Návrh praktické úlohy pro potřeby kybernetické laboratoře

Jirka Čamek

Bakalářská práce
2023

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav ochrany obyvatelstva

Akademický rok: 2022/2023

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Jirka Čamek**
Osobní číslo:	**L20292**
Studijní program:	**B1032A020002 Ochrana obyvatelstva**
Forma studia:	**Prezenční**
Téma práce:	**Návrh praktické úlohy pro potřeby kybernetické laboratoře**

Zásady pro vypracování

1. Proveďte teoretický vstup do řešené problematiky.
2. Identifikujte vhodné oblasti pro návrh praktické úlohy pro potřeby výuky studentů v rámci kybernetické laboratoře Fakulty logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně.
3. Navrhněte zadání vybrané praktické úlohy.
4. Zpracujte příkladové řešení navržené praktické úlohy.

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. EVANS, Lester. *Cybersecurity: What You Need to Know About Computer and CyberSecurity, Social Engineering, The Internet of Things + An Essential Guide to Ethical Hacking for Beginners*. USA: Lester Evans, 2019. ISBN 9781794647237.
2. GROW, Christopher, Philip CRAIG a Donald SHORT. *Cybersecurity essentials*. Indianapolis, Indiana: Sybex, John Wiley, 2018. ISBN 978-1-119-36239-5.
3. KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o. CZ.NIC, 2019. ISBN 978-80-88168-31-7.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **Ing. Petr Svoboda, Ph.D.**
Ústav ochrany obyvatelstva

Datum zadání bakalářské práce: **1. prosince 2022**
Termín odevzdání bakalářské práce: **5. května 2023**

L.S.

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2022

PROHLÁŠENÍ AUTORA
BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 5.5.2023

Jméno a příjmení studenta: Jirka Čamek

.....
podpis studenta

ABSTRAKT

Bakalářská práce se věnuje problematice kybernetické bezpečnosti a návrhu praktické úlohy pro potřeby výuky studentů v rámci kybernetické laboratoře. V teoretické části práce jsou uvedeny základní pojmy týkající se problematiky informačních a komunikačních technologií, kybernetické bezpečností a kybernetických hrozeb.

Praktická část práce se zabývá charakterizací kybernetické laboratoře, identifikací oblastí pro návrh praktické úlohy, šifrováním a následným vytvořením zadání a postupu praktické úlohy. V závěru práce je zpracován názorný postup, jak úspěšně splnit praktickou úlohu.

Klíčová slova: Kybernetická bezpečnost, Kybernetické hrozby, Kyberprostor, malware, šifrování,

ABSTRACT

The bachelor's thesis focuses on cybersecurity issues and the design of a practical role for the needs of teaching students within the cyber lab. The theoretical part of the thesis includes basic concepts relating to the issues of information and communication technologies, cybersecurity and cyber threats.

The practical part of the work deals with the characterization of the cyber laboratory, identification of areas for the design of the practical task, encryption and the subsequent creation of the assignment and procedure of the practical task. At the end of the work, an illustrative process is developed to successfully fulfil the practical role.

Keywords: Cyber security, cyber threats, cyberspace, malware, encryption,

Tímto bych chtěl poděkovat vedoucímu mé bakalářské práce panu, Ing. Petru Svobodovi, za poskytnutí cenných rad, za vstřícný přístup a za všechny připomínky.

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Rozsáhlý vývoj komunikačních a informačních technologií vytvořil závislost všech vlastníků telefonů, tabletů a počítačů na sdílení dat a různých informací. Tyto technologie uživatelé používají pro své osobní ale také pracovní účely a staly se tak nesmírnou součástí běžného života. Pro běžného uživatele je pohyb na internetu jenom forma komunikace týkající se práce nebo soukromého života. Spousta uživatelů si ale neuvědomuje že svým pohybem na internetu vytváří příležitosti pro útočníky a jejich kybernetické útoky. Celkový nárůst závislosti na technologiích vytvořil daleko víc nových kybernetických hrozeb. Proto je kybernetická bezpečnost velmi aktuálním tématem a jelikož se vyvíjejí nové a vyspělejší technologie ke kterým v budoucnu boudou mít přístup jak běžní uživatelé, tak i útočníci se dá očekávat nárůst kybernetických hrozeb. Mezi nejčastější cíle kybernetických útoků patří cenná uživatelská data jako jsou přístupová hesla, čísla kreditních karet, záznamy komunikací, projekty a spousta dalších cenných souborů. Tyto útoky nejčastěji cílí na jednotlivce, kteří spadají pod menší organizace a nemají zrovna dostatečné znalosti o kybernetické bezpečnosti a pro je důležité, aby se každý jednotlivec, který má přístup k internetu naučil, jak se před útoky chránit a držet své data a soubory v bezpečí.

Problematika kybernetické bezpečnosti je a bude velmi důležitou součástí našich životu, a proto je důležitá informovanost o vyvíjejících se kybernetických hrozbách a oblastech které se zabývají ochranou před těmito hrozbami. Z těchto důvodů byl jednoznačný výběr bakalářské práce, aby informovala běžné uživatele o možnostech ochrany před kybernetickými útoky.

Hlavním cílem bakalářské práce je návrh praktické úlohy pro potřeby výuky studentů v rámci kybernetické laboratoře Fakulty logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně. Pro splnění hlavního cíle bylo nutné splnit následující dílčí cíle:

1. Rešerše v oblasti kybernetické bezpečnosti.
2. Identifikace vhodných oblastí pro návrh praktické úlohy.
3. Návrh zadání praktické úlohy pro danou oblast.
4. Realizace příkladového řešení navržené praktické úlohy

Pro účely vypracování této bakalářské práce byly použity následující metody:

- Analýza – V práci je využita pro vybraní vhodných programů pro praktickou úlohu.

- Komparace – V práci je využita pro identifikování vhodné oblasti pro návrh praktické úlohy.
- Literární rešerše – V práci je využita pro vypracování teoretické části a úvodu do problematiky pro návrh praktické úlohy.
- Syntéza – Tato metoda je použita v závěru práce.

I. TEORETICKÁ ČÁST

1 KOMUNIKAČNÍ A INFORMAČNÍ TECHNOLOGIE

V průběhu let se informační a komunikační technologie (dále jen ICT) vyvinuli tak že se dostali do bodu, kdy se stali nesmírnou součástí všech našich životu jak v profesionální, tak i v osobní sféře. Tyto technologie nám přinášejí užitek pro naši práci a zábavu. Bohužel vývoj ICT technologií přinesl i starost o bezpečnost před zneužitím těchto systému a ztrátou důležitých dat. Mezi problémy uživatelů v kyberprostoru se řadí nízká počítačová znalost, ale hlavně nulové povědomí o tom, jak celé zákoutí kyberprostoru funguje. Většina uživatelů si právě kvůli těmto chybějícím znalostem neuvědomuje dopady svého chování na internetu.

1.1 Kyberprostor

Kyberprostor je virtuální svět počítačů, který tvoří globální počítačovou síť složenou z menších sítí, které používají TCP/IP protokol. Interakce subjektů v kyberprostoru je totožná s interakcí v reálném světě, ale bez potřeby fyzické přítomnosti. Informace jsou sdíleny v reálném čase nebo s určitým zpožděním a lidé mohou nakupovat, sdílet zkušenosti, prozkoumávat obsah, provádět výzkum, pracovat nebo se bavit.

Kyberprostor lze také charakterizovat jako prostředí, kde se informace vytvářejí, zpracovávají, ukládají a šíří pomocí elektromagnetického vlnění. V obecnosti je to virtuální svět, který je vytvořen moderními technologiemi. (KOLOUCH, 2016)

Kyberprostor lze rozdělit na tři části:

- Surface Web – Část internetu, která je dostupná velké části společnosti a lze se v ní pohybovat pomocí webových prohlížečů. Surface Web zahrnuje jenom 4 % celého internetu.
- Deep Web – Tato část internetu není viditelná pomocí klasických vyhledávačů. Deep Web obsahuje 96 % veškerých informací v kyberprostoru.
- Dark Web – Je součástí Deep Webu se zaměřením na nelegální činnosti. Dostat se do této části kyberprostoru vyžaduje speciální prohlížeč. (ALZA, © 2019)

1.2 Počítačová síť

Počítačová síť je skupina propojených počítačů, které umožňují sdílení dat, informací a zdrojů mezi jednotlivými uzly sítě. Tyto uzly mohou být počítače, servery, tiskárny nebo další zařízení, která jsou připojena k síti a umožňují komunikaci s ostatními uzly pomocí různých technologií, jako jsou Ethernet, Wi-Fi nebo Bluetooth. Komunikace mezi těmito

uzly probíhá podle předem stanovených pravidel a vysoké spolehlivosti komunikace. (HORÁK, KERŠLÁGER, 2011)

Počítačové sítě jsou dnes běžně používány v mnoha různých oblastech, jako jsou kancelářské prostředí, školy, nemocnice, průmysl, banky nebo dokonce domácí sítě pro sdílení internetového připojení a dalších zdrojů. Síťové technologie také umožňují vzdálený přístup k počítačům a datům, což umožňuje práci na dálku a zvyšuje efektivitu práce v mnoha oborech. Tyto počítačové sítě lze rozdělit do tří hlavních skupin. (KOLOUCH, 2016)

1.2.1 Dělení dle rozsahu sítí

Podle rozsahu sítí se sítě rozdělují na čtyři základní skupiny:

- Osobní síť (PAN) – Jedná se o malou privátní síť, která slouží pro potřeby jednotlivce nebo celé domácnosti. K propojení jednotlivých systémů tato síť využívá Bluetooth nebo WiFi.
- Lokální síť (LAN) – Jedná se o velkou lokální síť v rámci, které dochází k propojení jedné nebo více budov. K propojené dochází za pomocí routeru nebo switch zařízení.
- Metropolitní síť (MAN) – Jedná se o síť, která propojuje veškeré lokální sítě, které se vyskytují v dosahu desítek kilometrů.
- Vzdálená síť (WAN) – Jedná se o síť, která propojuje jednotlivé LAN a MAN sítě na geografické úrovni v rozsahu kontinentu ale i celosvětově. (KOLOUCH, 2016)

1.2.2 Dělení dle postavení síťových uzlů

- Peer-to-peer (rovný s rovným) – Jde o počítačovou síť, kde mezi sebou komunikují jednotlivé počítačové systémy. Používá se pro sdílení souborů a systémových prostředků.
- Klient-server – Je typ sítě, kde je jeden nebo více počítačových systému nadřazen jinému počítačovému systému. Na tomto modelu klient-server jsou založeny služby typu web a e-mail. (KOLOUCH, 2016)

1.2.3 Dělení dle vlastnictví sítí

- Privátní síť – Tato síť využívá privátní IP adresy a jsou používány hlavně v rámci sítě LAN. Tyto sítě se využívají z důvodu nedostatečného množství veřejných IP adres ve verzi IPv4.

- Veřejná síť – Tento typ sítě je využíván ke komunikaci a přenosu dat mezi širokou veřejností. Tyto sítě provozují spojové organizace, které splňují veškeré potřebné požadavky.
- Virtuální privátní síť (VPN) – VPN je mechanismus který propojuje počítačové systémy za pomocí nedůvěryhodné sítě tak, že komunikace mezi těmito systémy vypadá jako by byly propojeny důvěryhodnou sítí. (KOLOUCH, 2016)

1.3 Internetový Protokol a IP adresa

Internet Protocol (dále jen IP) zajišťuje přenos datagramů na základě síťových IP adres, které jsou uvedeny v jejich hlavičce. Datagram je samostatná datová jednotka, která obsahuje všechny potřebné informace o adresátovi a odesílateli, včetně pořadového čísla datagramu ve zprávě. Datagramy jedné zprávy jsou přenášeny nezávisle na sobě a mohou putovat sítí v různém pořadí, přičemž doručení nemusí odpovídat pořadí ve zprávě. (KOLOUCH, 2016)

Podstatnou informací je, že pro komunikaci v síti potřebuje každý počítačový systém unikátní IP adresu. IP adresy mohou být přidělovány staticky (kdy je adresa manuálně přidělena počítačovému systému) nebo dynamicky (kdy je nová IP adresa přidělena automaticky na základě MAC adresy při připojení k síti). IP adresa slouží jako jeden z identifikátorů počítačového systému při komunikaci s ostatními počítačovými systémy a standardně není anonymní. (DOSTÁLEK, 2003)

V současnosti existují dvě verze IP:

- IPv4 – Jedná se o první rozšířenou a stále nejpoužívanější verzi internet protokolu která využívá 32bitové adresy. Tyto adresy jsou psány dekadicky po jednotlivé osmici bitů.
- IPv6 – Tento nový internetový protokol byl vytvořen z důvodu nedostatku veřejných IPv4 adres a má délku 128 bitů, které jsou psány hexadecimálně. V této verzi protokolu byla odstraněna potřeba funkce překladu sítových adres. (ALZA, © 2021)

1.4 MAC Adresa

MAC adresa je speciální identifikátor, který se skládá ze 48 bitů. Mac adresa se používá pro síťová zařízení a je využívána různými protokoly druhé vrstvy. MAC adresa se přiděluje při výrobě síťové karty a je proto také označována jako fyzická adresa. Každá přidělená MAC adresa je unikátní na celém světě, ale teoreticky ji lze zfalšovat. Adresa je rozdělena na dvě

poloviny kde první polovina identifikuje výrobce síťové karty a druhá polovina je jedinečným identifikátorem karty, který byl přidělen výrobcem. (BROOKS, GROW, CRAIG, SHORT, 2018)

1.5 Legislativa

Následující právní normy regulují kyberprostor v České republice.

- Zákon č. 40/2009 Sb., trestní zákoník. (ČESKO, 2009)
- Zákon č. 141/1961 Sb., o trestním řízení soudním. (ČESKO, 1961)
- Zákon č. 127/2005 Sb., o elektronických komunikacích. (ČESKO, 2005)
- Zákon č. 480/2004 Sb., o některých službách informační společnosti. (ČESKO, 2004)
- Zákon č. 273/2008 Sb., o Policii České republiky. (ČESKO, 2008)
- Zákon č. 89/2012 Sb., Občanský zákoník. (ČESKO, 2012)
- Zákon č. 441/2003 Sb., o ochranných známkách. (ČESKO, 2003)
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů. (ČESKO, 2014)
- Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti . (ČESKO, 2018)
- Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích. (ČESKO, 2014)
- Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury. (ČESKO, 2010)
- Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby. (ČESKO, 2017)
- Vyhláška č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu. (ČESKO, 2021)
- Vyhláška č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci. (ČESKO, 2021)

2 KYBERNETICKÁ BEZPEČNOST

Kybernetická bezpečnost je pořád považována za nový obor, ale za posledních deset let získala velkou pozornost a stala se jednou z hlavních priorit mnoha národních politik. Je to z velké části způsobeno celosvětovým rozvojem informačních a komunikačních technologií ICT. Zvýšená závislost na těchto technologiích a kyberprostoru s sebou však přináší potenciální rizika a hrozby. Mezi hlavní otázky patří ochrana vládních tajemství a kritické infrastruktury. Pokud by se to nepodařilo, mohlo by to mít vážné důsledky pro národní bezpečnost, ekonomiku, administrativu i bezpečnost obyvatelstva. Kyberprostor není omezován hranicemi ani kontinenty, což umožňuje téměř neomezený přístup a relativní anonymitu. Zvážení těchto vlastností vytváří příznivé prostředí pro kyberkriminalitu. (VLÁDA ČR, © 2021)

V dnešní době, pokud jde o kybernetickou bezpečnost, pro mnoho lidí toto odvětví představuje obor, kterým se zabývají oddělení s informačními a komunikačními technologiemi. Nicméně tato teorie je chybná. Protože kybernetická bezpečnost se týká nás všech, kteří využíváme jakýkoliv prvek jejího ICT v našem každodenním životě. (KOLOUCH, BAŠTA, 2019)

„*Kybernetickou bezpečnost nelze v současné době ani podceňovat ani bagatelizovat. Je to oblast, která je pro řadu organizací, ale i jedinců samotných klíčová, a proto by měla být řešena dlouhodobě a systematicky*.“ (KOLOUCH, BAŠTA, 2019, s. 40)

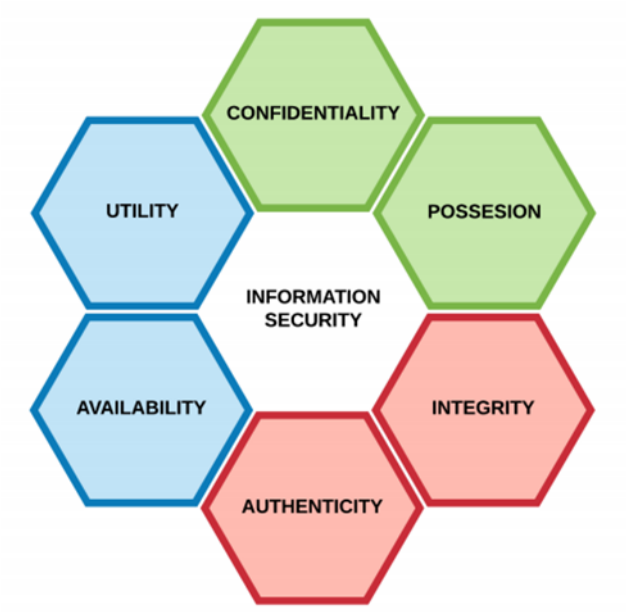
Pro zajištění kybernetické bezpečnosti je nejdůležitější, aby si všichni uživatelé, kteří vlastní jakoukoliv informační a komunikační technologii představili že veškerý jejich pohyb a jakékoliv chování v kyberprostoru ovlivňuje úspěšnost útočníků při kybernetických útocích. Kybernetickou bezpečnost a veškerou její aktivitu lze aplikovat i mimo kyberprostor a nesmí se podceňovat. (KOLOUCH, BAŠTA, 2019)

Při aplikaci kybernetické bezpečnosti jsou implementovány 3 hlavní principy, známé také jako triády kybernetické bezpečnosti. Mezi tyto triády se řadí CIA, prvky kybernetické bezpečnosti a životní cyklus kybernetické bezpečnosti. (KOLOUCH, 2016)

2.1 Triáda CIA

Důvěrnost, integrita a dostupnost, známá také jako Triáda CIA, je model vyvinutý jako vodítko pro politiku informační bezpečnosti v rámci organizací. Tyto 3 prvky triády jsou nejzákladnější a nejdůležitější principy kybernetické bezpečnosti. V této souvislosti je důvěrnost souborem pravidel, která omezují přístup k informacím, integrita je ujištění, že informace jsou důvěryhodné a přesné, a dostupnost je zárukou spolehlivého přístupu oprávněných osob k informacím. (KOLOUCH, BAŠTA, 2019)

Podle odborníků se Triáda CIA ale nepovažuje za dostačující. Donn B. Parker v roce 1998 potvrdil že Triáda CIA potřebuje rozšířit a doplnil ji o nové 3 principy. Tento nový soubor principů Parker nazval Parkerian hexad (viz. Obrázek 1).



Obrázek 1 - Parkerian hexad (MARKS, © 2023)

Do nového souboru principů zařadil držení a kontrolu, autentičnost a užitečnost:

- Držení a kontrola – Představuje stav, kdy neoprávněná osoba získá kontrolu nad něčím, co nevlastní, ale nedojde k jejímu zneužití.
- Autentičnost – Představuje stav, kdy je zdroj informací správně označen certifikátem pravosti.
- Použitelnost – Představuje stav, kdy data musejí splňovat dostupnost ale také užitečnost. (PENDER-BEY, 2012)

2.2 Prvky kybernetické bezpečnosti

Vhodná úroveň kybernetické bezpečnosti je dosažena díky vzájemné interakci mezi lidmi, technologiemi a procesy. Ačkoli technologie mohou být zásadním prvkem pro kybernetickou bezpečnost, důležitějšími stavebními kameny jsou správně nastavené procesy a zejména lidé, kteří jsou schopni tyto procesy aplikovat a dodržovat dohodnutá pravidla. (Q-COM, © 2023)

Lidé:

Lidé jsou klíčovým prvkem v oblasti kybernetické bezpečnosti. Jsou tvůrci bezpečnostních pravidel a zároveň jejich uživateli. Ale také jsou nejslabším článkem v celém systému a často se stávají cílem útočníků. Je nutné je pravidelně informovat o základních pravidlech a posilovat jejich vzdělání v oblasti kybernetické bezpečnosti, protože jsou největší hrozbou pro tuto oblast.

Lidé, kteří používají ICT by měli znát a dodržovat tyto principy a pravidla kyberprostoru:

- Základní principy a pravidla kybernetické bezpečnosti.
- Znát základní funkce počítačových systémů které používají.
- Zanalyzovat si aplikace které využívají.
- Vzdělávat se v oblasti kybernetické bezpečnosti. (KOLOUCH, BAŠTA, 2019)

Technologie:

Existuje celá řada technologií, které můžeme využívat, ale žádná z nich nevyřeší bezpečnostní problémy.

Technologie jsou pro uživatele obvykle prostředkem, který jim umožňuje připojení k internetu, sociálním sítím a dalším aplikacím. Tyto nástroje slouží k vytváření dokumentů, zasílání e-mailů a sledování videí. Běžný uživatel interaguje se svými koncovými technologiemi (PC, tablet, mobilní telefon), ale zpravidla se nezajímá o další technologie, které jsou nezbytné pro danou činnost v kyberprostoru.

