejmě proto, že obtížnost faktorizace nebyla v dané době dostatečně studována. (Rivest, n.d.)

Ron Rivest, Adi Shamir a Leonard Adleman uskutečnili během jednoho roku několik pokusů vytvořit jednosměrnou funkci – číselnou operaci, která je jednoduchá v jednom směru a obtížná v opačném. Rivest a Shamir, jakožto odborníci přes výpočetní techniku, navrhli mnoho potenciálních funkcí, zatímco matematik Adleman byl zodpovědný za zjištění jejich slabin. V dubnu 1977 byla sepsána finální podoba algoritmu, který byl pojmenován podle počátečních písmen příjmení svých autorů – RSA. (Rivest, n.d.)

Algoritmus byl poprvé zveřejněn v září téhož roku pod titulkem *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems* v časopisu *The Scientific American*. Autoři nabídli poslat svou kompletní zprávu každému, kdo o ni zažádá. NSA[6] se snažila zamezit mezinárodní distribuci kryptografického zdrojového kódu,

[5] Massachusetts Institute of Technology (Massachusettský technologický institut) je soukromá výzkumná univerzita ve městě Cambridge amerického státu Massachusetts. (MIT, 2016)

[6] The National Security Agency (Národní bezpečnostní agentura) je vládní kryptologická organizace Spojených států amerických spadající pod ministerstvo obrany, která oficiálně vznikla 4. listopadu 1952. (NSA, 2016)

nicméně neměla dostatečný právní základ, aby tak bylo učiněno. Následujícího roku byl algoritmus zveřejněn v Communications of the ACM[7]. (Wright, 2007)

Britský matematik Clifford Cocks popsal ekvivalentní systém ve svém interním dokumentu již v roce 1973. Pro uvedení algoritmu do praxe bylo ovšem zapotřebí použití drahé výpočetní techniky, proto jeho systém nebyl uznán jako veřejně použitelný. Jeho výzkum navíc nebyl až do roku 1997 zveřejněn z důvodu označení jako „*přísně tajné*“. (Matějová, 2005)

3.2 Popis fungování algoritmu

Algoritmus je založen na teoreticky jednoduché myšlence: *Je snadné vynásobit dvě dlouhá (minimálně 100-místná) prvočísla, ale bez jejich znalosti je prakticky nemožné zpětně provést rozklad výsledku na původní prvočísla.* Součin těchto čísel je tedy součástí veřejného klíče. Přitom obě prvočísla potřebujeme pro dešifrování. Vzhledem k tomu, že dosud není znám rychlý algoritmus na faktorizaci[8] velkého čísla, je algoritmus RSA považován za bezpečný. (Matoušek, 2006)

RSA algoritmus zahrnuje 3 základní kroky:

1. Vygenerování klíčového páru
2. Šifrování
3. Dešifrování

Vygenerování klíčového páru

Nejprve je třeba vygenerovat veřejný a soukromý klíč. Veřejný klíč se využívá především k zašifrování zprávy. Soukromý klíč se používá k dešifrování zpráv, které jsou zašifrované pomocí veřejného klíče.

1. Pro vygenerování klíčů si zvolíme dvě různá dostatečně velká náhodná prvočísla p a q. Prvočísla by měla být přibližně stejně dlouhá. V praxi se používají prvočísla o velikosti 1024 až 4096 bitů, někdy i delší.
2. Vypočteme součin zvolených prvočísel $n = p \cdot q$. Získaný součin bude sloužit jako modul pro oba dva klíče.
3. Spočítáme hodnotu Eulerovy funkce $\varphi(n) = (p-1)(q-1)$.

[7] Communications of the ACM je časopis vydávaný mezinárodně určenou společností pro výpočetní techniku Association for Computing Machinery (ACM). (Communications of the ACM, 2016)
[8] Faktorizací se rozumí rozklad složeného čísla na součin prvočísel. (Velebil, 2007)

4. Zvolíme celé číslo e tak, aby $1 < e < \varphi(n)$ a $\gcd(e, \varphi(n)) = 1$ (to znamená, že e a $\varphi(n)$ jsou nesoudělná). Číslo e se nazývá veřejný (šifrovací) exponent.
5. Vypočítáme číslo d, které je multiplikativní inverzí čísla e. To znamená $d \equiv e^{-1} \bmod \varphi(n)$. Číslo d je tzv. soukromý (dešifrovací) exponent.

Dvojice (n, e) zveřejníme jako náš veřejný klíč a dvojici (n, d) si ponecháme – jedná se totiž o náš soukromý klíč. Čísla p, q a $\varphi(n)$ musí také zůstat tajná, jelikož mohou být použita k vypočítání dešifrovacího exponentu d. (Velebil, 2007)

Šifrování

Po úspěšném vygenerování klíčů můžeme poslat zabezpečenou zprávu. Předpokládejme, že Bob chce zaslat Alici zabezpečenou zprávu M. Bob musí nejdříve převést zprávu M na celé číslo m, pro které platí, že $0 \leq m < n$. To se provádí pomocí předem dohodnutého reverzibilního protokolu. Bob poté zašifruje zprávu pomocí rovnice $c \equiv m^e \pmod n$ a pošle ji Alici.

Dešifrování

Alice od Boba získá zašifrovaný text c. Původní zprávu m získá pomocí rovnice $m \equiv c^d \pmod n$.

Fakt, že tímto výpočtem získáme původní zprávu, je důsledkem následujícího vztahu:

$$c^d \equiv (m^e)^d \equiv m^{ed} \pmod n$$

A jelikož $ed \equiv 1 \pmod{(p-1)}$ a $ed \equiv 1 \pmod{(q-1)}$, díky malé Fermatově větě[9] platí, že $m^{ed} \equiv m \pmod p$ a zároveň $m^{ed} \equiv m \pmod q$.

Jelikož p a q jsou různá prvočísla, pomocí Čínské věty o zbytcích je dáno

$m^{ed} \equiv m \pmod{(pq)}$,

neboli: $m^{ed} \equiv m \bmod n$,

tudíž: $c^d \equiv m \bmod n$.

(Matějová, 2005)

[9] Malá Fermatova věta tvrdí, že pro každé prvočíslo p a každé celé číslo a takové, že největší společný dělitel $(a, p) = 1$, platí $a^{p-1} \equiv 1 \pmod p$, anebo ekvivalentně $a^p \equiv a \pmod p$. To znamená, že číslo $(a^p - a)$ je dělitelné prvočíslem p. (Blažek, Calda, & Kussová, 1979)

3.2.1 Demonstrační příklad

Jedná se o velmi zjednodušený příklad. Použitá prvočísla jsou extrémně malá a v praxi by jejich použití nebylo dostatečně bezpečné.

Alice si chce vytvořit soukromý a veřejný klíč, aby je mohla využít pro zabezpečení svých internetových transakcí. Nejdříve si musí stanovit dvě libovolná prvočísla, například $p = 101$ a $q = 113$. Dále vypočítá jejich součin $n = 101 \cdot 113 = 11413$ a hodnotu Eulerovy funkce $\varphi(n) = (101 - 1)(113 - 1) = 11200$. Pro to, aby mohla určit veřejný exponent, musí zvolit číslo e pro které platí, že $1 < e < 11200$ a zároveň je s číslem 11200 nesoudělné. Pro tento příklad si Alice vybrala $e = 3533$. Nakonec musí Alice vypočítat d ze vztahu $d \equiv 3533^{-1} (\mathrm{mod}\ 11200)$, odkud $d = 6597$ (neboť opravdu $3533 \cdot 6597 \equiv 1 (\mathrm{mod}\ 11200)$)[10]. Nyní může Alice dvojici $(n = 11413, c = 3533)$ zveřejnit.

Pokud by Bob chtěl poslat Alici zprávu $m = 9726$, musel by vypočítat $c \equiv 9726^{3533} (\mathrm{mod}\ 11413) = 5761$. Zašifrovanou zprávu $c = 5761$ pošle Alici, která ji dešifruje pomocí svého soukromého klíče následujícím výpočtem: $m \equiv 5761^{6597} (\mathrm{mod}\ 11413) = 9726$[11]. (Blanda, 2014)

3.3 Bezpečnost

Po dobu téměř 40 let zůstává algoritmus RSA bezpečným systémem pro posílání šifrovaných zpráv. Za tuto skutečnost získali v roce 2002 Rivest, Shamir a Adleman cenu Alana Turinga, která je každoročně udělována Asociací výpočetní techniky (Association for Computing Machinery) jednotlivcům za jejich technický přínos v oboru informatiky. Jediným známým způsobem, jak zcela prolomit RSA kryptosystém, je v současnosti faktorizace modulu n. Tímto způsobem by se útočníkovi podařilo získat prvočísla p a q a byl by schopný vypočítat tajný exponent d z veřejného klíče (n, e). S tajným exponentem může útočník volně dešifrovat každou zprávu zašifrovanou veřejným klíčem vlastníka. Plné dešifrování RSA šifrovaného textu je ovšem obtížné, jelikož v současné době není znám algoritmus, který by byl schopný v polynomiálním čase faktorizovat velmi vysoká čísla na klasických počítačích.

[10] Nezapomeňme, že musí platit $e \cdot d \equiv 1 (\mathrm{mod}\ 11200)$.

[11] Pro výpočet či ověření příkladu je klasická systémová kalkulačka Windows nedostatečná. Lze využít např. bezplatný online program WolframAlpha, dostupný z: https://www.wolframalpha.com/input/?i=9726%5E3533(Mod11413).

Nicméně nebylo ani dokázáno, že takový algoritmus neexistuje. (SearchSecurity, 2014b; Blanda, 2014; Klíma & Rosa, 2004)

S rostoucím výkonem počítačů a s objevováním nových faktorizačních algoritmů roste schopnost faktorizovat čísla vyšších řádů. Síla šifrování je přímo úměrná velikosti klíče, tudíž zdvojnásobení velikosti klíče přináší exponenciální růst jeho bezpečnosti, ačkoliv za cenu snížení výkonu. V roce 2009 bylo největší univerzálními metodami faktorizované číslo 768 bitů dlouhé. Jak již bylo zmíněno, RSA klíče jsou typicky 1024–2048 bitů dlouhé[12], i když někteří odborníci se domnívají, že 1024 bitové klíče by v blízké budoucnosti mohly být prolomeny. Pro mimořádně zásadní účely (ovlivňující bezpečnost států apod.) se volí i 3072 či rovnou 4096 bitů. Nedojde-li k nepředvídanému průlomu v kvantovém počítání, mělo by trvat ještě dlouhou řadu let, než bude potřeba delších klíčů. (SearchSecurity, 2014b; Blanda, 2014; Klíma & Rosa, 2004)

V roce 1993 publikoval Peter Shor tzv. Shorův algoritmus, který ukazoval, že by kvantový počítač mohl v principu vykonávat faktorizaci v polynomiálním čase, což by znamenalo efektivní prolomení RSA a příbuzných algoritmů. Realizace principů kvantového počítání se však v současnosti potýká s takovými praktickými problémy, že se o bezpečnost zašifrovaných dat zatím není třeba obávat. (Matějová, 2005)

3.3.1 Útoky na RSA

RSA je velmi bezpečný kryptografický systém, který je používán v posledních čtyřiceti letech k zajištění bezpečnosti v milionech aplikací na internetu. Algoritmus ovšem utrpěl řadu kryptografických útoků nebo pokusů o nalezení a využití jeho slabin.

Ve své publikaci kategorizuje autor Dan Boneh (1999) útoky na RSA kryptosystém do čtyř různých tříd:

1. Elementární útoky
2. Útoky zapříčiněné malým soukromým exponentem (klíčem)
3. Útoky zapříčiněné malým veřejným exponentem (klíčem)
4. Útoky na implementace

[12] Od 1. 1. 2010 je Ministerstvem vnitra stanovena minimální přípustná délka klíče RSA algoritmu v České republice na 2048 bitů. Vychází z dokumentu ETSI TS 102 176-1 V2.0.0 („ALGO Paper“). (MVCR, 2009)

Elementární útoky

Elementární útoky představují zcela otevřené zneužití systému RSA. Jedním z příkladů je stanovení společného modulu n pro všechny uživatele veřejného registru. Na první pohled se to může zdát jako vhodné řešení, protože tato metoda je mnohem jednodušší než počítání odlišné hodnoty n pro každého uživatele systému zvlášť. Místo toho by každý uživatel měl jedinečné hodnoty pro e a d. Uživatel A ovšem pomocí svých hodnot e_A a d_A může snadno odvodit hodnotu n a použitím veřejně dostupného exponentu e_B uživatele B může vypočítat jeho tajný exponent d_B. Z této situace tedy vyplývá, že by v systému neměla existovat dvojice uživatelů se stejnou hodnotou n. (Cui, 2005; Boneh, 1999; Wang, 2011)

Útoky zapříčiněné malým soukromým exponentem

Výhodou výběru nízké hodnoty vlastního exponentu je to, že snižuje čas potřebný pro dešifrování zprávy a tím zvyšuje výkonnost. Dešifrování zprávy je totiž lineární k $\log_2 d$. Ovšem při použití hodnoty d, která je menší než 256 bitů, vznikne systém, ve kterém může být hodnota d snadno získána pomocí n a e. (Cui, 2005; Boneh, 1999; Wang, 2011)

Útoky zapříčiněné malým veřejným exponentem

Výhodou použití malého veřejného exponentu je opět snížení výpočetního času potřebného k šifrování a dešifrování zprávy a také k ověření podpisu. Pokud uživatel A pošle uživateli B dvě příbuzné zprávy, které byly zašifrovány použitím stejné hodnoty n a e, a uživatel C je schopen zachytit zašifrovaný text zpráv, je tento uživatel schopen obnovit původní hodnoty těchto dvou zpráv. Na rozdíl od předchozího, útoky použitelné v případě malého e jsou svou nebezpečností daleko od úplného prolomení systému. Jejich užitečnost tkví spíše ve zjednodušování postupů pro jiné útoky. (Cui, 2005; Boneh, 1999; Wang, 2011)

Útoky na implementace

Jedná se o velkou skupinu útoků, které přímo neútočí na samotný algoritmus nebo celý kryptosystém. To znamená, že se nesnaží faktorizovat modul n. Místo toho zneužívají

specifické chyby implementace systému na jednotlivých výpočetních zařízeních. Pokud například uživatel nezabezpečeně uloží svůj klíč, útočník jej může nalézt a zneužít přesným změřením času, který zařízení potřebuje k vykonání šifrování. Útočník tak může rychle zjistit soukromý exponent d využitím algoritmu pro opakované umocňování. V tomto případě by se jednalo o tzv. časovací útok. (Cui, 2005; Boneh, 1999; Wang, 2011)

3.3.2 Správa klíčů

Efektivita kryptografických systémů závisí na více různých faktorech – například na síle algoritmu, rozličných fyzických prvcích (mimo jiné na omezení přístupu ke klíčovému hardwaru či odolnosti hardwaru pro nabourání) a také právě na správě klíčů. Silný algoritmus jako RSA je používán proto, aby útočník nemohl vypočítat klíč, jeho význam se ovšem výrazně snižuje, pokud si útočník může klíč opatřit jiným způsobem. (Piper & Murphy, 2006)

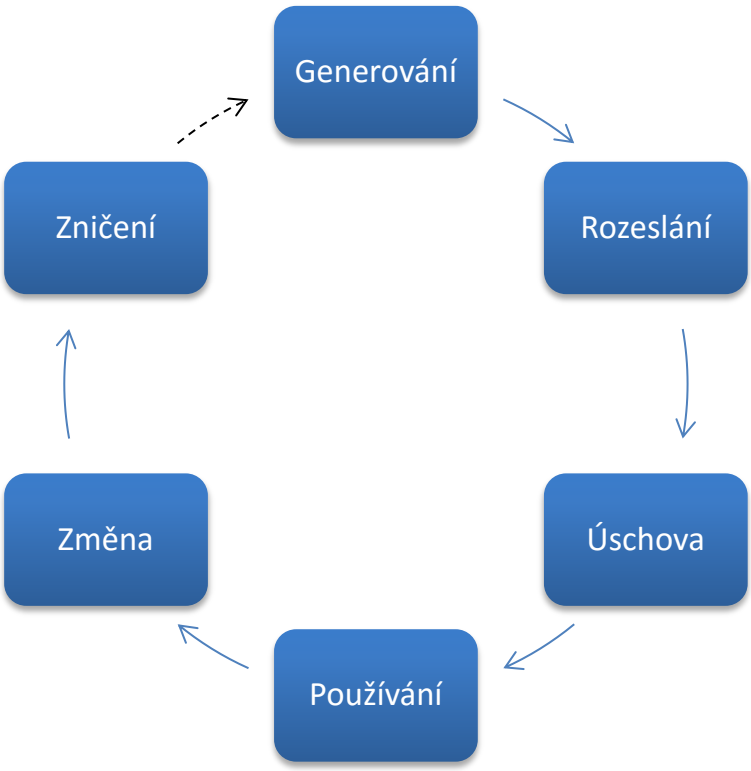
Zabezpečení kryptografického systému RSA (lze aplikovat na kryptografické systémy obecně) je zcela závislé na zabezpečení klíčů. Ty je zapotřebí chránit po celou dobu jejich životního cyklu. Pro zachování efektivity správy klíčů musí být schéma správy navrženo velice obezřetně, protože by jinak nemuselo vyhovovat obchodním potřebám a implementačním požadavkům systému. Přespříliš komplikované kryptografické bezpečnostní systémy mohou pro organizaci představovat zbytečně velkou zátěž. (Piper & Murphy, 2006)

3.3.2.1 Životní cyklus klíče

Životní cyklus klíče začíná procesem jeho generování a končí ve chvíli, kdy již není zapotřebí a je zničen. Hlavní fáze celého cyklu znázorňuje obrázek 5

Téměř ve všech situacích je klíč dříve nebo později nahrazen nějakým jiným. Proto se jedná svým způsobem o uzavřený cyklus, ve kterém je zničení následováno nahrazením novým klíčem. Nový klíč se ovšem generuje, odesílá a ukládá ještě před tím, než je starý klíč znehodnocen. (Piper & Murphy, 2006)

Obrázek 5: Životní cyklus klíče



Zdroj: Vlastní zpracování podle Piper & Murphy (2006)

Generování klíčů

Generování klíčů v asymetrických systémech je mnohem náročnější než u systémů symetrických a je důležité věnovat správnému generování zvýšenou pozornost. Pro generování je zapotřebí využít sofistikovaných matematických postupů a výkonných výpočetních prostředků. Uživatelé musejí často důvěřovat externě generovaným klíčům či externě psanému softwaru. (Piper & Murphy, 2006)

Postup pro generování klíčového páru v RSA systému je popsán v kapitole 3.2.

Distribuce a uchovávání klíčů

Veřejné klíče jsou distribuovány v cerifikátech a jsou nahrávany na veřejně přístupné servery, kde jsou přístupné všem, kteří chtějí uživateli poslat soukromou zašifrovanou zprávu. Pro uchovávání RSA klíčů se používají tzv. containery (key containers). Konajnerem je typicky soubor uložený na harddisku počítače, který je chráněn prostředky operačního systému, nebo může být uložený i na speciálním hardwarovém zařízení (čipová karva, šifrovací token). (Valášek, n.d.)

Používání klíčů

Ve většině systémů má každý klíč předepsaný způsob využití a není možné jej použít k jiným účelům. Neexistuje ovšem žádný způsob, jak zajistit, aby byl tento požadavek naplněn. Existuje mnoho případů, kdy z důvodu vícenásobného používání jednoho klíče došlo k oslabení systému. Dnes se považuje za standard, aby měl každý klíč jen jedno jediné využití. (Piper & Murphy, 2006)

Změna klíčů

Každý kryptografický systém musí být schopen měnit klíče. Ke změnám by mělo docházet buď pravidelně, nebo v důsledku podezření z vyzrazení či neoprávněného zneužití klíče. Má-li uživatel podezření, že byl jeho klíč zneužit, mělo by dojít k jeho okamžité změně. Důvodem pro pravidelnou výměnu klíčů je, aby bylo sníženo riziko jejich vyzrazení a zároveň aby nebyly pro útočníka tak cenné. Například systém EFTPOS[13] mění klíče po každé provedené transkaci. V takovém případě je velice nepravděpodobné, že by utočník investoval usílí a prostředky do útoku, jehož výsledkem by bylo získání klíče k jediné transakci. Otázkou tedy je, jak často klíče měnit. Na její zoodpovězení neexistují žádná přesná pravidla, nicméně je zřejmé, že doba mezi změnami by měla být kratší, než je doba k úspěšnému provedení útoku, a také by měla odpovídat nákladům a problémům způsobeným výměnou klíčů za nové. (Piper & Murphy, 2006)

Likvidace klíče

Nepotřebné klíče je nutné bezpečným způsobem zničit. V příslušném standardu ANSI[14] stojí: *„Klíčový materiál na papíru či podobném záznamovém prostředku by měl být rozstříhán, roztrhán, spálen nebo skartován. Klíčový materiál na všech jiných typech záznamových prostředků by měl být zničen tak, aby jej nešlo fyzicky ani elektronicky obnovit.“* To je velice důležité především u softwarových aplikací, jež ukládají klíče

[13] EFTPOS (Electronic Funds Transfer at Point of Sale) je elektronický platební systém zajišťující elektronický převod peněz při placení platební kartou přes terminál. (KB, 2013)

[14] ANSI (American National Standards Institute) je americkou standardizační organizací sídlící ve Washingtonu. Jedná se o neziskovou organizaci, která vytváří průmyslové standardy ve Spojených státech. Je členem organizace ISO a IEC. (Staudek, 2004)

do paměti. Po smazání klíče by v paměti mohly být uchovány informace, které by utočník mohl zneužít. (Piper & Murphy, 2006)

3.4 Výhody a nevýhody RSA a šifrování s veřejným klíčem

RSA Laboratories (2000) uvádí jako hlavní výhodu šifrování s veřejným klíčem obecně zvýšenou bezpečnost a pohodlí v tom smyslu, že není potřeba zabezpečeně distribuovat klíč (ať již fyzicky, či přes komunikační kanál) jako u šifer symetrických, u kterých existuje šance, že útočník během přenosu klíč získá a zneužije.

Dále jako velkou výhodu algoritmu uvádí možnost jeho využití při elektronickém podepisování. Systém soukromého a veřejného klíče zabezpečuje již zmíněnou identitu odesílatele, integritu a nepopiratelnost zprávy. Např. autentizační systém Kerberos zahrnuje centrální databázi s kopiemi tajných klíčů všech uživatelů (využívá symetrickou kryptografii), úspěšný útok na tuto databázi by umožnil rozšířené padělání různých elektronických dokumentů. Systém operující s veřejným klíčem tento typ útoku znemožňuje. Každý uživatel si samostatně zodpovídá za svůj soukromý klíč, čímž je zajištěna i výše uvedená nepopiratelnost, kdy uživatel nemůže popřít, že zprávu odeslal právě on.

Velikou nevýhodou šifrovacího algoritmu RSA, jak následně RSA Laboratories (2000) uvádí, je jeho šifrovací a dešifrovací rychlost. Existuje velké množství symetrických kryptografických metod, které jsou výrazně (až tisíckrát) rychlejší než RSA.

V některých situacích není úplně nutné a vhodné použít systém šifrování s veřejným klíčem, tajný klíč symetrického šifrování může být zcela dostačující. Patří sem situace, kdy se může uskutečnit bezpečná výměna klíče, např. při osobním setkání uživatelů v soukromí. Obdobně se zahrnují situace, kdy všechny klíče spravuje jediný orgán, např. uzavřený bankovní systém. Jelikož orgán již zná klíče všech uživatelů, není potřeba používat veřejné a soukromé klíče. Ovšem v případě příliš velkého počtu uživatelů by tento systém mohl být velmi nepraktický. Takové omezení by v případě šifrování s veřejným klíčem neexistovalo. Systém šifrování s veřejným klíčem obvykle není nutný ani v prostřední s jedním uživatelem. Pokud například chceme, aby naše osobní soubory byly zašifrované, můžeme tak učinit s jakýmkoliv šifrovacím algoritmem, kde tajným klíčem bude naše heslo. Obecně platí, že systém šifrování

s veřejným klíčem je nejvhodnější pro otevřené prostředí s více uživateli. (RSA Laboratories, 2000)

Cílem asymetrického šifrování nikdy nebylo nahradit šifrování symetrické, ale spíše jej doplit a více zabezpečit. Šifrování s veřejným klíčem bylo poprvé použito, jak RSA Laboratories (2000) uvádí, k zabezpečení distribuce klíče symetrického kryptografického systému – to je stále jedna z jeho primárních funkcí.

3.5 Využití RSA

Kryptografický systém RSA se v současnosti využívá v široké škále produktů, platforem a průmyslových odvětví po celém světě. Je také k nalezení v mnoha komerčních softwarových produktech − v současných operačních systémech od značky Microsoft, Apple, Sun a Novell. V oblasti hardware se RSA používá především v mobilních telefonech, síťových a čipových kartách. Kromě toho je algoritmus začleněn do všech hlavních protokolů pro bezpečnou internetovou komunikaci jako např. S/MIME, SSL a S/WAN. Nelze opomenout ani jeho využití ve státní správě, korporacích, národních laboratořích, univerzitách a bankovnictví. V běžném životě se ještě můžeme s RSA setkat například při výběru hotovosti z bankomatu a při užívání systému placené televize. (Běhálek, 2007; RSA Laboratories, 2000)

Systém RSA se běžně využívá společně se symetrickým kryptografickým systémem, jako například DES[15], k vytvoření RSA digitální obálky[16]. Představme si Alici, která si přeje poslat zašifrovanou zprávu Bobovi. Nejdříve zašifruje zprávu pomocí algoritmu DES použitím náhodně zvoleného klíče. Poté si zjistí Bobův veřejný klíč a pomocí něho zašifruje zvolený DES klíč. Tento klíč zašifrovaný pomocí RSA a DES zašifrovaná zpráva tvoří společně RSA digitální obálku, která je odeslána Bobovi. Po přijetí obálky Bob nejdříve dešifruje klíč pomocí svého soukromého klíče a poté klíč použije k dešifrování samotné zprávy. Tento způsob kombinuje vysokou rychlost algoritmu DES společně s bezpečnou a pohodlnou správou klíčů, kterou přináší RSA systém. (Běhálek, 2007; RSA Laboratories, 2000)

[15] DES (Data/Digital Encryption Standard) je symetrická kryptografická šifra vyvinutá v 70. letech. (Steiner, 2008)

[16] Elektronická obálka je aplikace, ve které odesílatel zašifruje zprávu pomocí symetrických (obsah zprávy) a asymetrických (kódování tajného klíče) kryptografických algoritmů. (Běhálek, 2007)

Kryptografický systém RSA se dále využívá pro autentizaci či identifikaci osob a subjektů. Důvod, proč funguje tak dobře, je takový, že každý subjekt má přidružený svůj soukromý klíč, ke kterému (teoreticky) nemá nikdo jiný přístup. Tím je umožněna jednoznačná identifikace. Příkladem může být elektronické podepisování. Předpokládejme, že Alice chce poslat Bobovi podepsanou zprávu. Nejdříve aplikuje hashovací funkci na zprávu, aby vytvořila hash otisk. Poté tento otisk zašifruje svým soukromým klíčem. Zašifrovaný hash otisk tvoří elektronický podpis, který Alice odešle společně se samotnou zprávou. Po přijetí zprávy Bob dešifruje podpis pomocí Alicina veřejného klíče, aby získal hash otisk. Pro zkontrolování, zda zpráva nebyla v průběhu odesílání modifikována, Bob pomocí stejné hashovací funkce, kterou použila Alice, také vypočítá otisk a oba otisky porovná. Pokud jsou otisky zcela totožné, byl podpis úspěšně ověřen a Bob si může být jistý, že zpráva skutečně pochází od Alice. Pokud otisky totožné nejsou, pochází zpráva od někoho jiného nebo byla po podepsání v průběhu odesílání změněna. Tímto způsobem může každý, kdo zprávu přečte, ověřit její původ. Pokud ovšem nastane situace, kdy si Alice bude přát zachovat tajnost dokumentu, pak nejdříve dokument podepíše a poté jej zašifruje pomocí Bobova veřejného klíče. Bob dokument dešifruje pomocí svého soukromého klíče a použitím Alicina veřejného klíče ověří podpis. Alternativně, pokud by byla nezbytná existence třetí osoby, která by ověřovala integritu zprávy bez možnosti dešifrovat její obsah, může být otisk vypočten ze samotné zašifrované zprávy místo z původního nešifrovaného textu. (Běhálek, 2007; RSA Laboratories, 2000)

3.5.1 Pretty Good Privacy (PGP)

Pretty Good Privacy (v překladu „dost dobré soukromí“) je světově rozšířený program používaný k šifrování a dešifrování elektronické pošty, ale také k ověřování zpráv s elektronickým podpisem a s uloženými zašifrovanými dokumenty. PGP byl jedním z nejrozšířenějších programů zajišťujících soukromí pro jednotlivce a mnohé společnosti. Autorem je Philip R. Zimmermann, který jej vyvinul v roce 1991. PGP se stal de facto standardem pro zabezpečení elektronické pošty. (SearchSecurity, 2014a)

PGP byl dříve dostupný pod licencí freeware, dnes je ovšem komerční a k dostaní za nízký poplatek. K dostání je dnes ve více podobách, například jako program Symantec Encryption Desktop Storage nebo Plug-in OpenPGP pro šifrování e-malů, který lze použít v internetovém prohlížeči Google Chrome. (SearchSecurity, 2014a)

Fungování PGP

PGP funguje jako hybridní kryptografický systém, používá tedy symetrickou i asymetrickou kryptografii, ale také systém elektronických podpisů. Z důvodu rychlejšího zašifrování zprávy využívá PGP symetrický algoritmus, jehož tajný klíč je následně zašifrován veřejným klíčem a spolu se zprávou zaslán příjemci. Příjemce nejdříve dešifruje tajný klíč svým soukromým klíčem a poté se získaným klíčem dešifruje celou zprávu. (SearchSecurity, 2014a)

PGP má dvě verze veřejného klíče – RSA a Diffie-Helman. RSA verze využívá algoritmus IDEA pro generování krátkého tajného klíče, kterým je šifrována celá zpráva, a RSA algoritmus pro zašifrování tohoto klíče. Verze Diffie-Hellman využívá algoritmus CAST pro generování tajného klíče a Diffieho-Hellmanův algoritmus pro zašifrování tohoto tajného klíče. (SearchSecurity, 2014a)

Při elektronickém podepisování využívá RSA verze pro vypočítání hash otisku algoritmus MD5 a Diffie-Hellman využívá algoritmus SHA-1. (SearchSecurity, 2014a)

4 Metodika

4.1 Cíl práce

Hlavním cílem této bakalářské práce je zjištění a zhodnocení informovanosti uživatelů internetového bankovnictví ohledně zásad jeho bezpečného využívání, a to za pomocí údajů sesbíraných pomocí elektronických dotazníků.

4.2 Metodický postup

Prvním krokem k vytvoření této práce bylo stanovení a definování cílů, na jejichž základě byla sestavena osnova práce a rozčlenění na jednotlivé kapitoly. Jednotlivé kapitoly byly následně rozpracovány.

Literární rešerše je vypracována na základě tištěné, ale i elektronické odborné literatury. Veškeré použité tituly jsou uvedeny v seznamu použitých zdrojů na konci této práce.

4.2.1 Dotazníkové šetření

Zadáním dotazníkového šetření bylo zjistit informovanost různých skupin obyvatel z hlediska bezpečnosti odesílání důvěrných dat. Z důvodu aplikace využití RSA algoritmu v obchodní sféře byla zvolena informovanost z hlediska bezpečného využívání internetového bankovnictví, na jehož zabezpečení se algoritmus významně podílí. Cílovou skupinou dotazníkového šetření byly tudíž uživatelé internetového bankovnictví.

Dotazník byl sestaven v prosinci roku 2015 pomocí nástroje Google Formuláře, který podporuje rychlé elektronické rozesílání a snadné vyplňování dotazníku a odpovědi ukládá na online úložiště – Google Drive. Dotazník byl vytvořen tak, aby byl jednoduchý a srozumitelný a zároveň, aby jeho výsledky byly schopné interpretovat cíl výzkumu. Struktura dotazníku je následující. Na začátku se nachází úvodní sdělení, které respondenta informuje o účelu a způsobu zpracování výsledků. Následuje úvodní a zároveň filtrační otázka, která zajišťuje správnou cílovou skupinu. Dotazník pokračuje 3 zahřívacími, 11 specifickými otázkami a je zakončen 4 identifikačními otázkami. Otázek je celkem 19, z nichž je 14 uzavřených a 5 polouzavřených. Z uzavřených otázek se jedná o 5 dichotomických a 9 polytomických. Z polytomických otázek se jedná o 6 selektivních a 3 alternativní.

Před zahájením dotazníkového šetření proběhl pilotní výzkum na deseti respondentech z důvodu kontroly srozumitelnosti a formulace jednotlivých otázek. Na základě této pilotáže byly provedeny drobné korektury. Následně byl odkaz na dotazník rozesílán respondentům prostřednictvím elektronické pošty, sociální sítě (Facebook) a internetových diskuzí.

Sběr odpovědí probíhal od 1. 1. 2016 do 29. 2. 2016. Dotazník vyplnilo celkem 284 lidí, z toho se v 21 případech nejednalo o uživatele internetového bankovnictví, validních odpovědí je tedy celkem 263. Samotný dotazník je k nahlédnutí v příloze 1.

Za účelem objektivního hodnocení výsledků dotazníkového šetření byl sestaven hodnotící rámec. Rámec je tvořen doporučenými bezpečnostními zásadami, které každá banka uvádí na svých webových stránkách. Jednotlivé otázky dotazníku zkoumají informovanost a znalost respondentů ohledně těchto bezpečnostních zásad. Pro účely dotazníkového šetření bylo zvoleno 5 největších bank v České republice (z hlediska celkových aktiv, viz tabulka 2), jejichž zveřejněné bezpečnostní zásady jsou následně shrnuty.

Tabulka 3: Banky v ČR dle celkových aktiv

Banka	Aktiva [mil. Kč]
	2014
ČSOB	865,639
Česká spořitelna	902,589
Komerční banka	953,261
UniCredit Bank	508,616
Raiffeisenbank	226,029

Zdroj: Vlastní zpracování podle www.relbanks.com

4.2.2 Bezpečnostní zásady internetového bankovnictví

Bezpečnostní údaje

Mezi základní zásadu využívání internetového bankovnictví uvádějí banky ochranu svých bezpečnostních údajů. Těmi se rozumí:

- **Heslo, uživatelské číslo, PIN**

  Své heslo, číslo a PIN by uživatelé neměli nikomu dalšímu sdělovat a tyto údaje se nedoporučuje ani nikam poznamenávat (do mobilního telefonu, počítače, diáře apod.). Heslo by mělo být silné – tj. mělo by obsahovat velká i malá

písmena, číslice i speciální znaky. Nemělo by být tvořeno ze snadno odhadnutelných informací, jako jsou jména, data narození, telefonní čísla apod. Uživatelé by měli heslo pravidelně měnit a mělo by být odlišné od hesel, které používají do jiných systémů.

- **Certifikát**

  Uživatel by neměl čipovou kartu se svým klientským certifikátem nechávat ve čtečce čipových karet, pokud neprovádí bankovní operace. Karta je potřeba pouze pro přihlášení a autorizaci transakcí. Uživatelé by neměli ponechávat kartu bez dozoru.

- **Autorizační SMS**

  Autorizační SMS obsahuje potvrzující unikátní kód a také detailní informace k dané transakci. Uživatel by tedy měl před zadáním kódu dbát na důslednou kontrolu uvedených údajů.

Nedůvěryhodná elektronická pošta

Banky vynakládají velké úsilí, aby varovaly své klienty před nedůvěryhodnou a podvodnou elektronickou poštou. Zprávy od neznámých adresátů nebo s podezřelým předmětem či obsahem by měli uživatelé ignorovat či lépe ihned smazat. Uživatelé by v žádném případě neměli stahovat přílohy a soubory či otevírat neznámé odkazy. Banky nikdy nebudou žádat své klienty o zaslání jejich bezpečnostních údajů (klientského čísla a hesla), zvláště prostřednictvím elektronické pošty či telefonního hovoru.

Ochrana proti spamu

Toto doporučení se váže na předchozí. Nejlepším nástrojem, jak většinu nechtěné a nebezpečné pošty eliminovat, je prostřednictvím využívání aktivní ochrany proti spamu. Většina veřejných služeb ji nabízí, stejně tak mnoho softwarových klientů pro elektronickou poštu, jako je např. Outlook. Banky dále doporučují použití i dalších bezpečnostních programů jako antispyware a antiadware, které spolehlivě ochrání počítač či mobilní telefon před nechtěnými reklamami a nebezpečnými programy.

Zabezpečený počítač a mobilní telefon

Uživatelé by do svého účtu internetového bankovnictví měli přistupovat pouze ze svého osobního počítače či mobilního telefonu, který mají plně pod kontrolou a mohou ovlivnit jeho bezpečnostní nastavení. Měli by se vyhnout neznámým počítačům nebo počítačům v internetových kavárnách či na jiných veřejných místech.

Za účelem ochrany svého osobního počítače a mobilního telefonu by na nich uživatel měl mít nainstalovaný aktualizovaný operační systém a antivirový program. Pravidelně by měl provádět kontrolu svých zařízení prostřednictvím antivirového programu. Neméně důležitá je i aktualizace internetového prohlížeče a všech jeho zásuvných modulů v počítači i telefonu. Nedoporučuje se vypínat bránu Firewall. Pokud má uživatel podezření, že jeho osobní počítač či mobilní telefon napadl virus, neměl by jej používat pro přístup do internetového bankovnictví ani k jiným službám s jeho osobními údaji (elektronická pošta, sociální sítě, internetové obchody, atd.).

