УДК 581

АЛГОРИТМ ДЕЛЕНИЯ БОЛЬШИХ ЧИСЕЛ

к.т.н. В.Я. Певнев, В.О.Агафонова
(представил д.т.н., проф. С.В. Смеляков)

В статье предлагается алгоритм деления больших чисел, позволяющий обеспечить работу по криптоанализу асимметричных криптосистем.

Использование алгоритмов шифрования предполагает работу с большими числами. Особенно это становится видно при работе с несимметричными алгоритмами. Числа при этом могут состоять из 150 – 200 и более десятичных цифр [1]. Языки программирования C^{++}, Pascal, пакеты Matcad, Matlab различных версий не предусматривают работу с числами таких размеров. К настоящему времени разработан ряд методов и алгоритмов выполнения операций с большими числами [2-5], однако оценки их эффективности противоречивы. В Internet распространяются различные библиотеки: MIRACL[6], RSAREF[7], CRYPTO++ [7] и др. Проведенные исследования показали, что их производительность является недостаточной.

Как известно операция деления является одной из самых медленных при работе ЭВМ. Поиск алгоритмов деления больших чисел в различных источниках не дал положительного результата. В большинстве случаев предлагается использование операций с плавающей точкой. Но одним из ограничений при работе с асимметричными системами является то, что работать приходится с целыми числами. Целью представленной работы является разработка и исследование алгоритма деления больших чисел. Суть представленного ниже алгоритма заключается в реализации способа деления в столбик, а его схема показана на рис. 1.

1. Начало алгоритма.

2. Делимое и делитель должны быть отсортированы таким образом, чтобы младшая цифра числа имела индекс (длина числа-1), а старшая - 0.

3. Если делимое и делитель равны по длине, тогда выполняем ДелениеМинус делимого и делителя по их соответствующим длинам и получаем результат деления и остаток. Переход к п. 9.

4. Организовывается цикл j от 0 до (длина делимого - длина делителя) с шагом 1.

5. Выполняем ДелениеМинус делимого и делителя соответственно по длине делителя+1+j и длине делителя.

6. Сортируем делитель по его длине, результативное число - по длине делителя+j, результативное число - по длине делителя+j+1.

7. Прибавляем к результату деления результативное число.

8. Сортируем остаток по длине делителя+j+1.Если j не равно (длина делимого - длина делителя), то переход к п.4.