Technologie jsou pro organizace nezbytné, a to včetně zařízení, která jsou určena pro uživatele (mobilní zařízení), kompletní infrastruktury sítě (LAN, Wi-Fi prvky), služeb (servery, aplikace) a prvky zajišťující bezpečnost, ať už v perimetru (firewall, IDS/IPS) nebo v rámci infrastruktury (prvky pro autentizaci a autorizaci, monitoring a analýzu). (SMEJKAL, SOKOL, KODL, 2019)

Technologie jsou obvykle nevyhnutelnou součástí kybernetické bezpečnosti, které, bez ohledu na to, zda jsou používány jednotlivci nebo organizací. Pro zajištění kybernetické bezpečnosti je tedy nutné udržovat technologie v takovém stavu, aby byly schopné reagovat na změny, které souvisejí s vývojem ICT. Hlavním způsobem, jak toho dosáhnout, je pravidelné aktualizování a zabezpečení technologií včetně hardwaru a softwaru. (Q-COM, © 2023)

Procesy:

Procesy představují činnosti, které je nutné provést, aby bylo možné lidem umožnit využívat implementované technologie a příslušné služby.

Mezi základní procesy se řadí:

- Definování aktiv a analýza rizik.
- Implementace ICT a aplikací.
- Zpráva uživatelů a rolí.
- Autorizace a autentizace.
- Údržba systémů a služeb.
- Testování zabezpečení jednotlivých systémů.
- Analýza a realizace opatření.
- Školení a cvičení atd.

Tyto procesy se týkají celého životního cyklu ICT, informací a dat a zahrnují i uživatele. Implementace, údržba a modifikace těchto procesů představují nejnáročnější část budování kybernetické bezpečnosti a vyžadují vysokou úroveň odbornosti ze strany správců systémů. Pokud organizace implementuje pravidla kybernetické bezpečnosti, je důležité udržovat software a hardware aktuální a dodržovat přístupová pravidla pro jednotlivé systémy. (KOLOUCH, 2016)

2.3 Životní cyklus kybernetické bezpečnosti

Při budování kybernetické bezpečnosti je nutné brát v úvahu časový průběh a uplatňovat nebo modifikovat triádu CIA a další prvky v průběhu celého cyklu. Prevence, detekce a reakce na útok jsou klíčovými prvky. Diagramy jsou často používány k zobrazování životního cyklu kybernetické bezpečnosti pro lepší přehlednost. (HUB, 2013)

Obrázek 2 - Životní cyklus Kybernetické bezpečnosti (KYBEZ, 2021)

Kybernetickou bezpečnost lze přirovnat k neustálému hodnocení rizik, ale kromě běžné analýzy je nutné provádět i další podpůrné procesy, které mohou přispět ke zlepšení kybernetické bezpečnosti organizace. (KOLOUCH, BAŠTA, 2019)

3 KYBERNETICKÝ ÚTOK

Kybernetické útoky jsou početnější více než v předchozích letech, a to kvůli většímu využívání počítačových serverů a samotných počítačů ve všech možných oborech na kterých se jejich uživatelé stali více závislí. Každá firma už využívá počítačové servery pro své účely jakožto zálohování dat, provozování e-shopu a internetové bankovnictví. Většina z těchto útoků jsou zaměřené na servery s cílem získat data nebo je vyřadit z provozu. Jako další se využívají programy, které zablokují server nebo celý firemní systém a za jeho obnovu útočnici požadují peníze. Útoky cílí nejen na energetické společnosti, banky a vládní agentury, ale také na univerzity a zdravotnická zařízení. (KOLOUCH, BAŠTA, 2019)

Útok na IT infrastrukturu je úmyslný čin útočníka nebo skupiny útočníků. K útokům na cizí servery a počítače používají svou IT technologii, a to k získání kritických informací nebo k poškození či deaktivaci počítačových systémů. Všechny tyto aktivity se konají v kyberprostoru. Aktivity ve formě kybernetických útoků přitom mohou být jednáním sociálního inženýrství s jediným cílem získat informace, nebo naopak s cílem omezit pomocí DoS nebo DDoS útoku funkčnost jednoho nebo více serverů. (JIROVSKÝ, 2007)

Kybernetický útok lze také definovat jako nezákonné jednání v kyberprostoru s cílem ublížit jiné osobě nebo skupině osob. „*Tato jednání nemusí mít vždy podobu trestného činu, podstatné je, že narušují běžný způsob života poškozeného. Kybernetický trestný čin musí být zároveň kybernetickým útokem, avšak ne každý kybernetický útok musí být trestným činem. Řadu kybernetických útoků je, i díky absenci trestněprávní normy, možné subsumovat pod jednání, které bude mít povahu správněprávního, či občanskoprávního deliktu, případně se nemusí jednat o jednání, které je postižitelné jakoukoli právní normou.“* (KOLOUCH, 2016, s.55)

3.1 Kybernetická hrozba

Kybernetická hrozba je možný škodlivý pokus poškodit nebo narušit počítačovou síť nebo systém. Pohybují se od kybernetické špionáže, hackerských útoků a DDoS útoků až po narůstající internetové podvody a krádeže a další formy trestné a nežádoucí činnosti v prostředí informačních technologií. Hrozby v kyberprostoru jsou proto jednou z hlavních výzev naší doby. (MINISTERSTVO VNITRA, © 2023)

3.2 Druhy kybernetických útoků

Útočníci neboli hackeři se díky technologickému vývoji a s nekonečnou možností využití času dostali do bodu kdy je jednodušší proniknout do jakéhokoliv informačního systému a počítačové sítě. Pro své nezákonné aktivity v kyberprostoru využívají spousty škodlivých softwarů, které si postupem času vylepšují a mění, aby se co nejlépe přizpůsobovali ochranným prvkům. K vyvíjejícím se softwarům přidávají i různé fyzické nebo psychologické praktiky které v kombinaci s technologickým vybavením zvyšují úspěšnost kybernetických útoků. Některé nejznámější škodlivé softwary a praktiky si představíme v následujících podkapitolách.

3.2.1 Škodlivý software (Malware, Ransomware)

Malware neboli škodlivý software je obecný termín pro jakýkoli škodlivý program nebo kód, který napadá a poškozuje systém. Do jakéhokoliv zařízení se může dostat pomocí sociálních sítí nebo e-mailu. Nepřátelský, rušivý a záměrně škodlivý malware proniká a poškozuje počítače, počítačové systémy, sítě, tablety a mobilní zařízení, často tím, že částečně ovládá provoz zařízení. V zařízení narušuje normální fungování. (KOLOUCH, BAŠTA, 2019)

Tento škodlivý program může být navržen tak, aby na vás vydělával peníze, narušoval vaši schopnost pracovat, činil politická prohlášení nebo se jednoduše chlubil vašimi zprávami. Malware nemůže poškodit fyzický hardware systémů nebo síťových zařízení, ale může krást data, šifrovat, mazat, upravovat nebo napadat základní funkce vašeho počítače a špehovat aktivity vašeho počítače bez vašeho vědomí. (MALWAREBYTES, © 2023)

Nyní si rozebereme nejčastější varianty malwaru, které útočníci používají:

- Virus – Tento škodlivý program se s pomocí člověka dostane do počítače kde kopíruje sám sebe do ostatních souborů a provádí škodlivou činnost.
- Počítačový červ – Tento škodlivý program má stejné chování jako virus jen pro své šíření hledá chyby v softwaru.
- Trojský kůň – Tento škodlivý program se schovává v uživateli již ověřeném programu. Při infikování systému okamžitě působí škody a uděluje útočníkovi vzdálený přistup.
- Spyware – Tento škodlivý program bez vědomí krade a ukládá si důvěrné informace o uživateli a následně je zasílá útočníkovi.

- Adware – Tento škodlivý program posílá nežádoucí reklamy, ze kterých generuje zisky, které posílá tvůrci programu.
- Scareware – Tento škodlivý program využívá techniky sociálního inženýrství za účelem nalákat uživatele na škodlivé webové stránky.
- Rootkity – Tyto počítačové programy slouží jako maskovací zařízení jiných škodlivých programů. V počítači se rootkity chovají tak že mění chování operačního systému aby neodhalil malware.
- Keylogger – Tento typ škodlivého program zaznamenává konkrétní stisky kláves na napadeném počítači. Využívá se ke zjištění přihlašovacích údajů. (KOLOUCH, 2016)

Ransomware

Tento druh malwaru známý jako Ransomware je typ škodlivého programu, který uživatelům blokuje přístup k jejich systémům, osobním souborům, počítačům, tabletům a taky telefonům. Za jejich následné odblokování útočník požaduje peníze v podobě platby kreditními kartami nebo převodem kryptoměny. Ransomware je jednou z nejpopulárnějších a největších kybernetických hrozeb v dnešní době kterou útočníci používají. Útočníci se zaměřují na všechny druhy jednotlivců, firem a organizací. (MALWAREBYTES, © 2023)

Nyní si rozebereme nejčastější varianty ransomwaru, které útočníci používají:

- Diskcoder – Zabraňuje uživateli používat operační systém tím, že blokuje záznamy z pevného disku.
- Screen locker – Zablokuje uživateli přístup k hlavní obrazovce.
- PIN locker – Zablokuje uživateli přístup tím, že vytváří falešný PIN kód.
- Kryptografický ransomware – Blokuje uživateli přístup k datům pomocí šifrování. (ESET, © 1992–2023)

3.2.2 Phishing

Phishing je typ kybernetického útoku, který využívá techniky sociálního inženýrství, pomocí kterých se útočník snaží získat důvěrné informace ze zařízení nebo na něm spustit škodlivý kód. Nejzákladnější formou těchto útoků jsou podvodné e-maily požadující informace o platební kartě nebo záznamy internetového bankovnictví. Útočníci se nejčastěji vydávají za

již známe firmy, ke kterým mají oběti důvěryhodný vztah. V e-mailu pak už jen stačí otevřít falešný odkaz a vyplnit přístupové údaje. Výjimkou ale nejsou ani chatovací aplikace a sociální sítě. (ESET, © 1992–2023)

Nejčastější typy phishingových útoků:

- E-mail phishing – Hromadné posílaní podvodných e-mailů.
- Spear phishing – Posílaní podvodných e-mailů které jsou vytvořeny přesně pro daného jednotlivce nebo skupinu.
- Whaling – Spear phishingové zprávy které se soustředí na majitele firem.
- CEO fraud – Hromadné posílaní podvodných e-mailů které cílí na zaměstnance.
- Vishing – Podvodné útoky za pomocí falešných telefonátů.
- Smishing – Podvodné útoky za pomocí SMS zpráv.
- Page hijacking – Podvodné útoky za pomocí falešných webových stránek. (KOLOUCH, 2016)

3.2.3 Sociální inženýrství

Sociální inženýrství je typ kybernetického útoku, při kterém se útočníci snaží zmanipulovat své oběti, aby získali přístup k datům, počítačům, firemním systémům nebo přístup do objektů. Tyto techniky spoléhají na lidskou zvědavost, chamtivost a závist. Oběti se mylně domnívají, že jim poskytnuté informace od útočníků jsou pravdivé. Cílem je donutit oběť k provedení konkrétní akce (poskytnutí hesla, provedení platby nebo fyzického přístupu k počítači nebo jinému systému). Pro útočníky je sociální inženýrství nejjednodušší způsob k získání toho, co potřebují, jelikož nemusejí složitým způsobem dešifrovat heslo nebo se dostávat do systému. Stačí si získat důvěru od správného člověka a podvodem vylákat vše potřebné. (AVAST, © 1988-2023)

Kybernetické útoky za pomocí sociálního inženýrství nesouvisejí s klasickými metodami, které hackeři používají, ale ve zjišťování důležitých informací o firmách a jejich zaměstnancích. Skvělým nástrojem k hledání těchto informací perfektně slouží sociální sítě a různé webové stránky. Tyto útoky se mohou uskutečňovat online, osobně a telefonicky. Klíčovým faktorem pro nejjednodušší průběh tohoto útoku je dlouhá ale velmi důkladná příprava. (EVANS, 2019)

Aby se snížili riziko sociálního inženýrství, musí se zvýšit povědomí o možných hrozbách nejen pro organizace, ale i pro společnost jako celek. Pro útočníky je mnohem snazší zaměřit své útoky na velké množství neznalých a neinformovaných lidí než na relativně dobře chráněné podniky. (KOLOUCH, 2016)

3.2.4 Denial of service attack

Denial of service (dále jen DoS) je typ kybernetického útoku za účelem omezit uživatelům používání některých síťových služeb nebo znepřístupnit počítač a tím zamezit normální fungování daného zařízení. Pro tento typ útoku stačí vlastnit jeden počítač, a proto je velice oblíbený mezi útočníky. Útoky DoS se zaměřují na internetové služby, které mohou zahrnovat e-mail, webové stránky, internetové bankovnictví nebo jiné služby které závisí na dotčeném počítači nebo síti. Stavu odepření služby dochází ze dvou důvodů. V první možnosti se útočník snaží přetížit sít nebo aplikaci uživatele velkým objemem provozu což způsobí zpomalení nebo zhroucení systému. V druhé možnosti se útočník pokouší dosáhnout zpomalení nebo zhroucení systému za pomocí posílání velkého množství paketů v nefunkčním formátu. (CISA.GOV, © 2021)

Distributed Denial of Service (dále jen DDoS) je efektivnější typ kybernetického DoS útoku. Hlavní rozdíl mezi těmito útoky je ten, že DDoS využívá celou síť napadených zařízení. Počítače v této síti jsou napadána bot malwarem a stávají se z nich zombie zařízení. Pomocí řídících serverů posílají přes zombie zařízení nežádoucí požadavky. Tyto zařízení pak útočí na síťové prvky systému, které se potřebují připojit k internetu, webovým stránkám, serverům nebo databázím, dokud nedojde k přetížení systému. (ESET, © 1992–2023)

Distributed Reflected Denial of Service (dále jen DRDoS), je typ distribuovaného DoS útoku, který využívá mechanismus odražení. Tento útok funguje tak, že útočník rozesílá podvržené požadavky na spojení na mnoho počítačových systémů, kteří na ně odpovídají. Tyto podvržené požadavky mají jako zdrojovou adresu uvedenou adresu oběti, což má za následek zahlcení oběti odpověďmi na tyto požadavky. Tím se mnoho počítačových systémů stává nevědomými účastníky útoku. (KOLOUCH, 2016)

Mezi typy DoS útoků řadíme:

- Ping flood – Za pomocí Internet Control Message Protokol a nástroje Ping útočník zjistí, zda je zařízení připojené v síti. Po zjištění útočník posílá co nejrychleji velké množství zpráv, na které dané zařízení nezvládá odpovídat, a proto přestává správně fungovat.

- SYN-flood – Útočník se pokouší zahlcovat svou oběť množstvím požadavků na navázání spojení. Cílový systém se snaží na požadavky odpovědět, ale útočník neodpovídá. Cílový počítačový systém čeká na finální potvrzení a drží pro toto spojení omezené zdroje. To může vést k vyčerpání systémových zdrojů a jeho selhání.
- DNS flood – Útočník provádí útok, při kterém zasílá falešné DNS dotazy na DNS server z mnoha podvržených IP adres. Počet falešných dotazů je tak velký, že DNS server není schopen odpovídat včas a dochází k jeho zpomalení nebo dokonce k jeho zhroucení.
- Falšování zdrojové adresy – Metoda nazývaná IP spoofing spočívá v úpravě zdrojové adresy odesílaných datových paketů. Tento postup umožňuje útočníkovi zesílit DoS útoky. Útočník používá tuto techniku tehdy, když nepotřebuje odpověď od cíle na svou žádost o navázání spojení, ale pouze chce cílový systém přetížit a zahlcovat ho tak, aby způsobil jeho výpadek. (KOLOUCH, 2016)

4 DÍLČÍ ZÁVĚR

Teoretická část této bakalářské práce byla věnována základním charakteristikám jednotlivých oblastí týkající se problematiky informačních a komunikačních technologií a základních definic kybernetické bezpečnosti. Dále byli vymezeny tři hlavní principy známé jako triády kybernetické bezpečnosti. Nedílnou součásti teoretické části je legislativní rámec, který reguluje kyberprostor v České republice. Hlavní součástí teoretické části je problematika kybernetických hrozeb, kde byly uvedeny ty nejznámější typy kybernetických útoků a nejpoužívanější psychologické praktiky které útočnici využívají pro proniknutí do různých systémů a následné krádeži citlivých dat. Tyto praktiky se na základně prvků kybernetické bezpečnosti ve vysoké míře týkají lidí, kteří vlastní a využívají informační a komunikační technologie. Proto je potřeba ve vysoké míře informovat a poučit běžné uživatele v kyberprostoru, jak se jednoduše před těmito útoky chránit a zamezit zneužití citlivých informací které vlastní.

II. PRAKTICKÁ ČÁST

5 LABORATOŘ KYBERNETICKÉ BEZPEČNOSTI NA FLKŘ

„Laboratoř kybernetické bezpečnosti na Fakultě logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně, která vznikla ve spoluprací s firmou T-Soft, a.s., se zaměřuje na výuku a vědeckou činnost týkající se procesů v oblasti kybernetické bezpečnosti." Vybavení kybernetické laboratoře zahrnuje hardwarové vybavení a různé softwarové nástroje které mají využití v oblasti kybernetické bezpečnosti. Vybavení umožňuje řešit jak současné, tak i budoucí hrozby, a to s vysokou mírou customizace, včetně implementace nových scénářů. Díky tomu může laboratoř okamžitě reagovat na nově vznikající hrozby a související reaktivní opatření v turbulentních situacích. (FLKŘ.UTB, © 2023)

5.1 Softwarové a technologické vybavení

Kybernetická laboratoř disponuje různými typy nástrojů, softwarů a dalšími technologiemi, které využívá pro výuku studentů v oblasti kybernetické bezpečnosti na pracovištích. Laboratoř disponuje následujícím vybavením:

Kamery a kamerové technologie:

- *„Kamera AXIS Q1615 MK II S/N ACCC8EF1C4E8"*
- *„Bezdrátový mikrofon MBD 840 S/N 21891201907026"*
- *„AXIS M3015 pro modul People Counter"*
- *„Analytické SW moduly People Counter a Motion Guard"*

Systémy pro monitorování infrastruktury:

- *„Flowmon"*
- *„LogManager"*

Uměla inteligence a virtuální/smíšená realita:

- *„Microsoft Azure Machine Learning Studio"*
- *„3D VR brýle HTC VivePro Eye"*
- *„Microsoft Hololens"*

Softwary pro podporu a simulaci scénářů a zobrazení společné situace:

- *„Riskan"*

- *„Terrex“*
- *„Practis“*
- *„Practis GO“*
- *„Situnet“*
- *„Situboard“*

Scénáře pro cvičení:

„Součástí laboratoří je knihovna scénářů sloužících k procvičení různých kritických situací a reakce na tyto typy situací.“ (KM.FLKŘ.UTB, © 2020)

5.2 Využití laboratoře

Hlavním cílem laboratoří na Fakultě logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně (dále jen FLKŘ) je získání praktických dovedností v oblastech kybernetické bezpečnosti, krizového řízení a logistiky. Pro dosažení tohoto cíle jsou poskytovány veškeré potřebné pomůcky, nástroje a scénáře, které umožní porozumět bezpečnostním pravidlům, vytvořit si návyky a detekovat potenciální hrozby v těchto oblastech.

V těchto laboratořích je jednou z hlavních možností, jak připravit studenty na reálné kritické situace v oblastech určených pro tyto laboratoře, a to za pomocí simulování daných scénářů do patřičné míry připravenosti. Výuka je prováděna v technické ale i procesní rovině. Technické a technologické znalosti jsou důležitým základem pro přípravu na kritické situace ale zejména je kladen důraz na procesy dané problematiky.

„Jde o různé způsoby využití učeben krizového řízení, které zahrnují specializované vybavení a slouží k rozšíření a prohloubení znalostí a dovedností odborníků nejen z veřejné správy, ale také ze soukromého sektoru, zejména z organizací patřících do kritické infrastruktury státu.“ (KM.FLKŘ.UTB, © 2020)

Konkrétně nabízí laboratoř v případě personálního zabezpečení potenciál v oblasti kybernetické a informační bezpečnosti:

- *„Realizovat specializované přednášky a workshopy na aktuální téma.“*
- *„Reálně ověřit přípravu a akceschopnost území na vybrané mimořádné události a krizové situace.“*

- *„Simulace jednání pracovních skupin při řešení nastalé mimořádné události nebo krizové situace.“*
- *„Komunikace s veřejností a médii.“* (KM.FLKŘ.UTB, © 2020)

6 OBLASTI PRO NÁVRH PRAKTICKÉ ÚLOHY

V problematice kybernetické bezpečnosti se nachází spousta možností, jak využít technologické vybavení pro proniknutí do systému a do sítí za účelem získání citlivých dat. Hackeři nejčastěji pro své útoky využívají různé škodlivé programy, které hledají chyby v softwaru a díky tomu se dostávají k citlivým informacím jako jsou přístupové údaje a různé důležité informace pro jednotlivce nebo organizaci.

Při seznámení se s prostředím laboratoře a jejím technologickým vybavením jsem na základě vyvíjející se situace v problematice kybernetické bezpečnosti identifikoval následující oblasti, na něž je vhodné se ve výuce zaměřit.

