Technická univerzita v Liberci

Ekonomická fakulta

Využití šifer v informační komunikační technologii

Usage of Cryptography in information communication technology

Cyril Steger

Vedoucí seminární práce:	Ing. David Kubát, Ph.D.
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Navazující studium prezenční

Liberec 2024

Obsah

1 Úvod

Tématem této seminární práce je použití šifer v oblasti informačních a komunikačních technologií (dále jen ICT). Kryptografie, jako vědní disciplína, hraje klíčovou roli při zajišťování bezpečnosti a ochrany dat nejen v digitálním světě, kde je bezpečný přenos informací nezbytný pro každodenní komunikaci a sdílení informací. Cílem této práci je seznámit čtenáře se základními pojmy používané v dnešní kryptografii a zvýšit tak povědomí o tom kde a jak je v dnešní oblasti ICT využívána.

V první části nás práce stručně seznámí s historií a základními pojmy používanými v oblasti kryptografie, které jsou důležité k pochopení pro následující kapitoly. Nejprve bude představena Shannonova teorie informace, která tvoří teoretický základ moderní kryptografie a komunikačních systémů. Tato teorie je zásadní pro pochopení principů šifrování a bezpečné výměny dat.

Další část práce je rozdělena do tří hlavních kapitol, z nichž každá se zaměřuje na jednu z kategorií šifer používaných v současné kryptografii. První kategorie jsou symetrické šifry, též známé jako šifry s tajným klíčem. Následující kapitola se věnuje asymetrickým šifrám, kde bude podrobně vysvětlena šifra RSA, která je jedním z nejpoužívanějších šifer s veřejným klíčem (Drake, 2024). Poslední kategorií jsou hybridní šifry, které kombinují výhody symetrických a asymetrických šifer a jsou využívány v mnoha moderních komunikačních protokolech.

Závěrem se práce bude věnovat oblasti postkvantové kryptografie, která se zabývá vývojem šifrovacích algoritmů odolných vůči kvantovým počítačům. V této části se seznámíme s aktuálními výzvami a vývojem v oblasti kryptografie, včetně Shorova algoritmu, který představuje hrozbu pro současné asymetrické šifry, zejména RSA.

2 Kryptografie

Kryptografie je vědní disciplína zaměřená na ochranu informací. Cílem kryptografie je zajistit, aby určité informace zůstaly skryté před neoprávněnými osobami. K tomu využívá různé metody a techniky, které zajišťují nejen důvěrnost dat, ale také jejich autentičnost. Kryptografie se dále zaměřuje na prevenci neautorizovaných změn v datech, zajišťuje, že odesílatel nemůže popřít svůj podpis nebo provedení akce, a chrání informace před jejich zneužitím. Využívá se tedy pro zajištění bezpečnosti a integrity informací nejen v digitálním světě (Tesař, 2021).

Kryptografie primárně vznikla k ochraně zpráv během jejich přenosu a tak až donedávna byly její doménou přenosové systémy. Později se ukázalo, že matematické metody lze použít nejen k utajování obsahu zpráv, ale rovněž k zajištění bezpečnosti mnoha dalších systémů. Mezi ně patří například systém řízení přístupu, elektronických plateb, síťových protokolů apod. S aplikacemi kryptografie proto přicházíme do styku každý den, avšak všeobecné povědomí o tom, jak fungují a na čem jsou založené, je nízké (Burda, 2019).

Jak již bylo uvedeno, v dnešním světě se kryptografie nejvíce soustředí na komunikaci mezi přenosovými kanály, ke kterému mají kromě autora zprávy a adresáta přístup i jiné (neoprávněné) osoby. Některé z těchto osob totiž usilují o čtení, resp. pozměňování přenášených zpráv a získat tak co nejvíce (citlivých) informací. Kryptografické techniky, které budou více rozebrány v této práci, umožňují autorovi a adresátovi zajistit ochranu přenášených zpráv před těmito hrozbami (Sedlák; Konečný, 2021).

