Лабораторная работа №1 по курсу криптографии

Выполнил студент группы М8О-308Б-18 Коростелев Дмитрий

Условие

Разложить каждое их чисел n1 и n2 на нетривиальные сомножители
Вариант 11

n1 =
36199672745678487185560418105660567208862266620757816081129106087399715170888 7

n2 =
19162420871806801568617129945097280525351590911288448056586790252967165594044346648117256191866527259013257746490175941447883606374071784769363169152207581445356819643713116570717509704147072181122228045395187521359163973501984457964262201487421259483804145780046492118234512749646088825008417181554035121174581354219296962410856750448190529031735941575253507798593150790972216736431298009983402302302121276710704030134439278341757598100259379669607444268950730 1

Метод решения

Так как задание имело свободный способ выполнения, первое, что было опробовано – наивный перебор за O($\sqrt{n}$), однако после получаса вычислений было предпринято решение получить приблизительное время работы алгоритма: для числа в 12 знаков ответ можно получить за 0.001 секунду (алгоритм был написан на Java), для числа в 78 знаков потребуется около $4*10^{24}$ дней! Позже было опробовано еще несколько алгоритмов, однако ввиду низкой скорости и количества излишних операций выполняемых на Java программах, такие алгоритмы в простой реализации имеют крайне низкую скорость работы. После целого дня экспериментов, стало очевидно, что нельзя легко найти факторизацию большого числа, образованного при помощи перемножения больших простых чисел. Адекватный ответ можно получить только использовав специальные программы, разработанные для решения данной задачи. Одной из таких программ является msieve, написанная на си и оптимизированная всеми возможными способами – программными и математическими. Однако даже msieve имеет свои ограничения в максимальное количество чисел в цифре – 100. Для разложения больших (>100-разрядных чисел) требуется знать дополнительную информацию, своего рода ключ, по которому можно найти факторизацию.

Результат работы программы

Результат работы msieve:

```
Thu Feb 18 23:04:38 2021  Msieve v. 1.53 (SVN 1005)
Thu Feb 18 23:04:38 2021  random seeds: cc3da450 d8e22486
Thu Feb 18 23:04:38 2021  factoring
361996727456784871855604181056605672088622666207578160811291060873997151708887 (78 digits)
Thu Feb 18 23:04:39 2021  searching for 15-digit factors
Thu Feb 18 23:04:39 2021  commencing quadratic sieve (78-digit input)
Thu Feb 18 23:04:39 2021  using multiplier of 17
Thu Feb 18 23:04:39 2021  using generic 32kb sieve core
Thu Feb 18 23:04:39 2021  sieve interval: 12 blocks of size 32768
Thu Feb 18 23:04:39 2021  processing polynomials in batches of 17
Thu Feb 18 23:04:39 2021  using a sieve bound of 999199 (39176 primes)
Thu Feb 18 23:04:39 2021  using large prime bound of 99919900 (26 bits)
Thu Feb 18 23:04:39 2021  using trial factoring cutoff of 27 bits
Thu Feb 18 23:04:39 2021  polynomial 'A' values have 10 factors
Thu Feb 18 23:04:39 2021  restarting with 14525 full and 152193 partial relations
Thu Feb 18 23:05:15 2021  39615 relations (20355 full + 19260 combined from 212215 partial), need 39272
Thu Feb 18 23:05:15 2021  begin with 232570 relations
Thu Feb 18 23:05:15 2021  reduce to 56489 relations in 2 passes
Thu Feb 18 23:05:15 2021  attempting to read 56489 relations
Thu Feb 18 23:05:15 2021  recovered 56489 relations
Thu Feb 18 23:05:15 2021  recovered 45362 polynomials
Thu Feb 18 23:05:15 2021  attempting to build 39615 cycles
Thu Feb 18 23:05:15 2021  found 39615 cycles in 1 passes
Thu Feb 18 23:05:15 2021  distribution of cycle lengths:
Thu Feb 18 23:05:15 2021     length 1 : 20355
Thu Feb 18 23:05:15 2021     length 2 : 19260
Thu Feb 18 23:05:15 2021  largest cycle: 2 relations
Thu Feb 18 23:05:15 2021  matrix is 39176 x 39615 (5.8 MB) with weight 1216184 (30.70/col)
Thu Feb 18 23:05:15 2021  sparse part has weight 1216184 (30.70/col)
Thu Feb 18 23:05:15 2021  filtering completed in 3 passes
Thu Feb 18 23:05:15 2021  matrix is 27666 x 27730 (4.4 MB) with weight 939432 (33.88/col)
Thu Feb 18 23:05:15 2021  sparse part has weight 939432 (33.88/col)
Thu Feb 18 23:05:15 2021  saving the first 48 matrix rows for later
Thu Feb 18 23:05:15 2021  matrix includes 64 packed rows
Thu Feb 18 23:05:15 2021  matrix is 27618 x 27730 (2.7 MB) with weight 657106 (23.70/col)
```

```
Thu Feb 18 23:05:15 2021  sparse part has weight 421517 (15.20/col)
Thu Feb 18 23:05:15 2021  commencing Lanczos iteration
Thu Feb 18 23:05:15 2021  memory use: 2.7 MB
Thu Feb 18 23:05:19 2021  lanczos halted after 438 iterations (dim = 27614)
Thu Feb 18 23:05:19 2021  recovered 18 nontrivial dependencies
Thu Feb 18 23:05:19 2021  p39 factor:
439569685844479604455249506524271148907
Thu Feb 18 23:05:19 2021  p39 factor:
823525231867012416449127740764970659141
Thu Feb 18 23:05:19 2021  elapsed time 00:00:41
```

Для поиска множителей большего числа был применена функция НОД к остальным числам из других вариантов.

Результат работы программы перебора НОД:

```
f1 :
163293273491323423813718250415724354506272599158350870439971669103635652659935643004482831489242678221800658262859359551639300440700014162773951243513304159307962059110327063693116472159225989885945735405828148563381462677904094802373237140070461921154426170136349806758308479922324825981244249788766867642123
f2 :
117349725816017739426964712767708461794941720813142181701433728856788756690106242131237773261229871421988776217003626848619751999854306140618107804707662 87
rem : 0
```

Выводы

Простые числа обладают интересным незамысловатым свойством, однако на практике поиск больших простых чисел невозможен в адекватное время даже с учетом современных технологий и вычислительных мощностей, что делает использование простых чисел крайне эффективным в криптографии.