Исследование алгоритмов факторизации полупростых чисел в вычислительной кластерной системе

Булыгин Л.Э., Семенов М.Е.

Томский политехнический университет

leb1@tpu.ru

Целью работы является получение сравнительной оценки эффективности алгоритмов факторизации полупростых чисел при различных входных данных. На данный момент вычислительная сложность задачи разложения полупростых чисел на делители активно используется в криптографических алгоритмах, в частности, в алгоритме шифрования RSA[1].Для достижения поставленной цели необходимо выполнить следующие задачи:

- реализовать алгоритмы факторизации в кластерной системе;
- провести тестирование алгоритмов;
- сравнить и сделать выводы об эффективности алгоритмов.

В данной работе будет проведено сравнение следующих алгоритмов факторизации[2]: метод Ферма, *p*-метод Полларда, метод эллиптических кривых, метод квадратичного решета, а также алгоритм, основанный на упорядоченном переборе сумм цифр полупростого числа. Данные алгоритмы будут реализованы на языке C++ и протестированы в кластерной системе «СКИФ-Политех» (cluster.tpu.ru). Сравнительная оценка будет проведена на целых числах различной разрядности, с учетом длины простых сомножителей и расстояния между ними в натуральном ряду.

Литература

1 Rivest R. L., Shamir A., Adleman L. A method for obtaining digital signatures and public-key cryptosystems. New York, NY, USA: ACM, 1978. — Vol. 21, no. 2, Feb. 1978. — P. 120—126.

2 Brent R.P. Parallel Algorithms for Integer Factorisation. Canberra: Australian National University. – P. 3-9.