**UNIVERZITA OBRANY**

**FAKULTA VOJENSKÝCH TECHNOLOGIÍ**

**Studijní program: Vojenské technologie**

Studijní obor: Informační technologie

Ev. číslo: xxxx/22



**DIPLOMOVÁ PRÁCE**

Název: Využití postkvantových algoritmů pro zabezpečení informačního systému

Zpracoval: Vojtěch Bžatek

Vedoucí práce: Prof. Dr. Ing. Alexandr Štefek

BRNO 2022

Zadání

I. Upřesnění podmínek zpracování závěrečné práce

V souvislosti se zpracováním závěrečné práce NEBUDE studentem nakládáno s utajovanými informacemi.

V souvislosti se zpracováním závěrečné práce NEBUDE studentem nakládáno s informacemi pro služební potřebu.

Závěrečná práce NEBUDE obsahovat utajené informace.

Závěrečná práce NEBUDE obsahovat informace pro služební potřebu.

Při zpracování závěrečné práce NEBUDOU zpracovávány osobní údaje.

II. Cíl závěrečné práce

Navrhnout možnosti využití nejnovějších poznatků z oblasti kvantového šifrování a využití blockchain pro potřeby ochrany dat v informačních systémech.

Nezbytné součásti diplomové práce:

Přehled algoritmů a jejich open source implementací z kategorie tzv. postkvantového šifrování.

Přehled ochranných mechanismů pro zabezpečení dat v informačním systému s ohledem na možnost odhalení manipulace s daty.

Implementace mikroslužby zabezpečující operace typu šifrování a podepisování nad datovými bloky.

Implementace mikroslužby zabezpečující technologii blockchain nad logovými soubory informačního systému.

III. Pokyny pro zpracování závěrečné práce

Zpracujte přehled dostupných opensource implementací šifrování (tzv. postkvantové algoritmy), specificky výstupy ze soutěží nist.gov.

Zpracujte přehled možných útoků na standardně implementované informační systémy (datové úložiště).

Zpracujte přehled možných protiopatření (ochranných mechanismů).

Implementujte mikroslužbu využívající tzv. postkvantových algoritmů pro šifrování pro zabezpečení dat proti specifickým modifikacím dat.

Průběžně udržujte aktualizovaný přehled použité literatury a ke každé dílčí etapě zpracujte cca 7 stran shrnutí.

**PODĚKOVÁNÍ (nepovinné)**

**ČESTNÉ PROHLÁŠENÍ**

Prohlašuji, že jsem zadanou diplomovou práci na téma „xxx“ vypracoval samostatně, pod odborným vedením vedoucího xxx a použil jsem pouze literární zdroje uvedené v práci.

Dále prohlašuji, že jsem seznámen s tím, že se na moji diplomovou práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména skutečnosti, že Univerzita obrany má právo na uzavření licenční smlouvy o užití této bakalářské (diplomové) práce jako školního díla podle § 60 odst. 1 výše uvedeného zákona, a s tím, že pokud dojde k užití této diplomové práce mnou nebo bude poskytnuta licence o užití díla třetímu subjektu, je Univerzita obrany oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladu, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše. Souhlasím se zpřístupněním své diplomové práce pro prezenční studium v prostorách knihovny Univerzity obrany.

V Brně, dne xx. května. 2024

..........................................

Jméno studenta

**ABSTRAKT**

**Klíčová slova:**

**Kryptografie, Postkvantové algoritmy, blockchain, blockchainová síť**

**ABSTRACT**

**Key words:**

Obsah

[SEZNAM POUŽITÝCH ZKRATEK 9](#_Toc162788413)

[SEZNAM OBRÁZKŮ 10](#_Toc162788414)

[SEZNAM TABULEK 11](#_Toc162788415)

[ÚVOD 12](#_Toc162788416)

[2 Postkvantová kryptografie 15](#_Toc162788417)

[2.1 Současný stav 15](#_Toc162788418)

[2.2 NIST 15](#_Toc162788419)

[2.3 Seznam algoritmů 15](#_Toc162788420)

[2.3.1 Kyber 15](#_Toc162788421)

[2.3.2 DILITHIUM 15](#_Toc162788422)

[2.3.3 Falcon 15](#_Toc162788423)

[2.3.4 Sphincsplus 15](#_Toc162788424)

[3 Přehled ochraných mechanismů pro zabezpečení dat v informačním systému s ohledem na možnost odhalení manipulace s daty 15](#_Toc162788425)

[4 Blockchain 15](#_Toc162788426)

[4.1 Blockchainová síť 15](#_Toc162788427)

[5 Praktická část 15](#_Toc162788428)

[5.1 Cíl praktické části a její omezení 15](#_Toc162788429)

[5.2 Mikroslužba zabezpečující postkvantovou kryptografii 15](#_Toc162788430)

[5.2.1 Popis jednotlivých částí 15](#_Toc162788431)

[5.2.2 Nastavení symetrického klíče 15](#_Toc162788432)

[5.2.3 Získání podepisovacího klíče 15](#_Toc162788433)

[5.2.4 Průběh komunikace při odeslání zprávy 15](#_Toc162788434)

[5.2.5 Průvodce pro spuštění mikroslužby 15](#_Toc162788435)

[5.3 Mikroslužba zabezpečující technologii blockchain nad logovými soubory informačního systému. 15](#_Toc162788436)

