МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский Авиационный Институт»
(Национальный Исследовательский Университет)

Институт: №8 «Информационные технологии и прикладная математика»
Кафедра: 806 «Вычислительная математика и программирование»

Лабораторная работа № 2
по курсу «Криптография»

Группа: М8О-307Б-21

Студент: Дубровин Д.К.

Преподаватель: А. В. Борисов

Оценка:

Дата: 10.09.2024

Москва, 2024

Оглавление

1 Тема

Факторизация чисел

2 Задание

Разложить каждое из чисел n_1 и n_2 на нетривиальные сомножители.

Вариант №7:

$n_1 =$ 10876235329244848744124766368551365889316764693062717894612888996764317215412 7

n_2

$=$ 16117655691488048562428673842586807198500102862981912046351541529420432197290447526886147483136114545465725205417369977940016871273001825655775233013745768986374654630793295442477747872835121549831617371165626457442345657277097463641140055832315479670230254145694131224473280404169708453094322175307224333415061668790581352676527375610862399155982339310065668240742080964683365204046938632685331174477299911625792360364160144090922283544048098857799988000765501 37

3 Теория

Факторизация числа — это процесс разделения числа на несколько множителей так, что при их перемножении получается исходное число. Если говорить простыми словами, это похоже на разбиение числа на кусочки, которые являются меньшими числами, и все эти кусочки при умножении друг на друга дают первоначальное число. Обычно, когда мы говорим о факторизации, мы имеем в виду разбиение числа на простые множители, то есть такие числа, которые делятся только на 1 и на самих себя. Например, факторизация числа 12 будет $2 \times 2 \times 3$, где 2 и 3 являются простыми числами.

4 Ход лабораторной работы

При просмотре задания у меня закрались подозрения, что тут есть подвох. Я узнал в интернете что есть разные методы для факторизации числа. Мне больше приглянулся Ро-алгоритм Полларда. Ну я изучил, реализовал на языке Python и тут появился нюанс, что считать то он будет долго. Очень долго. Я уже просрочу срок сдачи лабораторной. Я посмотрел на другие алгоритмы в надежде найти самый быстрый. Но как-то все сомнительно выглядело. Да и самый быстрый алгоритм реализовать как-то сложновато. Я даже посмотрел в книжке под названием «Алгебраические основы криптографии» от Э.А. Применко. Но там ничего не нашел, хотя я не знаю, что я должен был там найти.

Я решил узнать у своей подруги со старших курсов в чем суть. Мне поведали, что, в общем и целом, я не смогу ее сделать на основе своих ресурсов. Поэтому есть опция прибегнуть к готовым решениям. Это оказались библиотека `mseive` на языке C (метод решета числового поля) и сайт https://www.cryptool.org/en/cto/msieve. Я прибегнул ко второму способу и получил такой результат:

1. 260951289862485772644727258162652873363
2. 41679178267240329566284173772868575822 9

Со вторым числом мне дали наводку в какую сторону копать. Суть заключается в том, что при факторизации второго числа первый множитель находится как НОД с числом другого варианта, а второй множитель – простым делением первоначального и первого множителя.

Вот что получилось:

1. 16339769606582107468090265599682557015970679523604590652155946096257851907885610572564896855656907271140661652972318293950181279472266236681488363161964007279292058185071950349333064642775523089637311981469057198581127811557725160954236258017514857831373908089824469638166526008447964338943479264542190871291 3
2. 98640654547512198461686735271387621307710174210524295953742724991750025274822105961746483874198806284532829711161949056537539457020970189775360371646791 68

5 Выводы

Первоначально я не понимал идеи лабораторной. Но когда я узнал, как делать, то я восхитился уловкой. Отдаю дань уважения преподавателю, который придумал это, и первому студенту, который додумался до этого. Это показало, что не нужно все задачи решать в тупую, нужно искать какие-то альтернативные способы, а не думать, что задача нерешаема. Так же было полезно узнать о том какие есть алгоритмы факторизации. Отличная лабораторная работа!

6 Список используемой литературы

1. https://ru.wikipedia.org/wiki/%D0%A4%D0%B0%D0%BA%D1%82%D0%BE%D1%80%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F_%D1%86%D0%B5%D0%BB%D1%8B%D1%85_%D1%87%D0%B8%D1%81%D0%B5%D0%BB
2. https://habr.com/ru/sandbox/163811/
3. https://algorithmica.org/ru/pollard