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 **2**

Seznam literatury **3**

Seznam obrázků **4**

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.

Seznam literatury

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].

Seznam obrázků