# Generátor velkých prvočísel

### Katarína Kúdelová Dávid Gregora Andrej Pecník

### Skupina 10

### BPC-IBE

Obrázok, na ktorom je snímka obrazovky, čierno-biela, vzor, čierny

Automaticky generovaný popis

**Popis spustenia a fungovania programu**

Po spustení programu sa vypíše 5 možností.

1. **Výpis všetkých prvočísiel po zadané číslo.** Po vybraní tejto možnosti, sa zobrazia ďalšie dve možnosti. A to či chceme číslo zadať **ručne**, alebo ho chceme **naimportovať** zo súboru. Ak si nevyberieme ani jednu z týchto možností, vypíše sa na obrazovku „Nesprávny výber“.   
   Pri výbere možnosti „ručne“ nás program vyzve na zadanie hodnoty čísla, po ktoré chceme, aby program vypísal prvočísla. Pri výbere možnosti „import“ program sám vypíše zadané prvočíslo. Program vypíše všetky prvočísla do konzoly, a taktiež aj do samostatného súboru. Následne sa do log-u vypíše, „Eratosthenovým sitom vypísané prvočísla po číslo: “, kde je doplnené číslo, ktoré sme zadali/ktoré program importoval a „Doba trvania: “, kde je vypísaná doba, za ktorú program vypísal prvočísla, zaokrúhlená na 7 desatinných miest. Log sa pred týmto vypísaním odšifruje a po vypísaní sa naspäť zašifruje.
2. **Test prvočíselnosti zadaného čísla.** Znovu sa nás program opýta, či chceme číslo zadať ručne alebo importovať zo súboru. Ak si vyberieme ručne, program nás vyzve k zadaniu čísla na otestovanie a zadaniu počtu iterácií. Pri výbere „import” nás program vyzve, aby sme zadali počet iterácii a číslo naimportuje zo súboru. Po zadaní program vypíše do konzoly „Zadané prvočíslo je: “ s naším prvočíslom, ktoré sme dali otestovať. Následne program otestuje zadané číslo za pomoci troch testov: Solovay-Strassenovho, Miller-Rabinovho testu a Eratosthenovho sita. Do logu sa vypíšu všetky tri tieto testy so zadaných číslom, či ide o prvočíslo, dobou testovania a počtom bitov. Do konzoly sa na základe týchto testov vypíše len či ide o prvočíslo, alebo nie. (Pri Eratosthenovom site je nastavený limit na 30 sekúnd, ak trvá test dlhšie, tak program vypíše, že je odpoveď irelevantná.) Log sa znova pred vypísaním odšifruje a po vypísaní opäť zašifruje.
3. **Generovanie veľkého prvočísla na základe zadanej bitovej dĺžky.** Program nás vyzve, aby sme zadali koľko bitové číslo má vygenerovať. Následne vygeneruje toľko bitové číslo za pomoci Miller-Rabinovho, Lucas-Selfridgeovho a Solovay-Strassenovho testu. Čísla vygenerované týmito testami sa uložia do zvlášť súborov a taktiež do logu s dobou trvania a počtom bitov. Log sa znova odšifruje a naspäť zašifruje.
4. **Prezeranie logu.** Pri výbere tejto možnosti nás program vyzve, aby sme zadali heslo na odšifrovanie logu. (heslo je tajneheslo) Následne sa log odšifruje, ukáže obsah a po stlačení ľubovoľného tlačidla sa znova zašifruje. Pri zadaní nesprávneho hesla, sa vypíše „Nesprávne heslo!“
5. **Ukončenie programu.**

Knižnice:

* random – verzia 3.10 (generovanie náhodných čísel)
* os – verzia 3.7 (manipuláciu so súbormi)
* math – verzia 3.10. (matematické operácie)
* timeit – verzia 3.7 (meranie času)
* logging – verzia 3.10 (vytvorenie a fungovanie logu)
* time – verzia 3.7 (manipulovanie s dátumami a časom)
* cryptography fernet – verzia 42.0.5 (zašifrovanie súborov)
* base64 -verzia 1.3.2 (preklad binárnej sústavy do ASCII znakov)
* msvcrt – verzia 3.10. (operácie so súbormi a konzolou)

