УДК 004.056.55 + 004.021

А.С. Витер, А.О. Голубенко, Е.В. Бычкова
Донецкий национальный технический университет, г. Донецк
кафедра программного обеспечения интеллектуальных систем

СТОЙКОСТЬ СОВРЕМЕННЫХ КРИПТОСИСТЕМ С ОТКРЫТЫМ КЛЮЧОМ ПЕРЕД ТЕХНИЧЕСКИМ ПРОГРЕССОМ

Аннотация

Витер А.С., Голубенко А.О., Бычкова Е.В. Стойкость современных криптосистем перед техническим прогрессом. *Проанализированы математические обоснования стойкости современных криптосистем с открытым ключом. Приведены причины успеха атак на системы защиты информации. Выдвинуты предположения авторов о будущем современных методов защиты информации на основе развития современных технологий.*

Ключевые слова: *защита информации, криптосистема, взлом, дискретное логарифмирование, факторизация чисел, квантовые компьютеры, квантовая криптография.*

Постановка проблемы. Защита информации - весьма актуальная проблема. В связи с этим несколько десятков лет ученые занимаются разработкой методов защиты данных. В основе современных криптосистем с открытым ключом лежат вычислительно сложные задачи, которые весьма долго решаются на компьютерах архитектуры фон Неймана, например:

- вычисление дискретного логарифма;
- факторизация числа и др.

Анализ литературы. Проведен анализ сложности вычисления входных значений односторонних функций, на которых основаны современные алгоритмы шифрования, невозможности их вычисления на компьютерах архитектуры фон Неймана за полиномиальное время. В статье описывается возможность решения данных алгоритмов на квантовых компьютерах.

Цель статьи – проанализировать влияние развития в области компьютерных технологий на современные подходы защиты данных.

Криптография с открытым ключом. До середины семидесятых годов прошлого столетия криптография развивалась очень медленно и использовалась в основном людьми, которых сейчас бы назвали представителями спецслужб. Однако с открытием публичной криптографии (или криптографии с открытым ключом) американскими учеными Диффи и Хеллманом, которые опубликовали протокол выработки общего секретного ключа при использовании открытых каналов связи [1], а также с открытием

позднее криптографической системы RSA [2] (Rivest, Shamir, Adleman) криптография превратилась в популярную прикладную науку. В дальнейшем стали появляться новые криптосистемы с открытым ключом и различные протоколы обмена данными на их основе.

В отличие от симметричных алгоритмов [3], которые имеют один ключ для шифрования и дешифрования, ассиметричные методы шифрования [2] имеют два ключа: один открытый, а другой закрытый. Одним можно зашифровать, а другим расшифровать - одним и тем же ключом провести два действия невозможно.

Общий принцип шифрования с открытым ключом состоит в следующем.

1. Субъект 1 выбирает пару (e, d) и шлёт ключ шифрования e (открытый ключ) субъекту 2 по открытому каналу, а ключ расшифрования d (закрытый ключ) защищён и секретен.

2. Чтобы послать сообщение m Субъекту 1, Субъект 2 применяет функцию шифрования, определённую открытым ключом e:$E_e(m) = c$, где c - полученный шифротекст.

3. Субъект 1 расшифровывает шифротекст c , применяя обратное преобразование D_d, однозначно определённое значением d.

Для криптосистемы с открытым ключом схема шифрования показана на рис.1.

