Московский авиационный институт
(Национальный исследовательский университет)

Факультет: «Информационные технологии и прикладная математика»
Кафедра: 806 «Вычислительная математика и программирование»
Дисциплина: «Криптография»

Лабораторная работа № 1

Тема: факторизация чисел

Студент: Хренов Геннадий
Группа: 80-307Б
Преподаватель: Борисов А. В.
Дата:
Оценка:

Москва, 2021

1. Постановка задачи
   Разложить каждое из чисел n1 и n2 на нетривиальные сомножители.
   n1=11976063958394105372565280373132841969764973917624384102191562124280761860859 1,
   n2=19162420871806801568617129945097280525351590911288448056586790252967165594044346648117256191866527259013257746490175941447883606374071784769363169152207581445356819643713116570717509704147072181122228045395187521359163973501984457964262201487421259483804145780046492118234512749646088825008417181554035121174581354219296962410856750448190529031735941575253507798593150790972216736431298009983402302302121276710704030134439278341757598100259379669607444268950730 1

2. Метод решения

   Вначале я попробовал вероятностные методы типа Полларда p-1 и Полларда p-0, которые не дали нужных результатов. Затем я приступил к реализации квадратичного решета на языке C++, используя довольно быструю библиотеку длинной арифметики gmp, в написании которой используется ассемблер. Программа показала хорошие результаты по факторизации 100-битовых чисел (в районе секунды или меньше в зависимости от числа), однако для заданных чисел такая реализация не подходит по времени. Разложить первое число удалось с помощью msieve – библиотека на Си для факторизации больших чисел, которая содержит реализацию алгоритмов SIQS и GNFS. Второе число длиной в 463 цифры обычным алгоритмом разложить за небольшое время невозможно. Но один из множителей этого числа можно найти как НОД с числом из другого варианта. В моем случае это число варианта 12. Второй множитель находим делением начального числа на первый.

3. Структура программы
   lab1.cpp - пробная реализация квадратичного решета
   secondFactor.cpp – разложение второго числа

4. Результаты работы

   Разложение первого числа с помощью msieve

```
Mon Mar 08 14:19:17 2021  Msieve v. 1.53 (SVN 1005)
Mon Mar 08 14:19:17 2021  random seeds: cef2741c 37ae084a
Mon Mar 08 14:19:17 2021  factoring 119760639583941053725652803731328419697649739176243841021915621242807618608591 (78 digits)
Mon Mar 08 14:19:18 2021  searching for 15-digit factors
Mon Mar 08 14:19:18 2021  commencing quadratic sieve (78-digit input)
Mon Mar 08 14:19:18 2021  using multiplier of 1
Mon Mar 08 14:19:18 2021  using generic 32kb sieve core
Mon Mar 08 14:19:18 2021  sieve interval: 12 blocks of size 32768
Mon Mar 08 14:19:18 2021  processing polynomials in batches of 17
Mon Mar 08 14:19:18 2021  using a sieve bound of 958739 (37824 primes)
Mon Mar 08 14:19:18 2021  using large prime bound of 95873900 (26 bits)
Mon Mar 08 14:19:18 2021  using trial factoring cutoff of 27 bits
Mon Mar 08 14:19:18 2021  polynomial 'A' values have 10 factors
Mon Mar 08 14:21:17 2021  38098 relations (19372 full + 18726 combined from 208557 partial), need 37920
Mon Mar 08 14:21:17 2021  begin with 227929 relations
Mon Mar 08 14:21:17 2021  reduce to 54557 relations in 2 passes
Mon Mar 08 14:21:17 2021  attempting to read 54557 relations
Mon Mar 08 14:21:17 2021  recovered 54557 relations
Mon Mar 08 14:21:17 2021  recovered 44108 polynomials
Mon Mar 08 14:21:17 2021  attempting to build 38098 cycles
Mon Mar 08 14:21:17 2021  found 38098 cycles in 1 passes
Mon Mar 08 14:21:17 2021  distribution of cycle lengths:
Mon Mar 08 14:21:17 2021     length 1 : 19372
Mon Mar 08 14:21:17 2021     length 2 : 18726
Mon Mar 08 14:21:17 2021  largest cycle: 2 relations
Mon Mar 08 14:21:17 2021  matrix is 37824 x 38098 (5.6 MB) with weight 1150652 (30.20/col)
Mon Mar 08 14:21:17 2021  sparse part has weight 1150652 (30.20/col)
Mon Mar 08 14:21:18 2021  filtering completed in 3 passes
Mon Mar 08 14:21:18 2021  matrix is 27205 x 27268 (4.3 MB) with weight 912343 (33.46/col)
Mon Mar 08 14:21:18 2021  sparse part has weight 912343 (33.46/col)
Mon Mar 08 14:21:18 2021  saving the first 48 matrix rows for later
Mon Mar 08 14:21:18 2021  matrix includes 64 packed rows
Mon Mar 08 14:21:18 2021  matrix is 27157 x 27268 (2.9 MB) with weight 677854 (24.86/col)
Mon Mar 08 14:21:18 2021  sparse part has weight 494813 (18.15/col)
Mon Mar 08 14:21:18 2021  commencing Lanczos iteration
Mon Mar 08 14:21:18 2021  memory use: 3.0 MB
Mon Mar 08 14:21:21 2021  lanczos halted after 431 iterations (dim = 27155)
Mon Mar 08 14:21:21 2021  recovered 17 nontrivial dependencies
Mon Mar 08 14:21:21 2021  p39 factor: 317975550097572442113430236685690984033
Mon Mar 08 14:21:21 2021  p39 factor: 376634742976910904214589735439587770927
Mon Mar 08 14:21:21 2021  elapsed time 00:02:04
```