2.1 Historie

V počátcích internetu se šifrování prakticky nevyužívalo, protože větší důraz byl kladen na ochranu citlivých informací tajných orgánů států. Síť tehdy používala otevřené pakety, které byly přenášeny pomocí protokolů, jež, i když byly postupně upravovány, jsou používány stále v současnosti. To znamenalo, že veškerá komunikace probíhala v otevřeném textu, což umožňovalo snadné odposlechy a manipulaci s daty (Erben, 2014).

Například protokol FTP „(“File Transfer Protocol), který byl navržen v roce 1985 v dokumentu RFC 959, neobsahoval žádnou podporu pro šifrování. Obsah zpráv, stejně jako řídicí informace - například uživatelské jméno a heslo sloužící k připojení - byly snadno dostupné pro třetí stranu. S postupným rozvojem internetu a dostupností široké veřejnosti se začaly objevovat i první vážné problémy s jeho bezpečností (Černá; Černý, 2012).

První vážné problémy s bezpečností v síti se objevily v roce 1989, kdy počítačový

červ WANK „(Worms Against Nuclear Killers)“ napadl systémy NASA. Po infikování systému zobrazoval při přihlášení politicky motivovanou zprávu, která kritizovala jaderný program a plánovaný start sondy Galileo. I když červ data nepoškozoval, jeho hlavním cílem bylo šíření anti-jaderného poselství a byl jedním z prvních virusů s tímto motivem vydírání (Erben, 2014).

Dalším případem je útok na americkou banku Citibank, na kterou se zaměřil ruský hacker Vladimir Levin. Celkem jednoduše získal přístup k účtům významných korporátních klientů a pokusil se převést přibližně 10,7 milionu dolarů na účty svých kompliců. Tento incident vyvolal mezinárodní pozornost, upozornil na zranitelnosti elektronického bankovnictví a vedl k posílení bezpečnostních opatření v bankovním sektoru (Erben, 2014).

Bylo jasné, že pokud má internet stát běžně používanou komunikační platformou, je nezbytné zaměřit se na zabezpečení přenosu informací, tedy na šifrování. Šifrování internetového provozu se dnes stalo standardem a jeho implementace se nejčastěji provádí prostřednictvím protokolu SSL/TLS nebo S/MIME pro bezpečnou elektronickou poštu (Pavlíček; Galba, 2012). Tyto síťové protokoly využívají asymetrickou kryptografii, což je podrobněji vysvětleno v kapitole Využití Asymetrických šifer.

I když jsou z matematického hlediska šifry prakticky neprolomitelné, největším současným problémem zůstává sociální (mezilidský) aspekt - otázka důvěry. V praxi to znamená, že si každá ze stran komunikace musí klást otázku: „Je protistrana opravdu tím, za koho se vydává?“ Ve fyzickém světě se můžeme orientovat pomocí svých smyslů, ale v digitálním světě to není možné, což vedlo k rozvoji nových metod a technologií pro ověření identity účastníků komunikace (Burda, 2019). Tato problematika je více rozebrána v kapitole Problém Distribuce klíčů.

3 Symetrické šifry

Šifra s tajným klíčem je taková šifra, u nichž pro dešifrování nějaké informace je povětšinou identický jako klíč pro zašifrování. Bezpečnost a integrita dat utě chto šifer je dána tím,že příslušný klíč je znám pouze oprávněným stranám (Tesař, 2021).

Jedním z nejznámějších systémů založených na symetrické kryptografii jsou šifry zpracovávající data po blocích. Standard AES „(Advanced Encryption Standard)“ není bloková šifra, jak je často ve veřejných publikacích zmiňováno. Tento standard totiž používá symetrickou blokovou šifru pod názvem Rijndael. Algoritmus provádí několik předem definovaných cyklů (rund), které zahrnují substituce, permutace a klíčem. Princip funkce těchto jednotlivých etap je složitý na popis a je v podstatě důležitý jen pro ty, kteří tento algoritmus implementují do svého systému (Standards; Technology, 2023).

V praxi se AES nejčastěji využívá k šifrování disků nebo zabezpečení síťové komunikace. Pro urychlení výpočtu tohoto algoritmu byly od roku 2010 zavedeny speciální instrukce do procesorů, například Intel ® AES-NI, které jsou dostupné nejen na procesorech od Intelu, ale také u procesorů AMD a dalších výrobců. Tyto instrukce jsou implementovány i v mobilních zařízeních, což umožňuje efektivnější šifrování a dešifrování dat, potřebnou pro nižší spotřebu energie Abdallah et al. (2020).