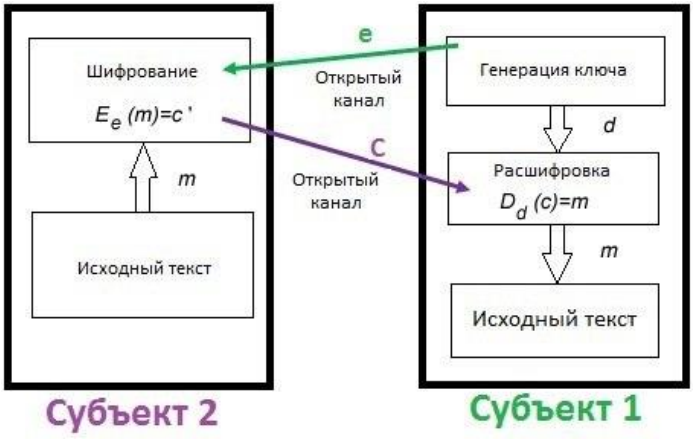

Рисунок 1 – Схема шифрования с открытым ключом

Криптосистемы с открытым ключом основаны на так называемых односторонних, функциях, то есть функциях, которые легко вычисляются для любого входного значения. Но найти входное значение по заданному значению функции в достаточной степени проблематично. Здесь сложность вычисления стоит понимать как количество операций, которые нужно совершить для нахождения ответа. Данные функции были бы бесполезны,

если бы не существовала «лазейка» - некий секрет, с помощью которого можно легко найти аргумент функции. Примерами односторонних функций, используемых в ассиметричных методах шифрования, являются следующие.

1. Умножение двух больших простых чисел. Функция f принимает на вход два простых числа p и q и возвращает их произведение N. Эта функция может быть вычислена за время порядка $O\left(n^{\log_2 3}\right)$ (алгоритм Карацубы), где n - общая длина входных данных в бинарном представлении.

Обратной к данной функции является функция нахождения множителей заданного целого числа N (факторизация).

В настоящее время самым быстрым методом факторизации чисел, применимым ко всем числам, является общий метод решета числового поля [4]. Его сложность оценивается формулой:

$$\exp\left(\left(\sqrt[3]{\frac{64}{9}+o(1)}\right)(\log n)^{\frac{1}{3}}(\log\log n)^{\frac{2}{3}}\right)=L_n\left[\frac{1}{3};\sqrt[3]{\frac{64}{9}}\right] \quad (1)$$

На сложности факторизации чисел основывается алгоритм шифрования RSA.

2. Возведение числа в заданную степень по данному модулю (на эллиптических кривых или в мультипликативной группе). Данная функция f принимает в качестве аргументов простое число p, целое $g \in Z_p$ и целое x в интервале от 0 до $p-1$ и возвращает остаток от деления g^x на p. Эта функция может быть вычислена за время $O(n^3)$, где n — количество битов в числе p.

Обращение данной функции требует вычисления дискретного логарифма по модулю p: необходимо найти такое значение x, при котором выполняется равенство: $g^x = y \bmod p$.

В мультипликативной группе конечного поля наилучший из известных алгоритмов, решающий проблему дискретного логарифмирования [5], - метод квадратичного решета в числовом поле. Сложность вычисления дискретных логарифмов в этом случае оценивается как $L_p\left[\frac{1}{3};\ c\right]$, где c — некоторая константа, зависящая от типа поля, например, от его характеристики.

Для групп, подобных эллиптической кривой, задача дискретного логарифмирования еще более трудна. Наилучший из доступных на сегодняшний день методов, вычисляющих дискретные логарифмы над общей эллиптической кривой над полем, называется p-метод Полларда [4]. Эвристическая оценка сложности данного алгоритма составляет $O(p^{1/2})$ операций.

На сложности вычисления дискретного логарифмирования основываются такие алгоритмы шифрования, как алгоритм Эль-Гамаля и алгоритм Диффи - Хеллмана [6].

3.Возведение в квадрат по модулю числа p. Данная функция f принимает два целых числа: x и N и возвращает остаток от деления x^2 на N, где N - произведение двух простых чисел p и q.

Нахождение обратной функции требует вычисления квадратного корня по модулю N, то есть значение числа x, если известно значение y, где $x^2 = y \pmod N$. Доказано, что эта задача сравнима по сложности с задачей факторизации числа N [6].

На сложности вычисления квадратного корня по модулю N основывается криптосистема Рабина [6].

Выше перечислены, естественно, не все односторонние функции, подробнее о подобных функциях можно прочесть в [7].

