VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY
A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

Zabezpečené úložiště pomocí postkvantové kryptografie

SEMESTRÁLNÍ PRÁCE
SEMESTRAL THESIS

AUTOŘI PRÁCE
AUTHOR

Tadeáš Zachoval, Adam Turek,
Tomáš Závada, Nguyễn Phúc

BRNO 2023

Obsah

Úvod

V posledních třech desetiletích se kryptografie s veřejným klíčem stala nedílnou součástí globální digitální komunikační infrastruktury. Bezpečnost mnoha dnes používaných důležitých komunikačních protokolů se opírá o tři základní kryptografické funkce: šifrování s veřejným klíčem, digitální podpisy a výměnu klíčů. V současné době se tyto funkce realizují především pomocí Diffie-Hellmanovy výměny klíčů, kryptosystému RSA a kryptosystému eliptických křivek. Bezpečnost těchto kryptosystémů je založena na obtížných problémech, jako je numerická analýza, diskrétní logaritmy.

V roce 1994 Peter Shor z Bellových laboratoří ukázal, že kvantové počítače, nová technologie, která využívá fyzikální vlastnosti hmoty a energie pro výpočty, mohou řešit složité problémy efektivněji než výpočty pomocí tradičních počítačů. To vytváří riziko, že všechny informační systémy využívající kryptografii s veřejným klíčem přestanou být bezpečné. Stojíme před otázkou: Můžeme se ubránit útočníkovi, který používá klasické a kvantové výpočty?

Vznik kvantových počítačů přilákal vědce zabývající se kryptografií k řešení problému budoucího zabezpečení informací, které by bylo odolné vůči útokům pomocí kvantových počítačů. Tato věda se nazývá postkvantová kryptografie. Výsledkem této vědy jsou různé přístupy ke kvantovému šifrování. Za zmínku stojí např: Algoritmus učení s chybami (LWE), McElieceův kryptosystém, NTRU kryptosystém, Kvantová distribuce klíčů a Merkle-Damgårdova konstrukce hashe. [1]

V tomto projektu přezkoumáme a vyhodnotíme přístup využívající algoritmus McEliece. Poté bude algoritmus aplikován na sestavení databáze s vlastnostmi kompletní aplikace. Projekt je založen na dostupných knihovnách v kombinaci s programovacím jazykem Python s cílem ověřit teoretický základ a demonstrovat použití postkvantové kryptografie v praxi.

Cíle

Cílem našeho semestrálního projektu je vytvořit zabezpečené úložiště pomocí postkvantové kryptografie. Aplikace bude schopná vytvořit zabezpečené spojení typu klient-klient (peer-to-peer), které bude šifrováno pomocí symetrického šifrovacího algoritmu. K výměně/ustanovení symetrického klíče mezi klienty využijeme algoritmus postkvantové kryptografie. Úložiště bude ovládáno pomocí grafického rozhraní. Při přenosu dat mezi úložištěm a uživatelem bude zajištěna důvěrnost, integrita a autentičnost přenášených dat.

Úložiště bude vytvářet logy o přístupu a akcích uživatele (kdy byl autentizován, jaké soubory četl, změnil, kopíroval, smazal, stahoval, nahrával apod.) a informace o provedených akcích (čas, činnost, použitý algoritmus, velikost zpracovávaného souboru atd.). Logy o přístupu a akcích uživatele budou chráněny proti jejich změně.

Teoretická část

Zabezpečené uložiště

Zabezpečené úložiště [2] je důležitou součástí bezpečnosti informací, která se týká chráněného ukládání cenných nebo citlivých dat. Data mohou zahrnovat osobní nebo finanční informace, duševní vlastnictví, obchodní tajemství nebo jiné důvěrné informace. Zabezpečené úložiště je tak nezbytné prozajištění důvěrnosti, integrity a pro dostupnost informací. Potřeba zabezpečeného úložiště vzniká v důsledku rostoucí závislosti na ukládání digitálních dat a stále rostoucích hrozeb kybernetických útoků narušení bezpečnosti dat.