Využívá-li uživatel mobilní telefon pro přístup ke svému účtu, měl by tak učinit prostřednictví speciální aplikace své banky, dále by neměl mobilní telefon nechávat bez dozoru a ani ho půjčovat jiným osobám.

Webová adresa

Uživatel by měl před přihlášením do svého účtu internetového bankovnictví zkontrolovat webovou adresu stránky. Musí se jednat o zabezpečenou stránku s bezpečnostním protokolem (https) a ve správné formulaci (např. u České spořitelny https://www.servis24.cz). Samotný prohlížeč případně upozorní uživatele zelenou barvou nebo symbolem zamčeného zámku před adresou webu. Tuto kontrolu by měl uživatel provádět hlavně z důvodu, aby se nestal obětí tzv. phishingu. V případě útoku by se uživatel ocitl na stránkách, které vypadají k nerozeznání od pravých stránek banky, nicméně mají odlišnou adresu. Vyplněním přihlašovacích údajů by je uživatel přímo odeslal útočníkovi.

Informace o bezpečnosti

Banky zveřejňují informace a aktuality ohledně bezpečnostní situace na svých internetových stránkách nebo kontaktují své klienti prostřednictvím elektronické pošty

či zpráv přímo v internetovém bankovnictví. Uživatel by tudíž měl tyto zprávy pečlivě sledovat.

V případě, že uživatel zpozoruje cokoliv podezřelého v souvislosti s internetovým či mobilním bankovnictvím, měl by okamžitě kontaktovat klientskou linku své banky.

(Česká spořitelna, 2015b; ČSOB, 2015; Komerční banka, 2015; UniCredit bank, 2015; Raiffeisenbank, 2015)

5 Praktická část

5.1 Vyhodnocení jednotlivých otázek

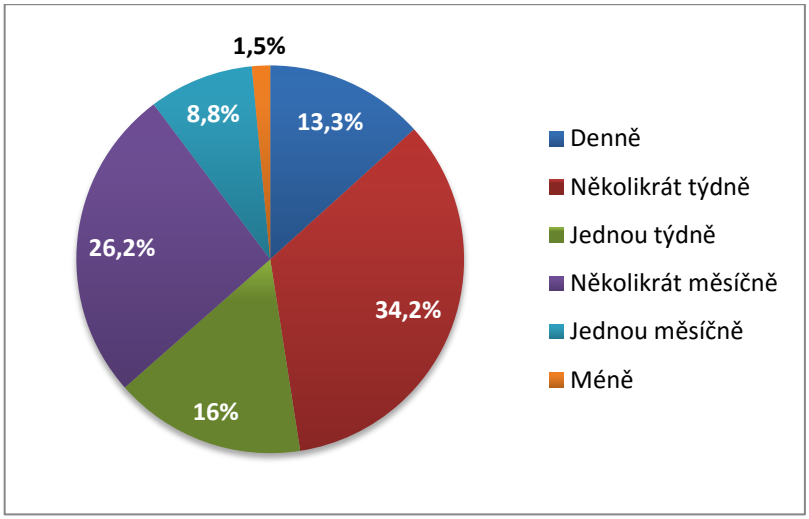
- **Otázka č. 1: „Využíváte internetové bankovnictví?“ (R=284)**

Pro větší efektivitu a ušetření času byla pvní otázka formulována jako filtrační. Respondenti, kteří odpověděli, že internetové bankovnictví nevyužívají (21 respondentů), byli přesměrováni na konec dotazníku bez možnosti jeho vyplnění, tím se tedy zamezil sběr nepoužitelných odpovědí.

- **Otázka č. 2: „Jak často internetové bankovnictví využíváte?“ (R=263)**

Druhá otázka je tzv. úvodní. Jejím učelem bylo respondenta mírným tempem uvést do zkoumané problematiky. Celkem 167 respondentů (63,5 %) využívá službu internetového bankovnictví alespoň jednou týdně, z toho 35 (13,3 %) denně. Zbylých 92 respondentů (35 %) využívá internetové bankovnictví alespoň jednou měsíčně a 4 respondenti (1,5 %) méně než jednou měsíčně.

Graf 1: Frekvence užívání internetového bankovnictví

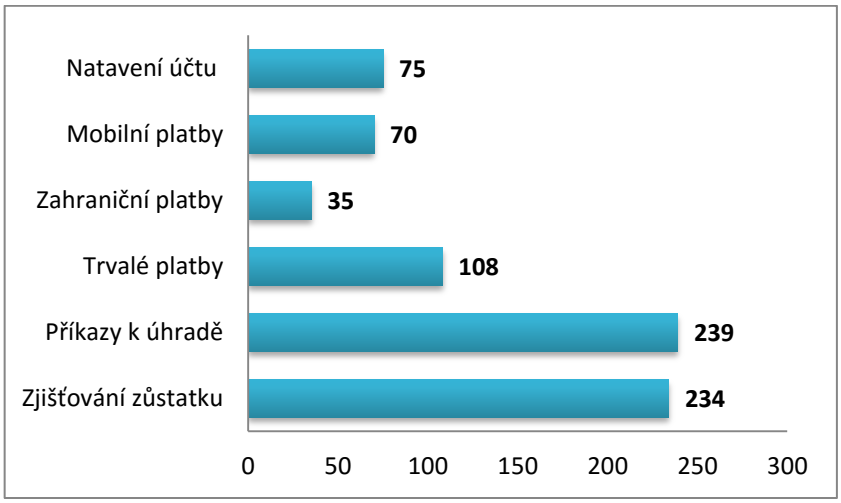


Zdroj: Vlastní zpracování

- **Otázka č. 3: „K jakým účelům využíváte internetové bankovnictví?“ (R=263)**

Třetí otázka je zahřívací s možností více odpovědí. Z grafu 2 můžeme vidět, že respondenti primárně využívají internetové bankovnictví ke zjišťování zůstatku na účtu (234 respondentů) a k obvyklým příkazům k úhradě (239 respondentů). Dalším nejčastějším účelem využití internetového bankovnictví jsou trvalé platby, které zvolilo celkem 108 respondentů. 70 respondentů využívá internetové bankovnictví i pro mobilní platby, pod které spadá mimo jiné dobíjení SIM karet. Možnost změny nastavení svého bankovního účtu skrze internetové bankovnictví využívá 75 respondentů. Nejmenší využití mají zahraniční platby, pouze 35 respondentů.

Graf 2: Využití internetového bankovnictví



Zdroj: Vlastní zpracování

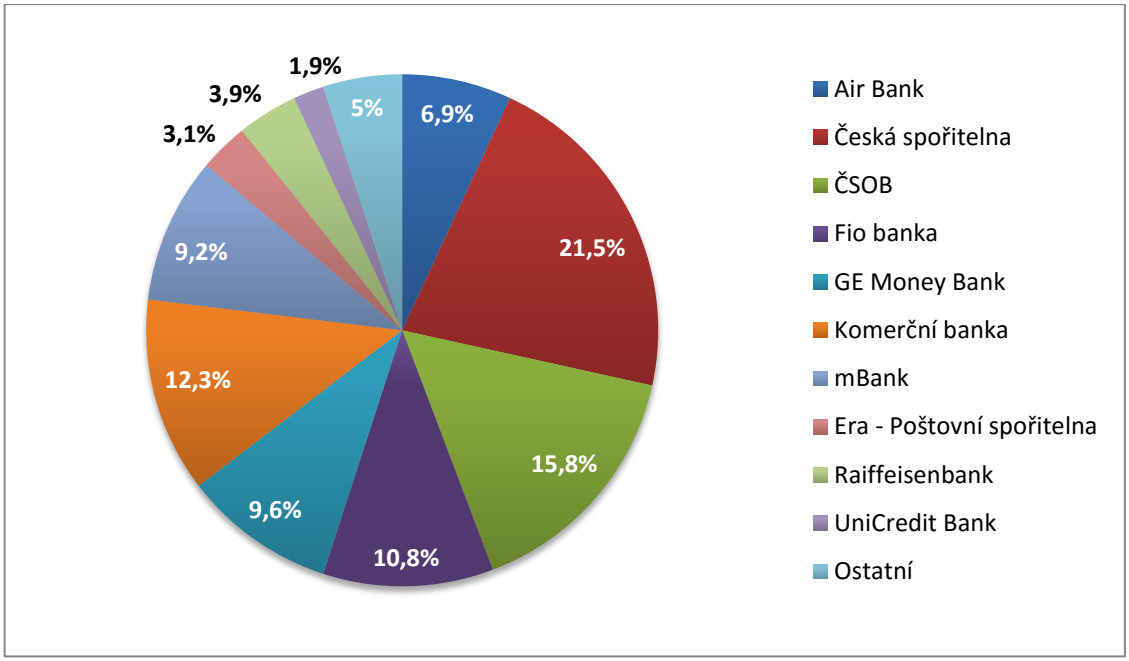
- **Otázka č. 4: „U jaké banky máte vedený běžný účet?“ (R=260)**

Čtvrtá otázka je také zahřívací a vypovídá o procentuálním zastoupení bank mezi respondenty – tedy u jaké banky mají respondenti vedený běžný účet (v případě vedení více účtů, ten, který považují za významnější). Graf 3 nám ukazuje nejvíce zastoupené banky. Banky jako Equa bank, Tatra banka, Sberbank jsou v grafu uvedeny jako ostatní, jelikož jejich zastoupení bylo nižší než 1,6 %.

Na prvním místě je Česká spořitelna, u které má 56 (21,5 %) respondentů vedený běžný účet. Druhé místo náleží ČSOB – 41 respondentů (15,8 %) a třetí místo Komerční bance – 32 respondentů (12,3 %). Zmíněné tři banky skutečně patří mezi pět největších bank

v České republice z hlediska celkových aktiv (viz tabulka 2). Nicméně zbylé dvě banky UniCredit bank a Raiffeisenbank jsou až na posledních místech. Před nimi se nacházejí jiné banky s větším zastoupením respondentů, jako například Fio banka, kterou zvolilo 28 respondentů (10,8 %) nebo také GE Money Bank s 25 respondenty (9,6 %). Graf koresponduje s výsledky výzkumu řadící banky dle počtu klientů[17], kde mezi první tři banky patří právě Česká spořitelna, ČSOB Komerční banka a další významné banky jako GE Money Bank a mBank.

Graf 3: Zastoupení bank u respondentů



Zdroj: Vlastní zpracování

- **Otázka č. 5: „Sdělili jste Vaše přihlašovací údaje do internetového bankovnictví někomu dalšímu?“ (R=262)**

Patá otázka je již specifická a zabývá se problematikou jedné z bezpečnostních zásad využívání internetového bankovnictví, a to konkrétně zásadou ochrany bezpečnostních údajů. Celkem 246 respondentů (93,9 %) tuto zásadu skutečně dodržuje a své přihlašovací údaje do internetového bankovnictví nikomu dalšímu nesdělilo. Nicméně 16 respondentů (6,1 %) odpovědělo, že údaje sdělilo. Tito uživatelé si musí uvědomit,

[17] Data výzkumu pochází z 1. čtvrtletí 2015, s výjimkou mBank, která udala stav ke konci roku 2014. Výzkum je dostupný zde: http://zpravy.aktualne.cz/finance/jak-velke-jsou-banky-v-cesku-novy-zebricek-klientu-i-vkladu/r~c6b9b70efe0211e499590025900fea04/.

že sdělením přihlašovacích údajů někomu jinému, byť blízkému člověku, si nijak nepomohou, ba naopak tím vzniká riziko ztráty peněz či jiná nepříjemná situace.