9. Конец алгоритма

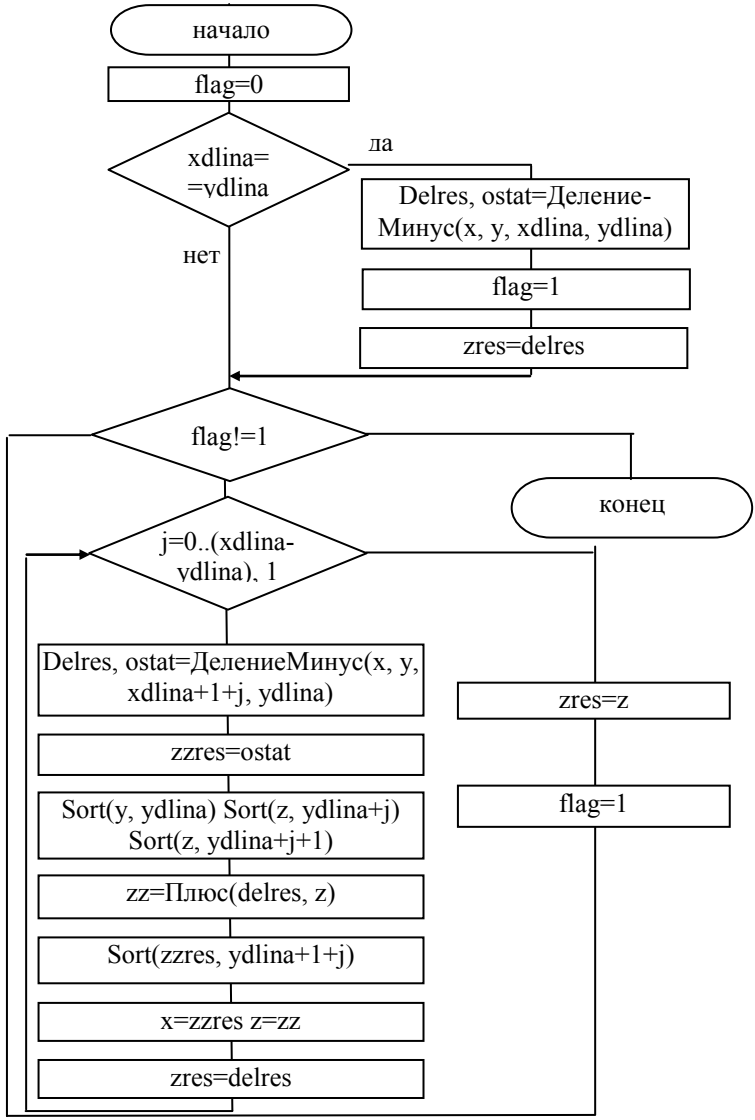

Рис. 1. Схема алгоритма деления

В представленном алгоритме выделяется модуль ДелениеМинус. Этот модуль играет большую роль при организации процесса вычисления. Суть

этого модуля состоит в вычитании делителя из делимого, начиная со старших разрядов. После каждого такого действия частное увеличивается на единицу. Операции производятся до тех пор, пока делитель не становится больше делимого. Формализованное описание модуля ДелениеМинус представлено следующим алгоритмом.

1. Начало алгоритма.

2. Делимое и делитель должны быть отсортированы таким образом, чтобы младшая цифра числа имела индекс (длина числа-1), а старшая - 0.

3. Если делимое равно 0,то переход к п. 9.

4. Если делимое меньше делителя, то переход к п. 9.

5. Вычитаем из делимого делитель и результат записываем в делимое, результативное число увеличиваем на 1.

6. Если делимое меньше делителя, то переход к п. 9.

7. Если делимое равно делителю, тогда результативное число увеличиваем на 1 и переход к п. 9.

8. Если делимое больше делителя, то переход к п. 4.

9. *Конец алгоритма.*

Схема рассмотренного модуля ДелениеМинус представлена на рис. 2.

Таблица 1

Результаты эксперимента

Кол-во разрядов делимого (**N**)	Отношение делимое / делитель (**k**)	Время выполнения операции **t**, **C***10^{-3}
40	3	3.81
	5	4.08
	10	5.52
80	3	6.93
	5	7.47
	10	10.98
120	3	10.5
	5	11.66
	10	15.46
160	3	14.8
	5	16.14
	10	20.88
200	3	17.53
	5	19.72
	10	26.01
240	3	21.08
	5	22.98
	10	32.4

С целью определения эффективности разработанного алгоритма был проведен эксперимент. Задачей эксперимента было определение зависимости времени работы алгоритма от размера делимого и делителя. Реализация эксперимента производилась на процессоре Pentium 1 с тактовой частотой 100 МГц. В ходе эксперимента было проведено 30 реализаций для каждой точки. Ввиду того, что время выполнения операции мало, производилось 1000 вычислений в одной реализации. Другими словами одно и тоже число делилось на один делитель 1000 раз. Для того, чтобы не учитывать время переходов при организации цикла было последовательно определено время выполнения деления одного и двух чисел. Время выполнения деления определялось как разница между ними, деленная на 1000. Результаты эксперимента приведены в табл. 1.