6.1 Vhodné oblasti

Bezpečnostní analýza sítě:

Analýza zabezpečení sítě je proces hodnocení bezpečnosti dané informační sítě s cílem identifikovat a posoudit rizika spojená s možnými hrozbami. Cílem je určit, co je třeba udělat pro zabezpečení sítě a minimalizaci rizik. Během analýzy zabezpečení sítě se obvykle zkoumají různé aspekty sítě, jako jsou síťové prvky, směrovače, přepínače, firewally, přenosová média, kabely a bezdrátová připojení, stejně jako aplikace a služby používané v síti. V rámci analýzy zabezpečení sítě lze identifikovat potenciální hrozby, jako jsou útoky skupin hackerů, malware a neoprávněný přístup. Tyto hrozby jsou posuzovány na základě závažnosti a pravděpodobnosti výskytu. Na základě výsledků analýzy zabezpečení sítě jsou navržena opatření ke snížení rizik. (SHINDER, 2003)

Penetrační testování:

Penetrační testování neboli pentesting je legální proces testování bezpečnosti informačních systémů za účelem zjištění potenciálních bezpečnostních hrozeb a slabin. Během penetračního testování se používají různé techniky a nástroje k simulaci útoků, které by na systém mohl provést skutečný útočník.

Cílem penetračního testování je odhalit bezpečnostní slabiny, které by mohly být zneužity k získání neoprávněného přístupu k systému nebo odcizení dat. Testování může být prováděno interně v rámci organizace nebo externě třetí stranou bez znalosti systému, čímž se simuluje perspektiva skutečného útočníka. Výsledkem penetračního testu by měla být zpráva, která identifikuje slabá místa a navrhne kroky, které lze podniknout k posílení bezpečnosti systému. (NUKIB, © 2017–2023)

Konfigurace a správa firewallu:

Konfigurace a správa firewallu jsou dva důležité prvky zabezpečení počítačové sítě. Konfigurace brány firewall se týká nastavení jejích pravidel a zásad, které určují, jak brána firewall kontroluje a filtruje příchozí a odchozí síťový provoz. Tato pravidla určují, jaké typy síťového provozu jsou povoleny a blokovány.

Správa firewallu zahrnuje pravidelné aktualizace, sledování a údržbu firewallu. To zahrnuje zajištění toho, aby byla brána firewall aktualizována nejnovějšími aktualizacemi zabezpečení a její pravidla byla správně nakonfigurována. Správa firewallu také zahrnuje monitorování síťového provozu a identifikaci potenciálních hrozeb pro zabezpečení sítě. Správná konfigurace a správa brány firewall je zásadní pro udržení vaší sítě zabezpečené a chráněné před vnějšími útoky. (MALINA, 2010)

Řízení přístupu:

Řízení přístupu je proces určování, jak může uživatel nebo systém přistupovat k určitým zdrojům nebo službám. Tyto prostředky mohou například zahrnovat soubory, složky, zařízení, sítě, aplikace a tak dále.

Řízení přístupu se obvykle provádí pomocí autentizace a autorizace. Autentizace zajišťuje ověření identity uživatele nebo systému, zatímco autorizace určuje, ke kterým zdrojům a oprávněním má uživatel nebo systém přístup. Existuje mnoho různých způsobů řízení přístupu, včetně řízení přístupu na úrovni síťových zařízení, operačních systémů, aplikací a webových stránek. Kontrola přístupu je důležitou součástí zabezpečení informačního systému a může pomoci chránit citlivé informace a data před neoprávněným přístupem nebo zneužitím. (MANAGEMENTMANIA, 2018)

Monitorování sítě:

Monitorováním sítě se rozumí proces sledování a sběr dat o provozu a stavu počítačových sítí. Cílem monitorování sítě je získat informace o výkonu a využití sítě, identifikovat možné chyby, varovat před výpadky a chránit síť před neoprávněným přístupem. Monitorování sítě se provádí pomocí softwarových nástrojů, které vám umožňují sledovat různé aspekty vaší sítě, jako je propustnost, latence, využití zařízení a směrování přenosu. Tyto nástroje mohou také poskytovat informace o síťovém provozu, jako jsou informace o přenášených datech, typech aplikací, které síť využívají, a množství přenášených dat. Monitorování sítě je velmi důležité pro správu a údržbu sítě, aby byla zajištěna vysoká dostupnost a výkon sítě. (SPRÁVA SÍTĚ, © 2022)

Řízení identit:

Proces řízení identit je soubor technologií, postupů a standardů, které dané organizaci umožňují spravovat digitální identity a přístupová práva uživatelů k digitálním zdrojům a aplikacím.

Primárním cílem správy identity je zajistit, aby přístup k relevantním informacím a zdrojům měly pouze autorizované osoby, a to při respektování bezpečnosti a soukromí. Toho se obvykle dosahuje ověřením totožnosti uživatele, jeho autorizací (určením uživatelských práv) a správou identity (správou digitální identity uživatele). Procesy řízení identity jsou důležité zejména pro organizace, které spravují citlivé informace, jako jsou osobní údaje a finanční záznamy. S rostoucím využíváním digitálních technologií a cloudových služeb nabývá řízení identity na stále větším významu, aby byla chráněna digitální aktiva a aby se zabránilo únikům dat. (MANAGAMENTMANIA, 2017)

6.2 Šifrování dat

Šifrování neboli kryptografie je věda, která se zabývá zabezpečováním informací prostřednictvím matematických a algoritmických technik. Kryptografie se využívá pro mnoho účelů, jako je například zabezpečená komunikace, ukládání dat a ověřování identity. Opakem kryptografie je kryptoanalýza což je věda, která se zabývá metodami získávání přístupu k tajným informacím ale hlavně Jak získat tajný šifrovací klíč.

Kryptografie pro zabezpečení daných zpráv nebo souborů využívá takzvané kryptografické algoritmy které mohou být symetrické nebo asymetrické. Symetrické algoritmy používají pro dešifrování a šifrování jeden klíč, zatímco asymetrické algoritmy používají 2 různé klíče pro šifrování a dešifrování dat. Tyto algoritmy využívají šifrovací klíč, který určuje průběh daného algoritmu. Kryptografické algoritmy se také dělí na blokové a proudové. Blokové algoritmy pracují s daty ve fixních blocích a používají klíč k šifrování každého bloku zvlášť, zatímco proudové algoritmy pracují s daty v proudech a používají klíč k šifrování každého bitu zvlášť. (BURDA, 2019)

Z hlediska kybernetický útoku představují běžní uživatelé nejsnadnější cíl, jelikož si nejčastěji žádným způsobem nechrání svá data. Šifrování dat je snadnou odpovědí na tento problém v kybernetické bezpečnosti, a proto jsem zvolil tuto oblast pro návrh praktické úlohy pro účely výuky studentů v rámci kybernetické laboratoře.

6.2.1 Šifrovací klíč

Šifrovací klíč je tajný nebo veřejný kód, který se používá k zašifrování nebo k dešifrování zpráv v kryptografii. Tajný klíč se využívá v symetrickém šifrování, kdy se stejný klíč používá jak pro šifrování, tak pro dešifrování zpráv. Na druhou stranu v asymetrickém šifrování se využívají 2 různé klíče – veřejný a soukromý. Veřejný klíč se používá k šifrování zpráv, které může dešifrovat pouze majitel soukromého klíče. To umožňuje bezpečnou komunikaci mezi 2 stranami, aniž by museli sdílet tajný klíč.

Délka neboli složitost šifrovacího klíče závisí na zvoleném šifrovacím systému a typu šifrovacího algoritmu. Mezi nejvyužívanější algoritmy patří Advanced Encryption Standard (dále jen AES) a Rivest-Shamir-Adleman (dále jen RSA). Tyto algoritmy se liší v použitých technikách a úrovních zabezpečení, a používají se pro různé účely v závislosti na potřebách uživatele. (BURDA, 2019)

6.2.2 Advanced Encryption Standart (AES)

AES je symetrický šifrovací algoritmus používaný pro zabezpečení přenosu dat prostřednictvím sítě. AES byl vytvořen jako náhrada za starší šifrovací algoritmy, jako je Data Encryption Standart, které již nebyly dostatečně bezpečné pro moderní požadavky na bezpečnost. AES používá blokovou šifrovací metodu, což znamená, že data jsou šifrována po blocích pevné délky. AES používá šifrovací klíče o délce 128, 192 nebo 256 bitů. Šifrování probíhá postupným opakováním jednotlivých kroků nad každým blokem dat a každým blokem klíče. Mezi základních operace pro šifrování a dešifrování dat využívá, nahrazování bitů, posuny, míchání a různé operace. Tyto operace jsou prováděny v různých krocích, což zajišťuje, že data jsou řádně zakódována.

Klíčovým faktorem bezpečnosti AES je délka šifrovacího klíče. Čím delší klíč, tím složitější bude šifrování a tím méně pravděpodobné je, že útočník bude schopen prolomit šifrování a získat přístup k datům. Algoritmy AES-128, AES-192 a AES-256 jsou tedy odolné proti různým druhům útoků a jsou považovány za jedny z nejbezpečnějších symetrických šifrovacích algoritmů. AES se používá v mnoha aplikacích, jako jsou bezdrátové sítě, mobilní telefony, bankovní aplikace a online transakce. (BERNSTEIN, COOB, © 2000–2023)

6.2.3 Rivest-Shamir-Adleman (RSA)

RSA je šifrovací algoritmus, který umožňuje šifrovat a dešifrovat data pomocí asymetrického klíče. K šifrování a dešifrování používá šifrovací klíče. Soukromý klíč je tajný a používá ho vlastník k dešifrování šifrovaných zpráv, zatímco veřejný klíč je sdílený a používá ho kdokoliv k zašifrování zprávy.

RSA funguje na principu matematického problému faktorizace velkých čísel. Proces šifrování zprávy začíná tak, že se veřejný klíč použije k zašifrování zprávy. To se provádí tak, že se zpráva rozdělí do bloků a každý blok se převede na číslo. Poté se použije veřejný klíč k zašifrování každého bloku, což vytvoří šifrovanou zprávu. Při dešifrování zprávy se používá soukromý klíč, který se použije k dešifrování každého bloku šifrované zprávy, což umožní získat původní zprávu.

RSA se používá především pro bezpečné přenosy dat přes internet, jako jsou bankovní transakce nebo přihlašování k účtům. RSA je považován za jednu z nejbezpečnějších metod šifrování a zůstává stále populární díky své spolehlivosti a bezpečnosti. (ENCRYPTION CONSULTING, © 2023)

6.3 Programy pro šifrování

Existuje celá řada programů, které se zabývají problematikou šifrování. Většinou jsou tyto programy volně dostupné v open source nebo freeware verzi, a proto je lze využívat bezplatně ale existují i placené programy které nabízejí víc funkcí. Šifrovací programy lze rozdělit do několika kategorií podle způsobu použití. Mezi tyto kategorie patří tvorba šifrovacích disků, šifrování pomocí šifrovacích klíčů, tvorba zašifrovaného USB disku a další. Tyto programy využívají k šifrování různé a jinak složité algoritmy a funkce díky kterým je šifrování jednodušší. Některé tyto programy, které lze využívat zdarma si zde představíme.

6.3.1 BitLocker

Program BitLocker je freeware software a primárně se využívá pro šifrování disků a diskových svazků. Tento program je vyvíjený společností Microsoft a je integrován ve verzích operačního systému Windows 8, 10. Účelem tohoto programu je ochrana dat, které jsou uloženy na zašifrovaných discích. Funkci tohoto programu si lze aktivovat jednoduše v operačním systému Windows.

6.3.2 VeraCrypt

Program VeraCrypt je open source software, který se využívá pro tvorbu zašifrovaných diskových oddílů nebo celého pevného disku a ke své funkci využívá algoritmy AES, TwoFish a Serpent. Tento program je napsán v programovacím jazyce C a C++ a lze jej využít na zařízeních s operačními systémy Windows, macOS a Linux. Lze jej využít i k tvorbě zabezpečeného flash disku. Vytvořený zašifrovaný diskový oddíl je možné otevřít a odšifrovat jen na zařízení které vlastní tento program.

6.3.3 Secure Archive 1

Program secure archiv 1 je freeware software který umožňuje vytvářet zašifrované a heslem chráněné archivy do kterých lze uložit potřebné soubory a data. Podporuje algoritmy AES, Blowfish a NASCCL s možností vytvoření speciálního souboru pro jeho otevření a nastavení správné úrovně komprese. V tomto programu lze vytvořit více různých archivů s různými hesly a také samorozbalovací archivy. Lze jej využívat na zařízení s operačním systémem Windows 8 a novější. Program obsahuje i funkci bezpečného mazání dat.

6.3.4 OpenPGP (Kleopatra)

Program OpenPGP je freeware software, který umožňuje šifrování pomocí asymetrické kryptografie. Lze jej využít pro zasílání zabezpečených e-mailových zpráv nebo k šifrování souborů pomocí šifrovacích klíčů. Tento program lze používat na zařízeních s operačním systémem Windows pod názvem GPG4win nebo v systému Linux pod názvem Kleopatra. Pro šifrování využívá algoritmy RSA a DSA které mají tři funkce složitosti šifrování.

6.4 Programy pro praktickou úlohu

Šifrování dat je velice užitečný způsob, jak chránit své údaje a důležitá data před útočníky a jejich kybernetickými útoky. Na internetu lze najít spoustu programů které se zabývají šifrováním dat, ale jen některé mají možnost využití zdarma a uživatelsky přístupné prostředí pro snadnou tvorbu šifrovacích klíčů nebo zašifrovaných disků. Pro tvorbu praktické úlohy jsem zvolil programy Kleopatra a VeraCrypt se kterými mám vlastní zkušenost a jejich využití je zdarma.

Program Kleopatra disponuje velice příjemným prostředím a snadnou manipulací. Uživateli umožňuje snadno vytvořit šifrovací pár klíčů a pomocí těchto klíčů jednoduše šifrovat nebo dešifrovat dané soubory a zprávy které lze přímo v programu zaslat na e-mail. Veškeré funkce, které slouží k tvorbě a distribuci šifrovacích klíčů jsou chráněny vytvořeným heslem které si uživatel zvolí sám a díky tomu je aktivita v programu lépe chráněna.

Program VeraCrypt taktéž disponuje příjemným prostředím, ve kterém je snadné se pohybovat a využívat jeho veškeré funkce. Na rozdíl od jiných programů, které slouží k tvorbě šifrovacích disků a diskových svazků má VeraCrypt funkci připojování těchto disků přímo do programu, takže nelze zašifrovaný disk otevřít na jiném zařízení. Uživatel si v tomto programu pro veškeré aktivity zvolí dostatečně silné heslo, pomocí kterého manipuluje s vytvořeným diskem a bez tohoto hesla se nelze dostat k datům na disku. Při otvírání těchto disků na jiném zařízení program disponuje možností vymazání historie, a tudíž je bezpečné tento program používat i jinde.

Díky veškerým funkcím, které tyto programy nabízejí je jejich použití snadné i pro začátečníky kteří začínají se šifrováním a díky příjemnému prostředí programu mají vše přehledně na jednom místě.

7 PRAKTICKÁ ÚLOHA

Praktická úloha pro potřeby kybernetické laboratoře (viz. Příloha P I) se skládá ze tří hlavních částí, které se primárně týkají problematiky šifrování. Každá část úlohy se skládá z několika kroků, které studenta provedou daným programem a všemi jeho funkcemi pro dosažení správného řešení. V první části úlohy se studen seznámí s programem Kleopatra, který se zaměřuje na šifrovací klíče, pomocí kterých si může uživatel díky šifrovacím algoritmům chránit libovolné soubory. Dané soubory lze dešifrovat druhou částí klíče za pomocí stejného programu. Druhá část je zaměřena na program VeraCrypt, který se primárně zaměřuje na tvorbu zašifrovaného disku, který lze využít pro ochranu více souborů najednou. Zašifrovaný disk pak lze otevřít jen na zařízení které obsahuje program VeraCrypt. Poslední část úkolu se zaměřuje na odevzdání pracovního protokolu, ve kterém je krok po kroku nastíněn postup celé úlohy a následně zašifrován pomocí šifrovacích klíčů.

Zadání praktické úlohy:

V první častí úkolu zpracujte tvorbu šifrovacích klíčů:

1. Stáhněte si program Kleopatra.
2. V programu Kleopatra si vytvořte šifrovací klíče dle návodu.
3. Zálohujte si tajný klíč pro další použití.
4. Celý postup zaznamenejte do úkolu.

V druhé části úkolu zpracujte tvorbu zašifrovaného disku:

1. Stáhněte si program VeraCrypt.
2. V programu VeraCrypt si vytvořte zašifrovaný disk dle návodu.
3. Aktivujte si svůj disk v programu VeraCrypt.
4. Na vytvořený disk nahrajte Soubor pod názvem (Jméno, Třída, Předmět) a screen vložte do úkolu.
5. Celý postup zaznamenejte do úkolu.

Odevzdávací část úkolu:

1. Semestrální úkol zašifrujte v programu Kleopatra.
2. Zašifrovaný úkol a tajný klíč odevzdejte.

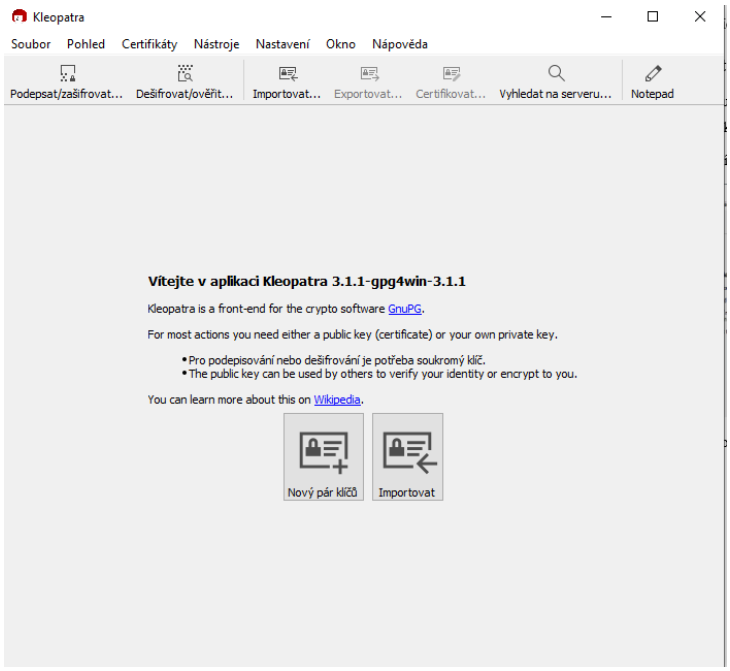
7.1 Příkladové řešení úlohy

Po úspěšné instalaci programů Kleopatra a VeraCrypt (viz. Příloha P I) si v následujících podkapitolách nastíníme, jak pracovat s oběma programy a jak by mělo vypadat řešení praktické úlohy.

7.1.1 Vytvoření šifrovacích klíčů

V této podkapitole si nastíníme manipulaci v programu Kleopatra a příkladový postup, jak splnit první část zadané úlohy která se zabývá tvorbou šifrovacího páru klíčů:

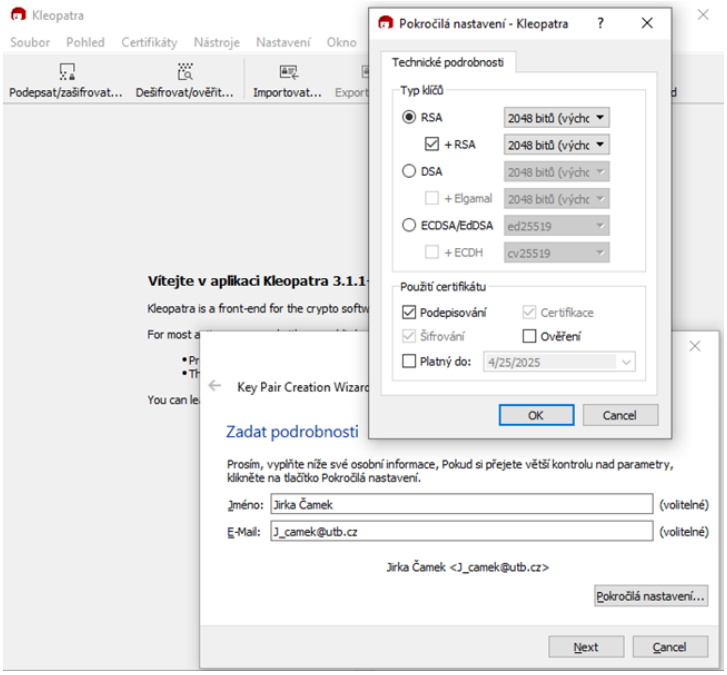
1. Po vstoupení do programu zvolíme kolonku Nový pár klíčů (viz. Obrázek č.3).



Obrázek 3 - Vytvoření nového páru klíčů (Vlastní)

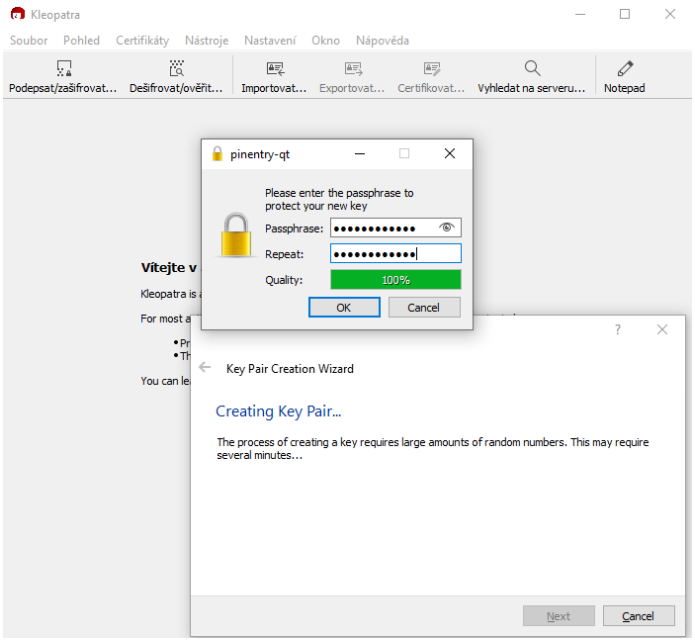
2. Při vytváření klíčů zvolíme Jméno a Email totožné s naším (viz. Obrázek č.4).
3. Přepneme do kolonky Pokročilá nastavení.