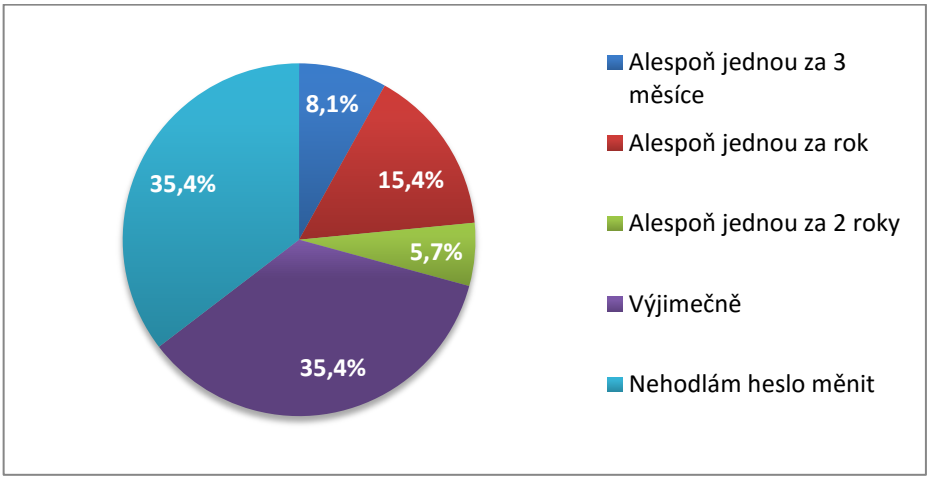
- **Otázka č. 6: „Vaše heslo do internetového bankovnictví je kombinací:“ (R=259)**

Šestá otázka se také zabývá ochranou bezpečnostních údajů, tentokrát konkretizací hesla. Uživatelé mají nastavené určité podmínky pro vytvoření vlastního hesla, ovšem tyto podmínky se u různých bank liší. Doporučená délka hesla je minimálně 8 znaků – kombinace malých, velkých písmen, číslic a nejlépe i speciálních znaků (např. @ # & $ ^ _ *). Nejčastější kombinací, kterou respondenti zvolili, bylo heslo složené alespoň z 8 znaků, malých, velkých písmen a číslic. Tuto kombinaci zvolilo celkem 93 respondentů (35,9 %). Druhou nejčastější kombinací, kterou uvedlo 39 respondentů (15,1 %), je kombinace alespoň 8 znaků, malých a velkých písmen, číslic a speciálních znaků. Tato možnost je ideální, jelikož poskytuje heslo na vyšší úrovni bezpečnosti, než ostatní mají kombinace.

- **Otázka č. 7: „Jak často měníte Vaše heslo do internetového bankovnictví?“ (R=260)**

Sedmá otázka stále zůstává u problematiky hesla. Podle bezpečnostních zásad internetového bankovnictví by si uživatel měl heslo pravidelně měnit. Respondenti se touto zásadou příliš neřídí, jelikož většina z nich (70,8 %) své heslo měnit nehodlá nebo pouze ve výjimečném případě. Tato volba může být pro uživatele nebezpečná, jelikož riziko prolomení hesla roste s růstem doby jeho neměnnosti. Podle Josefa Šustra (2002) by stejné heslo nemělo být používáno déle než jeden rok, optimální dobu platnosti hesla uvádí 3 měsíce. Toto doporučení by splňovalo pouze 61 respondentů (23,5 %), z toho 40 repondentů mění heslo jednou ročně a pouze 21 respondentů (8,1 %) jednou za 3 měsíce.

Graf 4: Častost změny hesla do internetového bankovnictví



Zdroje: Vlastní zpracování

- **Otázka č. 8: „Shoduje se Vaše heslo do internetového bankovnictví s heslem, které používáte pro přihlášení na jiné stránky?“ (R=262)**

Osmá otázká je poslední otázkou dotazníku týkající se hesla. Řeší problém užívání stejného hesla pro více různých systémů. Celkem 219 respondentů (83,6 %) odpovědělo, že pro svůj účet internetového bankovnictví užívá unikátní heslo. Přesně 43 respondentů (16,4 %) ovšem odpovědělo, že jejich heslo do internetového bankovnictví se shoduje s heslem, které používají pro přihlášení na jiné stránky. V tomto případě opět roste riziko prolomení či zjištění hesla.

- **Otázka č. 9: „Jakým způsobem přistupujete do Vašeho internetového bankovnictví?“ (R=261)**

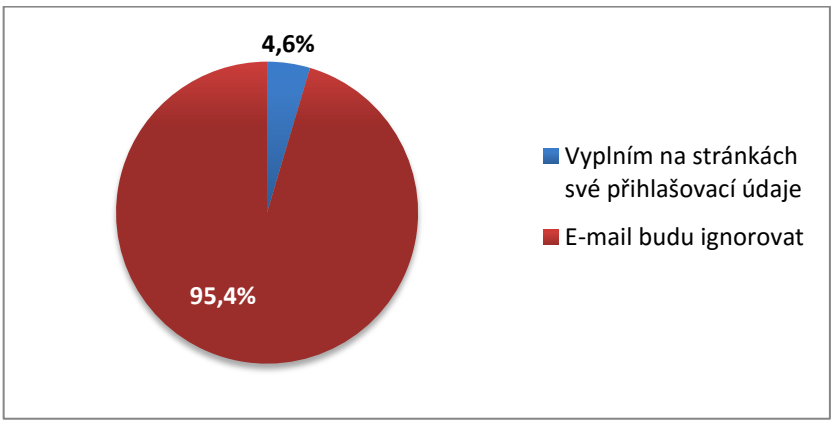
Devátá otázka se zaobírá bezpečností zařízení, které uživatel využívá k přihlášení do internetového bankovnictví. Uživatel by dle bezpečnostní zásady měl k přihlášení používat výhradně svůj osobní počítač či mobilní telefon (přes oficiální smartbanking aplikaci). Velké množství respondentů (51,3 %) skutečně používá výhradně svůj osobní počítač. Další nejpočetnější odpovědí byla kombinace osobního počítače a mobilního telefonu (přes oficiální smartbanking aplikaci), kterou zvolilo 71 respondentů (27,2 %). Celkem lze tedy říci, že osobní počítač (v jakékoliv kombinaci s jinými možnosti) k přihlášení používá 254 respondentů (97,3 %) a mobilní telefon (přes oficiální smartbanking aplikaci) používá 91 respondentů (34,9 %). Tyto možnosti jsou

nejbezpečnější. Méně bezpečné je přistupovat do internetového bankovnictví přes klasický internetový prohlížeč v mobilu, tuto možnost v kombinaci s osobním počítačem zvolilo 20 respondentů (7,7 %).

- **Otázka č. 10: „Jak budete postupovat v případě, že od banky obdržíte e-mail odkazující na internetové stránky banky, kde máte vyplnit přihlašovací údaje (např. z bezpečnostních důvodů)?“ (R=263)**

Desátá otázka poskytuje modelovou situaci tzv. phishingového útoku. Během tohoto útoku je uživatelům rozeslán e-mail, který může na první pohled vypadat tak, že byl poslán uživatelovou bankou. Ve zprávě je uživatel vyzván k zaslání přihlašovacích údajů. V těchto zprávách se ovšem poměrně často vyskytují gramatické chyby, což by měl být pro uživatele první alarmující signál. Banky se snaží své klienty před akutálními útoky neustále varovat a upozorňovat na fakt, že sama banka po uživateli nikdy nebude chtít sdělit jeho přihlašovací údaje. Většina respondentů tuto bezpečnostní zásadu zná, jelikož 249 respondentů (95,4 %) by podobný e-mail ignorovala. Z tohoto počtu by celkem 36 repondentů dokonce i kontaktovalo svou banku a útok by nahlásilo. Bohužel 12 respondentů (4,6 %) by na stránkách vyplnilo své přihlašovací údaje a tím je zaslalo útočníkovi.

Graf 5: Modelová situace - Phishing



Zdroj: Vlastní zpracování

- **Otázka č. 11: „Jakým způsobem chráníte svůj počítač?“ (R=260)**

Jak jsme se již dozvěděli z otázky č. 9, většina respondentů používá k přihlášení do internetového bankovnictví svůj osobní počítač. Počítač proto bývá hlavním cílem útoků a je tudíž nutné ho patřičně zabezpečit. Banky svými bezpečnostními zásadami vyzývají klienty, aby věnovali patřičnou pozornost právě zabezpečení počítače. Standardním zabezpečovacím prvkem počítače je antivirový software, který také většina respondentů (83,1 %) využívá. Je také nutné pracovat s aktualizovaným operačním systémem a iternetovým prohlížečem a nevypínat bránu Firewall, což splňuje 198 respondentů (76,2 %). Antispyware ochranu již používá méně respondentů, celkem 81 (31,2 %). Tento ochranný software je velmi užitečný, chrání totiž uživatele před tzv. „špionážními programy.“ Jedná se o programy, které shromažďují osobní informace, aniž by o tom uživatele nejprve informovaly. Výrazně tedy zasahují do soukromí uživatele na internetu a mohou zaznamenávat seznamy webových stránek, které uživatel navštěvuje, nebo citlivější informace, jako jsou právě uživatelská jména a hesla. (Antivirové centrum, 2015)

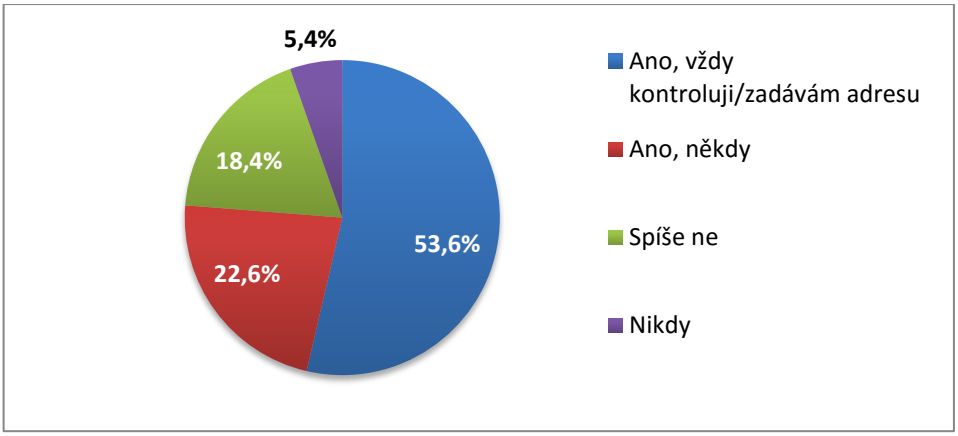
Několik respondentů (2,7 %) se spoléhá čistě na svůj operační systém. Jedná se hlavně o uživatele systému Linux a Mac OS, pro které skutečně v současnosti neexistují téměř žádné viry.

- **Otázka č. 12: „Kontrolujete při přihlášení do internetového bankovnictví adresu stránky?“ (R=261)**

Dvanáctá otázka opět řeší problematiku phishingového útoku. Uživatelé by měli přistupovat na stránky internetového bankovnictví přes oficiální stránky své banky nebo by měli adresu sami přímo zadávat. Například u Komerční banky by se jednalo o adresu https://www.mojebanka.cz. Klienti by se tedy měli vyvarovat používání neznámých odkazů. Prostřednictvím adresového řádku je možné kontrolovat validitu stránek, na kterých se uživatel nachází. Oficiální stránky internetového bankovnictví, jak již bylo zmíněno v bezpečnostních zásadách, jsou chráněny bezpečnostním protokolem a je k vidění i certifikát. Celkem 140 respondentů (53,6 %) adresu vždy buď kontroluje, či ji sami zadávají do adresového řádku. Celkem 59 (22,6 %) respondentů odpovědělo, že adresu kontrolují pouze někdy. Nicméně značné množství respondentů odpovědělo, že adresu nekontrolují nikdy (5,4 %) nebo pouze málokdy (18,4 %). Tento přístup je pro

ně nebezpečný, jelikož šance, že se stanou oběťmi phishingového útoku, se tím pádem zvyšuje.

Graf 6: Kontrola webové adresy



Zdroj: Vlastní zpracování

- **Otázka č. 13: „Které z následujících termínů dokážete vysvětlit?“ (R=260)**

Třináctá otázka ověřuje znalosti respondetů ohledně několika hrozeb, se kterými se v rámci práce s internetem mohou setkat.

Spyware je software, který shromažďuje osobní informace o uživateli. Více informací o spyware je k dispozici u otázky č. 11. Celkem 177 respondentů (68,1 %) odpovědělo, že tento pojem dokáže vysvětlit.

S phishingem jsme se také setkali již výše, jedná se o podvodné e-mailové zprávy, které mají vzbudit dojem, že jejich odesílatelem je uživatelova banka. Tato zpráva obsahuje webový odkaz na údajné stránky banky a vyzývá k potvrzení osobních bankovních údajů. Cílem je získat klientské číslo a heslo adresáta a jejich následné zneužití (Česká spořitelna, 2015a). Phishing by dokázalo vysvětlit 170 (65,4 %) respondentů.

Počítačový virus, zvaný též malware[18], je počítačový program, který se šíří bez vědomí uživatele a jeho úkolem je především škodit. Může zapříčinit například zpomalení a nestabilitu systému, krádež dat, hesel a jiné (Miklas & Světlík, n.d.). Pojem virus je v současnosti mezi uživateli internetového bankovnictví velmi známý, celkem 251 respondentů (96,5 %) odpovědělo, že pojem dokáže vysvětlit.

[18] Malware – „Malign Software“ znamená v překladu z angličtiny škodlivý software.

