

# UPB – Zadanie 3

APLIKÁCIA NA ŠIFROVANIE A DEŠIFROVANIE S VYUŽITÍM RSA A KONTROLY INTEGRITY

Jazyk : **Python 3.9.7**

Knižnica : **Pycryptodome** (na inštaláciu do konzoly napíš „pip install pycryptodome“)

Šifra : **AES 128 bit** ([zdroj](#))

Mód : **GCM** ([zdroj](#))

Encrypted súbor : **JSON**

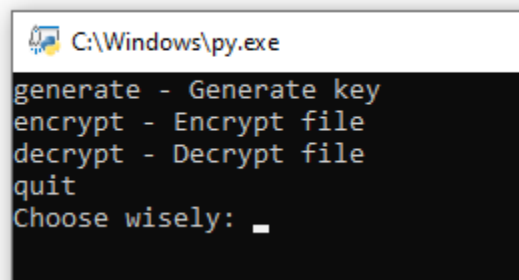
Decrypted súbor : **BIN**

## Inštalácia

Priečinkok extrahujte a súbor main.py otvorte v rovnakom priečinku ako je súbor, ktorý chcete zašifrovať.

## Návod

Po spustení main.py sa otvorí konzola, ktorá vypíše funkcie a čaká na váš vstup.



```
C:\Windows\py.exe
generate - Generate key
encrypt - Encrypt file
decrypt - Decrypt file
quit
Choose wisely: _
```

Do konzoly vypíš možnosť. Ak chceš jednoducho otestovať na súbore, zbežni ich postupne zhora. Teda „generate“, „encrypt“ a „decrypt“.

**generate** - vygeneruje privátny a verejný kľúč do súborov, slúžiace na šifrovanie a následne aj dešifrovanie (*private.pem* resp. *public.pem*)

**encrypt** - po zadaní názvu súboru sa vytvorí *encrypted.json* súbor, ktorý v hlavičke obsahuje zašifrovaný kľúč a dáta

**decrypt** - dešifruje *encrypted.json* do súboru *decrypted.bin*

**quit** - ukončí program

## Popis

Pre začatím šifrovanie si vytvoríme pár kľúčov (RSA, privátny a verejný). Pomocou spustenej „gen“ funkcie po zašifrovaní súbor už s rozdielnym kľúčom dešifrovať nepôjde, teda sa jedná o kontrolu integrity. Šifru AES využíva napríklad americká vláda a patrí k najpoužívanejším a najbezpečnejším šifrám, v tomto prípade sa jedná o 128 bitovú dĺžku kľúča, čo je dostatočné na zabránenie útoku. V preklade to znamená že najrýchlejší PC (z roku 2019, výkon 93.02 petaflopov) by potreboval 885 kvadriliónov rokov na prelomenie šifry „brutálnou silou“ pri použití 128 bitovej AES. [\(zdroj\)](#)

Program neobsahuje žiadne overenia inputov, preto vkladajte správne vstupy.