Zadanie 2

Použité nástroje

- Python
- Knižnica cryptodome

Inštalácia

- Nie je potrebná žiadna inštalácia aplikácie

Použitie

- Aplikácia sa spúšťa z prikazového riadka (CMD, Poweshell … atd). A používa naslednovné prepínače
- -e/-d
    - -e encrypt
    - -d decrypt
- -f <cesta k súboru>
    - Cesta k vstupnému súboru, v prípade použitia -e je to súbor ktorých chceme zašifrovať. V opačnom prípade je to súbor ktorý chceme rozšifrovať.
- -k <cesta k súboru s kľúčom>
    - Tento prepínač je potrebné len pri rozšifrovaní súboru (-d). Je to cesta ku súboru s kľúčom ktorý bol vygenerovaný aplikáciou pri zašifrovaní súboru.

Príklad použitia

- Zašifrovanie súboru test.txt
    - .\main.exe -e -f .\test.txt
- Rozšifrovanie súboru
    - .\main.exe -d -f .\test.txt.encrypted -k .\test.txt.key

1 GB súbor

- Zašifrovanie súboru veľkosti 1GB trvá približne 7 sekúnd.

Formát zašifrovaného súboru

- Prvých 16 bytov tvorí takzvaný nonce
- Druhých 16 bytov je tag
- Zbytok je zašifrovaný obsah pôvodného súboru

Šifrovanie

- Použitá symetrická šifra AES v móde EAX
- Použitý 128 bitový kľúč