Лабораторная работа № 1 по курсу Криптография

Выполнила студентка группы 08-307 МАИ *Усачева Елизавета*.

Задание

Разложить каждое из чисел n1 и n2 на нетривиальные сомножители.

Вариант 0:

n1 = 284994967805859272853477327862245466978346919806585432133556769
959269315271111
n2 = 588334127500298760075185369594470830068532538546945053004260193
945595259217406786089770982249290901568725608451508611541771305401
493870045176537915940249286141846560042142211542409633392281206603
637954450433183517707796541972311424681336480578342707287553065652
703205564979626673694073622920569912786167694946557747760150408914
919705012801904512377092934509169841743698528816250385854697524916
330387856905603362762198545848392715027208817212275244652775338978
6619

Введение

Факторизация больших целых чисел является нетривиальной задачей. На вычислительной сложности задачи факторизации больших целых чисел основывается криптографический алгоритм с открытым ключом RSA, который стал первой системой, пригодной для шифрования и цифровой подписи. Трудоемкость алгоритмов, работающих с большими числами, оценивается количеством битовых операций. Зная количество операций, выполняемых компьютером за 1 секунду, можно оценить машинное время, необходимое для выполнения алгоритма. Оценка трудоемкости наиболее быстрых алгоритмов факторизации натуральных чисел имеет вид $O(\exp\sqrt{\log n * \log\log n})$.

Метод решения

Одним из самых быстрых и простых для реализации является так называемый метод квадратичного решета. Алгоритм пытается найти такие квадраты чисел, которые равны по модулю n (факторизуемое число), что часто приводит к факторизации n. Алгоритм работает в два этапа: этап сбора данных, где он собирает информацию, которая может привести к равенству квадратов и этап обработки данных, где он помещает всю собранную информацию в матрицу и обрабатывает её для получения равенства квадратов. Первый этап может быть легко распараллелен на много процессов, но второй этап требует большие объемы памяти и его трудно распараллелить. Один из простых методов отыскания равных квадратов заключается в том, чтобы выбрать случайное число,

возвести его в квадрат и надеяться, что остаток от деления на n является квадратом какого-либо другого числа.

Для нахождения множителей заданных чисел я решила воспользоваться утилитой *msieve*, которая как раз содержит алгоритм квадратичного решета(SIQS), а также общий алгоритм решета числового поля(GNFS).

- Сгенерированный *msieve* лог факторизации первого числа n_1 :

```
Wed Mar 04 16:49:40 2020  Msieve v. 1.53 (SVN 1005)
Wed Mar 04 16:49:40 2020  random seeds: 96097530 0fbb0776
Wed Mar 04 16:49:40 2020  factoring 284994967805859272853477327862
245466978346919806585432133556769959269315271111 (78 digits)
Wed Mar 04 16:49:40 2020  searching for 15-digit factors
Wed Mar 04 16:49:40 2020  commencing quadratic sieve (78-digit input)
Wed Mar 04 16:49:40 2020  using multiplier of 7
Wed Mar 04 16:49:40 2020  using generic 32kb sieve core
Wed Mar 04 16:49:40 2020  sieve interval: 12 blocks of size 32768
Wed Mar 04 16:49:40 2020  processing polynomials in batches of 17
Wed Mar 04 16:49:40 2020  using a sieve bound of 996067 (39176 primes)
Wed Mar 04 16:49:40 2020  using large prime bound of 99606700 (26 bits)
Wed Mar 04 16:49:40 2020  using trial factoring cutoff of 27 bits
Wed Mar 04 16:49:40 2020  polynomial 'A' values have 10 factors
Wed Mar 04 16:51:52 2020  39688 relations (20266 full + 19422 combined
from 216084 partial), need 39272
Wed Mar 04 16:51:52 2020  begin with 236350 relations
Wed Mar 04 16:51:52 2020  reduce to 56754 relations in 2 passes
Wed Mar 04 16:51:52 2020  attempting to read 56754 relations
Wed Mar 04 16:51:52 2020  recovered 56754 relations
Wed Mar 04 16:51:52 2020  recovered 46081 polynomials
Wed Mar 04 16:51:52 2020  attempting to build 39688 cycles
Wed Mar 04 16:51:52 2020  found 39688 cycles in 1 passes
Wed Mar 04 16:51:52 2020  distribution of cycle lengths:
Wed Mar 04 16:51:52 2020     length 1 : 20266
Wed Mar 04 16:51:52 2020     length 2 : 19422
Wed Mar 04 16:51:52 2020  largest cycle: 2 relations
Wed Mar 04 16:51:53 2020  matrix is 39176 x 39688 (5.7 MB) with weight
1183174 (29.81/col)
Wed Mar 04 16:51:53 2020  sparse part has weight 1183174 (29.81/col)
Wed Mar 04 16:51:53 2020  filtering completed in 4 passes
Wed Mar 04 16:51:53 2020  matrix is 27699 x 27763 (4.3 MB) with weight
917229 (33.04/col)
Wed Mar 04 16:51:53 2020  sparse part has weight 917229 (33.04/col)
```

```
Wed Mar 04 16:51:53 2020  saving the first 48 matrix rows for later
Wed Mar 04 16:51:53 2020  matrix includes 64 packed rows
Wed Mar 04 16:51:53 2020  matrix is 27651 x 27763 (2.7 MB) with weight
641206 (23.10/col)
Wed Mar 04 16:51:53 2020  sparse part has weight 433368 (15.61/col)
Wed Mar 04 16:51:53 2020  commencing Lanczos iteration
Wed Mar 04 16:51:53 2020  memory use: 2.7 MB
Wed Mar 04 16:51:56 2020  lanczos halted after 439 iterations
(dim = 27649)
Wed Mar 04 16:51:56 2020  recovered 16 nontrivial dependencies
Wed Mar 04 16:51:57 2020  p39 factor:
397695326178862814397952263440193307813
Wed Mar 04 16:51:57 2020  p39 factor:
716616336792661370154476211778412420347
Wed Mar 04 16:51:57 2020  elapsed time 00:02:17
```

Чтобы найти делители второго числа необходимы очень большие вычислительные мощности. Поэтому, "поигравшись"с другими вариантами, найдя НОД с несколькими из них, мне удалось найти делители второго числа.

Ответ

Сомножители первого числа:

- 397695326178862814397952263440193307813
- 716616336792661370154476211778412420347

Сомножители второго числа:

- 173898131987626431931004096200786737606541838091006931156969162857337493988686728504886499535100950282677998340866958942336693980592488570677190293064210473382113132886393256481868029607456308153276907685660972586040254314861433154825271413719376151482980877601333538598980788495631730047954340530991123331495287892948976768112961746416751204252421927528765511805664988839598851273818734120021659869151861668180073133397324121097968323527833037466494673716717807731
```
```

Выводы

В данной лабораторной работе я познакомилась с новой для меня областью на стыке математики и программирования - криптографией. В частности, изучила алгоритм шифрования RSA и различные алгоритмы факторизации больших чисел. В настоящее время задача факторизации некоторых больших чисел можно считать неразрешимой.