4. Zvolíme typ Klíčů RSA – 2048 bitů (viz. Obrázek č.4).
5. Pro vytvoření klíče je potřeba zvolit dostatečně silné heslo (viz. Obrázek č.5).



Obrázek 4 – Zvolení typu šifrování a pojmenování klíčů (Vlastní)

Zvolené heslo musí být dostatečně silné a pro nás snadno zapamatovatelné abychom zabránili jeho zneužití při nežádoucím přístupu do aplikace.



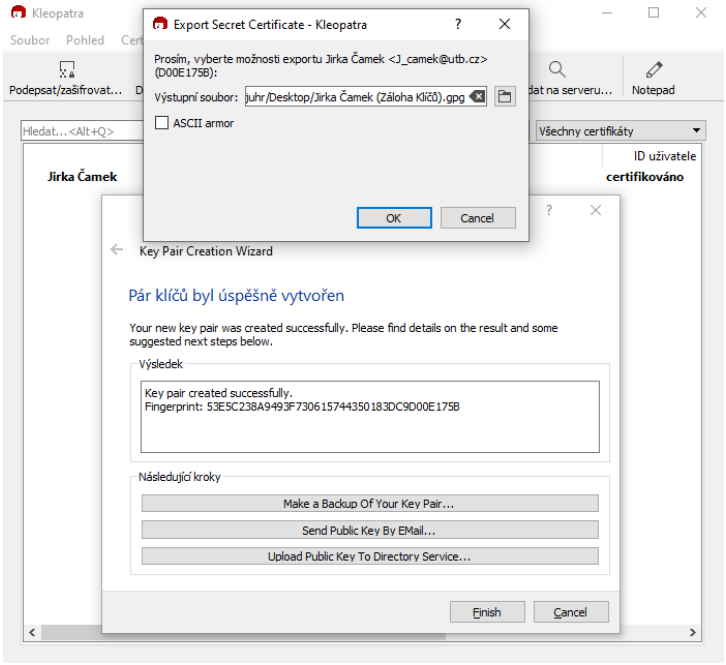
Obrázek 5 – Zvolení hesla pro šifrovací klíče (Vlastní)

Zvolené heslo slouží k potvrzování akcí při další manipulaci s šifrovacími klíčí.

7.1.2 Záloha klíčů

Při práci s šifrovacími klíči je vždy dobré si vytvořit zálohu daných klíčů abychom zabránili ztrátě klíčů při přeinstalaci počítače nebo při odinstalaci programu Kleopatra. Postup vytvoření zálohy je zdokumentován níže:

1. Pro vytvoření zálohy zvolíme kolonku (Make a Backup of Your Key Pair).
2. Zvolíme místo úložiště a pojmenujeme (viz. Obrázek č.6).
3. Pro potvrzení tvorby zálohy je potřeba zadat zvolené heslo.



Obrázek 6 – Záloha zašifrovaných klíčů (Vlastní)

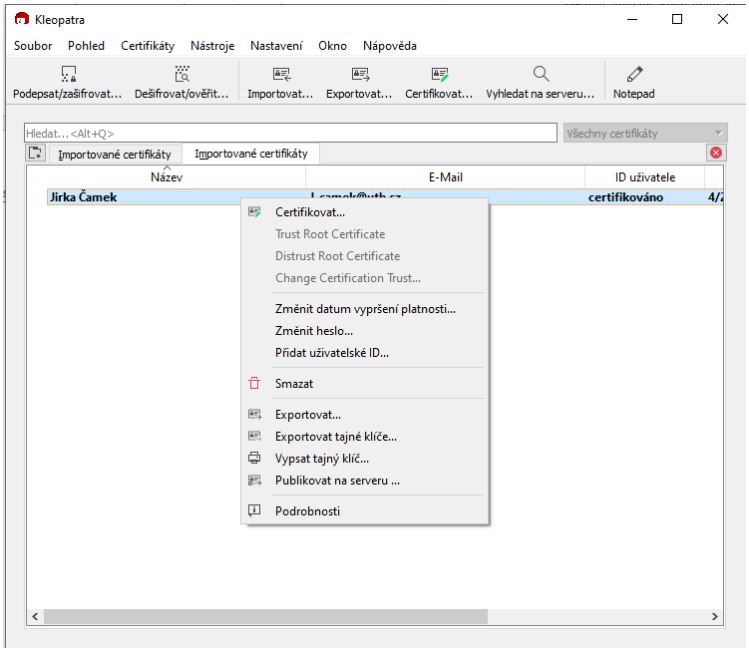
Bez zálohy klíčů nelze při jejich ztrátě jiným způsobem odšifrovat soubory které jsme zabezpečili. Zálohované klíče lze poté vložit na externí disk pro další použití.

7.1.3 Export tajného klíče

Šifrovací klíč se skládá ze dvou částí. První část klíče se nazývá tajný klíč a ten se primárně využívá pro dešifrování souborů které zašifrujete druhou částí klíče. Druhá část klíče se nazývá veřejný klíč a je určená pro šifrování souborů a certifikaci. Pomocí veřejného klíče vám ostatní uživatelé mohou zasílat zprávy které sami dešifrujete. V programu Kleopatra je i třetí možnost, jak zašifrovat soubory, a to za pomocí hesla které si zvolí uživatel sám.

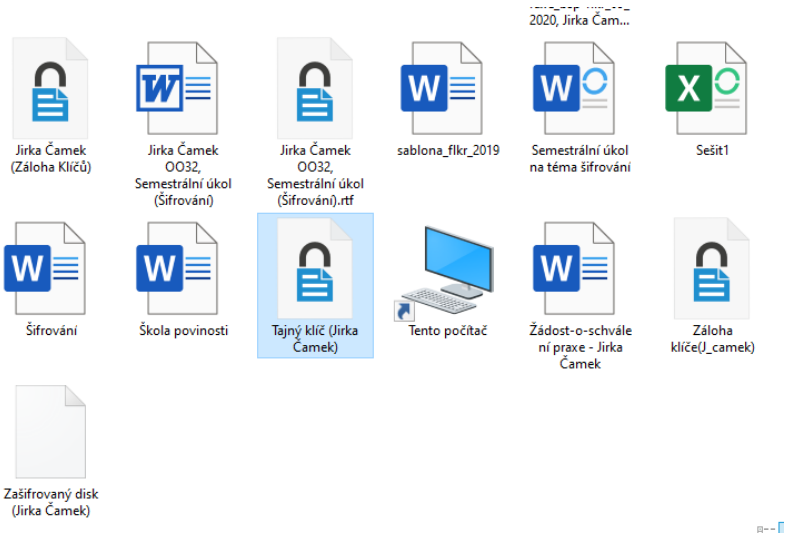
1. Pro export tajného klíče zvolíme kolonku Exportovat tajné klíče (viz. Obrázek 7).
2. Zvolíme místo úložiště a pojmenujeme.

3. Export tajného klíče je nutné potvrdit heslem.



Obrázek 7 – Export tajného klíče (Vlastní)

Bez exportu a následného sdělení tajného klíče nebo hesla není možné, aby se cílový uživatel dostal k odšifrování souborů.



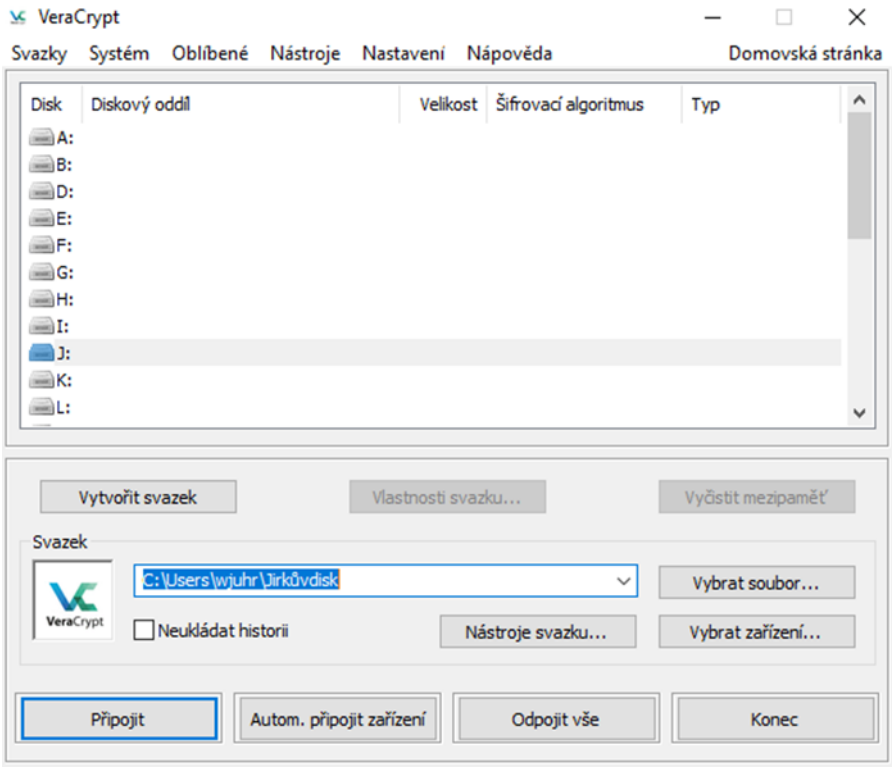
Obrázek 8 – Tajný klíč (Vlastní)

Námi exportovaný tajný klíč se uloží do zvolené cílové oblasti. Volba exportu tohoto klíče je jen pro potřeby semestrálního úkolu.

7.1.4 Vytvoření zašifrovaného disku

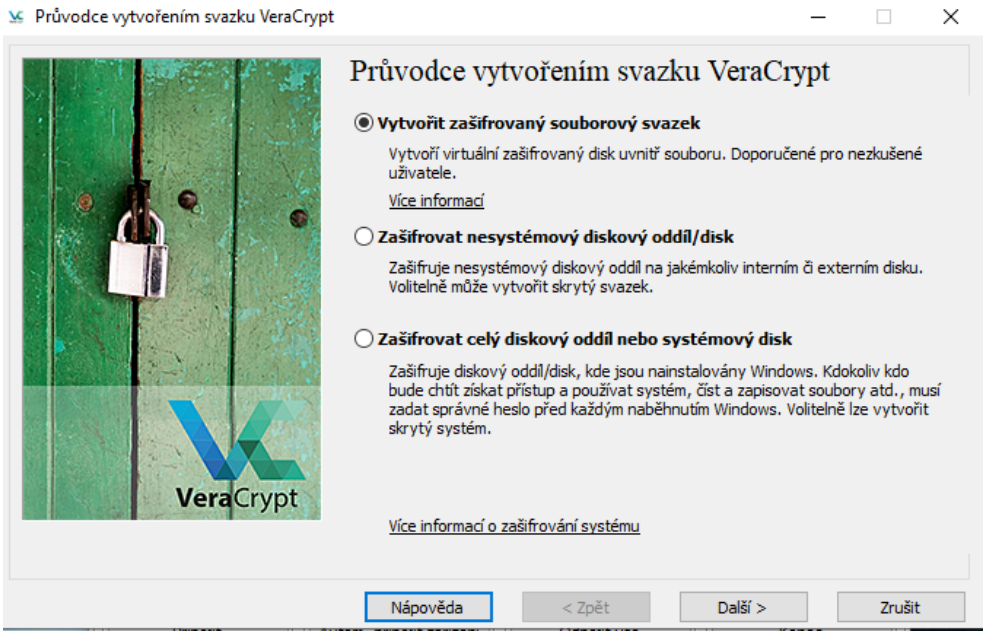
V programu VeraCrypt si vytvoříme vlastní zašifrovaný disk, který lze použít pro ukládání a následnou ochranu více souborů najednou. Zašifrovaný disk lze vložit na externí disk nebo flash disk a poté jej otevřít na jiném zařízení na kterém je program VeraCrypt. Přesný postup druhé části úlohy a vytvoření zašifrovaného disku je zdokumentován níže:

1. Pro vytvoření disku zvolíme kolonku Vytvořit svazek (viz. Obrázek č.9).



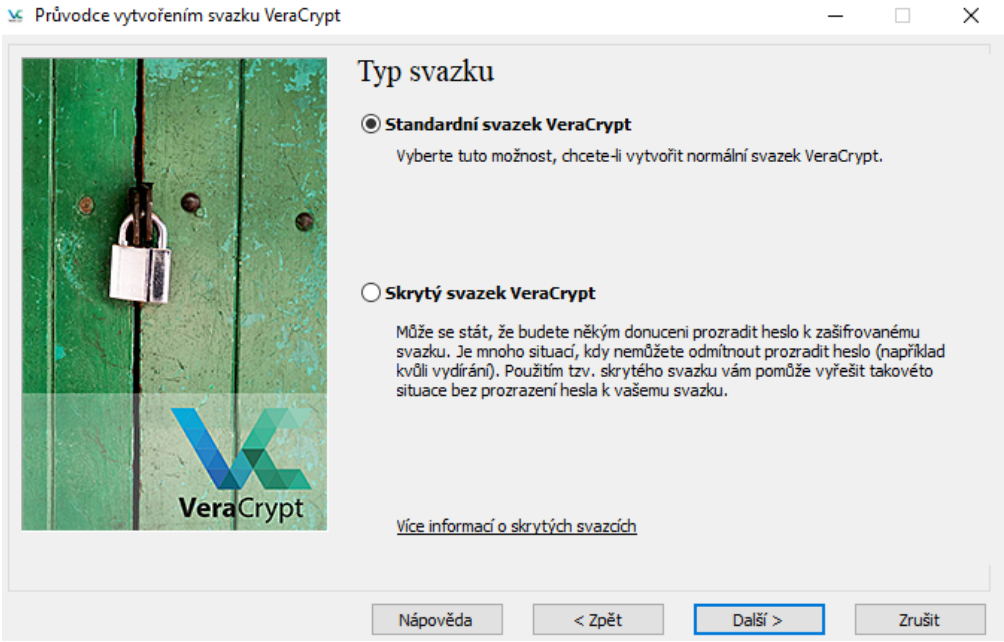
Obrázek 9 - Vytvoření svazku (Vlastní)

2. Zvolíme možnost vytvořit zašifrovaný souborový svazek (viz Obrázek č.10).
3. Typ svazku zvolíme Standardní (viz Obrázek č.11).
4. Svazku přidělíme libovolné místo pro uložení v počítači (viz Obrázek č.12).
5. Šifrovací algoritmus pro svazek zvolíme AES (viz Obrázek č.13).
6. Velikost svazku zvolíme 100 MB (viz Obrázek č.14).
7. Pro další manipulaci se svazkem zvolíme bezpečné heslo (viz Obrázek č.15).
8. Pro dokončení svazek naformátujeme pro systém FAT (viz Obrázek č.16).



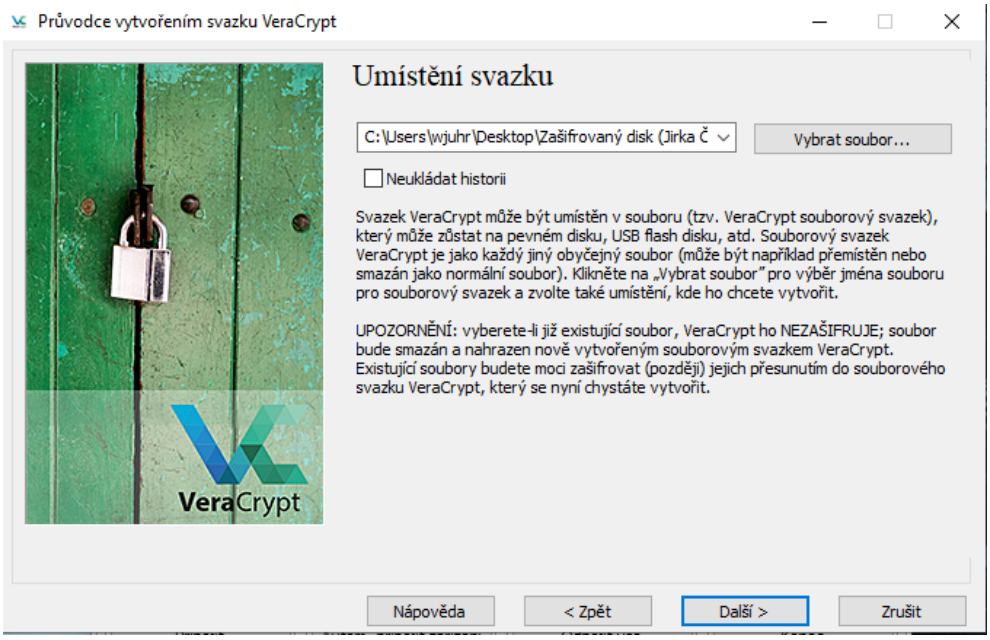
Obrázek 10 – Zvolení typu zašifrovaného disku (Vlastní)

V programu VeraCrypt lze vytvořit zašifrovaný disk třemi způsoby. Tyto způsoby se rozdělují podle zkušenosti uživatele a formy využití zašifrovaného disku.



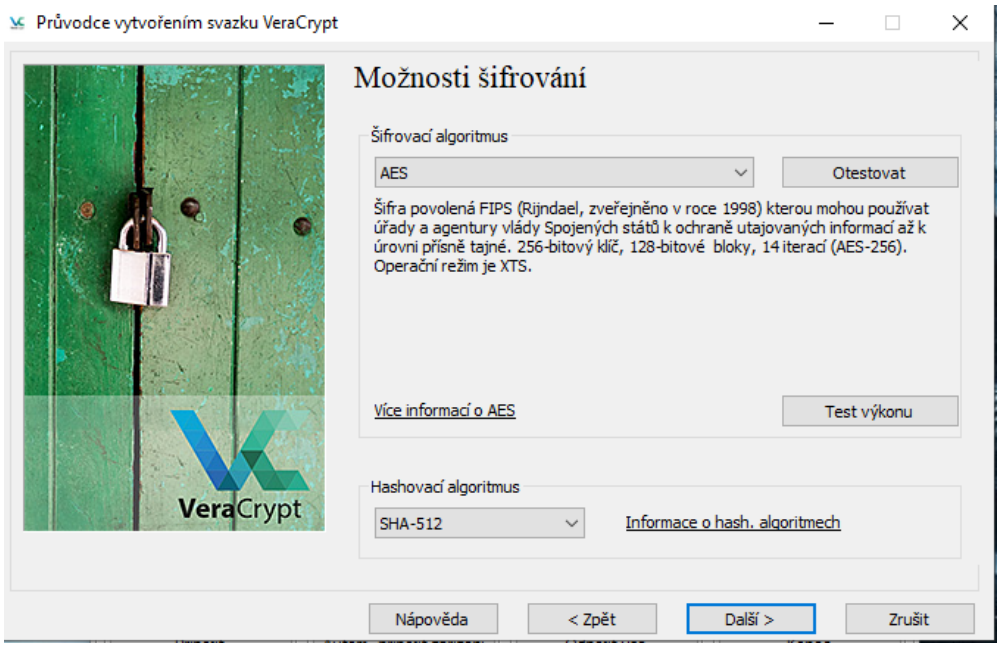
Obrázek 11 – Zvolení typu svazku (Vlastní)

Typ zašifrovaného disku lze zvolit standardní nebo skrytý. Standardní svazek umožní vytvoření normálního disku, zatímco skrytý svazek vytvoří lepé chráněný disk, který je stále chráněn i při odcizení hesla.



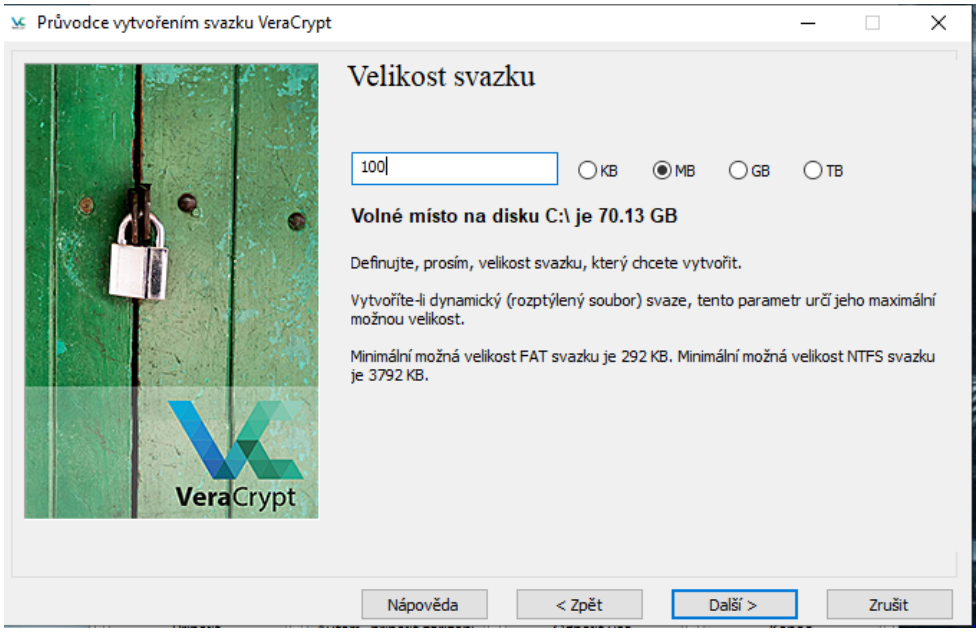
Obrázek 12 – Umístění svazku na zařízení (Vlastní)

Pro umístění disku je nejlepší zvolit složku kterou na našem zařízení snadno najdeme. Vytvořený disk se chová jako obyčejný soubor, který lze smazat nebo přemístit.