Pharming velmi úzce souvisí s phishingem. Rozdíl je v tom, že uživatel zadá do internetového vyhledávače správnou adresu své banky, ale je i přesto přesměrován na podvodnou stránku, která vypadá shodně. Toto je zapříčiněné tím, že se útočníkovi podařilo změnit DNS záznam na počítači uživatele, čímž nedojde k přesměrování na správnou IP adresu (Miklas & Světlík, n.d.). Tento pojem je mezi respondenty již méně známý, vysvětlit by jej dokázalo 52 respondentů (20 %).

- **Otázka č. 14: „Víte, že Vaše banka na svých stránkách uvádí bezpečnostní zásady internetového bankovnictví?“ (R=263)**

Otázka zjišťuje povědomí uživatelů o existenci bezpečnostních zásad internetového bankovnictví. Celkem 226 respondentů (86 %) odpovědělo, že si je vědomo toho, že banky tyto zásady uvádějí na svý stránkách. Relativně málo respondentů (14 %) odpovědělo, že o zásadách nevědí.

- **Otázka č. 15: „Přečetl/a jste tyto bezpečnostní zásady internetového bankovnictví?“ (R=226)**

Pokud respondent odpověděl na předešlou otázku „Ano“, byla mu prezentována otázka č. 15. Některé bezpečnostní zásady jsou sice přirozené a intuitivní, nicméně samotné povědomí nestačí. Je proto lepší věnovat čas k přečtení zásad a tím zvýšit svou bezpečnost nejen v internetovém bankovnictví, ale na internetu obecně. Celkem vysoký počet respondentů (52 %) odpověděl, že bezpečnostní zásady nečetl. Zbylých 109 respondentů (48 %) se seznámilo se zásadami své banky.

- **Otázky č. 16 – 19 (R=263)**

Poslední čtyři otázky dotazníku byly identifikační, blíže tedy speficikují jednotlivé respondenty.

Pohlaví

Dotazník vyplnilo celkem 167 mužů (63,5 %) a 96 žen (36,5 %).

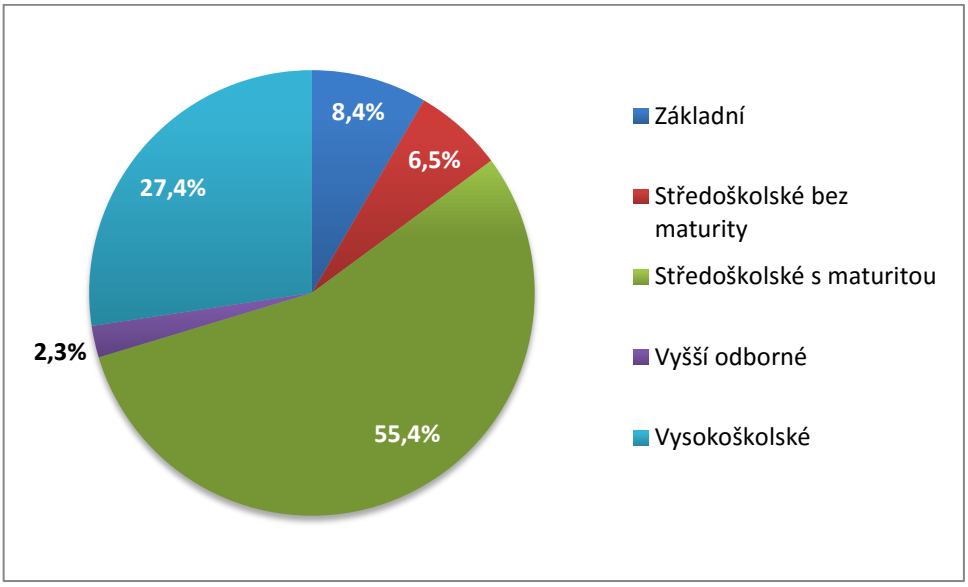
Věk

Převládají odpovědi od respondentů ve věku mezi 15–27 lety (70 %). Další nejpočetnější věkovou kategorií jsou respondenti ve věku od 28 do 40 let (17,9 %). Ve věku od 41 do 50 odpovědělo 20 respondentů (7,6 %), následně 6 respondentů (2,3 %) ve věku od 51 do 60 a ve věku nad 60 let odpovědělo také 6 respondentů.

Nejvyšší ukončené vzdělání

Nejvyšší ukončené vzdělání nadpoloviční většiny respondentů je středoškolské s maturitou (55,4 %). Další nejvyznamnější skupinou jsou respondenti s vysokoškolským vzděláním (27,4 %). Zbylé skupiny jsou méně zastoupené a jsou k nahlednutí společně s ostatními v grafu 7.

Graf 7: Nejvyšší ukončené vzdělání respondentů



Zdroj: Vlastní zpracování

Současný statut

Nejpočetnější skupinou respondentů jsou studenti, celkem 127 (48,3 %). Dotazník dále vyplnilo 70 zaměstnanců na plný úvazek (26,6 %) a 50 osob samostatně výdělečně činných (19 %). Mezi méně zastoupené skupiny patří osoby zaměstnané na částečný úvazek (1,9 %), nezaměstnaní (2,3 %) a důchodci (1,9 %).

5.2 Vyhodnocení výzkumné otázky

Výzkumná otázka dotazníkového šetření: „Jaká je všeobecná informovanost uživatelů iternetového bankovnictví o bankami doporučených bezpečnostních zásadách užívání internetového bankovnictví?“

Odpověď na výzkumnou otázku vychází z výsledků otázek č. 5, 7, 8, 10, 12, 14 a 15. Zmíněné otázky přímo ověřují znalost uživatelů ohledně bezpečnostních zásad bank. Z důvodu odlišného počtu odpovědí na jednotlivé otázky probíhá hodnocení informovanosti následovně.

Odpovědi na otázky jsou hodnoceny známkou ze škály 1–5, kdy hodnocení 1 je považováno za nejlepší, jelikož se jedná o optimální variantu vyplývající z bezpečnostních zásad bank ohledně využívání internetového bankovnictví. Odpovědi se známkou 5 jsou tudíž považovány za nedostatečné.

Otázky č. 5, 8, 10, 14 a 15 jsou dichotomické, mají tedy dvě možnosti odpovědi. Proto jsou hodnoceny známkou buď 1, nebo 5. Např. odpověď „Ne“ u otázky č. 5: „Sdělili jste Vaše přihlašovací údaje do internetového bankovnictví někomu dalšímu?“ je hodnocena známkou 1 a odpověď „Ano“ známkou 5.

Tabulka 4: Hodnocení dichotomických otázek

Otázka	Známka		Počet respondentů
	1	5	
5	93,9%	6,1%	262
8	83,6%	16,4%	262
10	95,4%	4,6%	261
14	85,9%	14,1%	263
15	48,2%	51,8%	226
Celkem	**81,4%**	**18,6%**	
Hodnocení	Dostatečné	Nedostatečné	

Zdroj: Vlastní zpracování

U otázky č. 7: „Jak často měníte Vaše heslo do internetového bankovnictví?“ má respondent na výběr mezi pěti odpověďmi, musí být proto hodnocena zvlášť. Dle zásad bezpečného využívání internetového bankovnictví je odpověď „Alespoň jednou za 3 měsíce“ optimální, a proto je hodnocena známkou 1. Odpověď „Alespoň jednou za rok“ je hodnocena známkou 2, odpověď „Alespoň jednou za 2 roky“ známkou 3, odpověď „Výjimečně“ známkou 4 a odpověď „Nehodlám heslo měnit“ je hodnocena

jako nejhorší, tedy známkou 5. Odpovědi se známkou 1–3 jsou považovány za dostatečné a odpovědi 4–5 jako nedostatečné.

Tabulka 5: Hodnocení otázky č. 7

Otázka	Známka					Počet respondentů
	1	2	3	4	5	
7	21	40	15	92	92	260
Celkem	8,1%	15,4%	5,8%	35,4%	35,4%	
	29,2%			70,8%		
Hodnocení	Dostatečné			Nedostatečné		

Zdroj: Vlastní zpracování

Otázka č. 12: „Kontrolujete při přihlášení do internetového bankovnictví adresu stránky?“ nabízela respondentům 4 možnosti odpovědi. Odpověď „Ano, vždy kontroluji/zadávám adresu“ je hodnocena známkou 1, odpověď „Ano, někdy“ je hodnocena známkou 2, odpověď „Spíše ne“ je hodnocena známkou 4 a odpověď „Nikdy“ je hodnocena známkou 5“. Odpovědi se známkou 1–2 jsou považovány za dostatečné a odpovědi 4–5 za nedostatečné.

Tabulka 6: Hodnocení otázky č. 12

Otázka	Známka				Počet respondentů
	1	2	4	5	
12	140	59	48	14	261
Celkem	53,6%	22,6%	18,4%	5,4%	
	76,2%		23,8%		
Hodnocení	Dostatečné		Nedostatečné		

Zdroj: Vlastní zpracování

Pro získání jednotné míry informovanosti byl proveden aritmetický průměr výsledků tabulek 3, 4 a 5. Z těchto výsledků vyplývá, že celkem 62,3 % odpovědí dosáhlo kladného hodnocení, z hlediska informovanosti ohledně bezpečnostních zásad bank je lze považovat za dostačující. Záporného hodnocení a tudíž nedostatečné informovanosti dosáhlo celkem 37,7 % odpovědí.

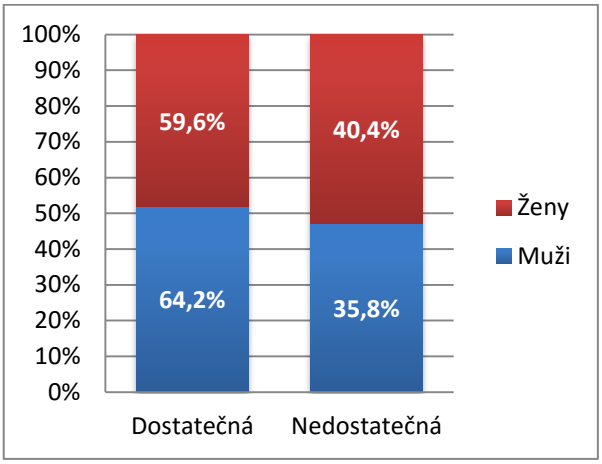
Tabulka 7: Míra informovanosti respondentů ohledně bezpečnostních zásad

Míra informovanosti	
Dostatečná	**62,3%**
Nedostatečná	**37,7%**

Zdroj: Vlastní zpracování

Za účelem vyhodnocení hypotézy č. 2 bylo zapotřebí tyto výsledky zhodnotit podle pohlaví respondenta. Z grafu 8je patrné, že míra informovanosti mužů je o 4,6 % vyšší než míra informovanosti žen. Celkem tedy měli 64,2 % dostatečně hodnocených a 35,8 % nedostatečně hodnocených odpovědí. Ženy měly 56,6 % odpovědí s dostatečným hodnocením a 40,4 % s nedostatečným hodnocením.

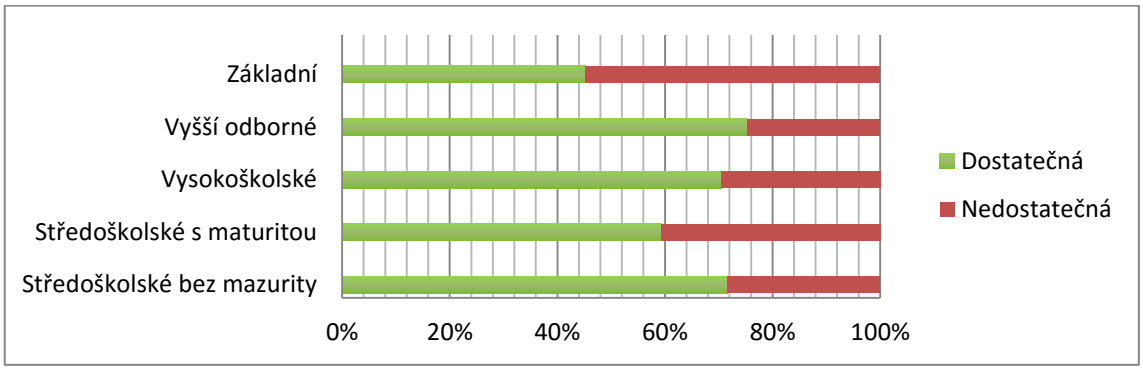
Graf 8: Míra informovanosti v závislosti na pohlaví



Zdroj: Vlastní zpracování

Za účelem vyhodnocení hypotézy č. 3 byly výsledky zhodnoceny podle dosaženého vzdělání respondentů. Jak vypovídá graf 9, nejlépe jsou informovaní respondenti s vyšším odborným vzděláním. Celkem 75,3 % jejich odpovědí dosáhlo dostatečného hodnocení a tudíž 24,7 % odpovědí dosáhlo nedostatečného hodnocení. Druhou nejlépe informovanou skupinou ohledně bezpečnostních zásad jsou respodenti se středoškolským vzděláním bez maturity. Celkem 71,7 % odpovědí dosáhlo dostatečného a 28,3 % odpovědí nedostatečného hodnocení. Další v pořadí je skupina respondentů s vysokoškolským vzděláním, celkem 70,4 % odpovědí dosáhlo dostatečného a 29,6 % odpovědí nedostatečného hodnocení. Na předposledním místě se umístili respondenti se středoškolským vzděláním s maturitou, kteří měli celkem 59,3 % odpovědí s dostatečným a 40,7 % odpovědí s nedostatečným hodnocením. Jako poslední se umístili respondenti se základním vzděláním, kteří měli celkem 45,2 % odpovědí s dostatečným a 54,8 % odpovědí s nedostatečným hodnocením.