Komunikace peer to peer

Peer-to-peer (P2P) [3] je model komunikace, ve které disponují jednotlivé strany rovnoměrnými možnostmi a kterákoli z nich může iniciovat komunikační relaci. Při tomto typu komunikace každý počítač funguje jako klient i server zároveň a umožňuje přímou výměnu dat mezi nimi. U komunikace klient-klient je nevýhodou, že soubory nejsou centrálně zálohovány a uspořádány v konkrétní sdílené oblasti, ale jsou ukládány v samostatných počítačích. Výhodou je že sítě pracují bez serveru, kde díky tomu není nutnost správce serveru, jelikož každý uživatel má ve správě svůj počítač

Klienti přitom působí jako pracovní stanice, přičemž nesdílejí informační a komunikační zdroje. Také mohou lépe provádět aktualizaci aplikací a souborů, protože tyto soubory jsou ukládány pouze na jednom jediném počítači

Symetrická kryptografie

Symetrická kryptografie[4] využívá k šifrování i dešifrování elektronické informace pouze jeden klíč (tajný klíč). Subjekty komunikující prostřednictvím symetrického šifrování si musí vyměnit klíč, aby jej bylo možné použít při dešifrování. Využíváním algoritmů symetrického šifrování jsou data "zakódována" takovým způsobem, že je nemůže rozpoznat žádná osoba, která nedisponuje tajným

klíčem k dešifrování. Po obdržení zprávy určeným příjemcem, který vlastní klíč, algoritmus obrátí svůj postup tak, aby se zpráva vrátila do své původní čitelné podoby.

Symetrická kryptografie je účinným nástrojem pro bezpečnou komunikaci, ale zároveň není nezranitelná. Mezi hlavní zranitelnosti symetrické kryptografie patří: Distribuce klíčů, Správa klíčů, Opakované použití klíče, Kryptoanalýza, Hrozby zevnitř

Rozdělení:

- Blokové šifry
  - Advanced Encryption Standard (AES)
  - Blowfish
  - Data Encryption Standard (DES)
  - Rivest Cipher 2 (RC2)
  - RC5
  - Triple DES
- Proudové šifry
  - FISH
  - RC4

Advanced Encryption Standard (AES)

AES [5] je nejrozšířenější symetrická šifra v současné době. Na rozdíl od DES, mohou být klíč a bloky nezávisle zvoleny. Velikosti klíče mohou být 128, 192 nebo 256 bitu a velikost bloku 128 bitu.

Rundovní operace:

- substituce (S-box): matice obsahující všechny možné kombinace po 8bitové sekvenci,
- row shift (bajtová permutace): jedná se o permutaci, kdy:
  - První řádek stavu se nepozmění.
  - Druhý řádek je posunut o 1 bajt doleva kruhovým způsobem.
  - Třetí řádek je posunut o 2 bajty doleva kruhovým způsobem.
  - Čtvrtý řádek je posunut kruhovým způsobem o 3 bajty doleva.
- column mix (lineární transformace): jedná se o substituci s využitím aritmetiky Gaisového pole (2^8). S každým sloupcem se pracuje jednotlivě a každá byte je namapován na novou hodnotu.
- key addition: bitový XOR s rundovním klíčem.

I když existují útoky na oslabené verze AES (nižší počet rund a menší velikost klíčů), jde o bezpečný protokol, který je využitý v TLS, OpenSSH a většině ostatních současných protokol.

Postkvantová kryptografie

Postkvantová kryptografie [6] je oblast kryptografie, jejímž cílem je vývoj kryptografických algoritmů, které jsou odolné vůči útokům kvantových počítačů. Podnětem pro postkvantovou kryptografii je potenciální hrozba, kterou kvantové počítače představují pro klasické kryptografické algoritmy. Pro kvantové počítače se předpokládá, že jsou schopny řešit některé výpočetní problémy, jako je faktorizace velkých čísel a výpočet diskrétních logaritmů, mnohem rychleji než klasické počítače. Zmíněné problémy reprezentují základ mnoha klasických kryptografických algoritmů, včetně těch, které se používají pro výměnu klíčů. Počet klíčů generovaných v postkvantové kryptografii závisí na konkrétním použitém algoritmu. Například algoritmy založené na mřížce (Lattice), jako jsou NTRUEncrypt a

NewHope, používají klíče o délce obvykle 256 až 512 bitů. Jiné algoritmy, jako je podepisování na základě hašování (XMSS) a kryptografie na základě kódu (McEliece), používají delší klíče, například 768 až 1536 bitů.

V oblasti výzkumu postkvantové kryptografie se v současné době pracuje především se čtyřmi hlavními typy přístupů:

- Kryptografie založena na mřížkách [7]: toto kryptografické schéma je postaveno na matematických problémech kolem mřížek. Mřížka v tomto kontextu připomíná mřížku grafického papíru – využívá množinu bodů umístěných na průsečících mřížky přímek. Tato mřížka není v žádném smyslu konečná. Místo toho mřížka popisuje vzor, který pokračuje do nekonečna. K odvození soukromého klíče z veřejného klíče by bylo nutné prohledat všechny možnosti hrubou silou, a i když kvantové počítače mohou toto prohledávání urychlit, stále by trvalo značně dlouho a nereálně. Předpokládá se, že ani kvantový počítač není schopen vyřešit těžké problémy založené na mřížkách v rozumném čase. Jako příklad algoritmů na bázi mřížky lze uvést CRYSTALS-KYBER a CRYSTALS-Dilithium.

- Multivariační kryptografie [8]: je založena na řešení soustav vícerozměrných rovnic. V multivariační kryptografii je veřejným klíčem vícerozměrný polynom a soukromým klíčem je řešení příslušné soustavy rovnic. Proces šifrování je transformaci zprávy s otevřeným textem na polynom, který je poté vyhodnocen pomocí polynomu veřejného klíče. Výsledná hodnota je šifrovaný text, který lze dešifrovat pomocí soukromého klíče. Jako příklad algoritmů na bázi multivariační kryptografie lze uvést například Rainbow Scheme.

- Kryptografie založena na kódování [9]: kryptosystémy, v nichž algoritmické primitivum (základní jednosměrná funkce) pracuje s kódem pro opravu chyb C. Toto primitivum spočívá v přidání chyby ke slovu C nebo ve výpočtu relativního syndromu k matici kontroly parity C.

  Jedním z nejznámějších kryptografických algoritmů založených na kódech je schéma McEliece. Soukromý klíč je náhodný binární neredukovaný Goppa kód a veřejným klíčem je náhodná generátorová matice z náhodně permutované verze tohoto kódu. Šifrovaný text je kódové slovo, do kterého byly přidány některé chyby, a pouze vlastník soukromého klíče (Goppa kódu) může tyto chyby odstranit. Není znám žádný útok, který by pro tento systém představoval vážnou hrozbu

- Kryptografie založená na supersingulárních eliptických křivkách [10]: s použitím supersingulárních křivek, jsou křivky generovány během výměny klíčů. Při této variantě metody jsou tajné klíče izogenické. Z toho vyplývá, že body jedné eliptické křivky mohou být mapovány na jinou křivku při zachovaní vrcholů křivek a samotné struktury křivky. To využivá skutečnost, že lze namapovat více bodů do jednoho bodu. Veřejným klíčem je pak samotná supersingulární eliptická křivka. Jako příklad algoritmů na bázi supersingulárních eliptických křivkách lze uvést například Diffie-Hellman key echange (SIDH), nebo Supersingular isogeny Key Encapsulation (SIKE).

Vývojový diagram

Viz **Příloha**.

Popis kódu

Viz Client.py a Storage.py

Popis spuštění a instalace

Viz README.md

Použité knihovny

Viz requirements.txt

Odkaz na GitHub práce

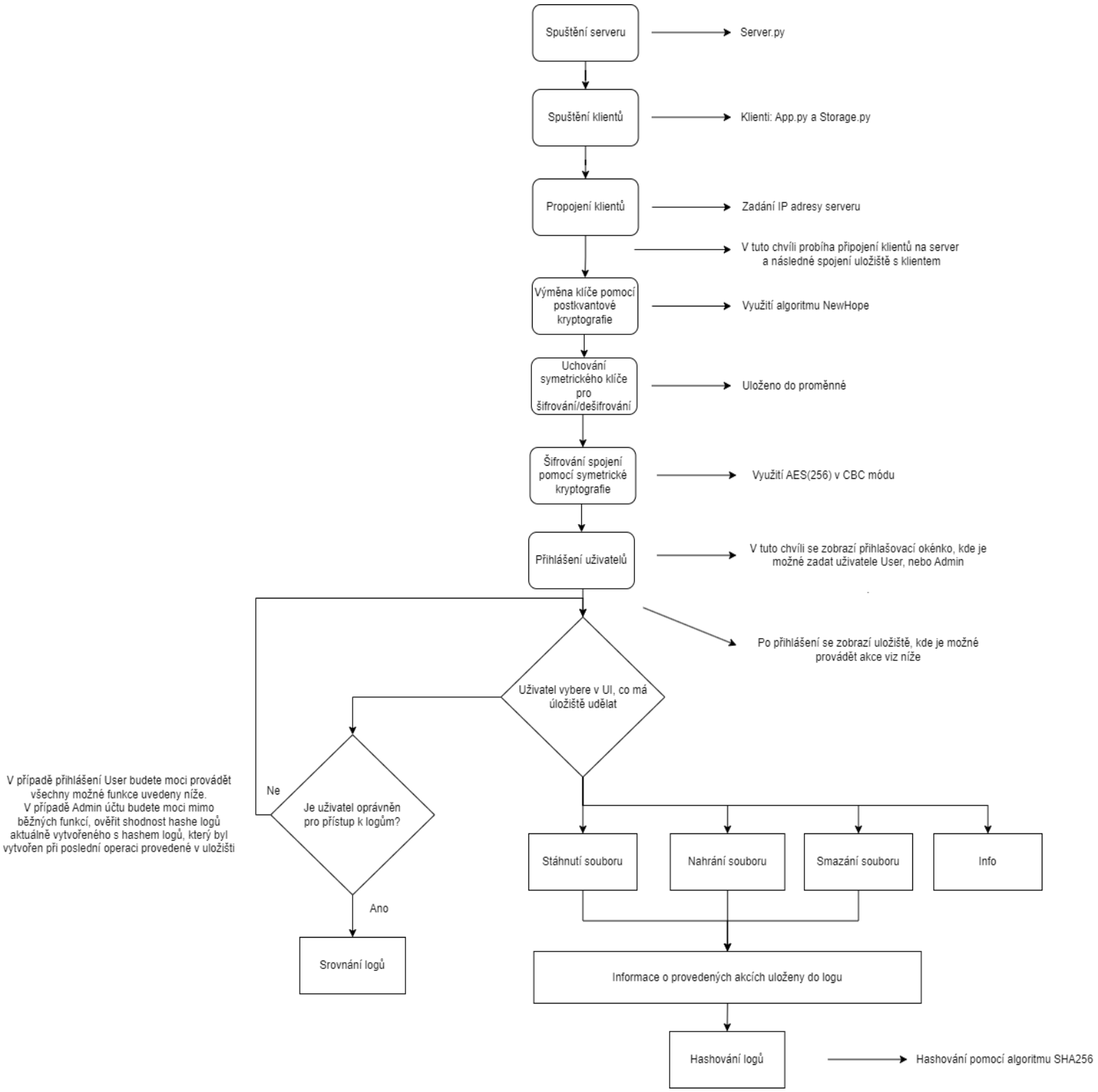
https://github.com/ChybaYg/Projekt-Krypto

Závěr

V průběhu projektu jsme vytvořili jednoduchou aplikaci pro komunikační účely v programovacím jazyce Python. Aplikace umožňuje navázat spojení šifrované symetrickým algoritmem AES-256, mezi uživateli na základě intuitivního uživatelského rozhraní. Klíč pro symetrické šifrování bylo ustanoveno pomocí postkvantového algoritmu známého jako NewHope. Uživatelské rozhraní také umožňuje uživateli přizpůsobit různé parametry relace. Aplikace zajišťuje základní funkce informačního systému, jako je nahrávání, mazání, stahování, či porovnávání záznamů, zda nebyly někým pozměněny. V rámci aplikace je zajištěna důvěrnost, integrita a autentičnost. Každá akce provedena na uložišti je zaznamenána a vložena do souboru, ke kterému má přístup pouze uživatel Admin.

Vzhledem k tomu, že je aplikace omezena na jeden semestr, je stále omezená, například, že soubory lze přenést pouze o maximální velikosti 65 kB a ve formátu *.txt. Tyto nedostatky mohou být podkladem pro další budoucí práci. Tato práce nám přinesla přehled o praktickém využití postkvantové kryptografie.

Příloha


Spuštění serveru
Server.py
Spuštění klientů
Klienti: App.py a Storage.py
Propojení klientů
Zadání IP adresy serveru
V tuto chvíli probíha připojení klientů na server a následné spojení uložiště s klientem
Výměna klíče pomocí postkvantové kryptografie
Využití algoritmu NewHope
Uchování symetrického klíče pro šifrování/dešifrování
Uloženo do proměnné
Šifrování spojení pomocí symetrické kryptografie
Využití AES(256) v CBC módu
Přihlášení uživatelů
V tuto chvíli se zobrazí přihlašovací okénko, kde je možné zadat uživatele User, nebo Admin
Po přihlášení se zobrazí uložiště, kde je možné provádět akce viz níže
Uživatel vybere v UI, co má úložiště udělat
Ne
Je uživatel oprávněn pro přístup k logům?
Ano
Srovnání logů
Stáhnutí souboru
Nahrání souboru
Smazání souboru
Info
Informace o provedených akcích uloženy do logu
Hashování logů
Hashování pomocí algoritmu SHA256
V případě přihlášení User budete moci provádět všechny možné funkce uvedeny níže.
V případě Admin účtu budete moci mimo běžných funkcí, ověřit shodnost hashe logů aktuálně vytvořeného s hashem logů, který byl vytvořen při poslední operaci provedené v uložišti

Literatura

[1] PINTO, Jose. *Post-Quantum Cryptography* [online]. 2022 [cit. 2023-03-26]. Dostupné z: https://www.researchgate.net/publication/367100840_Post-Quantum_Cryptography

[2] *Storage Security Professional's Guide to Skills and Knowledge* [online]. 2008 [cit. 2023-03-21]. Dostupné z: https://www.snia.org/sites/default/files/Storage-Sec-Prof-
a. Guidance.081015.Final_.pdf

[3] ROSENCRANCE, Linda. *Peer-to-peer (P2P)* [online]. 2022 [cit. 2023-03-22]. Dostupné z: https://www.techtarget.com/searchnetworking/definition/peer-to-peer

[4] SMIRNOFF, Peter a Dawn M. TURNER. *Symmetric Key Encryption - why, where and how it's used in banking* [online]. 2020 [cit. 2023-03-22]. Dostupné z: https://www.cryptomathic.com/news-events/blog/symmetric-key-encryption-why-where-and-how-its-used-in-banking

[5] *The Advanced Encryption Standard (AES)* [online]. [cit. 2023-03-24]. Dostupné z: http://www.facweb.iitkgp.ac.in/~sourav/AES.pdf

[6] *Post-quantum cryptography* [online]. [cit. 2023-03-22]. Dostupné z: https://en.wikipedia.org/wiki/Post-quantum_cryptography

[7] *What is Lattice-based Cryptography?* [online]. [cit. 2023-03-22]. Dostupné z: https://utimaco.com/products/technologies/post-quantum-cryptography/what-lattice-based-cryptography

[8] *Multivariate cryptography* [online]. [cit. 2023-03-22]. Dostupné z: https://utimaco.com/products/technologies/post-quantum-cryptography/what-lattice-based-cryptography

[9] Overbeck, R., Sendrier, N. (2009). *Code-based cryptography*. In: Bernstein, D.J., Buchmann, J., Dahmen, E. (eds) Post-Quantum Cryptography. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-88702-7_4

[10] MATULA, Lukáš. *POST-KVANTOVÁ KRYPTOGRAFIE NA OMEZENÝCH ZAŘÍZENÍCH*. BRNO, 2019. Dostupné také z: https://www.vut.cz/www_base/zav_prace_soubor_verejne.php?file_id=194065. Bakalářská práce. Vysoké učení technické.