Obrázek 13 – Typ šifrování pro svazek (Vlastní)

Pro zašifrování disku program využívá různé šifrovací algoritmy, které zajišťují složitost šifrování. Tyto algoritmy a jejich funkčnost lze otestovat přímo v programu.

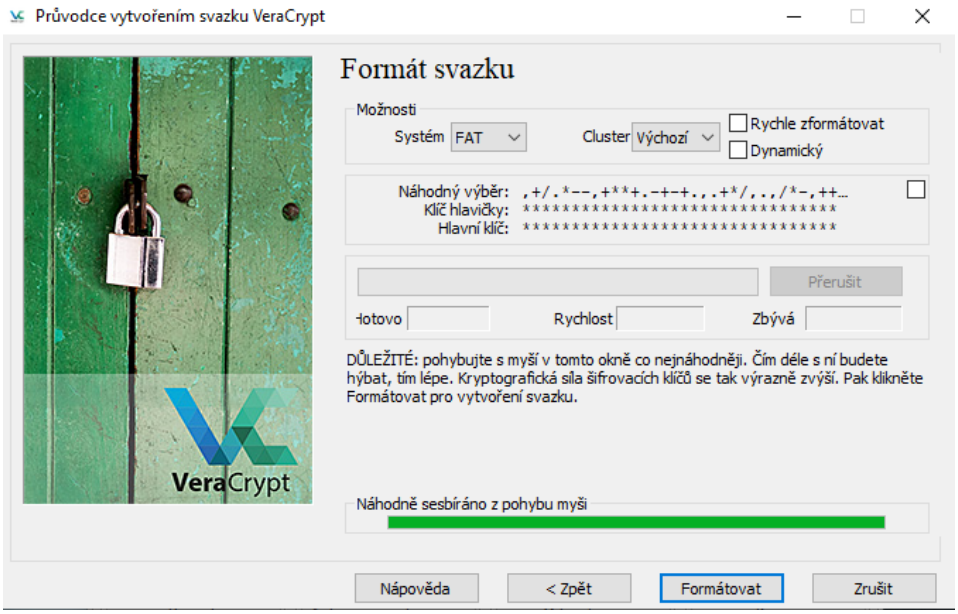


Obrázek 14 – Zvolení velikosti svazku (Vlastní)

Zvolená velikost svazku po připojení zabírá volné místo na hlavním disku, proto je důležité zvolit takovou velikost která je přiměřená velikosti hlavního disku.

Obrázek 15 – Zvolení bezpečného hesla pro svazek (Vlastní)

Pro veškerou manipulaci s diskem je důležité zvolit dostatečně silné heslo. Toto heslo zvolte různou kombinací znaků a držte v tajnosti před ostatními.

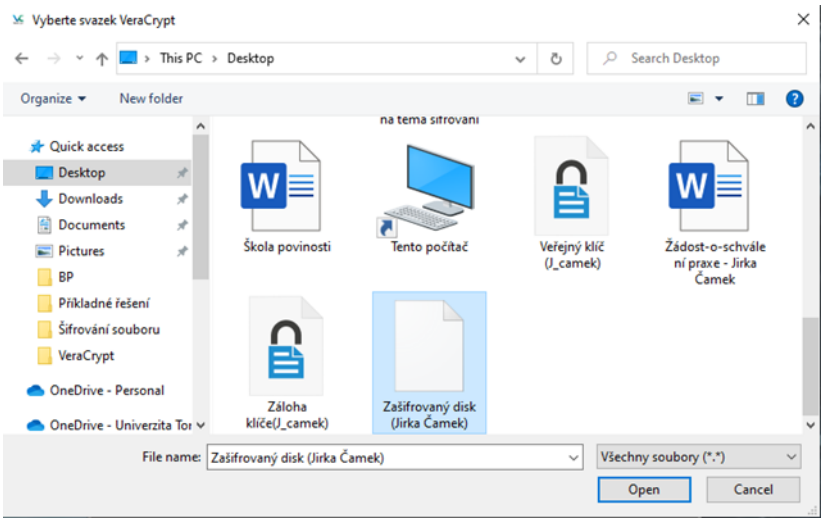


Obrázek 16 – Formátování svazku (Vlastní)

7.1.5 Připojení disku v programu VeraCrypt

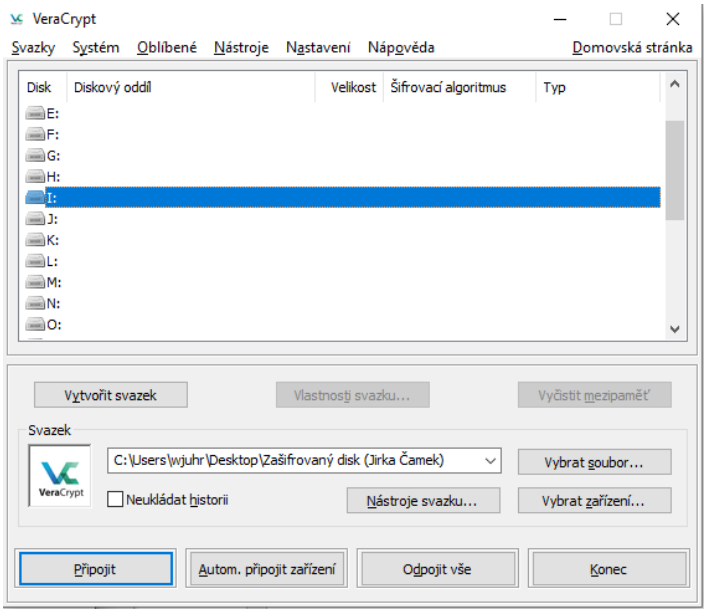
Vytvořený zašifrovaný disk nelze otevřít a vkládat na něj soubory bez připojení na diskový oddíl který se nachází v programu VeraCrypt. Postup, jak připojit disk a vložit do něj soubor je zdokumentován níže:

1. Vytvořený disk nahrajeme pomocí kolonky Vybrat soubor (viz Obrázek č.17).



Obrázek 17 - Nahrání zašifrovaného disku (Vlastní)

2. Nahrání disku musíme potvrdit zvoleným heslem.
3. Nahranému disku zvolíme Diskový oddíl (viz Obrázek č.18).
4. Pro připojení disku zvolíme kolonku Připojit.

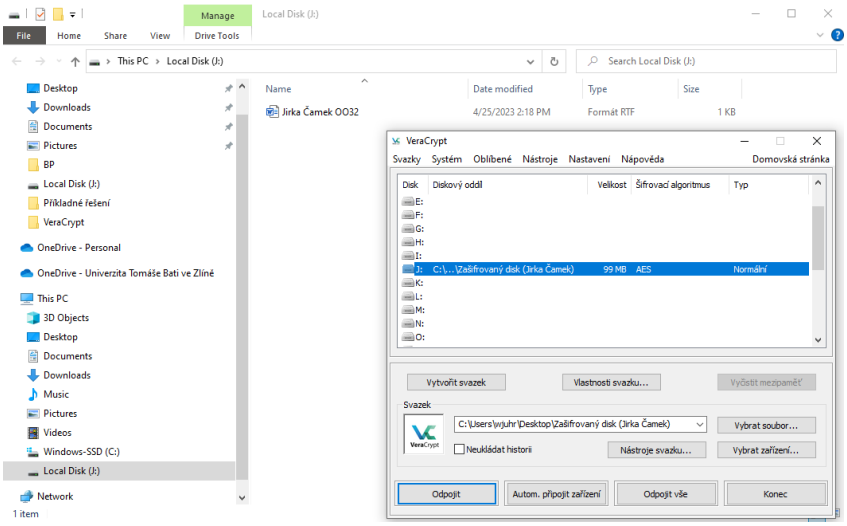


Obrázek 18 - Přidělení Diskového oddílu (Vlastní)

Na každý diskový oddíl je možné připojit jen jeden zašifrovaný disk. V programu VeraCrypt je možné mít v jednu chvíli aktivováno více disků.

7.1.6 Kontrola připojeného disku

Pro kontrolu, zda je zašifrovaný disk připojený správně a funguje si jej otevřeme a nahrajeme na něj libovolný soubor.



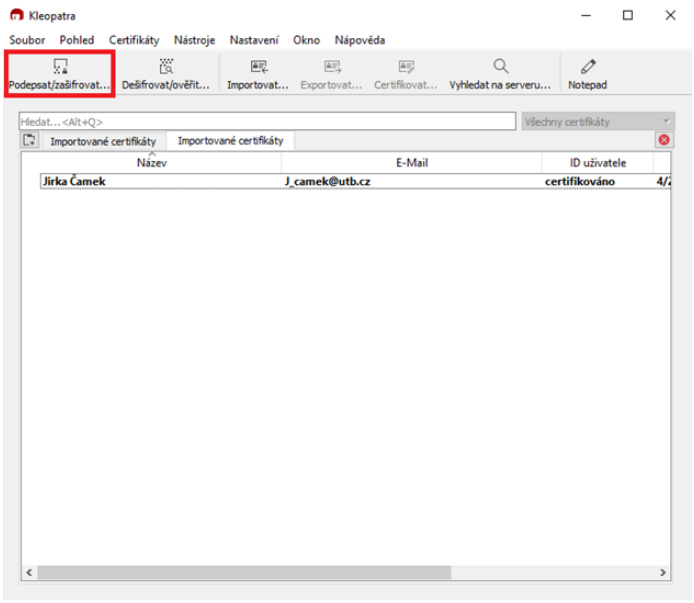
Obrázek 19 – Ověření zašifrovaného disku (Vlastní)

Na zašifrovaný disk lze vkládat jakýkoliv typ souborů které potřebujeme chránit. Na tento disk je možné vložit jen dané množství souborů jaké nám povoluje jeho maximální kapacita

7.1.7 Zašifrování semestrálního úkolu

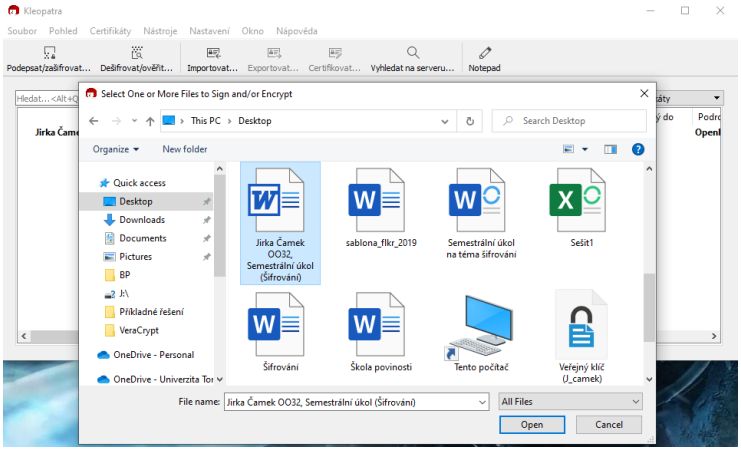
V první části úkolu jsme vytvořili šifrovací pár klíčů, které použijeme pro zašifrování semestrálního úkolu. Pro zašifrování souboru využijeme náš veřejný klíč a tento souboru pak odevzdáme i s tajným klíčem ke kontrole. Přesný postup, jak zašifrovat souboru je zdokumentován níže:

1. V programu Kleopatra zvolíme možnost Podepsat/Zašifrovat (viz Obrázek č.20).



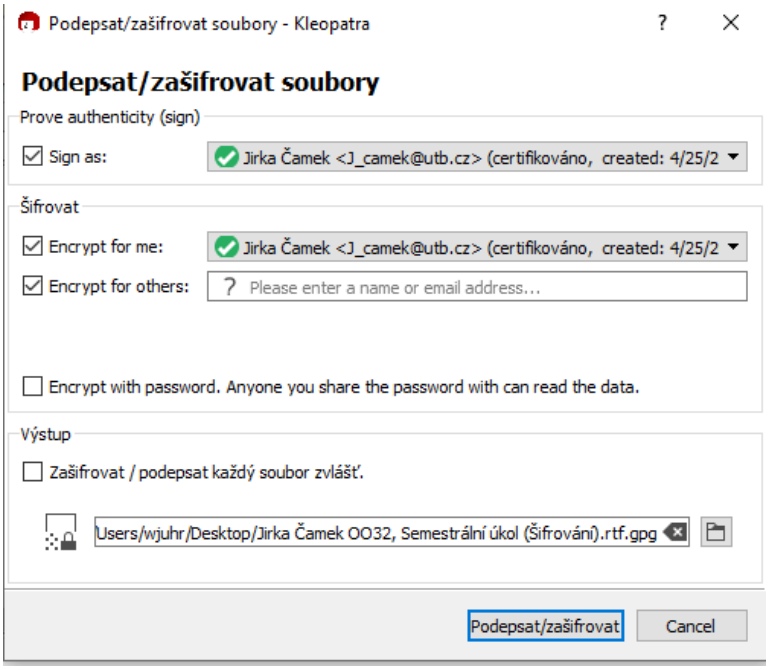
Obrázek 20 - Zvolení možnosti Podepsat/Zašifrovat (Vlastní)

2. Na zařízení vybereme soubor k zašifrování (viz Obrázek č.21).
3. Soubor zašifrujeme pomocí vytvořeného páru klíčů (viz Obrázek č.22).



Obrázek 21 – Vybrání souboru k zašifrování (Vlastní)

Při šifrování se vytvoří zašifrovaná kopie souboru. Vybraný soubor tak zůstane nedotčený a můžeme s ním dále manipulovat i bez dešifrování.



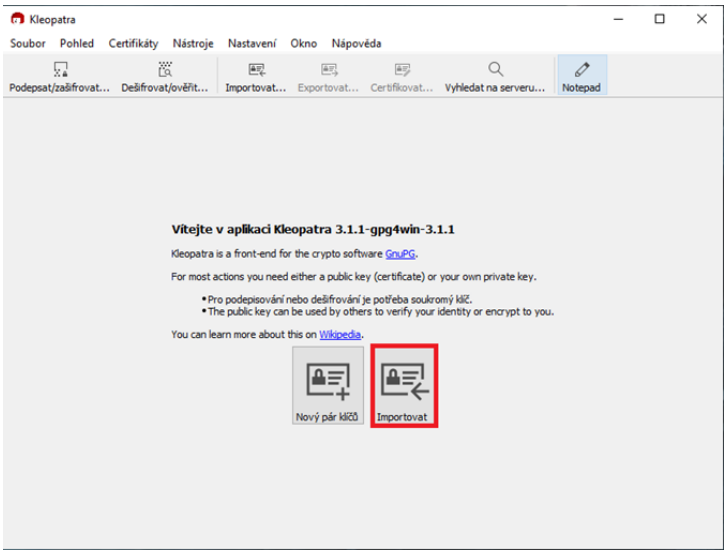
Obrázek 22 – Šifrování pomocí vytvořených klíčů (Vlastní)

Pro šifrování souboru lze zvolit jakýkoliv námi vytvořený pár klíčů a také lze zvolit možnost zašifrování pomocí hesla.

7.1.8 Dešifrování souboru

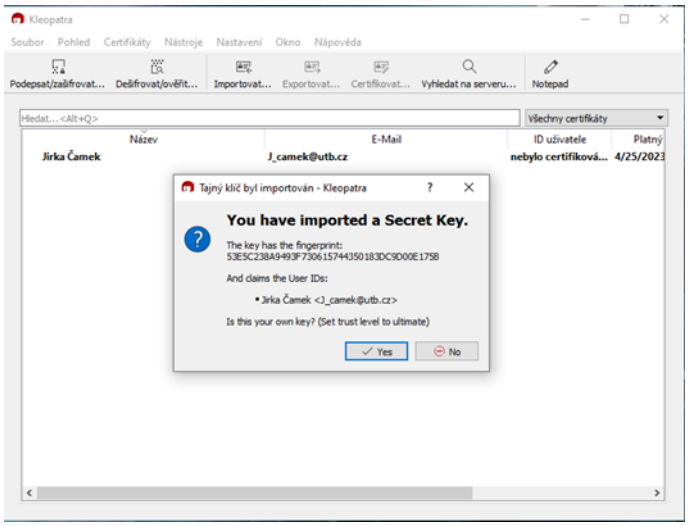
Aby byla možnost zkontrolovat studenty a jejich odevzdanou práci je potřeba si v programu Kleopatra ukázat, jak připojit privátní klíč a pomocí tohoto klíče zašifrovanou zprávu odšifrovat a uložit si do počítače v původním formátu. Postup, jak vložit tajný klíč a dešifrovat soubor je zaznamenán níže:

1. V programu Kleopatra použijeme funkci Importovat (viz Obrázek č.23).



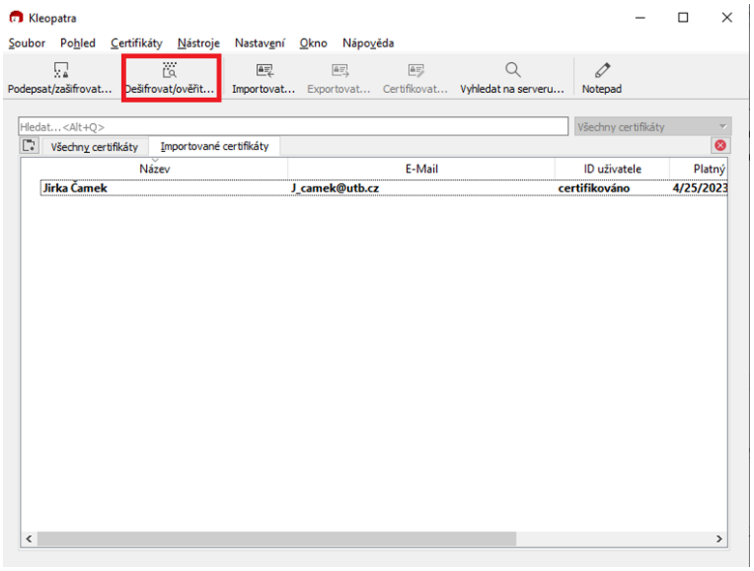
Obrázek 23 - Zvolení možnosti Importovat (Vlastní)

2. Vybereme klíč, který chceme do programu vložit.
3. Objeví se ověřovací hláška se jménem a e-mailem studenta který tento klíč vytvořil, to jednoduše potvrdíme a klíč máme vložený v programu. (viz Obrázek č.24).



Obrázek 24 - Hlášení o připojení tajného klíče (Vlastní)

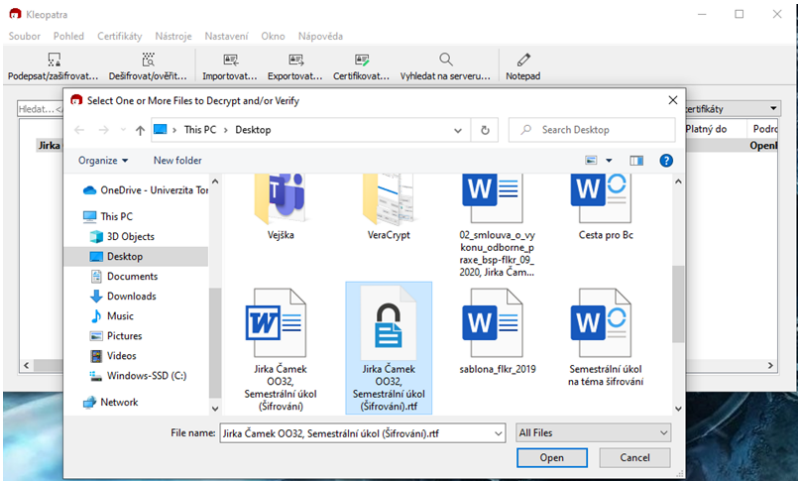
4. Po úspěšném připojení klíče zvolíme možnost dešifrovat/ověřit (viz Obrázek č.25).



Obrázek 25 - Zvolení funkce Dešifrovat/ověřit (Vlastní)

5. Vybereme soubor, který je určený k dešifrování (viz Obrázek č.26).

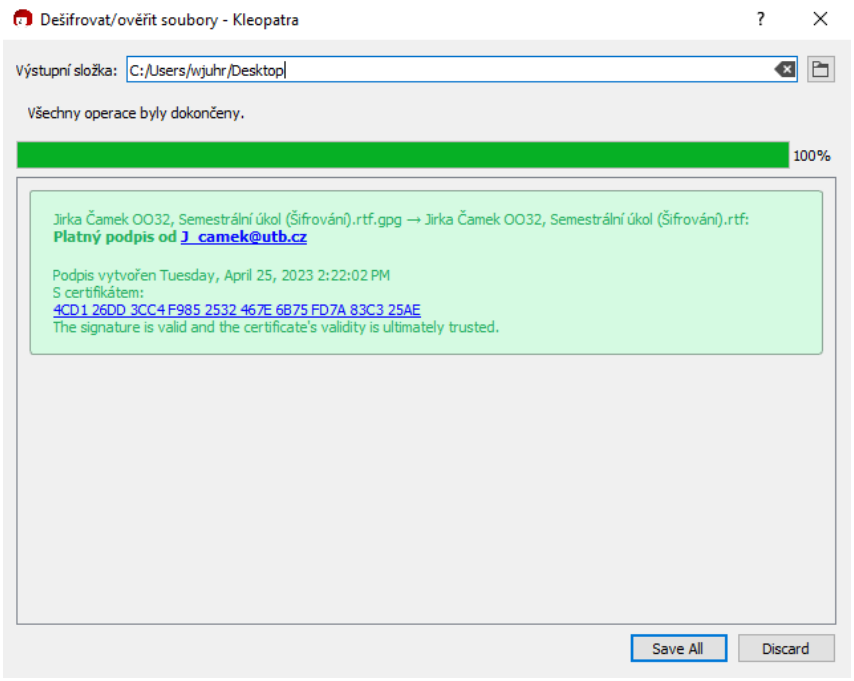
6. Pro dešifrovaný soubor vybereme místo k uložení.



