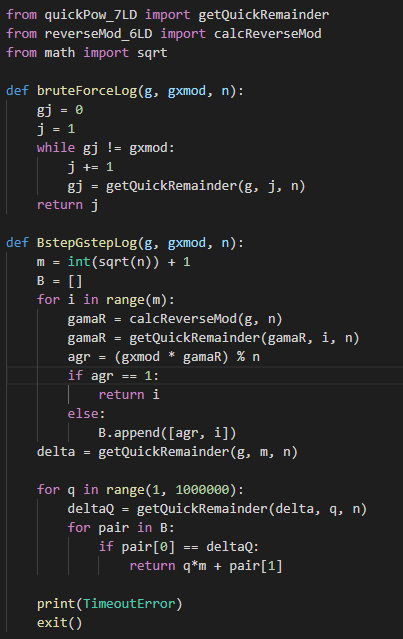
**Difi-Helman nulaužimo (bendrojo slaptojo rakto gavimo) algoritmas**

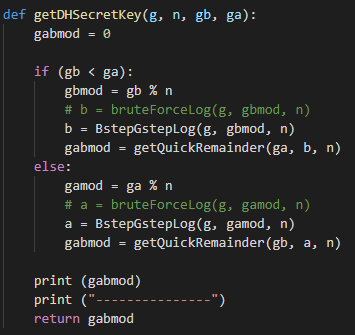
Kodas:

Diskretaus logaritmo radimas:



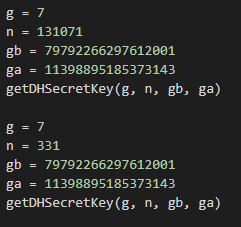
Parašiau kruopštaus parinkimo algoritmą, nes jo pilnai užtenka, kad atlikti duotą užduotį, bet taip pat realizavau ir „Baby-step Giant-step“ algoritmą, nes be jo šis laboratorinis atrodė per daug paprastas.

Nulaužimo algoritmas:



Patikrina kuris tarp gavėjo ir siutėjo skaičų mažesnis ir randa jo logaritmą, atkomentavus atitinkamas eilutes galima naudoti brute force arba baby-step giant-step algoritmą. Tada greitojo kėlima laipsnio algorimu randamas ir išvedamas (gb)a arba (ga)b priklausomai nuo to kurio skaičiaus logaritmo buvo ieškoma.

Išvedimas:



Pirmame variante naudojami jūsų duoti užduoties skaičiai, o antrame variante panaudojau tokius pačius g, GS ir SS kaip pirmame, bet pakeičiau n kad jis turėtų panaudoti giant-step, o ne tik baby-step ir patikrinau ar gaunamas geras atsakymas su brute force algoritmu.

Rezultatai:

