

**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: Разложить каждое из чисел n_1 и n_2 на нетривиальные сомножители.

Вариант 9: $n_1=284994967805859272853477327862245466978346919806585432133556769959269315271111$,
 $n_2=1447056357743040318789862961227509104744799081494678612383291986984923519316446287708049077918224656527429543673229364351887183390807262752423117298211041934655152276599225431751671588895981517419026471542932448198944496908361633132707640798039356570950500607895014150658740782042073630261733525635192524773901831150453706661904186439905176584194604732140346858078193623357352146946016549476780491073212953994660770169348211445199019386069469845306185323206439961$

1 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. Прощлое 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.

2 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>

3 Консоль

Первое число.

```
dobriy_alien@LAPTOP-2MM4OK81:~/Math/msieve$ ./msieve 284994967805859272853477327862245466978346919806585432133556769959269315271111
```

```
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 284994967805859272853477327862245466978346919806585432133556769959269315271111 (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: 397695326178862814397952263440193307813
Sat Feb 20 21:43:31 2021 p39 factor: 716616336792661370154476211778412420347
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 = 1324096931757745533632157859628707423791489175636191655643029462568265412
162420149235878801447829322271335187320099314107017038101752889419720705425181973
317227548103224812735617558451071099690522420741351532738899141412829992862938984
39152664763739123900136259988476643480939936695756174323885290426286858443

```

```
num2 = 1.0928628584782427e+154
```

```
dobriy_alien@LAPTOP-2MM4OK81:/mnt/c/Users/shoro/Desktop/MAI/3course/crypto$
```

4 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.