Obrázek 26 - Vybrání souboru pro dešifrování (Vlastní)

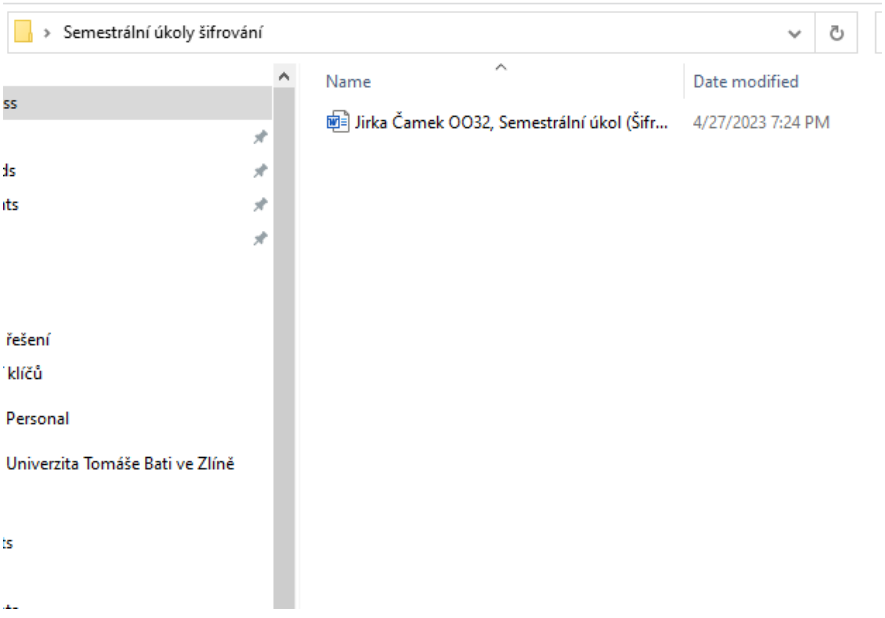
7. Celý proces potvrdíme kolonkou Save All (viz Obrázek č.27).

8. Ve vybrané složce se nám objeví dešifrovaný soubor (viz Obrázek č.28).



Obrázek 27 – Dokončení dešifrování (Vlastní)

Při dešifrování souboru se objeví okno, které hlásí, zda se dešifrování povedlo a jakým klíčem byl soubor odšifrován.



Obrázek 28 – Dešifrovaný soubor (Vlastní)

Po dokončení procesu dešifrovaní se nám v cílové složce objeví dešifrovaná kopie souboru.

ZÁVĚR

Kybernetická bezpečnost je velmi důležitým oborem, který má stále vetší význam v dnešní digitální společnosti. S vyvíjecím se digitálním prostředím roste počet kybernetický útoku a málo který uživatel jakékoliv technologie dokáže znemožnit nebo minimalizovat dopad těchto útoků.

Cílem této bakalářské práce bylo navrhnout praktickou úlohu pro potřeby výuky studentů v rámci kybernetické laboratoře Fakulty logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně na základě identifikovaných oblastí, které by se hodily pro výuku.

Bakalářská práce je rozdělena na teoretickou a praktickou část. V teoretické části jsou popsány základní pojmy, které jsou spjaty s kybernetickou bezpečností a informačními a komunikačními technologiemi. Teoretická část také uvádí do problematiky kybernetických útoků, které je nutné znát pro pochopení před čím je nejlepší se na internetu chránit.

V praktické části jsou identifikovány vhodné oblasti, které by bylo možno vyučovat studenty v rámci kybernetické laboratoře a na základě těchto identifikovaných oblastí a zjištěného poznatku že data jsou nejčastějším cílem při kybernetický útocích byla vybrána oblast šifrování. Tato problematika efektivně řeší ochranu citlivých dat před odcizením. V návaznosti na oblast šifrování byli analyzovány programy, které by bylo vhodné využít pro návrh praktické úlohy. Ze spousty nabízených programů na internetu byly vybrány dva programy, které své funkce nabízejí zdarma a v uživatelsky nejjednodušším prostředí. Na základně nejvhodněji vybrané oblasti bylo vypracováno zadání a postup praktické úlohy (viz. Příloha P I) které se skládá ze tří částí: seznámení se s tvorbou šifrovacích klíčů a jejich možné využití, tvorba zašifrovaného disku a jeho možnosti využití v osobním nebo pracovním životě a propojení těchto dvou znalostí k vytvoření semestrálního úkolu.

Hlavní cíl práce a dílčí cíle byly splněny. Přínosem práce je získání znalostí o kybernetické bezpečnosti a naučit se, jak chránit svá data před možným zneužitím, avšak je potřeba tuto problematiku neustále sledovat a zdokonalovat se v ní stejně rychle jak se vyvíjejí informační a komunikační technologie.

Závěrem lze říct že kybernetická bezpečnost pomáhá chránit všechny uživatele v kyberprostoru a je chyba se domnívat že aktivita jednotlivce na internetu nijak nemůže ovlivnit celá kyberprostor. Lidé jsou a budou pořád největší hrozbou pro kybernetickou bezpečnost, a proto je nejlepší je udržovat informované a připravené a všechny možnosti které se týkají kybernetické bezpečnosti.

SEZNAM POUŽITÉ LITERATURY

BERNSTEIN, Corinne a Michael COBB. Advanced Encryption Standard (AES). TechTarget [online]. TechTarget, © 2000–2023 [cit. 2023-04-27]. Dostupné z: https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard

BEZPEČNOSTNÍ POLITIKA: Bezpečnostní hrozby. Ministerstvo vnitra České republiky [online]. PRAHA: Ministerstvo vnitra České republiky, © 2023, © 2023 [cit. 2023-03-15]. Dostupné z: https://www.mvcr.cz/clanek/bezpecnostni-hrozby-337414.aspx?q=Y2hudW09Mw%3D%3D

BROOKS, Charles J., Christopher GROW, Philip CRAIG a Donald SHORT. Cybersecurity essentials. 1. Indianapolis, Indiana: Sybex, John Wiley, 2018. ISBN 978-1-119-36239-5.

BURDA, Karel. Kryptografie okolo nás [online]. Praha: CZ.NIC, z.s.p.o., 2019 [cit. 2023-04-27]. CZ.NIC. ISBN 978-80-88168-52-2. Dostupné z: https://knihy.nic.cz/files/edice/Kryptografie_okolo_nas.pdf

Co je deep web? Alza.cz [online]. Alza, © 1994–2023, 2019 [cit. 2023-03-20]. Dostupné z: https://www.alza.cz/co-je-deep-web

Co je ti IP adresa? Alza [online]. Alza.cz, © 1994–2023, 2021 [cit. 2023-03-12]. Dostupné z: https://www.alza.cz/co-je-ip-adresa

Co je to monitoring sítě. Správa sítě [online]. PRAHA: Aira GROUP, © 2022 [cit. 2023-04-28]. Dostupné z: https://www.sprava-site.eu/monitoring-site/

CyberCrime. In: KOLOUCH, Jan. CyberCrime. 1. Praha: CZ.NIC, z.s.p.o., 2016, s. 55. CZ.NIC. ISBN 978-80-88168-15-7.

ČESKO. Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury. In: Zákony pro lidi.cz [online]. © AION CS 2010-2023 [cit. 30. 4. 2023]. Dostupné z: https://www.zakonyprolidi.cz/cs/2010-432

ČESKO. Vyhláška č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci. In: Zákony pro lidi.cz [online]. © AION CS 2010-2023 [cit. 30. 4. 2023]. Dostupné z: https://www.zakonyprolidi.cz/cs/2021-315

ČESKO. Vyhláška č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu. In: Zákony pro lidi.cz [online]. © AION CS 2010-2023 [cit. 30. 4. 2023]. Dostupné z: https://www.zakonyprolidi.cz/cs/2021-316

ČESKO. Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích. In: Zákony pro lidi.cz [online]. © AION CS 2010-2023 [cit. 30. 4. 2023]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-317

ČESKO. Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby. In: Zákony pro lidi.cz [online]. © AION CS 2010-2023 [cit. 30. 4. 2023]. Dostupné z: https://www.zakonyprolidi.cz/cs/2017-437

ČESKO. Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). In: Zákony pro lidi.cz [online]. © AION CS 2010-2023 [cit. 30. 4. 2023]. Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82

ČESKO. Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích). In: Zákony pro lidi.cz [online]. © AION CS 2010-2023 [cit. 30. 4. 2023]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-127

ČESKO. Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád). In: Zákony pro lidi.cz [online]. © AION CS 2010-2023 [cit. 30. 4. 2023]. Dostupné z: https://www.zakonyprolidi.cz/cs/1961-14

ČESKO. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: Zákony pro lidi.cz [online]. © AION CS 2010-2023 [cit. 30. 4. 2023]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

ČESKO. Zákon č. 273/2008 Sb., o Policii České republiky. In: Zákony pro lidi.cz [online]. © AION CS 2010-2023 [cit. 30. 4. 2023]. Dostupné z: https://www.zakonyprolidi.cz/cs/2008-273

ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. In: Zákony pro lidi.cz [online]. © AION CS 2010-2023 [cit. 30. 4. 2023]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

ČESKO. Zákon č. 441/2003 Sb., o ochranných známkách a o změně zákona č. 6/2002 Sb., o soudech, soudcích, přísedících a státní správě soudů a o změně některých dalších zákonů (zákon o soudech a soudcích), ve znění pozdějších předpisů, (zákon o ochranných známkách). In: Zákony pro lidi.cz [online]. © AION CS 2010-2023 [cit. 30. 4. 2023]. Dostupné z: https://www.zakonyprolidi.cz/cs/2003-441

ČESKO. Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti). In: Zákony pro lidi.cz [online]. © AION CS 2010-2023 [cit. 30. 4. 2023]. Dostupné z: https://www.zakonyprolidi.cz/cs/2004-480

ČESKO. Zákon č. 89/2012 Sb., občanský zákoník. In: Zákony pro lidi.cz [online]. © AION CS 2010-2023 [cit. 30. 4. 2023]. Dostupné z: https://www.zakonyprolidi.cz/cs/2012-89

DDoS útok. ESET [online]. Praha: ESET, spol. s r.o., © 1992–2023, [cit. 2023-03-12]. Dostupné z: https://www.eset.com/cz/ddos-utok/

DOSTÁLEK, Libor. Velký průvodce protokoly TCP/IP: bezpečnost. 2. aktualiz. vyd. Praha: Computer Press, 2003. ISBN 80-722-6849-X.

EVANS, Lester. Cybersecurity: what you need to know about computer and cyber security, social engineering, the internet of things + an esential guide to ethical hacking for beginners. 1. HOUSTON, Texas, United States: Ergodebooks, 2019. ISBN 978-1794647237.

HORÁK, Jaroslav a Milan KERŠLÁGER. Počítačové sítě pro začínající správce. 5., aktualiz. vyd. Brno: Computer Press, 2011. ISBN 978-802-5131-763.

HUB, Miloslav. Bezpečnost a ochrana informací v prostředí internetu: bezpečnost. 2. aktualiz. vyd. Pardubice: Univerzita Pardubice, 2013. ISBN 978-80-7395-701-8.

JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. 2. aktualiz. vyd. Praha: Grada, 2007. ISBN 978-80-247-1561-2.

KOLOUCH, Jan a Pavel BAŠTA. CyberSecurity. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7.

KOLOUCH, Jan. CyberCrime. 1. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7.

Kybernetická bezpečnost. Q-COM [online]. Brno, © 2023 [cit. 2023-03-10]. Dostupné z: https://www.qcom.cz/systemy-rizeni/zokb/

Kybernetická bezpečnost. Vláda České republiky [online]. PRAHA: Vláda ČR, © 2009-2023, 2021 [cit. 2023-03-20]. Dostupné z: https://www.vlada.cz/cz/evropske-zalezitosti/umela-inteligence/kyberneticka_bezpecnost/kyberneticka-bezpecnost-192766/

Kybernetická bezpečnost: Regulace a kontrola: Legislativa. *NÚKIB* [online]. Brno, © 2021 [cit. 2023-04-17]. Dostupné z: https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/

MALINA, Patrik. Firewall ve Windows a jeho správa. Computerworld [online]. © 1997–2023, 2010 [cit. 2023-04-28]. Dostupné z: https://www.computerworld.cz/clanky/firewall-ve-windows-a-jeho-sprava/

Malware. Malwarebytes [online]. © 2023 [cit. 2023-04-15]. Dostupné z: https://www.malwarebytes.com/malware

MARKS, Paul. Cybersecurity and the Parkerian Hexad. In: *Staffhosturope* [online]. © 2023 [cit. 2023-04-27]. Dostupné z: https://www.staffhosteurope.com/blog/2019/03/cybersecurity-and-the-parkerian-hexad?source=google.com

PENDER-BEY, Gorgie. The parkerian hexad [online]. 2012, 31 [cit. 2023-03-08]. Dostupné z: https://cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.pdf

Phishing. Eset [online]. Praha: ESET, spol. s r.o., © 1992–2023 [cit. 2023-03-12]. Dostupné z: https://www.eset.com/cz/phishing/

Poskytované služby: Penetrační testování. Národní úřad pro kybernetickou a informační bezpečnost [online]. Brno, © 2017–2023 [cit. 2023-04-28]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/vladni-cert/poskytovane-sluzby/

Ramsomware. Eset [online]. Praha: ESET, spol. s r.o., © 1992–2023 [cit. 2023-03-12]. Dostupné z: https://www.eset.com/cz/ransomware/

Ramsomware. Malwarebytes [online]. © 2023 [cit. 2023-03-12]. Dostupné z: https://www.malwarebytes.com/malware

Řízení identit. Managementmania [online]. © 2011-2016, 2017 [cit. 2023-04-28]. Dostupné z: https://managementmania.com/cs/identity-management-rizeni-identit

Řízení přístupu. Managementmania [online]. © 2011-2016, 2018 [cit. 2023-04-28]. Dostupné z: https://managementmania.com/cs/rizeni-pristupu

SHINDER, Debra Littlejohn. Počítačové sítě: nepostradatelná prírucka k pochopení sítové teorie, implementace a vnitrních funkcí [sic]. Praha: SoftPress, c2003. Cisco systems. ISBN 80-86497-55-0.

SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL. Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti: bezpečnost. 2. aktualiz. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-807-3807-658.

Sociální inženýrství. Avast [online]. Avast Software, © 1988-2023 [cit. 2023-03-12]. Dostupné z: https://www.avast.com/cs-cz/c-social-engineering

Understanding Denial-of-Service Attacks. Cybersecurity and Infrastructure Security Agency [online]. Washington D.C: CISA.gov, © 2010-2023, 2021 [cit. 2023-03-12]. Dostupné z: https://www.cisa.gov/news-events/news/understanding-denial-service-attacks

Věda a výzkum: Vybavení: Laboratoř kybernetické bezpečnosti. Univerzita Tomáše Bati ve Zlíně – Fakulta logistiky a krizového řízení [online]. Uherské hradiště: Univerzita Tomáše Bati ve Zlíně, © 2023 [cit. 2023-04-27]. Dostupné z: https://flkr.utb.cz/o-fakulte/zakladni-informace/struktura/ustavy/ustav-ochrany-obyvatelstva/veda-a-vyzkum/vybaveni/

Vybavení. Univerzita Tomáše Bati ve Zlíně – Fakulta logistiky a krizového řízení [online]. Uherské hradiště: Univerzita Tomáše Bati ve Zlíně, © 2020 [cit. 2023-04-27]. Dostupné z: https://km.flkr.utb.cz/PortalLakb/Article.aspx?guid=d5dbc8bf-9ed9-44ce-8fc4-55221f68da79

Využití. Univerzita Tomáše Bati ve Zlíně – Fakulta logistiky a krizového řízení [online]. Uherské hradiště: Univerzita Tomáše Bati ve Zlíně, © 2020 [cit. 2023-04-27]. Dostupné z: https://km.flkr.utb.cz/PortalLakb/Article.aspx?guid=cef560cd-d3b4-494e-8b52-dbba4a57767d

What is RSA. Encryptionconsulting [online]. USA: Encryption Consulting, © 2023 [cit. 2023-04-27]. Dostupné z: https://www.encryptionconsulting.com/education-center/what-is-rsa/

Základní pojmy. Kybez [online]. Jihlava, © 2021 [cit. 2023-04-15]. Dostupné z: https://www.kybez.cz/zakladni-pojmy/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AES Advanced Encryption Standard

DDoS Distributed Denial of Service

DoS Denial of Service

DRDoS Distributed Reflected Denial of Service

FLKŘ Fakulta logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně

ICT Informační a komunikační technologie

IP Internet Protocol

IT Informační technologie

LAN Lokální síť

MAN Metropolitní síť

PAN Osobní síť

RSA Rivest-Shamir-Adleman

VPN Virtuální privátní síť

WAN Vzdálená síť

SEZNAM OBRÁZKŮ

SEZNAM PŘÍLOH

PŘÍLOHA P I: PRAKTICKÁ ÚLOHA NA TÉMA ŠIFROVÁNÍ

ÚVOD

Šifrování je proces, který se využívá k zabezpečení dat za pomocí kryptografie. Nezabezpečená data se šifrují různými metodami, a to, aby se zabránilo jejich zneužití. Zašifrovaná data lze dešifrovat jenom pomocí dešifrovacího klíče. Pro účely výuky v kybernetické laboratoři na Fakultě logistiky a krizového řízení je šifrování hlavním principem, jak naučit studenty chránit si své data.

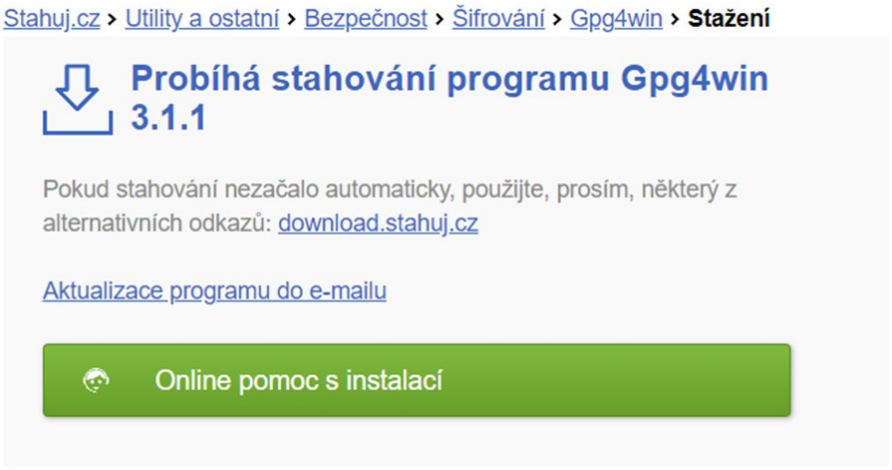
Tento protokol přehledně shrnuje instalaci programu Kleopatra a vytvoření šifrovacího páru klíčů pro potřeby šifrování souborů a také shrnuje instalaci programu VeraCrypt a jeho využití pro vytvoření zašifrovaného disku. Můj vypracovaný protokol je založen na protokolu se zadáním, kde byly nahrazeny některé texty a ty screenshoty (obrázky), které měly v zadaném protokolu červeně formátovaný titulek.

VYTVOŘENÍ ŠIFROVACÍHO KLÍČE

Níže následuje instalace programu Kleopatra a postup vytvoření virtuálního šifrovacího klíče pro potřeby zašifrování souboru pro finální část úkolu.

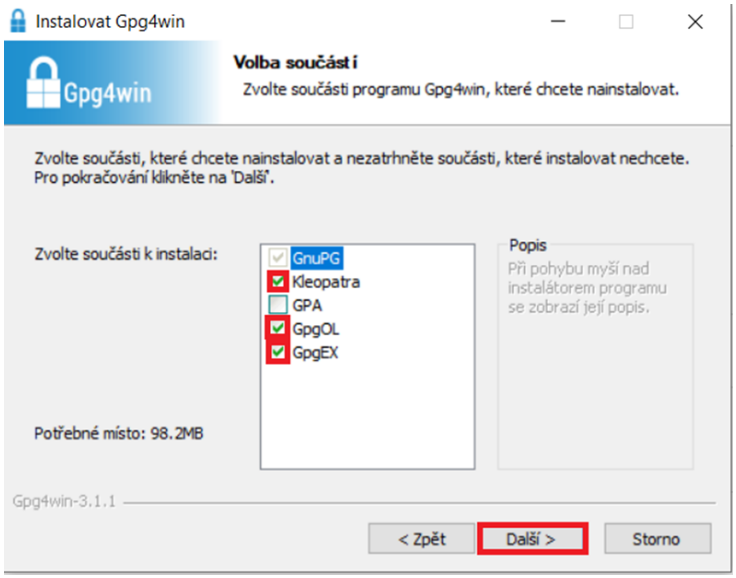
Instalace programu Kleopatra

Program Kleopatra potřebný k vytvoření šifrovacího klíče si stáhneme ze stahuj.cz.



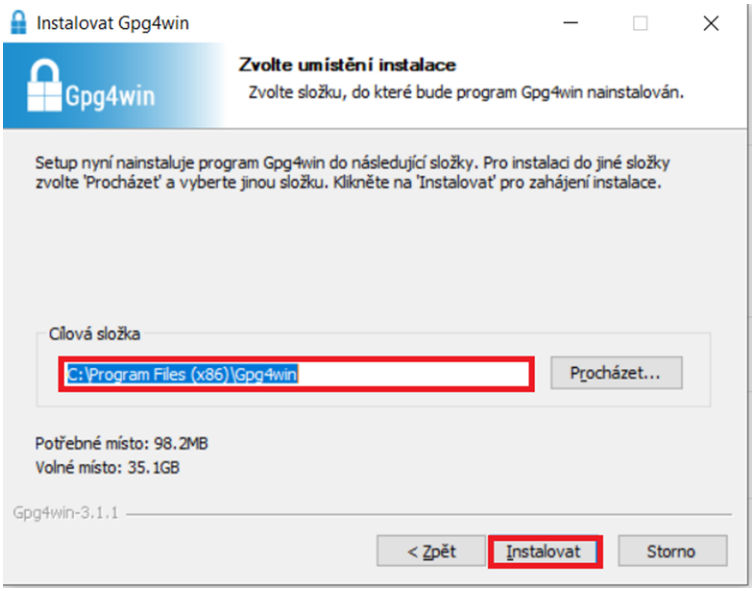
Výstřižek ze stránky stahuj.cz (Vlastní)

Krok č.1 (Vlastní)

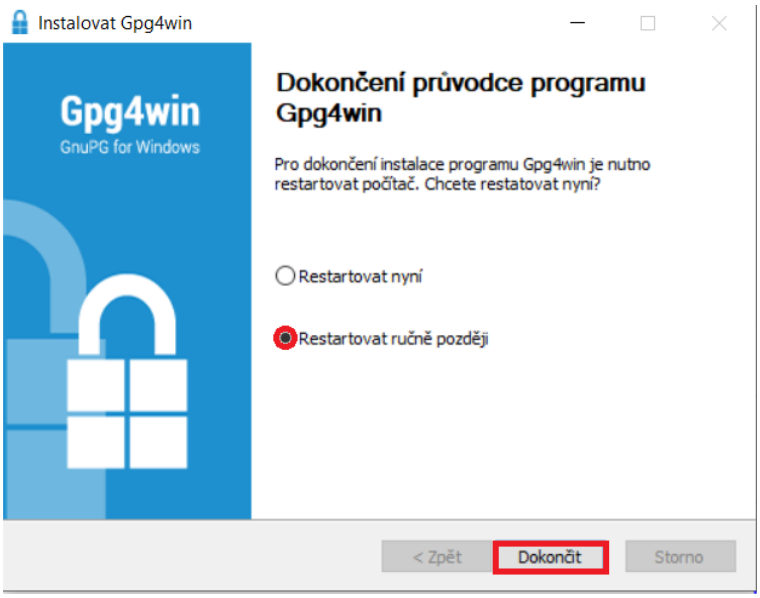


Krok č.2 Výběr správných součástí programu (Vlastní)

Pro instalaci programu si můžeme vytvořit vlastní složku nebo nechat přednastavenou.



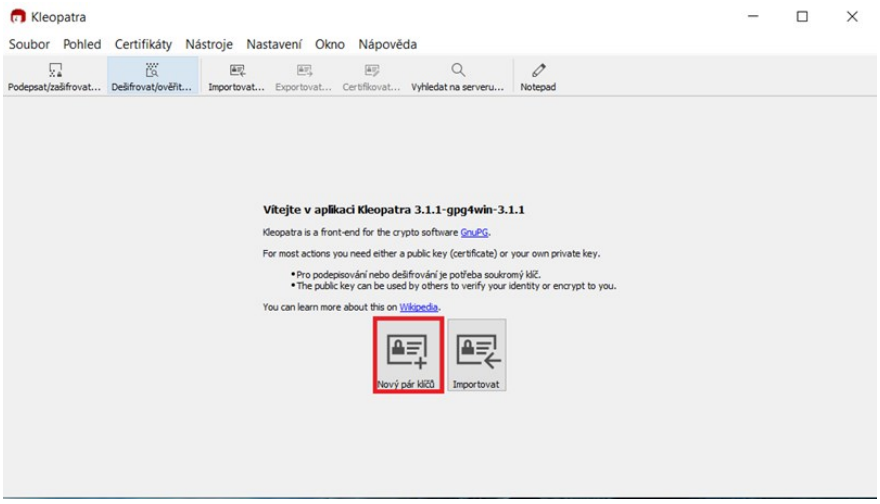
Krok č.3 Instalace do počítače (Vlastní)



Krok č.4 Dokončení instalace (Vlastní)

Práce v programu Kleopatra

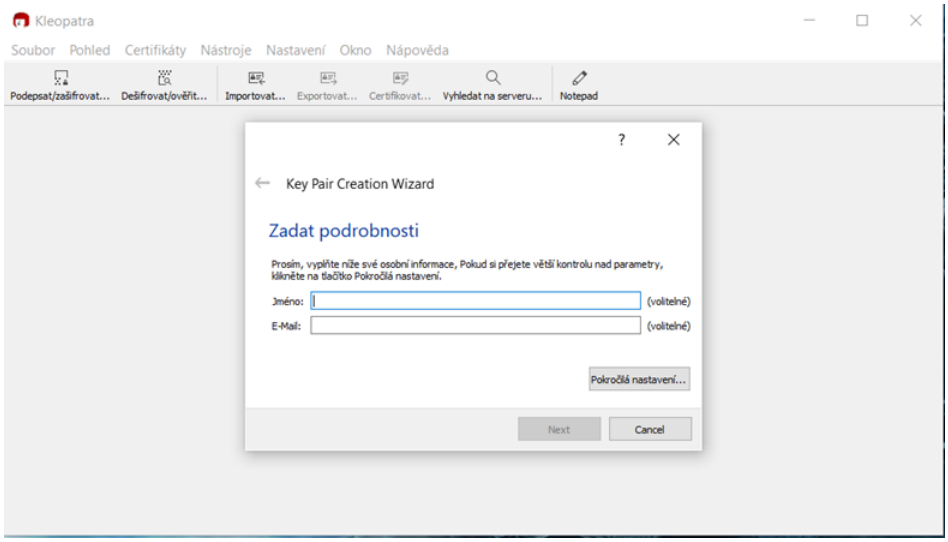
Po úspěšné instalaci aplikace Kleopatra si vytvoříme své vlastní šifrovací klíče. Jeden z těchto klíčů slouží k šifrování zpráv a souborů (ten je veřejný) a druhý slouží k dešifrování (ten je soukromý). Bez soukromého klíče příjemce zprávy nemůže danou zprávu přečíst ve správném formátu. Postup je zdokumentován níže.



Nový pár klíčů (Vlastní)

Název šifrovacího klíče

Pro zřetelné označení Klíčů si zvolíme jméno a fakultní e-mail.



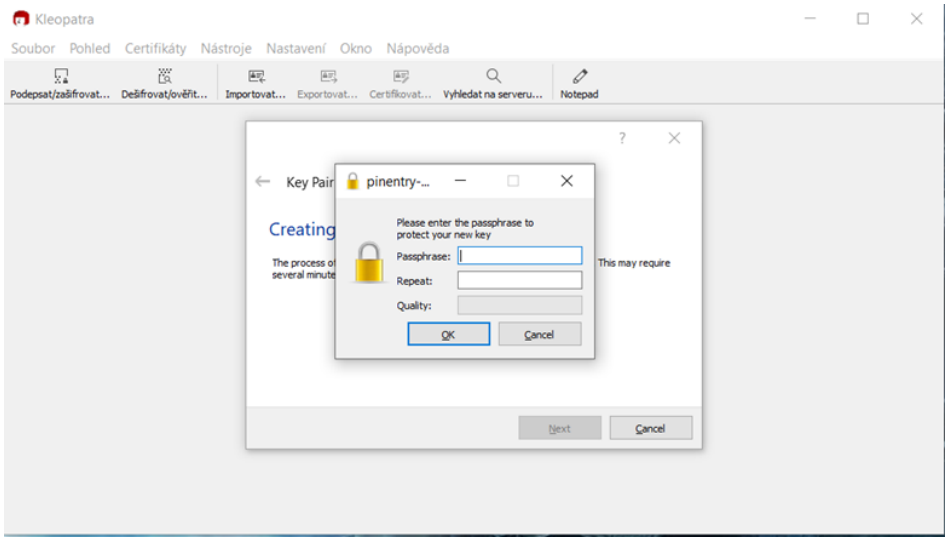
Zadání jména a e-mailu (Vlastní)

Složitost šifrování

- Nastavte typ šifrování RSA 2048 bitů
- Nastavte typ certifikování na (Podepisování, Šifrování, Certifikace)

Vytvoření hesla

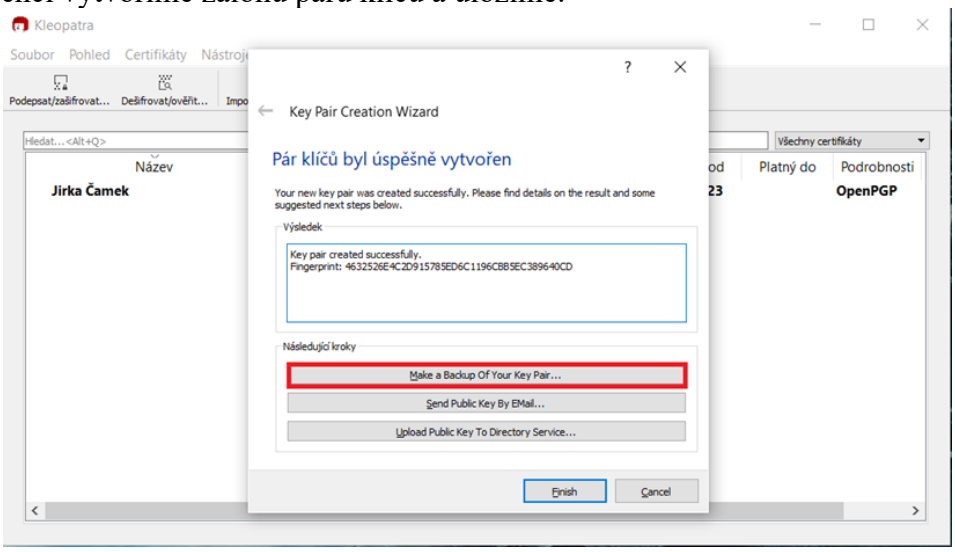
Pro potvrzování je potřeba si vytvořit silné ale zapamatovatelné heslo.



Vytvoření hesla (Vlastní)

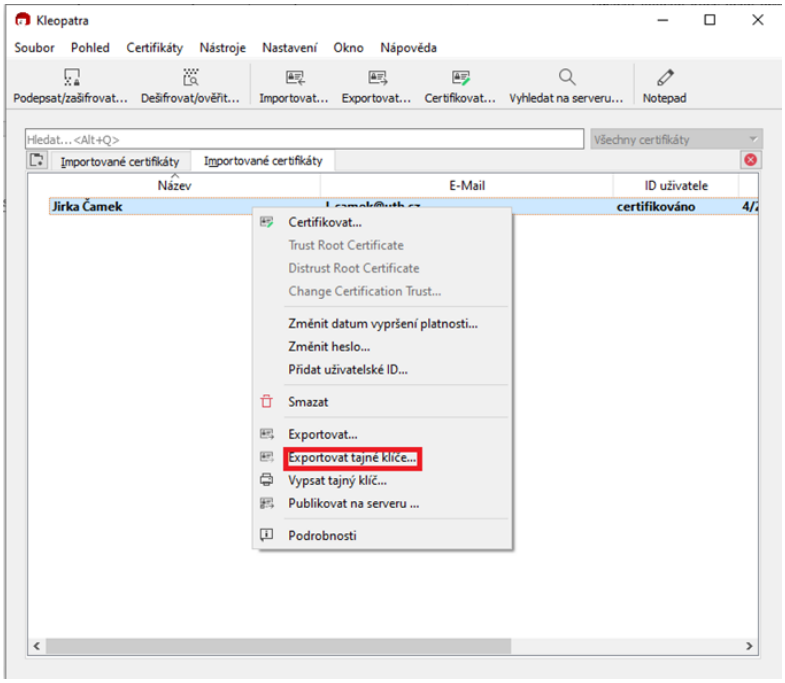
Záloha klíčů

Pro prevenci vytvoříme zálohu páru klíčů a uložíme.



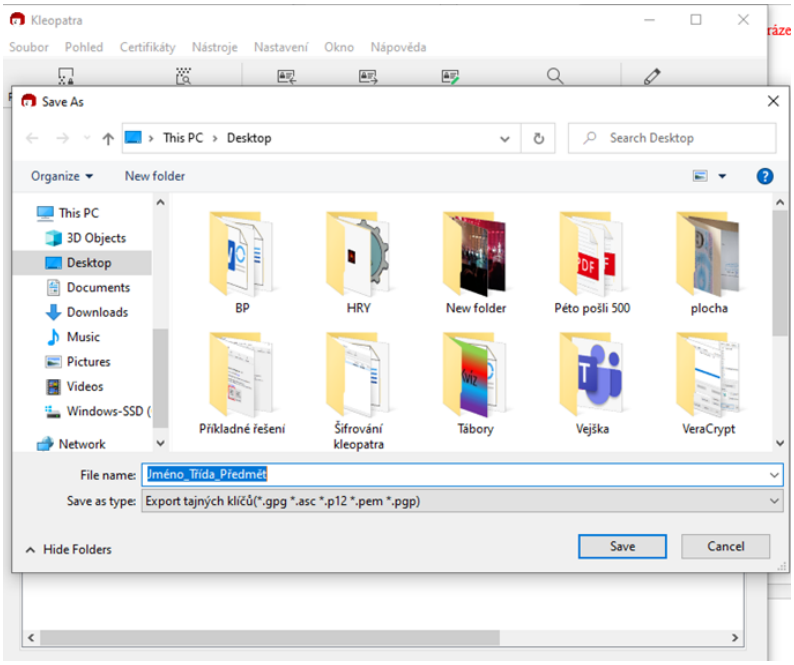
Záloha klíčů (Vlastní)

Vytvoření tajného klíče



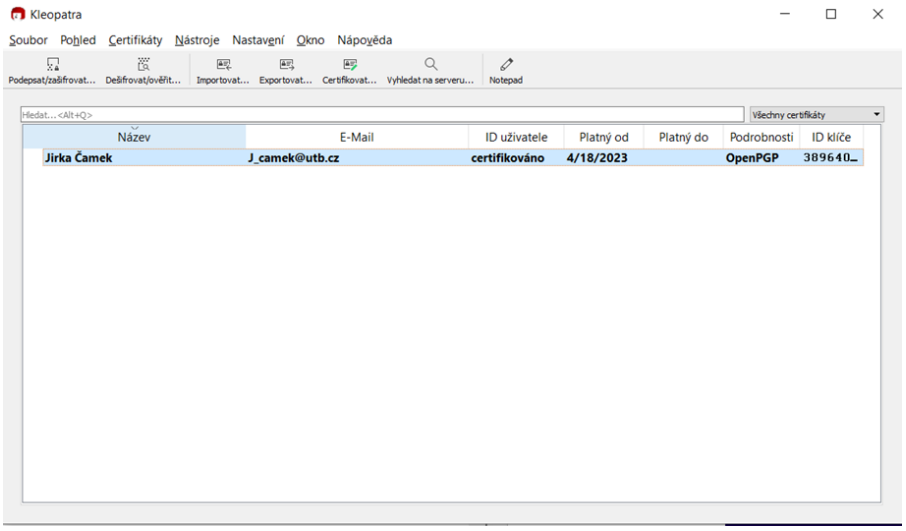
Exportování tajného klíče (Vlastní)

Tajný klíč



Uložení klíče Jméno, Třída, Předmět (Vlastní)

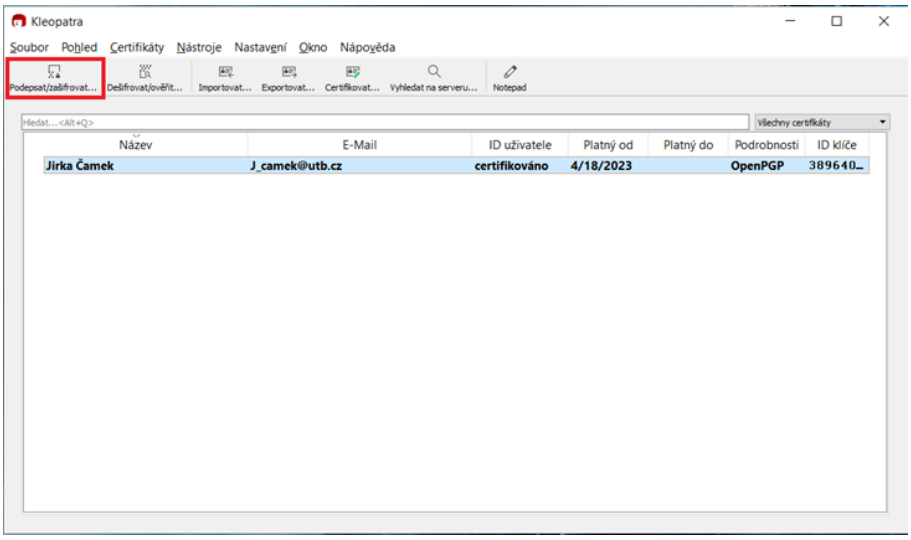
Výstřižek vytvořeného páru klíčů



Finální část postupu (Vlastní)

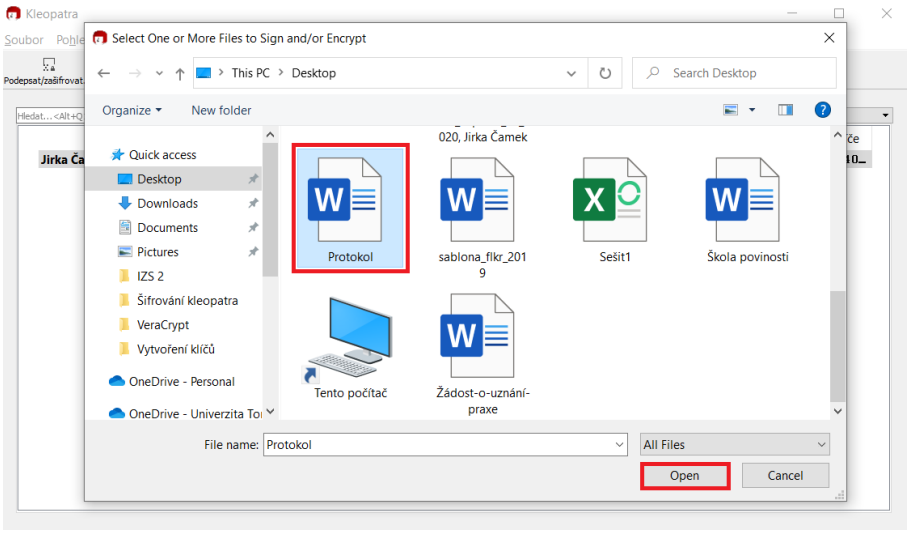
Šifrování v programu Kleopatra

V programu Kleopatra si zašifrujeme finální část semestrálního úkolu, kterou pak odevzdáme spolu s tajným klíčem.



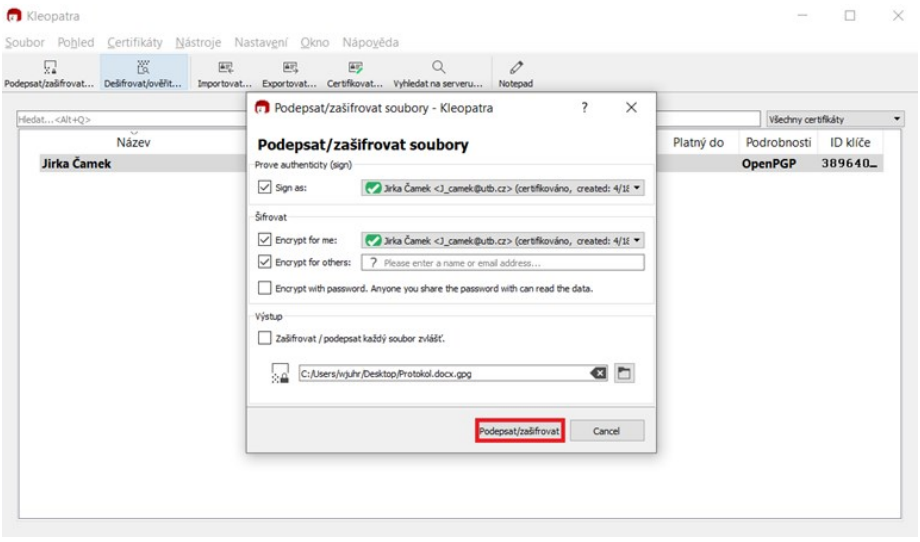
Podepsat/Zašifrovat (Vlastní)

Vybírání souboru pro šifrování



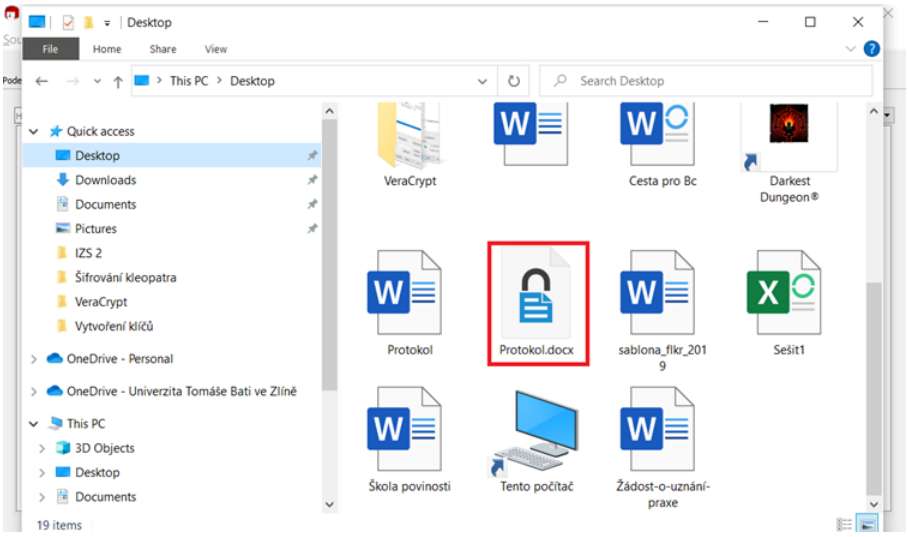
Soubor pro šifrování (Vlastní)

Potvrzení šifrování



Podepsat/Zašifrovat – Dokončení (Vlastní)

Zašifrovaný soubor



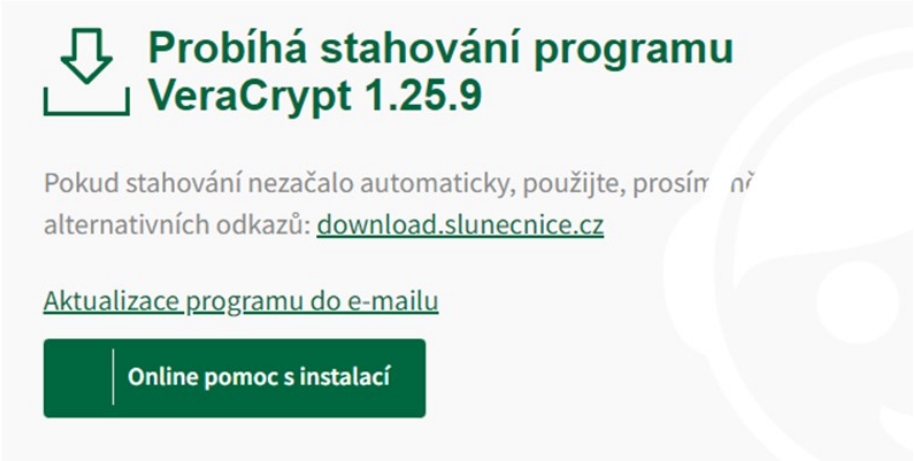
Zašifrovaný soubor (Vlastní)

VERACRYPT

Níže následuje postup pro stažení programu VeraCrypt a následné vytvoření vlastního zašifrovaného disku v počítači.

Instalace programu VeraCrypt

Program VeraCrypt stáhneme ze stránky slunečnice.cz a stejným postupem nainstalujeme do počítače jako v první části.



Výstřižek ze stránky slunečnice.cz (Vlastní)

VYTVOŘENÍ ZAŠIFROVANÉHO DISKU

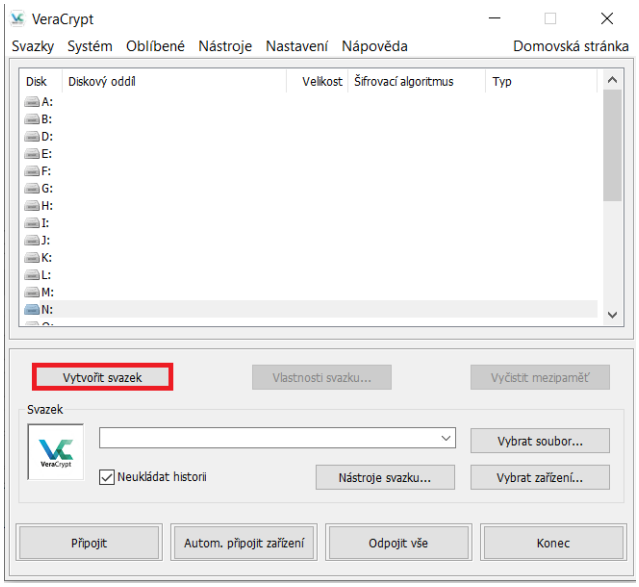
Po instalaci programu VeraCrypt následuje vytvoření vlastního zašifrované disku, který lze otevřít jen na zařízení na kterém je program VeraCrypt, přičemž tento postup je zdokumentován níže.

Práce v programu VeraCrypt

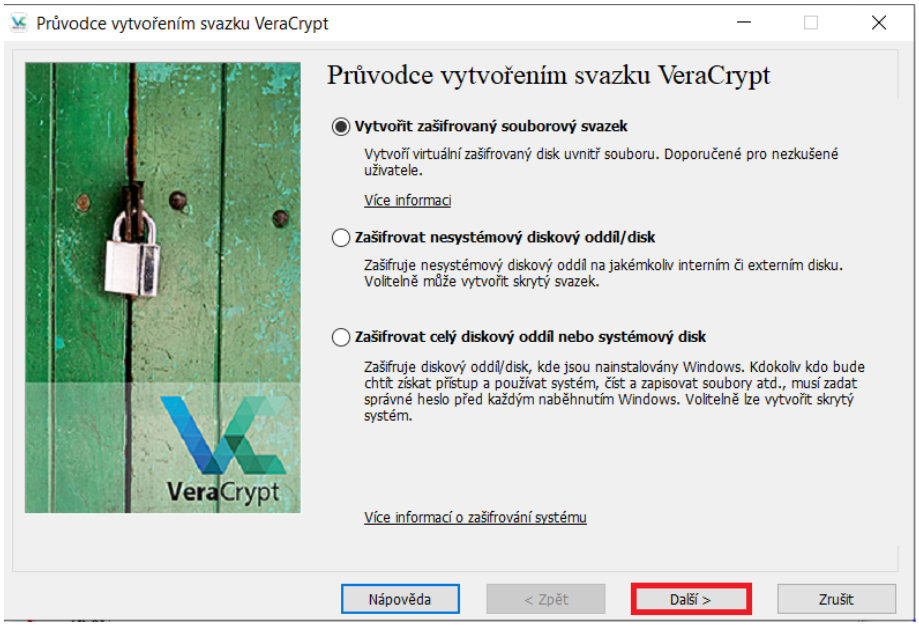
Otevřeme program VeraCrypt a vytvoříme v něm zašifrovaný disk do kterého pak vložíme podepsaný dokument.

1. Vstupte do Vytvořit svazek.
2. Vyberte možnost vytvořit zašifrovaný souborový svazek.
3. Vyberte standartní svazek.
4. Umístění svazku zvolte kdekoliv v počítači a disk pojmenujte svým jménem.
5. Zvolte možnost šifrování AES.
6. Velikost svazku zvolte 100 MB.
7. Zvolte si silné heslo pro váš svazek.
8. Naformátujte svazek.
9. Do zašifrovaného disku vložte dokument, který nese vaše jméno a třídu.

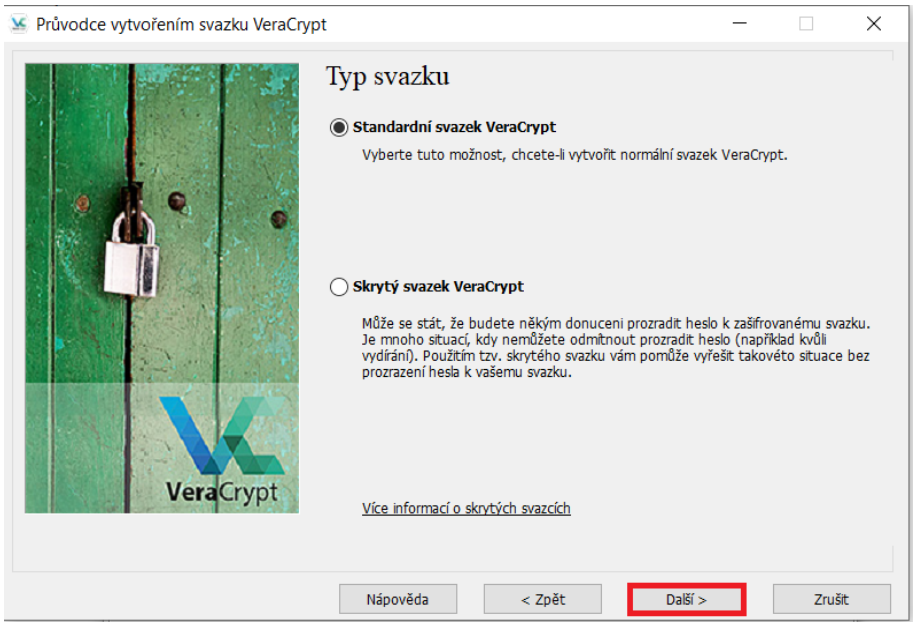
Vytvoření svazku



Vytvoření svazku (Vlastní)



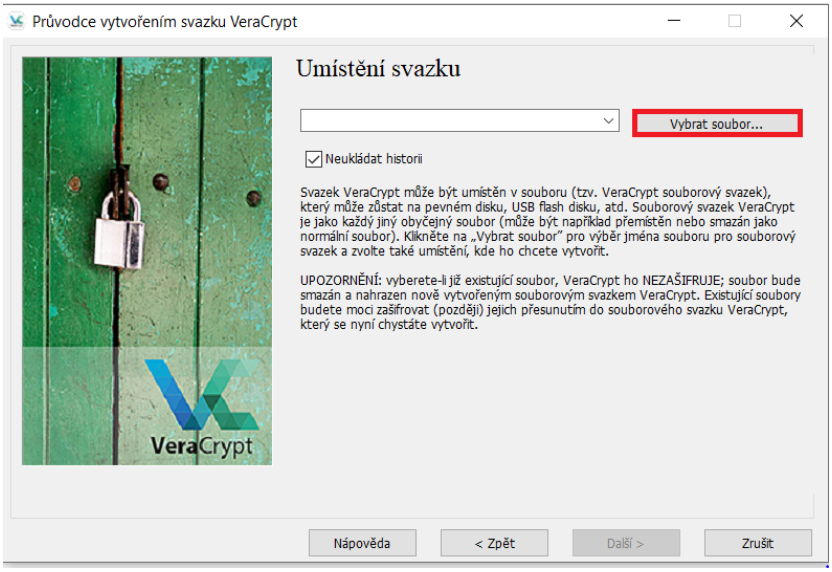
Vytvoření Zašifrovaného svazku (Vlastní)



Zvolení typu svazku (Vlastní)

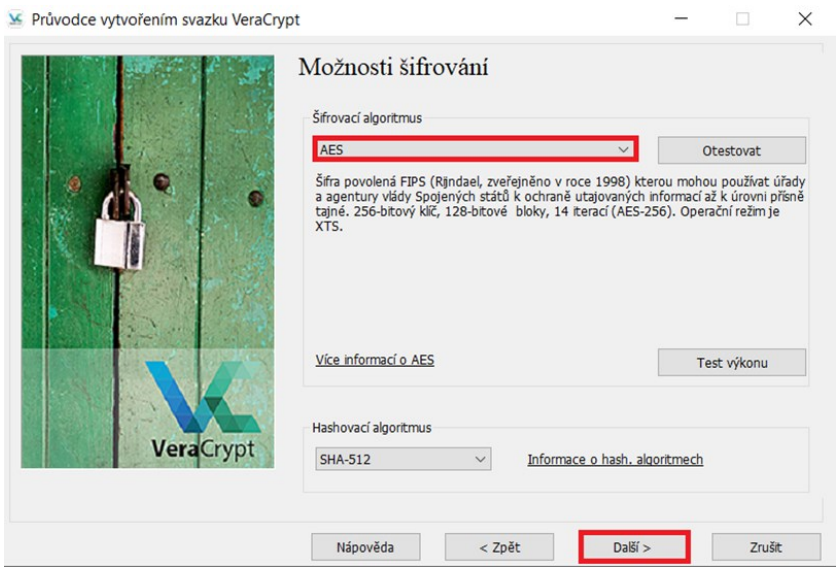
Umístění svazku

Umístění svazku zvolte kdekoliv v počítači a disk pojmenujte svým jménem.



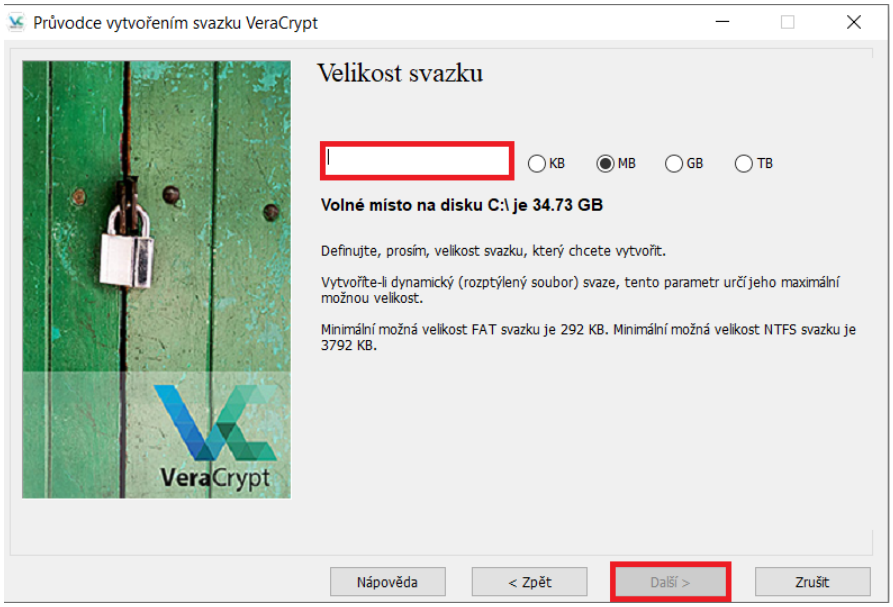
Umístění svazku (Vlastní)

Možnosti šifrování



Zvolení možnosti šifrování (Vlastní)

Velikost svazku



Velikost svazku (Vlastní)

Heslo svazku

Heslo nastavte dostatečné silné ale zapamatovatelné.

Heslo svazku (Vlastní)

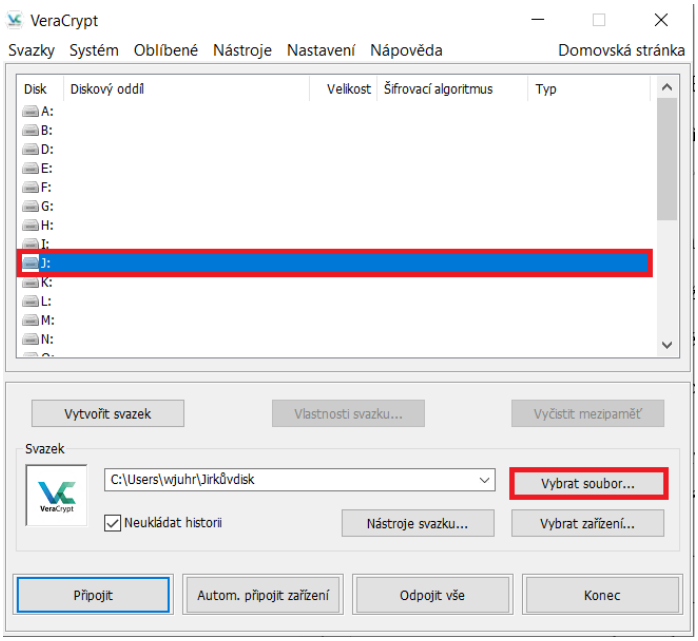
Hlavní formátování svazku

Formát svazku (Vlastní)

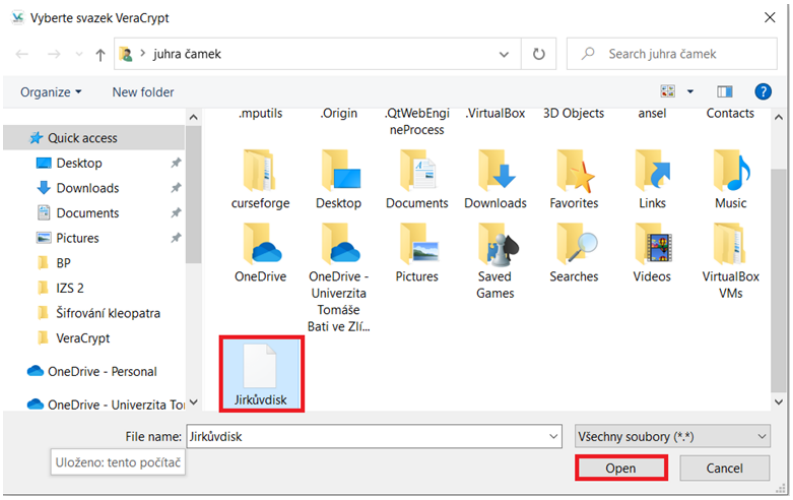
VYTVOŘENÝ DISK PŘIPOJTE DO VERACRYPT

Vytvořený zašifrovaný disk dále připojíme v programu VeraCrypt abychom ho mohli otevřít a vkládat na něj soubory. Na připojený disk vložíme soubor (Jméno, Třída).

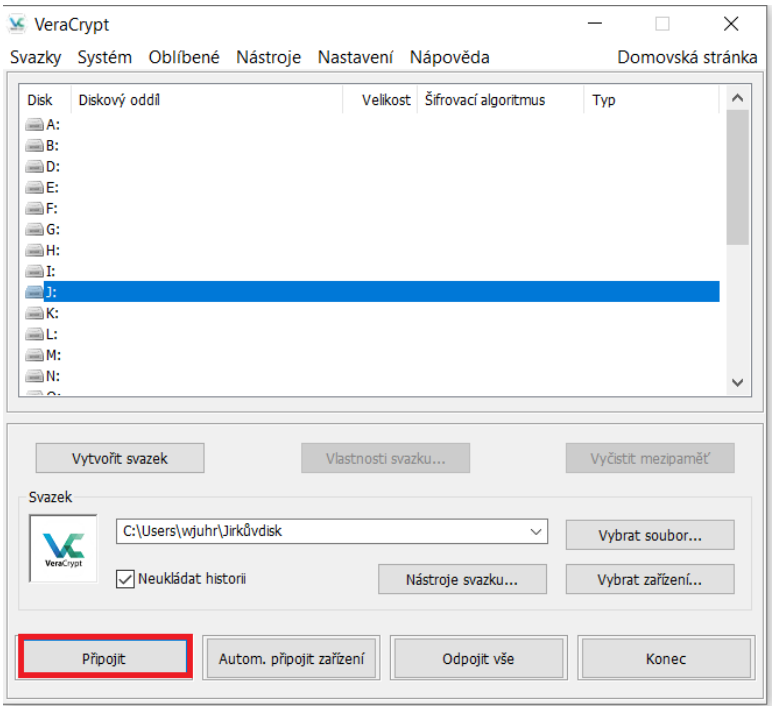
Připojení disku



Vybírání diskového oddílu (Vlastní)

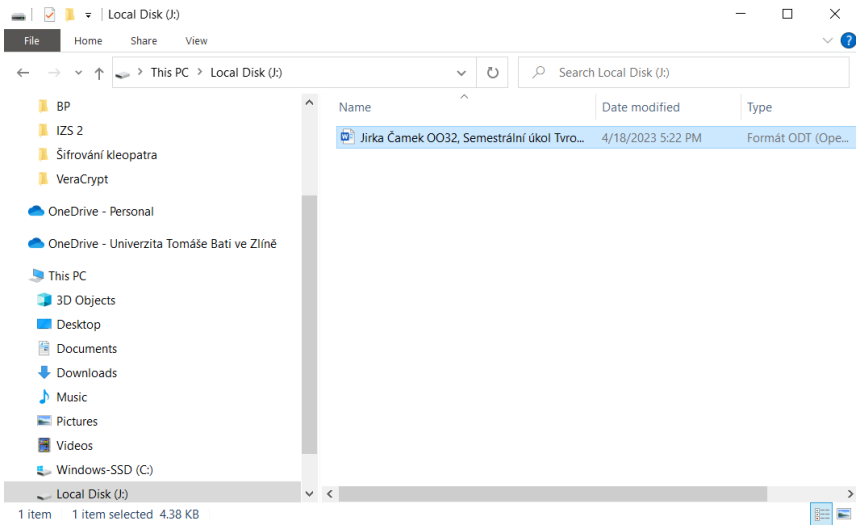


Vybírání šifrovaného disku (Vlastní)



Připojení disku (Vlastní)

Připojte screenshot disku se souborem



Zašifrovaný disk J (Vlastní)

ZÁVĚR

Výše popsaný postup umožnil instalaci programů Kleopatra a VeraCrypt a následné seznámení s jejich funkcemi jako je tvorba šifrovacích klíčů a zašifrovaného disku. Funkce těchto programů nám v budoucím využití mohou sloužit k zabezpečení pro nás důležitých dat a jejich možnému zneužití.