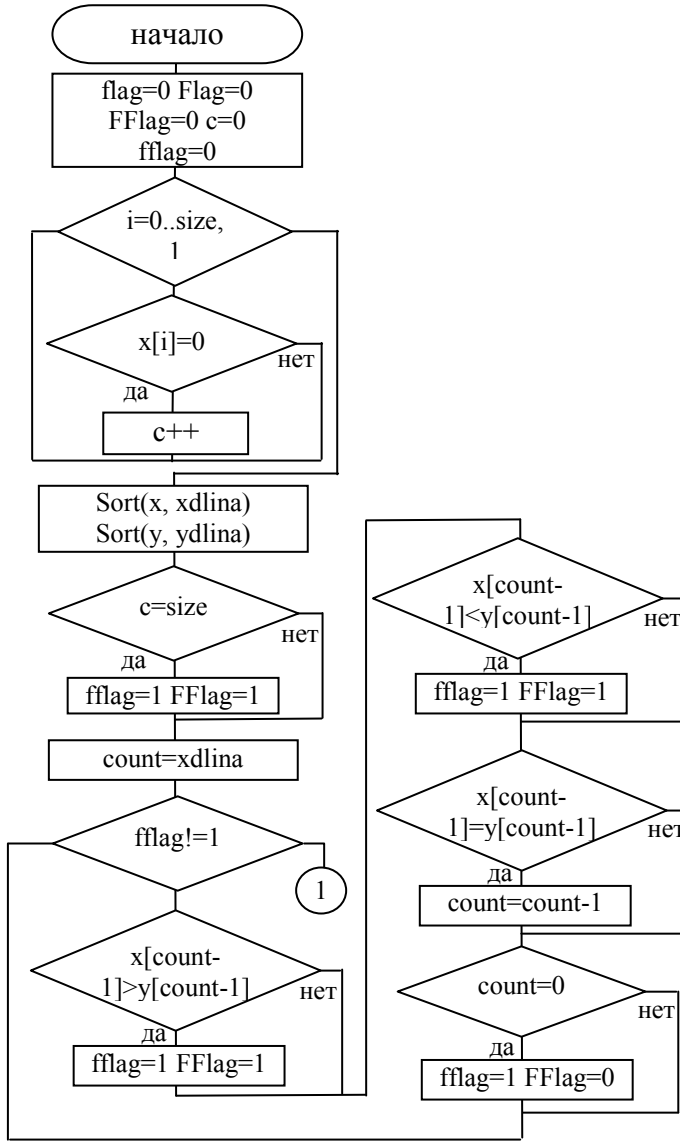

Рис. 2. Схема алгоритма ДелениеМинус

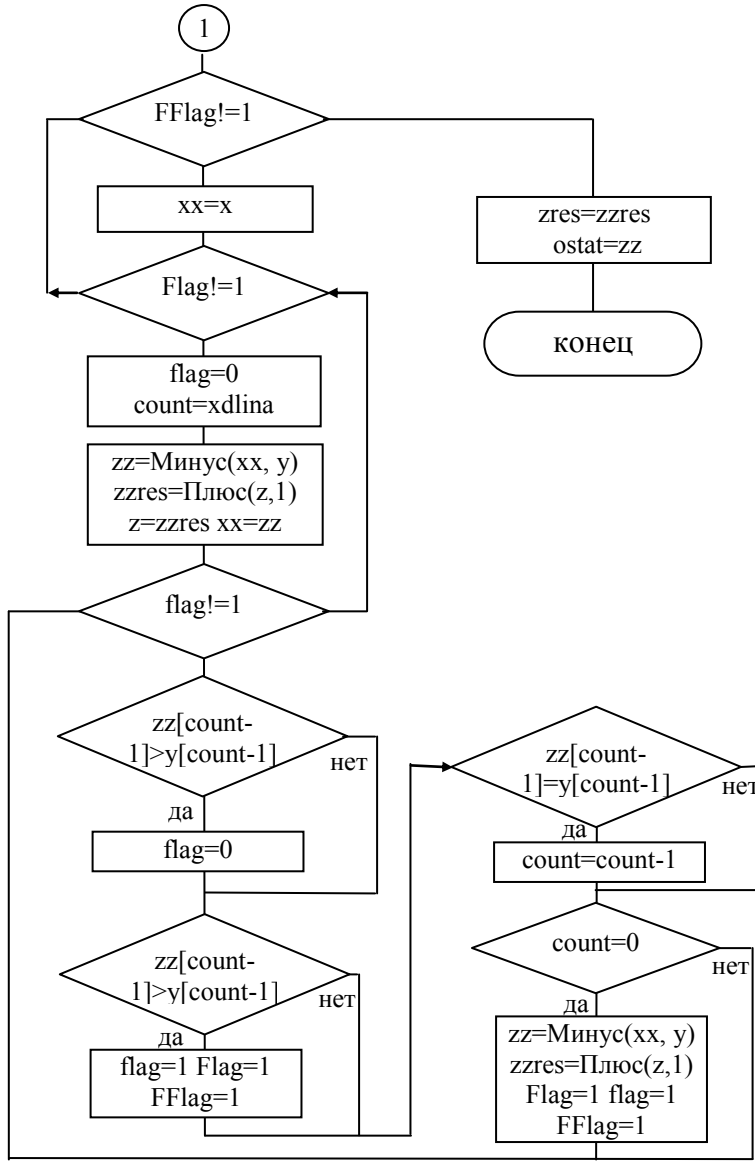

Рис. 2. Схема алгоритма ДелениеМинус (окончание)

По результатам эксперимента, приведенным в табл. 1, построено семейство кривых, изображенных на рис. 3. Проведенные исследования показали линейную зависимость времени работы разработанных алго-

ритмов от размера делимого и делителя. Совершенно очевидно, что при увеличении разности между их размерами время работы растет. Это хорошо видно на приведенном графике (рис. 3).

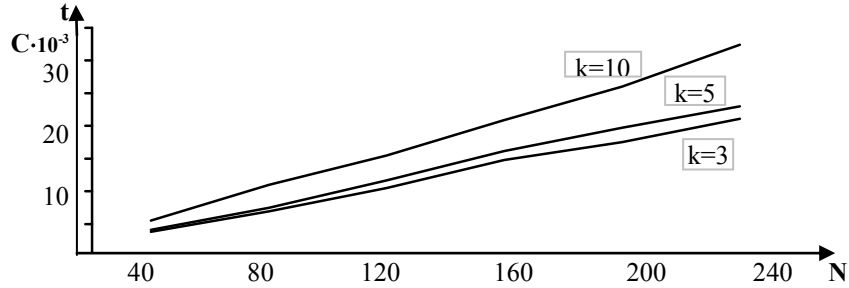

Рис. 3. Зависимость времени работы алгоритма деления от размеров делимого и делителя

Представленный в статье алгоритм позволяет осуществлять работу с большими числами. Данный алгоритм является частью библиотеки, которая позволяет осуществлять вычисления во многих прикладных областях. Примером такой области является криптоанализ несимметричных систем шифрования.

ЛИТЕРАТУРА

1. *Чмора А.Л. Современная прикладная криптография. – М.: Гелиос АРВ, 2001. – 256 с.*
2. *Кнут Д. Основы программирования для ЭВМ: В 3 т. – М.: Мир, 1977. Т.2. Получисленные алгоритмы. – 724 с.*
3. *Montgomery P. Modular multiplication without trial division // Math. Comp. – 1985. – №44. – P. 519 - 521.*
4. *Анисимов А.В. Методы быстрой модулярной редукции // Безопасность информации. – 1996. – № 2. – С. 10 - 16.*
5. *Бухштаб А.А. Теория чисел. – М.: Просвещение, 1966. – 384 с.*
6. *ftp://ftp.compapp.dcu.ie/pub/crypto/miracl.zip.*
7. *ftp://ftp.funet.fi/pub /crypt/cryptography/ asymmetric/rsa.*
8. *http://www.eskimo.com /~weidai/cryptlib.html.*

Поступила 20.03.2002

***ПЕВНЕВ Владимир Яковлевич**, канд. техн. наук доцент, ст. преп. ХВУ. В 1975 году окончил Харьковское ВВКУ. Область научных интересов – оптимизационные задачи на графах, системы защиты информации и их криптоанализ.*

***АГАФОНОВА Виолетта Олеговна**, студентка НТУ «ХПИ». Область научных интересов - системы защиты информации и их криптоанализ.*