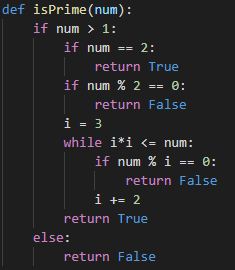
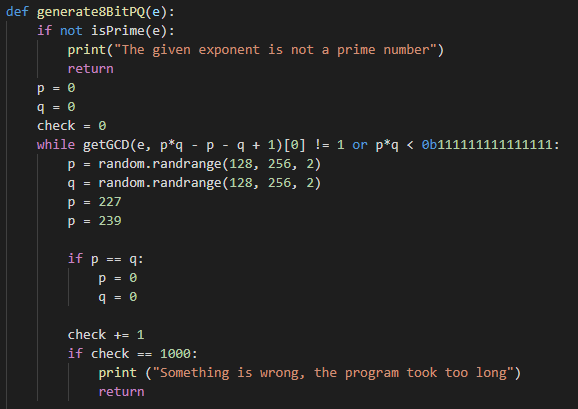
Kodas reikalingomis dalimis:

Patikrinimas ar skaičius yra pirminis:



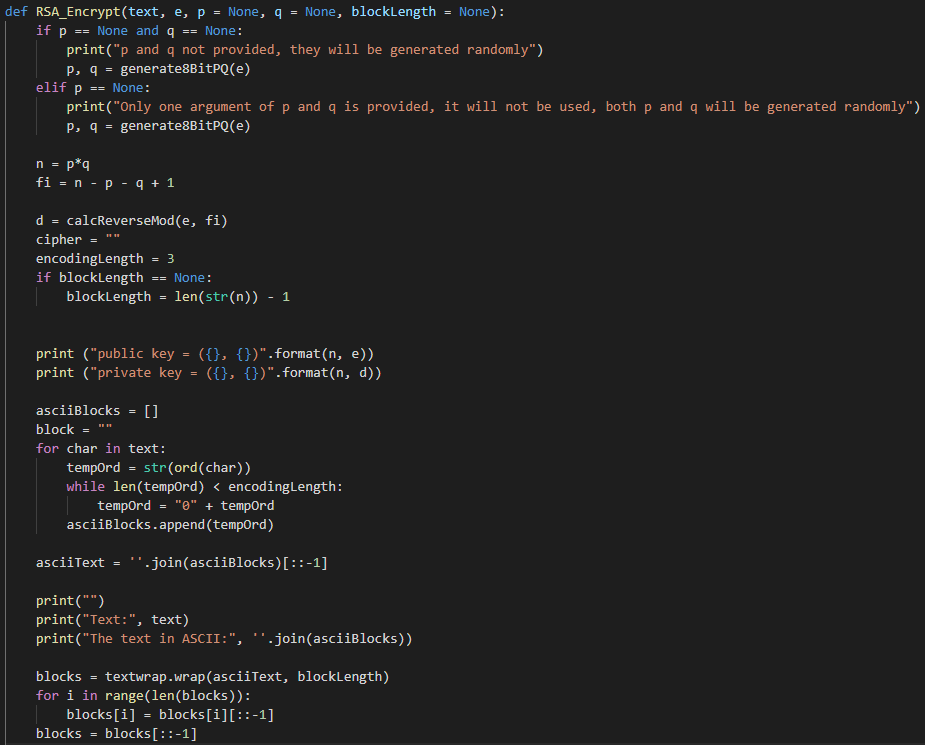
Patikrinu dvejetą atskirai ar jis yra pirminis, tada tikrinu ar num dalinasi su visais nelyginiais skaičiais nuo 3 iki šaknies iš tikrinamo skaičiaus. Tai greičiausias metodas kokį radau nerealizuojant jūsų skaidrėse pateiktų algoritmų.

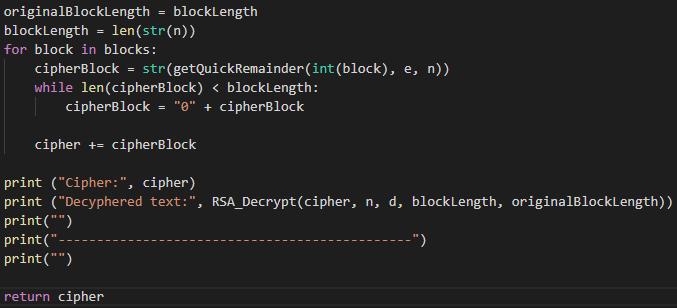
8 bitų p ir q generavimas:



Generuojami p ir q taip, kad duota exponentė būtų tinkama ir kad modulis būtų 16 bitų skaičius (32767 < p\*q < 65536). Nežinau kodėl, bet ne visi taip sugeneruoti skaičiai taip veikė, bet gavau porą veikiančių su kuriais atlinksiu šifravimą.

