

1 HODNOCENÍ OPONENTA

NAVRŽENÁ ZNÁMKA:

C (70)

Předložená práce „Implementace Kryptografických Primitiv“ je po formální stránce zpracována dobře, obsahuje pouze drobné překlepy a nedostatky (například str. 32, kde text vybočuje z bloku). Velice kladně hodnotím práci s aktuální, kvalitní a odbornou literaturou. K odborné části mám jen drobné výtky, například v úvodu, kdy autorka mluví o algoritmu DES, který bych nepovažoval již za moderní algoritmus, dále pak k výsledkům, kdy není popsáno, zda daná knihovna se skutečně soustředí na optimalizaci pro rychlost (jsou i například paměťově optimalizované knihovny, u kterých má větší význam měření velikosti užité paměti atd.), dále by bylo dobré porovnat výsledky i s dalšími implementacemi (dostupnými). Drobnou výtku mám také k nejednoznačnému rozlišení co je autorčin skutečný přínos a co je tedy ještě převzatá práce.

Práci jako celek hodnotím jako dobrou a tedy známkou C.

Na autorku mám ještě následující otázky:

1. Specifikujte prosím Váš skutečný přínos a rozlište převzatou práci a Vaši práci.
2. Je vámi použitá knihovna optimalizována? Pokud ano, je tedy optimalizována na rychlost?