Hlavním problémem těchto systémů však stále zůstává: Jak můžeme bezpečně sdílet příslušný klíč, aniž by hrozilo jeho prozrazení třetí straně, a ověřit, že druhá strana je opravdu ta, za kterou se vydává

3.1 Problém distribuce klíčů

Distribuce klíčů je základní problémem při používání symetrických šifer, protože pro šifrování a dešifrování se používá stejný tajný klíč. Bezpečnost komunikace mezi odesílatelem a příjemcem závisí na uchování tajnosti tohoto klíče, jelikož pokud by neoprávněná strana získala onen klíč, mohla by snadno tuto komunikaci odposlouchávat.

Představme si situaci, kdy klient (například webový prohlížeč) se pokouší získat přístup k serveru a je třeba zabezpečit tento komunikační kanál. Data, která jsou mezi stranami sdílena, jsou většinou většího objemu a komunikace probíhá neustále, takže není efektivní používat asymetrickou kryptografii. K tomu, aby mohl klient a server bezpečně komunikovat, je třeba vyměnit tajný klíč tzv. secret key *Diffie-Hellman Key Exchange* (2024). Vzniká zde otázka: Jak bezpečně vyměnit tajný klíč přes nezabezpečený kanál, jako je transportní vrstva sítě? Jedním z efek-

tivních řešení je právě Diffie-Hellmanův protokol, jenž je využíván napříč mnoha kryptografickými protokoly.

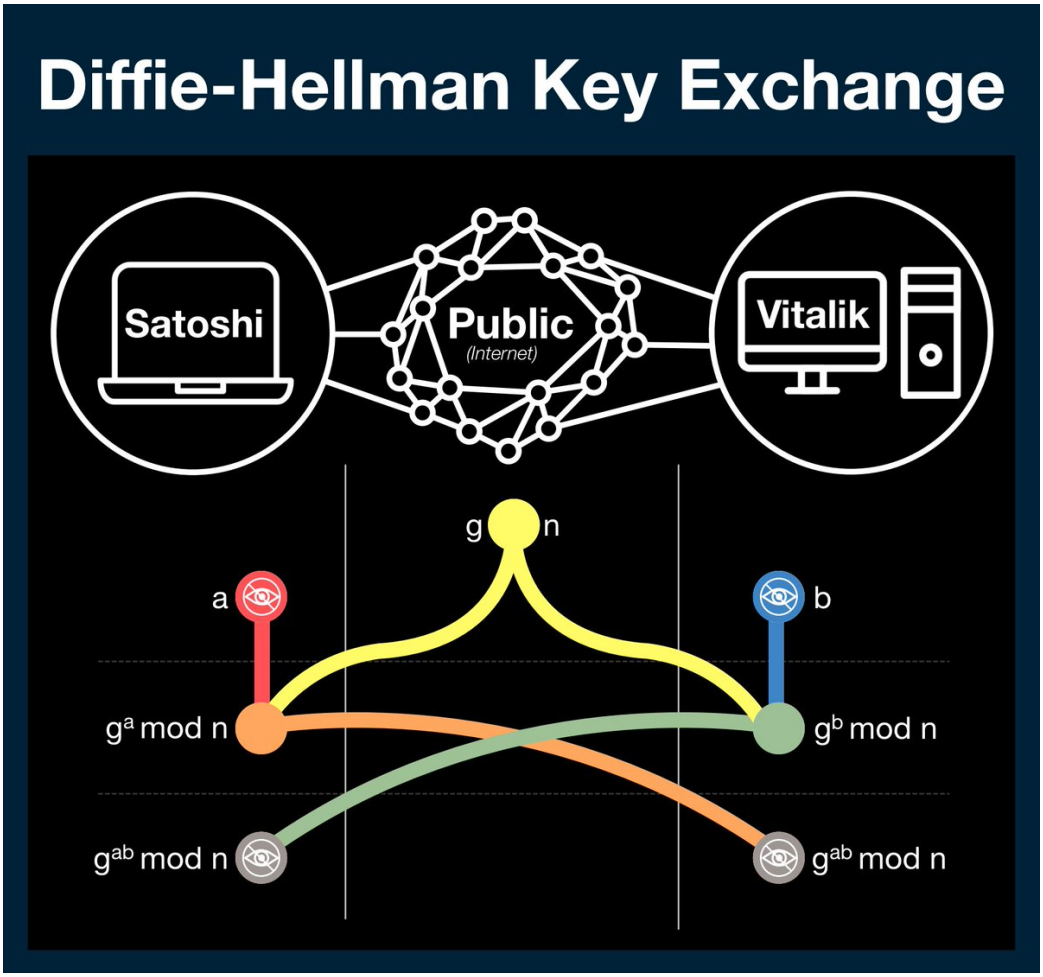
3.2 Diffie-Hellmanův protokol

Jak uvádí Diffie; Hellman (1976), princip tohoto protokolu spočívá ve vytvoření bezpečného klíče mezi dvěma stranami bez nutnosti předchozího sdílení tajných klíčů. Tento proces umožňuje stranám (např. klientovi a serveru) bezpečně vyměnit si šifrovací klíče přes veřejný kanál a zajistit tak důvěrnost při komunikaci.

Princip funkce výměny klíčů dle Diffie; Hellman (1976), by šel popsat následujícím způsobem:

1. **Volba veřejných parametrů:** Obě strany si zvolí dvě veřejné hodnoty, které jsou známé všem účastníkům komunikace. Tyto hodnoty jsou označeny jako g (základna) a n (modul). Parametry musí být vybrány tak, aby zaručovaly bezpečnost celého protokolu.
2. **Výběr tajných čísel:** Každá strana si poté náhodně vybere své vlastní tajné číslo. Konkrétně klient zvolí tajné číslo a a server tajné číslo b. Tato čísla zůstávají důvěrná a nejsou nikdy zveřejněna.
3. **Výpočet veřejných hodnot:** Na základě svých tajných čísel a veřejných parametrů obě strany spočítají své veřejné hodnoty. Klient vypočítá $A = g^a \mod n$ a server $B = g^b \mod n$. Tyto hodnoty jsou následně vyměněny mezi stranami.
4. **Vytvoření sdíleného klíče:** Po výměně veřejných hodnot každá strana využije své tajné číslo a přijatou veřejnou hodnotu k výpočtu sdíleného klíče. Klient vypočítá $s = B^a \mod n$ a server $s = A^b \mod n$. Díky vlastnostem modulární aritmetiky jsou obě vypočítané hodnoty shodné, čímž obě strany získají stejný sdílený tajný klíč.

I když jsou veřejné hodnoty A a B přenášeny přes nechráněný kanál, zpětné určení tajných čísel a a b je extrémně náročné. Tento problém, známý jako problém diskrétního logaritmu, má pro klasické počítače exponenciální složitost. To znamená, že výpočet je s rostoucí velikostí čísel extrémně časově náročný. Potenciální hrozbou mohou být jen kvantové počítače, které by mohly pomocí specifických algoritmů, jako je Shorův algoritmus popsaný více v kapitole Postkvantová kryptografie, snížit výpočetní složitost tohoto problému na polynomiální úroveň.



Obrázek 1: Schéma Diffie-Hellmanova protokolu. Zdroj: (Anon., 2021)

4 Asymetrické šifry

Asymetrickou šifrou se rozumí taková šifra, u které klíč pro dešifrování nelze výpočetně snadno získat z klíče pro zašifrování. Též se používá pojem šifra s veřejným klíčem jelikož jeden z vygenerovaných klíčů oprávněných stran, může být navíc veřejně dostupný (Tesař, 2021).

Asymetrickou šifrou lze také řešit problém ověření autora identity účastníků komunikace. Mohli bychom si představit situaci, kdy Alice chce poslat Bobovi šifrovanou zprávu a Bob si mohl být si jistý, že zpráva skutečně pochází od ní. Alice a Bob si vygenerují své páry soukromých a veřejných klíčů. Alice zašifruje zprávu svým soukromým klíčem (pro digitální podpis) a následně ji zašifruje Bobovým veřejným klíčem. Bob zprávu dešifruje svým soukromým klíčem a ověří autenticitu zprávy použitím veřejného klíče (Burda, 2019).

Tímto způsobem asymetrická kryptografie zajišťuje autenticitu odesílatele, integritu zprávy a důvěrnost komunikace. Typickým příkladem je právě šifra RSA.

4.1 Šifra RSA

RSA „(Rivest-Shamir-Adleman)“ je jednou z nejznámějších asymetrických šifer. Tento algoritmus, vyvinutý na základě myšlenky veřejného klíče, je inspirací inspirovanou prací Diffieho a Hellmana (Diffie; Hellman, 1976) a byl plně realizován v práci Rivest et al. (1978). RSA umožňuje nejen šifrování dat, ale také digitální podepisování, což zajišťuje autentizaci a integritu informací.

Dle Rivest et al. (1978) je základem RSA algoritmu následující postup:

1. **Generování klíčů:**
   - Vyberte dvě velká prvočísla p a q.
   - Vypočítejte modul $n = p \cdot q$, který slouží jako základ pro oba klíče.
   - Spočtěte Eulerovu funkci $\varphi(n) = (p-1)(q-1)$.
2. **Volba veřejného klíče:**
   - Zvolte celé číslo e tak, aby $1 < e < \varphi(n)$ a e bylo nesoudělné s $\varphi(n)$. Číslo e slouží jako veřejný exponent.
3. **Výpočet soukromého klíče:**
   - Určete číslo d, které je multiplikativní inverzí e modulo $\varphi(n)$, tedy splňuje rovnici:
   $$e \cdot d \equiv 1 \pmod{\varphi(n)}.$$

Číslo d je soukromým exponentem.

4. **Šifrování a dešifrování:**
   - Veřejný klíč je tvořen dvojicí (n, e) a soukromý klíč dvojicí (n, d).
   - Pro šifrování zprávy m (kde $m < n$) se vypočítá šifrovaná zpráva:

$$c = m^e \mod n.$$

   - Pro dešifrování se použije:

$$m = c^d \mod n.$$

Přestože veřejný klíč (n, e) je znám, bez znalosti velkých prvočísel p a q (délky alespoň 2048 bitů), je výpočetně velmi složité získat soukromý klíč (n, d). Tento bezpečnostní předpoklad vychází z faktu, že faktorizace čísla n na jeho prvočinitele je výpočetně velmi náročný úkol - tzv. NP-těžký problém, který má exponenciální složitost pro klasické výpočetní prostředky (Tesař, 2021).

Jedním z nejvýznamnějších využití tohoto kryptografického protokolu jsou digitální podpisy, které umožňují ověřovat jak autentifikaci, tak i integritu dat. V tomto procesu soukromý klíč slouží k podepsání zprávy, čímž garantuje její původ a nezaměnitelnost, zatímco veřejný klíč příjemci umožňuje ověřit, že zpráva pochází od oprávněného odesílatele a nebyla nijak pozměněna během přenosu třetí stranou.

V oblasti bezpečnosti internetových připojení nachází asymetrická kryptografie své praktické využití zejména v protokolech SSL a TLS, které slouží k vytváření bezpečného spojení mezi klientem a serverem. Během navazování spojení (tzv. handshake) asymetrické šifrování umožňuje autentifikaci serveru a bezpečnou výměnu symetrického klíče. Tento symetrický klíč je následně použít k šifrování přenášených dat již většího objemu (*Diffie-Hellman Key Exchange*, 2024). Pro výměnu příslušných klíčů je často využívána, díky její rychlosti, metoda Diffie--Hellman, jež byla popsána v předchozí kapitole.

Dalším významným využitím asymetrické kryptografie je v případě elektronické měny Bitcoin. V bitcoinu, používáme kryptografii pro vytvoření páru klíčů, které kontrolují přístup k bitcoinům. Tento pár klíčů se skládá ze soukromého klíče a z něho odvozeného jedinečného veřejného klíče. Veřejný klíč je použit pro příjem bitcoinů a soukromý klíč je použit pro podpis transakce, která tyto bitcoiny utrácí (Antonopoulos, 2014).

„Při utrácení bitcoinů, současný vlastník bitcoinů poskytuje jeho veřejný klíč a podpis (pokaždé různý, ale vytvořený ze stejného soukromého klíče) transakce, aby

mohl utratit tyto bitcoiny. Po poskytnutí veřejného klíče a podpisu, každý v bitcoinové síti může ověřit a přijmout transakci jako platnou, potvrdit, že osoba převádějící bitcoiny je vlastní v okamžiku převodu“ (Antonopoulos, 2014).

Asymetrická kryptografie hraje tedy významnou roli v vytváření klíčů a podepisování transakcí. Nutno podotknout že ze znalosti veřejného klíče, není výpočetně možné nalézt klíč privátní. Tento typ asymetrické kryptografie je založena na problému diskrétního logaritmu vyjádřeného sčítáním a násobením bodů na eliptické křivce (Antonopoulos, 2014).

Nevýhodou asymetrické kryptografie může být nižší rychlost šifrování oproti symetrickým šifrám, což ji činí nevhodnou pro přímé šifrování velkých bloků dat. Proto se asymetrická kryptografie často využívá v kombinaci se symetrickou, například při výměně klíčů v hybridních šifrovacích systémech.

Seznam literatury

ABDALLAH, Eslam G. et al., 2020. In: *Proceedings of the 2020 12th International Conference on Computer and Automation Engineering*. New York, NY, USA: ACM, s. 167–172. Dostupné z DOI: 10.1145/3384613.3384648. [citováno 2024-11-20].

ANON., 2021. *Diffie-Hellman Key Exchange*. Dostupné také z: https://inevitableeth.com/home/concepts/diffie-hellman. [citováno 2024-11-20].

ANTONOPOULOS, Andreas M., 2014. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. 1st. O'Reilly Media, Inc. ISBN 9781491902646.

BURDA, Karel, 2019. *Kryptografie okolo nás*. CZ.NIC. ISBN 9788088168508.

ČERNÁ, Zuzana; ČERNÝ, Michal, 2012. *Historie Internetu*. Dostupné také z: https://clanky.rvp.cz/clanek/k/g/14791/HISTORIE-INTERNETU.html. [citováno 2024-11-20].

DIFFIE, W.; HELLMAN, M., 1976. New directions in cryptography. *IEEE Transactions on Information Theory*. Roč. 22, č. 6, s. 644–654. Dostupné z DOI: 10.1109/tit.1976.1055638. [citováno 2024-11-20].

Diffie-Hellman Key Exchange, 2024. Wiki.js. Dostupné také z: https://inevitableeth.com/home/concepts/diffie-hellman. [citováno 2024-11-20].

DRAKE, Nate, 2024. *RSA encryption explained. What is it and why is it important?* hide.me. Dostupné také z: https://hide.me/en/blog/rsa-encryption-explained/. [Citováno 2024-11-24].

ERBEN, Lukáš, 2014. *Příchod hackerů: Vladimír Leonidovič Levin*. Internet Info, s.r.o. Dostupné také z: https://www.root.cz/clanky/prichod-hackeru-vladimir-leonidovic-levin/. [citováno 2024-11-20].

PAVLÍČEK, Antonín; GALBA, Alexander, 2012. *Moderní informatika*. Praha: Professional Pub. ISBN 978-80-7431-109-3.

RIVEST, R. L. et al., 1978. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*. Roč. 21, č. 2, s. 120–126. Dostupné z DOI: 10.1145/359340.359342. [citováno 2024-11-20].

SEDLÁK, Petr; KONEČNÝ, Martin, 2021. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. 1. vyd. CERM, akademické nakladatelství. ISBN 978-80-7623-068-2.

STANDARDS, National Institute of; TECHNOLOGY, 2023. *Advanced Encryption Standard (AES)*. Tech. zpr. NIST. Dostupné z DOI: 10.6028/nist.fips.197-upd1. [citováno 2024-11-20].

TESAŘ, Petr, 2021. *Bezpečnost informací - Historie a matematické základy kryptologie* [Internal document]. [Neveřejné PDF].

Seznam obrázků