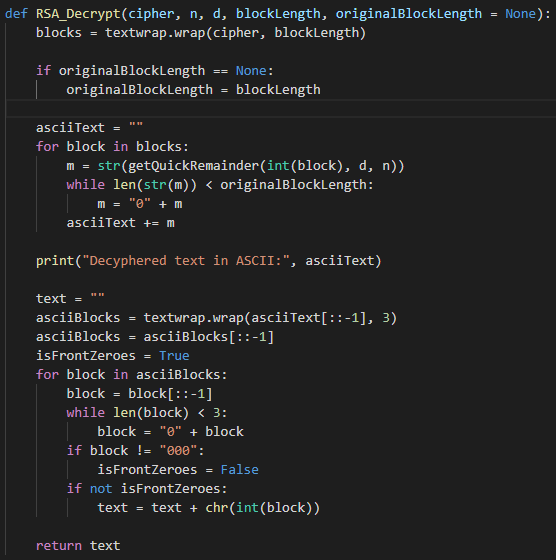
Teksto šifravimas:





Pagal jūsų patarimą šifruoju taip, kad gauti užšifruoti blokai bus didesni nei blokai su kuriais pradėjome jei bloko ilgis yra mažesnis jei modulio skaitmenų skaičius (kadangi 16 bitų modulis yra penkių skaitmėnų skaičius kai šifruojami blokai kurie yra mažesni pvz 4 skaitmenų ilgio, galimai gautas rezultatas bus 5 skaitmėnų), tokiais atvėjais dešifruojant yra gaunami blokai, kurie prasideda nuliais, tad prieš konveruojant iš ASCII atgal į tekstą reikia panaikinti tiek nulių iš blokų pradžios, kad blokai taptu pradinių blokų ilgio (pvz. uzšifravus 8610 bloką, dešifruojant gaunamas 08610 blokas).

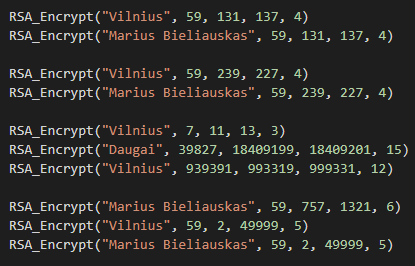
Dešifravimas:



Atliekamas dešifravimas ar atliekami papildomi veiksmai aprašyti prie šifravimo.

Kur reikalinga naudojami greito kėlimo laipsnio ir atvikštinio elemento paieškos algoritmai suprogramuoti praeituose darbuose.

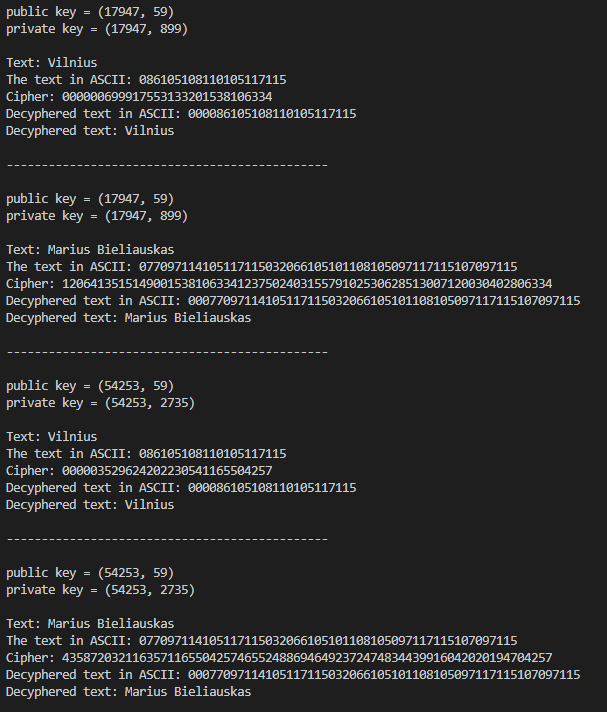
Išvestis:



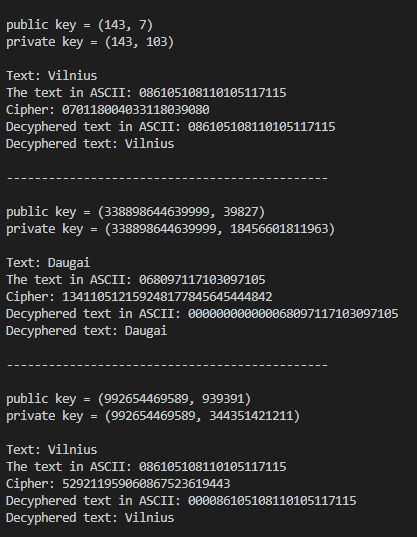
Užšifruoju savo vardą ir žodį „Vilnius“ su skirtingomis p ir q reikšmėmis ir blokų ilgiais. Pirmi 4 variantai yra gauti naudojant 8 bitų p ir q su blokų ilgiu 4 ir pagal eksponentę 59 kuri gauta pagal užduoties salygą (p\_{n+15}). Sekantys 3 yra skaidrėsė rodyti pavyzdžiai ir pagal duotą egzamino pavyzdinį klausimą parašytas miesto „Daugai“ pavadinimo šifravimas. Likę 3 yra pavyzdžai su didžiausiais šifravimui tinkamais moduliais kai modulis yra 6 ir 5 skaitmenų ilgio, kad parodyti, kad kai modulio ilgis ir bloko ilgis yra vienodi ir atitinka salygą m < n algoritmas veikia.

Rezultatai:

Pirmi 4:



3 pavyzdiniai:



3 mano pasirinkti:

