Московский авиационный институт
(национальный исследовательский университет)

Факультет информационных технологий и прикладной математики

Кафедра вычислительной математики и программирования

Лабораторная работа №1 по курсу «Криптография»

Студент: А. П. Шорохов
Преподаватель: А. В. Борисов
Группа: М8О-306Б
Дата:
Оценка:
Подпись:

Москва, 2021

Лабораторная работа №1

Задача: Разлжить каждое из чисел n1 и n2 на нетривиальные сомножители.

Вариант 9: n1=284994967805859272853477327862245466978346919806585432133556769959269
315271111,
n2=144705635774304031878986296122750910474479908149467861238329198698492351931644628
770804907791822465652742954367322936435188718339080726275242311729821104193465515227659922543175167158889598151741902647154293244819894449690836163313270764079803935657095050060789501415065874078204207363026173352563519252477390183115045370666190418643990517658419460473214034685807819362335735214694601654947678049107321295399466077016934821144519901938606946984530618532320643996 1

1 Характеристики машины

Lenovo ideapad 700-15ISK
Процессор - Intel Core i7-6700HQ @ 2.6GHz
Оперативная память - 12 Gb
ОС - Windows 10. Все программы были запущены через подсистему Unix в стандартной консоли Windows.

2 Описание

Факторизация - разложение числа на простые множители. Для решения данной задачи существует множество алгоритмов. Один из таких методов - Метод Полларда Ро.
Его я начал реализовывать, однако узнал о готовом продукте msieve. В целях экономии времени было решено воспользоваться им.

Второе число гораздо больше первого, и с самого начала не покидала мысль о том, что процесс его разложения будет заключаться в поиске какого-то тайного "ключа"в данных. Прошлое поколение студентов курса "Криптография"подтвердили эти догадки и намекнули, в какую сторону следует "копать".

В итоге, второе число имеет НОД с одним из других чисел в вариантах. Поэтому нам следует просто их перебрать, найти этот НОД и поделить на него исходное число. Для этого была написана программа на Python.

3 Исходный код

В силу того, что код длинный и содержит много длинных чисел, оставляю ссылку на github, где он лежит.

https://github.com/alien111/crypto1

4 Консоль

Первое число.

```
dobriy_alien@LAPTOP-2MM4OK81:~/Math/msieve$ ./msieve 284994967805859272853477327862245
69315271111

sieving in progress (press Ctrl-C to pause)
39693 relations (20672 full + 19021 combined from 214385 partial),need 39272
sieving complete,commencing postprocessing
dobriy_alien@LAPTOP-2MM4OK81:~/Math/msieve$ cat msieve.log
Sat Feb 20 21:41:07 2021
Sat Feb 20 21:41:07 2021
Sat Feb 20 21:41:07 2021  Msieve v. 1.54 (SVN 1038)
Sat Feb 20 21:41:07 2021  random seeds: f9506d45 0f7f372e
Sat Feb 20 21:41:07 2021  factoring 284994967805859272853477327862245466978346919
80658543213355676995926931527111 (78 digits)
Sat Feb 20 21:41:07 2021  searching for 15-digit factors
Sat Feb 20 21:41:07 2021  commencing quadratic sieve (78-digit input)
Sat Feb 20 21:41:07 2021  using multiplier of 7
Sat Feb 20 21:41:07 2021  using generic 32kb sieve core
Sat Feb 20 21:41:07 2021  sieve interval: 12 blocks of size 32768
Sat Feb 20 21:41:07 2021  processing polynomials in batches of 17
Sat Feb 20 21:41:07 2021  using a sieve bound of 996067 (39176 primes)
Sat Feb 20 21:41:07 2021  using large prime bound of 99606700 (26 bits)
Sat Feb 20 21:41:07 2021  using trial factoring cutoff of 27 bits
Sat Feb 20 21:41:07 2021  polynomial 'A' values have 10 factors
Sat Feb 20 21:43:25 2021  39693 relations (20672 full + 19021 combined from
214385 partial),need 39272
Sat Feb 20 21:43:25 2021  begin with 235057 relations
```

```
Sat Feb 20 21:43:25 2021  reduce to 56444 relations in 2 passes
Sat Feb 20 21:43:25 2021  attempting to read 56444 relations
Sat Feb 20 21:43:26 2021  recovered 56444 relations
Sat Feb 20 21:43:26 2021  recovered 45845 polynomials
Sat Feb 20 21:43:26 2021  attempting to build 39693 cycles
Sat Feb 20 21:43:26 2021  found 39693 cycles in 1 passes
Sat Feb 20 21:43:26 2021  distribution of cycle lengths:
Sat Feb 20 21:43:26 2021     length 1 : 20672
Sat Feb 20 21:43:26 2021     length 2 : 19021
Sat Feb 20 21:43:26 2021  largest cycle: 2 relations
Sat Feb 20 21:43:26 2021  matrix is 39176 x 39693 (5.7 MB) with weight 1178346
(29.69/col)
Sat Feb 20 21:43:26 2021  sparse part has weight 1178346 (29.69/col)
Sat Feb 20 21:43:26 2021  filtering completed in 3 passes
Sat Feb 20 21:43:26 2021  matrix is 27731 x 27794 (4.3 MB) with weight 913384
(32.86/col)
Sat Feb 20 21:43:26 2021  sparse part has weight 913384 (32.86/col)
Sat Feb 20 21:43:26 2021  saving the first 48 matrix rows for later
Sat Feb 20 21:43:26 2021  matrix includes 64 packed rows
Sat Feb 20 21:43:26 2021  matrix is 27683 x 27794 (2.7 MB) with weight 640429
(23.04/col)
Sat Feb 20 21:43:26 2021  sparse part has weight 430962 (15.51/col)
Sat Feb 20 21:43:26 2021  commencing Lanczos iteration
Sat Feb 20 21:43:26 2021  memory use: 4.0 MB
Sat Feb 20 21:43:31 2021  lanczos halted after 440 iterations (dim = 27682)
Sat Feb 20 21:43:31 2021  recovered 17 nontrivial dependencies
Sat Feb 20 21:43:31 2021  p39 factor: 39769532617886281439795226344019330781 3
Sat Feb 20 21:43:31 2021  p39 factor: 71661633679266137015447621177841242034 7
Sat Feb 20 21:43:31 2021  elapsed time 00:02:24
```

Второе число.

```
dobriy_alien@LAPTOP-2MM4OK81:/mnt/c/Users/shoro/Desktop/MAI/3course/crypto$
python3 hack.py
num1 =  132409693175774553363215785962870742379148917563619165564302946256826541
162420149235878801447829322271335187320099314107017038101752889419720705425181973
317227548103224812735617558451071099690522420741351532738899141412829992862938984
391526647637391239001362599884766434809399366957561743238852904262868584 43
```

```
num2 =  1.0928628584782427e+154
dobriy_alien@LAPTOP-2MM4OK81:/mnt/c/Users/shoro/Desktop/MAI/3course/crypto$
```

5 Выводы

Факторизация целых чисел используется для решения проблем сохранности информации. В процессе выполнения лабораторной работы я узнал много новой и интересной информации.
Мне очень понравилась поставленная задача, так как она заставила меня выйти за привычное представление о лабораторных работах и подумать не только об описанных в книгах алгоритмах.