Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Teze bakalářské práce

Porovnání kryptografických metod

Filipp Podriadchikov

Porovnání kryptografických metod

Souhrn

Bakalářská práce se podrobněji věnuje kryptografii, konkrétné se zabývá popisem metody ochrany dat. Nejčastěji používané metody kryptografie jsou následně podrobněji popsány. V této částí také najdeme shrnutí všech jejich výhod a nevýhod. Po podrobnější analýze jednotlivých metod, následuje výběr nejvhodnější metody pomocí párového porovnání. Na závěr jsou shrnuty, výsledky porovnání a předložena nejvhodnější metoda pro bezpečnost šifrovaných souborů.

Klíčová slova: symetrická kryptografie, asymetrická kryptografie, algoritmy šifrování, šifrování dat.

Cíl práce

Hlavním cílem práce je porovnat dostupné kryptografické metody pro oblast ochrany souborů doporučit vhodnou metodu, nebo skupinu metod v závislosti na jejich výkonnostích charakteristikách. Vedlejším cílem práce je vytvořit přehled aktuálně používaných kryptografických metod.

Metodika

Při studiu odborných pramenů bude využita metoda analýzy a syntézy. Pro výběr vhodné metody bude použita metoda párového porovnání. Měření výkonnosti bude realizováno testováním šifrovací funkce, rychlosti šifrování, délky klíče, rycholsti generování klíčů, a typy klíčů. Na základě zjištěných dat budou konkretizována doporučení pro výběr kryptografické metody vhodné pro ochranu souborů.

Teoretická část

V první části jsou analyzovány nejčastěji používané kryptografické metody z oblasti symetrické a asymetrické kryptografie.

Druhá část zaměřena na porovnání kryptografických metod.

Praktická část

Praktická část je zaměřena na porovnání kryptografických metod při pomoci programu Veracrypt.

Závěr

Prezentované výsledky porovnání ukázaly, že na základě výše uvedených testů, AES má lepší výkonnost než ostatní běžně používané šifrovací algoritmy. Vzhledem k tomu, že AES dosud nemá žádné známé bezpečnostní chyby, stává se vynikajícím kandidátem při zvážení pozice jako standardní šifrovací algoritmus. Algoritmus Kuznyechik vykázal nevyhovující výsledky ve srovnání s ostatními algoritmy, proto se stáva nejméně vhodným algoritmem. Toto tvrzení je podloženo nejhoršími výsledky v daných testech, které dokázali že kuznyechik vyžaduje nejvyšší výpočetní výkon.

Na základě výše uvedených testů jsem vyvodil závěr, že existuje přímý vztah mezi počtem kombinací algoritmů a výkoností vašeho procesoru. Tím pádem, pokud by jsté se chtěli vyhnout přetížení vašeho procesu, musíte zvolit nejjednodušší algoritmus.

Na základě těchto faktů, bych vám doporučil zvážit silný procesor, v případč že plánujete šifrovat velké soubory.

Seznam použitých zdrojů

(1) PARTYKA, Tatiana A., POPOV, Igor I. Information security. Publishing Infa-M, c2005. ISBN: 5-8199-0060-X.

(2) BRUEN, Aiden A., Mario FORCINITO. Cryptography, information theory. Hoboken, N.J.: Wiley-Interscience, c2005. ISBN 04-716-5317-9.

(3) TARASYUK, M.V. Secure information technology. Publishing "Solon-Press", c2004. ISBN 5-98003-143-X.