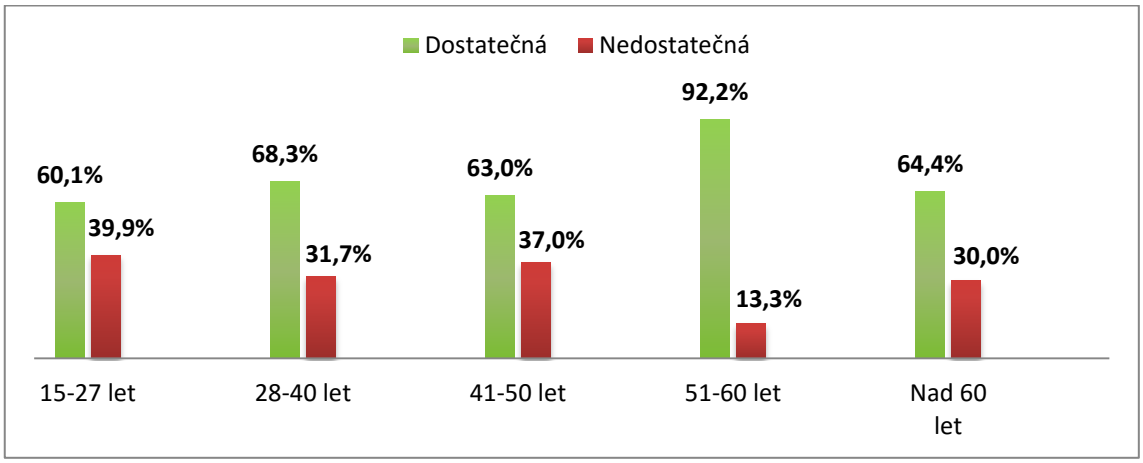
Graf 9: Míra informovanosti v závislosti na vzdělání



Zdroj: Vlastní zpracování

Za účelem vyhodnocení hypotézy č. 4 byly výsledky zhodnoceny podle dalšího kritéria, a to podle věkové skupiny respondentů. Nejlepších výsledků dosáhli respondenti z věkové skupiny 51–60 let, měli celkem 92,2 % odpovědí s dostatečným hodnocením. Na druhém místě se umístili respondenti z věkové skupiny 28–40 let, kteří měli celkem 68,3 % odpovědí s dostatečným hodnocením. Třetí místo obsadili respondenti z věkové skupiny nad 60 let, kteří měli 64,4 % odpovědí s dostatečným hodnocením. Předposlední místo patří respondentům z věkové skupiny 41–50 let, jelikož měli celkem 63 % odpovědí s dostatečným hodnocením. Na posledním místě se umístili respondenti z věkové skupiny 15–27 let, kteří měli 60,1 % odpovědí s dostatečným hodnocením. Nicméně je nutné vzít v potaz, že respondentů z věkové skupiny 51–60 let a ze skupiny nad 60 let bylo oproti ostatním skupinám výrazně méně, jejich dosažené výsledky jsou tudíž v porovnání s ostatními zkreslené.

Graf 10: Míra informovanosti v závislosti na věkové skupině



Zdroj: Vlastní zpracování

5.3 Vyhodnocení hypotéz

Hypotéza č. 1: Minimálně 2/3 respondentů nečetlo bezpečnostní zásady svých bank.

Odpověď na tuto hypotézu vyplývá z otázky č. 15. Bezpečnostní zásady své banky nepřečetlo 117 respondentů, což netvoří 2/3 všech respondentů, kteří odpověděli na tuto otázku, hypotéža č. 1 se tudíž **zamítá**.

Hypotéza č. 2: Pohlaví nemá vliv na informovanost o bezpečnostních zásadách (rozdíl míry informovanosti nepřesahuje 5 %).

Na základě výsledků, které ukazuje grafu 8, se hypotéza č. 2 **přijímá**. Rozdíl míry informovanosti mezi muži a ženy skutečně nepřesáhl 5 %, jelikož byl přesně 4,6 %.

Hypotéza č. 3: Se zvyšujícím se vzděláním roste míra informovanosti o bezpečnostních zásadách.

Odpověď na hypotézu vychází z grafu 9. Míra informovanosti je různá a neroste se zvyšujícím se vzděláním. Například nejlepšího hodnocení dosáhli respondenti s vyšším odborným vzděláním, nikoliv respondenti s vysokoškolským vzděláním. Hypotéza č. 3 se proto **zamítá**.

Hypotéza č. 4: Se zvyšujícím se věkem klesá míra informovanosti o bezpečnostních zásadách.

Na základě výsledků zobrazených v grafu 10 se hypotéza č. 4 **zamítá**. Z výsledků nevyplývá žádná závislost míry informovanosti na rostoucím věku. Závislost se neprojevuje ani tehdy, pokud bychom nebrali v potaz odpovědi respondentů z věkové skupiny 51–60 a ze skupiny nad 60 let (z důvodu výrazně menšího zastoupení než měly ostatní skupiny).

6 Závěr

Dílčí cíle práce byly splněny. V teoretické části byl popsán základní princip fungování RSA algoritmu a šifrování s veřejným klíčem, následně byly předloženy výhody a nevýhody jeho použití. Byl uveden konkrétní seznam institucí, které používají elektronický podpis k ověření autenticity odesílatele.

Hlavním cílem praktické části bylo zjistit informovanost různých skupin obyvatel z hlediska bezpečnosti odesílání důvěrných dat. Dotazníkové šetření se zaměřovalo na uživatele internetového bankovnictví, jelikož při jeho využívání dochází k odesílání citlivých údajů uživatele a je názorným příkladem systému, který je zabezpečený pomocí RSA v obchodní sféře. Byla zjištěna míra informovanosti uživatelů z hlediska zásad bezpečného využívání internetového bankovnictví, které banky zveřejňují na svých webových stránkách. Zásada o nesdělování svých přihlašovacích údajů jiným osobám je uživatelům velmi blízká a dodržují ji téměř všichni respondenti. Zásadu měnit heslo nejlépe jednou za 3 měsíce respondenti nedodržují a svá hesla nemění. Ke zlepšení této situace doporučuji bankám klienty vyzývat k povinné změně svých hesel po určité době. Tato doba by podle mého názoru měla být delší než tři měsíce (např. jeden rok), jelikož tato povinnost bude zřejmě neoblíbenou zátěží pro klienty. Většina respondetů přistupuje do internetového bankovnictví prostřednictvím zabezpečeného zařízení a tím dodržují zásadu bezpečného přístupu. Phishingový útok by úspěšně obstáli téměř všichni respondenti. Nicméně, respondenti příliš nekontrolují webovou adresu stránky, skrze kterou se přihlašují do internetového bankovnictví. Krátké upozornění, nacházející se např. nad přihlašovacím formulářem, by podle mého názoru mohlo být efektivní a zlepšilo by dodržování této bezpečnostní zásady. Pojem počítačový virus je všeobecně známý, ovšem pojmy jako phishing, spyware a hlavně pharming jsou pro respondenty již méně známé a jejich stručné vysvětlení na stránkách banky by mohlo přispět ke zlepšení bezpečnosti uživatelů. Většina respondentů si je vědoma toho, že jejich banka zveřejňuje bezpečnostní zásady na svých webových stránkách, ovšem nadpoloviční většina tyto zásady nečetla. Z tohoto důvodu by zásady měly být pojaty kreativnějším způsobem. Měly by být krátké, stručné a pokud možno zábavné. V úvahu by připadala i video instruktáž, která by nové klienty seznámila s bezpečností na internetu před svým prvním přihlášením do internetového bankovnictví.

Celková míra informovanosti uživatelů internetového bankovnictví ohledně bezpečnostních zásad mě mile překvapila. Nicméně, stále existuje prostor pro její zlepšení. O výsledky dotazníkového šetření také projevila zájem Česká bankovní asociace, která dotazník zveřejnila na svých stránkách.

Práce slouží k seznámí čtenáře s RSA algoritmem a pomáhá mu nahlédnout na problematiku bezpečnosti elektronické komunikace. Znázorňuje spojitost s matematickými postupy a jejich praktickou aplikací v reálném životě, nikoliv pouze ve školních lavicích. Dále obsahuje několik doporučení pro banky, jak zlepšit informovanost a tím i bezpečnost uživatelů internetového bankovnictví.

I. Summary and key words

This bachelor thesis focuses on the RSA algorithm and it‘s use in electronic communication. The RSA algorithm is curently one of the most widely used asymmetric encryption algorithms. It was first publicly described in 1977 by the mathematicians Ron Rivest, Adi Shamir, and Leonard Adleman. It is the first algorithm that is suitable for both electronic signature and public key encryption.

The theoretical part explains all related concepts of cryptography. The basic operating principle of the algorithm is described in specific simplified example. It also includes a description of public key encryption and a list of institutions, which use digital signature to verify authenticity of the sender.

The practical part focuses on a questionnaire survey, which investigates the awareness level of internet banking users in term of security of using internet banking and following the security policy recommended by banks. The results are analysed and evaluated at the end of the thesis.

Keywords: RSA algorithm, digital signature, encryption, decryption, internet banking

II. Seznam použitých zdrojů

Antivirové centrum. (2015). AntiSpyware. Retrieved from: http://www.antivirovecentrum.cz/antispyware.aspx

Banks around the world. (2015). *Banks in the Czech Republic*. Retrieved from: http://www.relbanks.com/europe/czech-republic

Banky v ČR – Informační portál. (2016). *Banky*. Retrievd from: http://www.banky.cz/prehled-bank

Běhálek, M. (2007). *Digitální obálky, podpisy a certifikáty.* Vysoká škola báňská - Technická univerzita Ostrava. Retrieved from: http://www.cs.vsb.cz/behalek/vyuka/pcsharp/text/ch09s02.html

Blanda, S. (2014). *RSA Encryption – Keeping the Internet Secure*. AMS Grad Blog. Retrieved from: http://blogs.ams.org/mathgradblog/2014/03/30/rsa/#sthash.z2Tfym3B.9oer1zOM.dpbs

Boneh, D. (1999). *Twenty Years of Attacks on the RSA Cryptosystem.* Staford University. Retrieved from: https://crypto.stanford.edu/~dabo/papers/RSA-survey.pdf

BusinessInfo.cz (2002). *Elektronický podpis a jeho využití*. Retrieved from: http://www.businessinfo.cz/cs/clanky/elektronicky-podpis-a-jeho-vyuziti-7476.html

Communications of the ACM. (2016). *About Communication.* Retrieved from: http://cacm.acm.org/about-communications

Cui, X.-l. (2005). *Attacks On the RSA Cryptosystem* . NC State University. Retrieved from: http://www4.ncsu.edu/~kksivara/sfwr4c03/projects/4c03projects/XCui-Project.pdf

Česká spořitelna. (2015a). *Stručně o phishingu*. Retrieved from: http://www.csas.cz/banka/nav/o-nas/strucne-o-phishingu-d00014563

Česká spořitelna. (2015b). *Zásady bezpečného používání Internetbankingu*. Retrieved from: http://www.csas.cz/banka/nav/o-nas/zasady-bezpecneho-pouzivani-internetbankingu-d00014438

ČSOB. (2015). *Zásady bezpečného užívání elektronického bankovnictví*. Retrieved from: https://www.csob.cz/portal/bezpecnost/jak-se-branit/zasady-bezpecneho-uzivani-elektronickeho-bankovnictvi

EARCHIVACE. (2014). *Úvod do kryptografie*. Retrieved from: http://www.earchivace.cz/technologie/uvod-do-kryptografie/

Entrust. (2001). *What Are Digital Signatures?* Retrieved from: https://www.entrust.com/digital-signatures/

Finance.cz – daně, banky, kalkulačky, spoření, kurzy měn. (2016). *Zdravotní pojišťovny*. Retrieved from: http://www.finance.cz/pojisteni/seznamy/zdravotni-pojistovny/

