Univerzita Pardubice
Fakulta elektrotechniky a informatiky

POSUDEK VEDOUCÍHO BAKALÁŘSKÉ PRÁCE

Jméno studenta: **Patricie Mecová**

Název práce: Porovnání postkvantových šifrovacích algoritmů s klasickými šifrovacími algoritmy

Autor posudku: Ing. Martin Pozdílek, Ph.D.

Cíl práce: Cílem této bakalářské práce je porovnání postkvantových šifrovacích algoritmů s šifrovacími algoritmy, které se dnes běžně používají. V teoretické části práce budou popsány bezpečnostní problémy současných šifrovacích algoritmů. Dále zde budou představeny nové postkvantové algoritmy podle standardu NIST. V praktické části práce bude porovnány výkonové parametry současných a postkvantových algoritmů.

Povinná kritéria hodnocení práce	**Stupeň hodnocení** (známka)					
	A	**B**	**C**	**D**	**E**	**F**
Práce svým zaměřením odpovídá studovanému oboru	☒	☐	☐	☐	☐	☐
Vymezení cíle a jeho naplnění	☐	☐	☒	☐	☐	☐
Zpracování teoretických aspektů tématu	☐	☐	☐	☒	☐	☐
Zpracování praktických aspektů tématu	☒	☐	☐	☐	☐	☐
Adekvátnost použitých metod, způsob jejich použití	☒	☐	☐	☐	☐	☐
Hloubka a správnost provedené analýzy	☒	☐	☐	☐	☐	☐
Práce s literaturou	☐	☒	☐	☐	☐	☐
Logická stavba a členění práce	☐	☒	☐	☐	☐	☐
Jazyková a terminologická úroveň	☐	☐	☒	☐	☐	☐
Formální úprava a náležitosti práce	☐	☐	☐	☒	☐	☐
Vlastní přínos studenta	☐	☒	☐	☐	☐	☐
Využitelnost výsledků práce v teorii (v praxi)	☒	☐	☐	☐	☐	☐

Celkové posouzení práce a zdůvodnění výsledné známky:

Cílem bakalářské práce bylo porovnat současné a postkvantové šifrovací algoritmy.

V teoretické části jsou popsány dnes běžně používané symetrické a asymetrické šifry, je představen kvantový počítač a jeho schopnost prolomit tyto šifrovací algoritmy. Dále je jsou popsány různé postkvantové algoritmy pro výměnu klíčů a podepisování dokumentů.

Teoretická část je zpracována správně, ale místy se vyskytují nepřesnosti nebo je použito vyjádření, které může být zavádějící. Například druhá věta v kapitole Režimy provozu (str 13.) lze vykládat různými způsoby, na str. 14 bych NIST nazval organizací nebo laboratoří a nikoliv společností. U proudových šifer se na základě klíče generuje proudový klíč (str. 14). Na str. 17 je ve stejné větě uvedena hashovací funkce SHA-256 a SHA-3. SHA-256 spadá do rodiny hashovacích funkcí SHA-2 a SHA-3 je zcela jiný typ hashovací funkce. Na str. 19 v kapitole 2.2.2 poslední věta v prvním odstavci nedává smysl.

Občas se vyskytují překlepy a chybná interpunkce. Str. 20 podobná RSA, str. 21 implementace má, na str. 38 jsou za větou dvě tečky.

V teoretické části by bylo dobré stručně popsat šifrovací algoritmy, které byly otestovány v praktické části práce. Například chybí algoritmus ECDSA. Zároveň mi chybí krátké shrnutí, které současné šifry jsou ohroženy kvantovými počítači a do jaké míry.

V některých kapitolách 2.1, 3. je odlišné formátování odstavce od ostatních částí práce. Všechny obrázky v kapitole 3.3 mají chybné popisky. Tabulku na straně 28. by bylo dobré pro přehlednost začít na nové stránce.

Praktická část práce je provedena v pořádku, ale opět by bylo vhodné použité algoritmy nebo jejich části lépe popsat. Například křivka P-256 str. 25, X22519 na str. 37, případně popsat, že asymetrické šifry byly použity pro výměnu klíčů.

Protože v nedávné době došlo ke standardizaci postkvantových šifer, je téma bakalářské práce velmi aktuální. Experimentální část byla provedena v pořádku, ale celkově lze říci, že by bylo vhodné zlepšit formální stránku práce a její výsledky přehledněji shrnout v závěru.

Celkově práce splňuje požadavky kladené na bakalářskou práci.

Vyhodnocení kontroly textu práce pomocí systému pro odhalování plagiátu:

Kontrola původnosti práce byla shledána s výsledkem, že práce není plagiát.

Otázky k obhajobě:

Měla jste nějaké potíže s implementací postkvantových šifer?

Práci doporučuji k obhajobě.

Navržená výsledná známka: D

V Pardubicích**, dne 21. května 2025**

podpis