Univerzita Pardubice
Fakulta elektrotechniky a informatiky

# POSUDEK VEDOUCÍHO BAKALÁŘSKÉ PRÁCE

Jméno studenta: **Martin Bárta**

Název práce: **Vizualizace šifrování AES v JavěFX**

Autor posudku: Ing. Zdeněk Šilar, Ph.D.

Cíl práce: Cílem práce bylo v jazyce JavaFX vytvořit program pro vizualizaci klíčových kroků šifry AES z důvodu její názorné demonstrace.

| **Povinná kritéria hodnocení práce** | **Stupeň hodnocení** (známka) | | | |
|---|---|---|---|---|
| | **1** | **2** | **3** | **4** |
| Práce svým zaměřením odpovídá studovanému oboru | **x** | | | |
| Naplnění cíle zadání práce | **x** | | | |
| Zpracování teoretických aspektů tématu | | **x** | | |
| Zpracování praktických aspektů tématu | **x** | | | |
| Adekvátnost použitých metod, způsob jejich použití | **x** | | | |
| Práce s literaturou | | **x** | | |
| Logická stavba a členění práce | **x** | | | |
| Jazyková a terminologická úroveň | **x** | | | |
| Formální úprava a náležitosti práce | **x** | | | |
| Vlastní přínos studenta | **x** | | | |
| Využitelnost výsledků práce v teorii (v praxi) | **x** | | | |

**Dílčí připomínky a náměty a hodnocení práce:**

V úvodu práce jsou uvedeny základní pojmy z oboru kryptografie s důrazem na symetrické a asymetrické šifrování a vysvětlen pojem kryptosystém. Ve třetí kapitole je podrobněji popsán princip symetrické blokové šifry a příklad kryptosystému DES. Ve čtvrté kapitole autor porovnává již nepoužívanou šifru DES se současně používaným šifrováním AES a matematicky popisuje její klíčové operace včetně zabezpečení. Pátá kapitola obsahuje popis tvorby grafického programu pro vizuální demonstraci klíčových kroků při (de)šifrování pomocí systému AES a to včetně popisu důležitých tříd, ukázek fragmentů kódu a popisu uživatelského rozhraní.

V práci se autor dopustil několika drobných chyb a překlepů.

Oceňuji kladný přístup autora k relativně obtížné tématice.

Univerzita
Pardubice
Fakulta elektrotechniky
a informatiky

**Otázky k obhajobě:**

1. Proč se při šifrování často používá operace XOR?

2. Jak vypadá útok typu „brute-force“ a jaké znáte další typy útoků?

**Práci doporučuji k obhajobě.**

**Navržená výsledná známka: výborně**

**V** Pardubicích**, dne 22. května 2017**

**podpis**