Šifrovanie

Na implementáciu aplikácie bol použitý programovací jazyk Python ktorého knižnica Crypto bola použitá na encryptovanie a decryptovanie súborov.

**B. SCHEMATICKY, AKÝ JE FORMÁT ZAŠIFROVANÉHO SÚBORU**

Šifrovanie 1,03GB súboru prebehlo za 9 sekúnd

Nakoľko bol použitý programovací jazyk Python aplikáciu netreba kompilovať. Je len potrebné mať nainštalovaný 64 bitovú verziu Pythonu a stiahnutú knižnicu Crypto

Aplikácia sa spúšťa troma spôsobmi pomocou príkazového riedku

1. python cesta\k\aplikácii\main.py G pre vygenerovanie privátneho a verejného kľúča
2. python cesta\k\aplikácii\main.py E názov\_súboru keys\názov\_verejného\_kľúča pre šifrovanie
   1. súbor ktorý má byť šifrovaný sa musí nachádzať v priečinku cesta\k\aplikácii\in
   2. verejný klúč sa musí nachádzať v priečinku cesta\k\aplikácii\keys
   3. šifrovaný súbor sa uloží do priečinku cesta\k\aplikácii\enc
3. python cesta\k\aplikácii\main.py D názov\_súboru pre dešifrovanie súboru
   1. súbor, ktorý má byť dešifrovaný sa musí nachádzať v priečinku cesta\k\aplikácii\enc
   2. dešifrovaný súbor šifrovaný súbor sa uloží do priečinku cesta\k\aplikácii\dec

Prvý krát je nutné spustiť aplikáciu spôsobom č. 1 pre vygenerovanie kľúčov. Potrebné priečinky vytvorí aplikácia automaticky

Pre zvýšenie bezpečnosti je potrebné aby používateľ nezdieľal svoj privátny kľúč s verejnosťou. Zamedzí sa tým neoprávnené čítanie šifrovaných súborov.

**G. STRUČNÝ POPIS VÁŠHO POSTUPU ŠIFROVANIA A DÔVODY VÝBERU DANEJ ŠIFROVACEJ FUNKCIE A VEĽKOSTI KĽÚČA Z HĽADISKA RÝCHLOSTI A BEZPEČNOSTI**