Implementace symetrické blokové šifry AES

KIV/BIT - Standardní zadání semestrální práce pro ak. rok 2019/20

Ve zvoleném programovacím jazyce implementujte symetrickou blokovou šifru AES. Při řešení budou splněny následující podmínky:

- Výsledek bude v hexadecimálním formátu.
- Použijte šifrovací mód ECB (Electronic Codebook), tzn. šifrovací algoritmus aplikujte přímo na bloky vstupních dat. Inicializační vektor není potřeba. Bude-li to nutné poslední blok zarovnejte zprava pomocí nul.
- Velikost (délka) klíče, resp. bloku bude 128 bitů, tzn. očekáván je klíč délky 16 Bytů. Klíč si může zvolit uživatel.
- Otestujte na souborech **Shea.jpg** a **message.txt** (oba dostupné z: http://home.zcu.cz/~jimar/BIT/), a jako klíč použijte: **josefvencasladek**

Poznámka: Pro kontrolu můžete využít např. nástroj:
http://aes.online-domain-tools.com/