Finanční správa. (2016). Finanční úřady. Retrieved from: http://www.financnisprava.cz/cs/financni-sprava/organy-financni-spravy/financni-urady

Hovorka, J. (2015). *Jak velké jsou banky v Česku? Nový žebříček klientů i vkladů*. Aktuálně.cz. Retrieved from: http://zpravy.aktualne.cz/finance/jak-velke-jsou-banky-v-cesku-novy-zebricek-klientu-i-vkladu/r~c6b9b70efe0211e499590025900fea04/

I.CA. (2015). *Elektronický podpis*. Retrieved from: http://www.ica.cz/Elektronicky-podpis

iPodnikatel.cz. (2011). *S úřady elektronicky*. Retrieved from: http://www.ipodnikatel.cz/Internet/s-urady-elektronicky.html

Jančařík, A. (2009). *Hashovací funkce*. Antonín Jančařík. Retrieved from: http://www.kryptografie.wz.cz/data/hash2.htm

Jančařík, A. (2009). *Teorie čísel a kryptologie*. Antonín Jančařík. Retrieved from: http://class.pedf.cuni.cz/Jancarik/DesktopDefault.aspx?tabindex=5&tabid=26&portalskce=2

Kessle, G. C. (2016). *The Purpose of Cryptography*. An Overview of Cryptography. Retrieved from: http://www.garykessler.net/library/crypto.html#purpose

Klíma, V., & Rosa, T. (2004). *Kryptologie pro praxi – metoda RSA.* Personal Page: Dr. Tomáš Rosa. Retrieved from: http://crypto.hyperlink.cz/files/ST_2004_03_xx_xx.pdf

Komerční banka, a.s.. (2013). *Pokyny pro provádění transakcí platebními kartami.* Retrieved from: https://www.kb.cz/file/cs/o-bance/dokumenty-ke-stazeni/kb-20140101-

pokyny-pro-provadeni-transakci-platebnimi-kartami.pdf?dcd7cffb92ebe8a20814066ac075023f

Komerční banka, a.s.. (2015). *Desatero bezpečnosti*. Retrieved from: https://www.kb.cz/bezpecnost/desatero-bezpecnosti/index.shtml

Kunderová, L. (n.d.). *Bezpečnost IS/IT*. Mendelova univerzita v Brně. Retrieved from: https://akela.mendelu.cz/~lidak/bis/8kryp.htm

Matějová, L. (2005). *RSA.* kryptografie.wz.cz. Retrieved from: http://www.kryptografie.wz.cz/data/RSA.htm

Matoušek, R. (2006). *Metody kódování.* Brno: Vysoké učení technické v Brně.

Mendelova univerzita v Brně. (n.d.). *Úvod do kryptologie*. Retrieved from: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=7021

Miklas, M., & Světlík, J. (n.d.). *Počítačové viry*. Informatika na Gymnáziu a Jazykové škole s právem státní jazykové zkoušky Zlín. Retrieved from: http://www.gjszlin.cz/ivt/esf/ostatni-sin/pocitacove-viry.php

Ministerstvo vnitra České republiky. (2009). *Změna v kryptografických algoritmech, které jsou používány pro vytváření elektronického podpisu*. Retrieved from: http://www.mvcr.cz/clanek/zmena-v-kryptografickych-algoritmech-ktere-jsou-pouzivany-pro-vytvareni-elektronickeho-podpisu.aspx

Ministerstvo vnitra České republiky. (2015). *Přehled kvalifikovaných poskytovatelů certifikačních služeb a jejich kvalifikovaných služeb*. Retrieved from: http://www.mvcr.cz/clanek/prehled-kvalifikovanych-poskytovatelu-certifikacnich-sluzeb-a-jejich-kvalifikovanych-sluzeb-320051.aspx

MIT - Massachusetts Institute of Technology. (2016). *About.* Retrieved from: http://web.mit.edu/aboutmit/

Národný bezpečnostný úrad (2015). *Elektronický podpis*. Retrieved from: http://www.nbusr.sk/sk/elektronicky-podpis/

NSA/CSS. (2016). *About NSA.* Retrieved from: https://www.nsa.gov/

Odborná zdravotní pojišťovna. (n.d.). *KRYPTOGRAFIE - informace o elektronické komunikaci*. Retrieved from: http://www.ozp.cz/elektronicka-komunikace/informace/kryptografie

Piper, F., & Murphy, S. (2006). *Kryptografie*. Praha: Dokořán, s. r. o.

Raiffeisenbank. (2015). *Bezpečnost internetového bankovnictví*. Retrieved from: https://www.rb.cz/informacni-servis/doplnkove-informace-k-produktum/bezpecne-bankovnictvi/bezpecnost-internetoveho-bankovnictvi

Rivest, R. L. (n.d.). *The Early Days of RSA -- History and Lessons.* Retrieved from: https://people.csail.mit.edu/rivest/pubs/ARS03.rivest-slides.pdf

RSA Laboratories. (2000). *Frequently A s ked Questions about Today's Cryptography.* NorduGrid. Retrieved from: http://www.nordugrid.org/documents/rsalabs_faq41.pdf

SearchSecurity. (2014). *Pretty Good Privacy (PGP)*. Retrieved from: http://searchsecurity.techtarget.com/definition/Pretty-Good-Privacy

SearchSecurity. (2014). *RSA algorithm (Rivest-Shamir-Adleman)*. Retrieved from: http://searchsecurity.techtarget.com/definition/RSA

Staudek, J. (2004). *Standardizace bezpečnosti informačních technologií*. Masarykova univerzita. Retrieved from: http://www.fi.muni.cz/usr/staudek/vystavelova/

Steiner, F. (2008). *Bezpečnostní mechanismy*. Studijní materiály a informace pro studenty FEL ZČU. Retrieved from: http://home.zcu.cz/~steiner/ZPI/P%C2%B0edn%C3%9F%C3%9Cka%208.pdf

Šustr, J. (2002). *(Ne)bezpečná hesla*. SystemOnLine.cz – ekonomické a informační systémy v praxi. Retrieved from: http://www.systemonline.cz/clanky/ne-bezpecna-hesla.htm

Tlustý, P. (2006). *Obecná algebra pro učitele.* České Budějovice: Jihočeská univerzita.

UniCreditBank. (2015). *Důležité informace - pravidla bezpečného chování na internetu a v internetovém bankovnictví*. Retrieved from: https://www.unicreditbank.cz/web/novinky/dulezite-informace-pravidla-bezpecneho-chovani-na-internetu-a-v-internetovem-bankovnictvi

Valášek, M. A. (n.d.). *Asymetrické šifrování RSA v .NET - správa klíčů*. ASPNET.cz. Retrieved from: http://www.aspnet.cz/articles/148-asymetricke-sifrovani-rsa-v-net-sprava-klicu

Velebil, J. (2007). *Diskrétní matematika.* Praha: České vysoké učení technické v Praze.

Vondruška, P. (2004). *Úvod do klasických a moderních metod šifrovaní ALG082 Elektronický podpis.* Crypto-World. Retrieved from: http://msekce.karlin.mff.cuni.cz/~tuma/nciphers/elektronicky_podpis.pdf

Wang, J. (2011). *Thirty Years of Attacks on the RSA.* Wang Jingjing – Master Student at Shanghai Jiao Tong University. Retrieved from: https://cryptjwang.files.wordpress.com/2012/05/rsa_attacks.pdf

Wright, D. (2007). *The RSA Algorithm.* An Interactive Mathematical Proof System. Retrieved from: http://imps.mcmaster.ca/courses/SE-4C03-07/wiki/wrighd/rsa_alg.html

Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů.

III. Seznam tabulek, obrázků a grafů

IV. Přílohy

Příloha č. 1

Dobrý den,

jmenuji se Stanislav Froula a jsem studentem Jihočeské univerzity. V rámci mé bakalářské práce bych Vás rád požádal o vyplnění tohoto krátkého dotazníku. Dotazník je anonymní a jeho výsledky budou použity výhradně k vypracování bakalářské práce.

Předem děkuji za Váš čas.

1. **Využíváte internetové bankovnictví?**
    a. Ano
    b. Ne

2. **Jak často internetové bankovnictví využíváte?**
    a. Denně
    b. Několikrát týdně
    c. Jednou týdně
    d. Několikrát měsíčně
    e. Jednou měsíčně
    f. Méně

3. **K jakým účelům využíváte internetové bankovnictví?**
    (Možnost více odpovědí)
    a. Zjišťování zůstatku a pohybů na účtu
    b. Příkazy k úhradě
    c. Trvalé platby
    d. Zahraniční platby
    e. Mobilní platby (dobíjení SIM karet)
    f. Nastavení účtu (kontaktní údaje, změna hesla, distribuce výpisů…)
    g. Jiné (prosím vypište):
    …….

4. **U jaké banky máte vedený běžný účet?**
   (Pokud máte běžný účet u více bank, vyberte jen banku, u které považujete svůj účet za významnější.)
   a. Česká spořitelna
   b. ČSOB
   c. Komerční banka
   d. GE Money Bank
   e. mBank
   f. Raiffeisenbank
   g. Fio banka
   h. Air Bank
   i. UniCredit Bank
   j. Zuno Bank
   k. Equa bank
   l. Sberbank
   m. Expobank
   n. Citibank
   o. Jiná (prosím uveďte):
      …….

5. **Sdělili jste Vaše přihlašovací údaje do internetového bankovnictví někomu dalšímu?**
   a. Ano
   b. Ne

6. **Vaše heslo do internetového bankovnictví je kombinací:**
   (Zaškrtněte vše pravdivé)
   a. Alespoň 8 znaků
   b. Malých písmen
   c. Velkých písmen
   d. Číslic
   e. Speciálních znaků (např. @ # & $ ^ _ *)

7. **Jak často měníte Vaše heslo do internetového bankovnictví?**
    a. Alespoň jednou za 3 měsíce
    b. Alespoň jednou za rok
    c. Alespoň jednou za 2 roky
    d. Výjimečně
    e. Nehodlám heslo měnit

8. **Shoduje se Vaše heslo do internetového bankovnictví s heslem, které používáte pro přihlášení na jiné stránky?** (např. E-mail, Facebook, Twitter apod.)
    a. Ano
    b. Ne

9. **Jakým způsobem přistupujete do Vašeho internetového bankovnictví?**
    (Možnost více odpovědí)
    a. Z osobního počítače
    b. Z veřejného počítače (např. ve škole, v práci, knihovně, internetové kavárně apod.)
    c. Z počítače u přátel
    d. Z mobilního telefonu přes oficiální smartbanking aplikaci
    e. Z mobilního telefonu přes klasický internetový prohlížeč
    f. Jinak (prosím specifikujte):
    ……

10. **Jak budete postupovat v případě, že od banky obdržíte e-mail odkazující na internetové stránky banky, kde máte vyplnit přihlašovací údaje** (např. z bezpečnostních důvodů)?
    a. Vyplním na stránkách své přihlašovací údaje
    b. E-mail budu ignorovat
    c. Jiné (prosím specifikujte):
    ……

11. Jakým způsobem chráníte svůj počítač?

(Možnost více odpovědí)

a. Pravidelně aktualizuji operační systém a internetový prohlížeč
b. Používám antivirový software
c. Používám antispyware software
d. Nevypínám bránu Firewall
e. Nepotřebuji svůj počítač nijak chránit
f. Jiné (prosím specifikujte):

……

12. **Kontrolujete při přihlášení do internetového bankovnictví adresu stránky?**

(např. https://servis24.cz nebo https://ib24.csob.cz apod.)

a. Ano, vždy kontroluji/zadávám adresu
b. Ano, někdy
c. Spíše ne
d. Nikdy

13. Které z následujících termínů dokážete vysvětlit?

(Možnost více odpovědí)

a. Spyware
b. Phishing
c. Vir
d. Pharming

14. Víte, že Vaše banka na svých stránkách uvádí bezpečnostní zásady internetového bankovnictví?

a. Ano
b. Ne (Přejděte na otázku č. 16)

15. Přečetl/a jste tyto bezpečnostní zásady internetového bankovnictví?

a. Ano
b. Ne

16. Váš věk:

a. 15-27 let
b. 28-40 let
c. 41-50 let
d. 51-60 let
e. Nad 60 let

17. Vaše nejvyšší ukončené vzdělání:

a. Základní
b. Středoškolské bez maturity
c. Středoškolské s maturitou
d. Vyšší odborné
e. Vysokoškolské

18. Váš současný statut:

a. Student
b. OSVČ
c. Zaměstnaný na plný úvazek
d. Zaměstnaný na částečný úvazek
e. Nezaměstnaný
f. Důchodce

Zdroj: Vlastní zpracování