В итоге получено разложение:

P1: 317975550097572442113430236685690984033

P2: 376634742976910904214589735439587770927

За время: 2 минуты 4 секунды

Разложение второго числа

```
D:\Kripta\newlaba1>g++ secondFactor.cpp -lgmpxx -lgmp

D:\Kripta\newlaba1>a.exe
p1 = 16329327349132342381371825041572435450627259915835087043997166910363565265993564300448283148924267822180065826285935955163930044070
00141627739512435133041593079620591103270636931164721592259898859457354058281485633814626779040948023732371400704619211544261701363498067583084799223248259812442497887668676421 23
p2 = 11734972581601773942696471276770846179494172081314218170143372885678875669010624213123777326122987142198877621700362684861975199985
4306140618107804707662 87
time: 0.015
```

В итоге получено разложение:

P1:

163293273491323423813718250415724354506272599158350870439971669103635652659935643004482831489242678221800658262859359551639300440700014162773951243513304159307962059110327063693116472159225989885945735405828148563381462677904094802373237140070461921154426170136349806758308479922324825981244249788766867642123

P2:

117349725816017739426964712767708461794941720813142181701433728856788756690106242131237773261229871421988776217003626848619751999854306140618107804707662 87

За время: 0.015 секунд

Характеристики ЭВМ
Процессор: AMD Ryzen 7 3750H with Radeon Vega Mobile Gfx 2.30 GHz
Оперативная память: 8.00ГБ
Тип системы: 64-разрядная операционная система, процессор x64

5. Выводы

В ходе работы я познакомился с алгоритмами факторизации чисел. Оказалось, что для больших чисел это довольно сложная задача и для ее решения потребовалось либо использовать специальные методы со всеми возможными оптимизациями времени работы стандартных алгоритмов, либо вовсе не использовать стандартные алгоритмы и искать обходные пути. Такую задачу по факторизации с достаточно длинным числом нельзя решить каким-то стандартным способом за малый промежуток времени, поэтому простые числа используются в криптографии.

СПИСОК ЛИТЕРАТУРЫ

1. Алгоритмы факторизации
https://e-maxx.ru/algo/factorization

2. Квадратичное решето
https://habr.com/ru/post/521876/