Zadanie 3

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. Na zašifrovanie sa v adresári musí nachádzať súbor s verejným kľúčom s názvom public.pem. Na rozšifrovanie privátny kľúč s názvom private.pem. Tieto subory dokáže vygenerovať aplikácia pomocou prepínača -g;
- -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.
- -g
    - Vygeneruje dvojicu: privatny/verejný kľúč.

Príklad použitia

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

Formát zašifrovaného súboru

- Prvých n (podľa dĺžky RSA private kľúča) bytov tvorí zašifrovaný kľúč symetrickej šifry
- Prvých 16 bytov tvorí nonce
- Druhých 16 bytov je tag
- Zbytok je zašifrovaný obsah pôvodného súboru

Šifrovanie

- Použitá symetrická šifra AES v móde EAX
- Použitý 128 bitový kľúč
- RSA: PKCS1 OAEP