– поддержка SNMP входит в состав почти всего создаваемого активного оборудования и во все сетевые операционные системы;

– протокол постоянно развивается, в том числе улучшаются и способы его защиты;

– благодаря заложенной клиент-серверной архитектуре подразумевает централизованное управление и мониторинг;

– поддержка асинхронной работы, так как агент, при возникновении ошибки или любого другого контролируемого события, может отсылать сообщение серверу не дожидаясь опроса.

К недостаткам SNMP можно отнести:

– программное обеспечение, способное управлять всеми аспектами крупномасштабной вычислительной сети являются дорогостоящими решениями;

– ограничения по информационным базам, так как своевременность и охват информационных баз зависит от производителя [2].

В силу своих преимуществ протокол SNMP отлично подходит для комплексного управления и мониторинга за всеми аспектами корпоративной сетевой инфраструктурой. Статус протокола обеспечивает ему постоянную поддержку и улучшение, в том числе и применяемых методов защиты.

Библиографические ссылки

1. RFC 1157 A Simple Network Management Protocol (SNMP) // ietf.org: Сервер Специальной комиссии интернет-разработок (Internet Engineering Task Force, IETF). URL: http://www.ietf.org/rfc/rfc1157.txt (Дата обращения: 17.03.2011).

2. 4.4.13 Протокол управления SNMP. Семенов Ю.А. (ГНЦ ИТЭФ) // book.itep.ru сервер электронного учебника «телекоммуникационные технологии v3.5». 2010. URL: http://book.itep.ru/4/44/snm_4413.htm (Дата обращения: 15.03.2011).

УДК 511.21

Д. Н. Пахоруков, М. Ю. Сидоров
Научный руководитель – О. Н. Жданов
Сибирский государственный аэрокосмический университет
имени академика М. Ф. Решетнева, Красноярск

РЕАЛИЗАЦИЯ РО-МЕТОДА ПОЛЛАРДА

Рассмотрены различные варианты реализации ро-метода Полларда. Предлагается оптимизация таких реализаций.

На современном этапе развития информационных технологий их неотъемлемой частью является прикладная криптография как одна из стадий обеспечения информационной безопасности. При этом все большее распространение получают информационные технологи, включающие криптографию с открытым ключом.

В связи с этим важной является трудная задача нахождения простых делителей числа n (задача факторизации). Один из популярных методов ее решения – ρ-метод Полларда [1]. Основная идея метода в следующем: выбираем случайное число x_0 и строим последовательность $x_{i+1} = f(x_i)$, пока не найдем такие i, j, что $i < j$ и $x_i = x_j$.

Если p – простой делитель числа n, $x_i \equiv x_j \pmod p$ и НОД $(x_i - x_j, n) > 1$, то этот нетривиальный НОД как раз и будет числом p [2]/

Описанный алгоритм реализован авторами на языке C++. Из-за ограничений, накладываемых на величину чисел ($256^8 - 1$ для типа long long), для выполнения операций над числами произвольной длины использовалась свободная библиотека GMP.

Целью работы было: проанализировав результаты работы алгоритма при различных исходных данных, найти их оптимальные значения для наиболее эффективного нахождения делителей числа n. При анализе был выбран самый часто применяемый в данном методе многочлен $ax^c + b$. На настоящий момент в результате работы были выяснены следующие факты:

1) количество итераций всегда меньше либо равно наименьшему простому делителю числа;

2) наилучшие результаты показали многочлены степеней кратных 2 и 3, но в степенях, кратных 2, вероятность неудачного разложения выше;

3) наилучшие результаты показали многочлены с четными коэффициентами a.

Библиографические ссылки

1. Маховенко Е. Б.Теоретико-числовые алгоритмы в криптографии. М. : Гелиос АРВ, 2006.

2. Жданов О. Н., Лубкин И. А. Алгоритм RSA : метод. указания к выполнению лабораторных работ ; Сиб. гос. аэрокосмич. ун-т. Красноярск, 2007.