Лабораторная работа № 1 по курсу Криптография

Выполнил студент группы М8О-306Б-17 *Ветренко Полина.*

Задание

Разложить каждое из чисел n1 и n2 на нетривиальные сомножители.

Вариант 2

n1 = 119760639583941053725652803731328419697649739176243841021915621242807618608591
n2 = 1916242087180680156861712994509728052535159091128844805658679025296716559404434664811725619186652725901325774649017594144788360637407178476936316915220758144535681964371311657071750970414707218112222280453951875213591639735019844579642622014874212594838041457800464921182345127496460888250084171815540351211745813542192969624108567504481905290317359415752535077985931507909722167364312980099834023023021212767107040301344392783417575981002593796696074442689507301

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

Процесс разложения числа на простые множетели называется факторизацией. Для решения этой задачи существует множество алгоритмов, позволяющих находить множетели, используя свойства простых чисел.

Для решения задачи был использован алгоритм ρ - *Полларда*, как один из наиболее простых и эффективных. Сложность алгоритма оценивается как $O(N^{1/4})$. Изначально ищем все простые делители исходного числа, затем, получаем все существующие делители перемножением простых делителей. Простые делители ищутся следующим способом: случайным образом выбирается число x, на каждой итерации вычисляется значение функции $f^i(x)$. В качестве функции взята $f(x) = ax^2+b$ для случайных a и b. На i-ом шаге получаем значения $x_i = f^i(x_0)(mod n), y_i = x_{2i} = f^{2i}(x_0)(mod n)$. $gcd(abs(x - y), n)$ даст нетривиальный сомножитель n. Функция выбирается каждый раз, когда количество итераций превышает $O(\sqrt{n})$. Проверка простоты числа осуществляется с помощью теста Миллера-Рабина, который позволяет выполнять проверку быстрее.

Результаты работы

```
Рабочий стол — -zsh — 80×26
[polzovatel@MacBook-Air-Polzovatel Desktop % python3 factor.py                 ]
 Первое число 1197606395839410537256528037313284196976497391762438410219156212428
 076186085911
 Простые делители
 7
 17
 49
 119
 509
 833
 3563
 8653
 24941
 60571
 423997
 2824563371531898898474583634585348945809751936363791277341953392189275363
 197719436007232922893220854420974426206682635554546538941393673745324927541
 48017577316042281274067921787950932078765782918184451714813207667217681171
 138403605205063046025254598094682098344677844881825772589755716217274492787
 336123041212295968918475452515656524551360480427291162003692453670523768197
 1437702756109736539323563070003942613417163735609169760167054276624341159767
 2352861288486071782429328167609595671859523362991038134025847175693666377379
 10063919292768155775264941490027598293920146149264188321169379936370388118369
 24440946853865521168500572190067024428091783505355885922839922702613799716039
 70447435049377090426854590430193188057441023044849318248185659554592716828583
 polzovatel@MacBook-Air-Polzovatel Desktop %
```

```
Рабочий стол — -zsh — 82×17
[polzovatel@MacBook-Air-Polzovatel Desktop % python3 gcd.py                      ]
 Второе число 191624208718068015686171299450972805253515909112884480565867902529671
 6559404434664811725619186652725901325774649017594144788360637407178476936316915220
 7581445356819643713116570717509704147072181122222804539518752135916397350198445796
 4262201487421259483804145780046492118234512749646088825008417181554035121174581354
 2192969624108567504481905290317359415752535077985931507909722167364312980099834023
 023021212767107040301344392783417575981002593796696074442689507301

 Делители
  163293273491323423813718250415724354506272599158350870439971669103635652659935643
 0044828314892426782218006582628593595516393004407000141627739512435133041593079620
 5911032706369311647215922598988594573540582814856338146267790409480237323714007046
 1921154426170136349806758308479922324825981244249788766867642123

  117349725816017739426964712767708461794941720813142181701433728856788756690106242
 13123777326122987142198877621700362684861975199985430614061810780470766287
 polzovatel@MacBook-Air-Polzovatel Desktop %
```

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.