[5.3.1 Popis jednotlivých částí 15](#_Toc162788437)

[5.3.2 Popis funkcionalit nodu 15](#_Toc162788438)

[5.3.3 Průvodce pro spuštění mikroslužby 15](#_Toc162788439)

[5.4 Kompilace mikroslužeb postkvatového šifrování a blockchainové sítě 15](#_Toc162788440)

[5.4.1 Popis jednotlivých částí 15](#_Toc162788441)

[5.4.2 Ukázka funkcionalit mikroslužeb 15](#_Toc162788442)

[5.4.3 Průvodce pro spuštění kompilace obou mikroslužeb 15](#_Toc162788443)

[6 Možnosti dalšího rozvoje 15](#_Toc162788444)

[7 Závěr 15](#_Toc162788445)

[ZÁVĚR 15](#_Toc162788446)

[SEZNAM POUŽITÉ LITERATURY (vzor) 16](#_Toc162788447)

[SEZNAM PŘÍLOH 19](#_Toc162788448)

# SEZNAM POUŽITÝCH ZKRATEK

|  |  |
| --- | --- |
| AČR | Armáda České republiky (→ Styl seznam zkratek) |
| ISO | International Organization for Standardization  Mezinárodní organizace pro standardizaci |

# SEZNAM OBRÁZKŮ

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | Strana |
| Obrázek 1 | − | Popis obrázku (→ styl Odstavec) | … XX |
| Obrázek 2 | − | Popis obrázku | … XX |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# SEZNAM TABULEK

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | Strana |
| Tabulka 1 | − | Popis tabulky | … XX |
| Tabulka 2 | − | Popis tabulky | … XX |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# ÚVOD

# Postkvantová kryptografie

## Současný stav

## NIST

## Seznam algoritmů

Kyber

DILITHIUM

Falcon

Sphincsplus

# Přehled ochraných mechanismů pro zabezpečení dat v informačním systému s ohledem na možnost odhalení manipulace s daty

# Blockchain

## Blockchainová síť

# Praktická část

## Cíl praktické části a její omezení

## Mikroslužba zabezpečující postkvantovou kryptografii

Popis jednotlivých částí

Alice

Bob

Nastavení symetrického klíče

Získání podepisovacího klíče

Soukromý podepisovací klíč

Veřejný podepisoací klíč

Průběh komunikace při odeslání zprávy

Průvodce pro spuštění mikroslužby

## Mikroslužba zabezpečující technologii blockchain nad logovými soubory informačního systému.

Popis jednotlivých částí

Blockchain

Klient/Postman

Popis funkcionalit nodu

Registrace v síti

Přijetí zprávy

Těžba

Ověření řetězu

Poskytnutí řetezu

Průvodce pro spuštění mikroslužby

## Postkvantová blockchainová síť

Popis jednotlivých částí

Agent

Node

Ukázka funkcionalit mikroslužeb

Průvodce pro spuštění Postkvantové blockchainové sítě

# Možnosti dalšího rozvoje

# ZÁVĚR

Je nutné věnovat stejnou, ne-li větší pozornost jako úvodu. V závěru musíte podat shrnutí, vyzvednout nejdůležitější postřehy a také vyhodnotit, zdali jste naplnili cíle, které jste si stanovili v úvodu své práce.

# SEZNAM POUŽITÉ LITERATURY (vzor)

**MONOGRAFIE**

1. ANTUŠÁK, Emil. *Strategie a ekonomika v bezpečnostním systému České republiky*. 1. vyd. Praha: Ministerstvo obrany České republiky, 2002. s. 141 – 180. ISBN 80-7278-143-x.
2. BRČÁK, Josef. *Česká republika ve světle ekonomických teorií*. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2012. s. 78 – 150. ISBN 978-80-7380-369-8.
3. KADEŘÁBKOVÁ, Anna. *Základy makroekonomické analýzy: růst, konkurenceschopnost, rovnováha*. 1. vyd. Praha: Linde, 2003. 175 s. ISBN 80-86131-36-x.

**ELEKTRONICKÉ ZDROJE**

1. BALCAROVÁ, Pavlína. *Konkurenceschopnost ekonomiky a její měření* [online]. Brno, 2007 [cit. 2014-12-30]. Dostupné z: ˂<http://is.muni.cz/th/75962/prif_m/diplomova_prace.pdf>˃. Diplomová práce. Masarykova univerzita.
2. Česká republika: hlavní makroekonomické ukazatele. *Český statistický úřad* [online]. 2014 [cit. 2015-01-28]. Dostupné z: ˂[https://www.czso.cz/documents/10180/20555311/HLMAKRO.xls](http://www.czso.cz/csu/redakce.nsf/i/cr:_makroekonomicke_udaje/$File/HLMAKRO.xls)˃.

* Pozn. ČSN ISO 690 Informace a dokumentace – Pravidla pro bibliografické odkazy a citace informačních zdrojů

# 

# SEZNAM PŘÍLOH

|  |  |  |  |
| --- | --- | --- | --- |
| Příloha č. 1 | − | Popis přílohy (→ styl Odstavec) |  |
| Příloha č. 2 | − | Popis přílohy (→ styl Odstavec) |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

(→ Styl Příloha – číslování) Příloha 1

Popis přílohy (→ styl Příloha – popis)

|  |
| --- |
|  |