Показатели сложности вычисления, приведенные выше, говорят о том, что для взлома криптосистем, которые на них основываются и имеют достаточно длинные ключи, самому мощному компьютеру понадобятся годы. Конечно, известны успешные случаи атак на многие популярные системы защиты данных. Успех этих атак заключается не в том, что был изобретен новый быстрый алгоритм или суперкомпьютер, а в ошибках реализации криптосистем. Злоумышленники пользуются «дырами» не только в программной реализации систем, но и ошибками, допущенными при создании аппаратного обеспечения.

Развитие квантовых вычислений. Решение сложных вычислительных задач при помощи квантовых вычислений [8]. Идея использования квантовых вычислений впервые была высказана в 1980 году советским математиком Ю.И. Маниным в его монографии «Вычислимое и невычислимое». В 1982 году была опубликована статья на ту же тему американского физика-теоретика, нобелевского лауреата Ричарда Фейнмана. Он заметил, что определенные квантово-механические операции нельзя в точности переносить на классический компьютер. Это наблюдение привело его к мысли, что подобные вычисления могут быть более эффективными, если их осуществлять при помощи квантовых операций. С этого момента началось развитие квантовых вычислений и квантовых компьютеров.

В 1994 году американским ученым Питером Шором были разработаны алгоритмы факторизации чисел и вычисления дискретного логарифма. Алгоритм факторизации позволил разложить число на простые множители за время $O\left(\log^2 N \log^3(\log N)\right)$, используя $O(\log N))$ логических кубитов.

В 2001 году специалисты компании IBM и Стэндфордского университета реализовали алгоритм, предложенный Шором, на своем прототипе квантового компьютера. Несмотря на то, что в том эксперименте квантовый компьютер разложил на множители всего лишь двузначное число, реализация масштабируемого квантового компьютера может привести к непригодности алгоритма шифрования RSA и других алгоритмах, опирающихся на односторонние функции, входные значения которых легко вычисляются с помощью квантовых компьютеров. Например, факторизация 155-значного

числа (512 бит) на современном компьютере займет около 35 лет, квантовый же справится за пару минут.

Выводы. Проанализировав причины устойчивости криптосистем с открытым ключом к взломам, в частности, вычислительную сложность современных алгоритмов факторизации и вычисления дискретного логарифма, мы видим, что современные методы защиты данных весьма хороши для современного уровня компьютерных технологий. Они плохо поддаются взлому, так как вычислительная сложность алгоритмов, на которых они основаны, достаточно велика, исключая те случаи, когда допущены ошибки в реализации криптосистем. Однако развитие современных компьютерных технологий, таких как квантовых вычислений, может привести к тому, что криптосистемы с открытым ключом станут практически непригодными.

На смену классической криптографии, обоснование стойкости методов которой основано, как правило, на предположении о вычислительных способностях криптоаналитика, может прийти квантовая криптография, в которой перехватчик может применять любые допустимые законами природы методы, но все равно не сможет узнать секретный ключ.

Список литературы

1. Болотов А.А. Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы / А.А. Болотов, С.Б. Гашков, А.Б. Фролов, А.А. Часовских - М.: КомКнига, 2006. - 328 с.
2. Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си: пер. с англ. / Брюс Шнайер. – М.: Издательство «Триумф», 2002. - 816 с.
3. Гатчин Ю.А. Основы криптографических алгоритмов. Учебное пособие / Ю.А. Гатчин, А.Г. Коробейников - СПб.: СПбГИТМО(ТУ), 2002.
4. Ишмухаметов Ш.Т. Методы факторизации натуральных чисел: учебное пособие / Ш.Т. Ишмухаметов.– Казань: Казан. ун., 2011. - 190 с.
5. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии / О.Н. Василенко - М.: МЦНМО, 2003. - 328 с.
6. Мао. Современная криптография: теория и практика: пер. с англ. / Мао, Венбо - М.: Издательский дом «Вильямс», 2005. - 768 с.: ил. – Парал. тит. англ.
7. Н. П. Варновский. Введение в криптографию. Интернет-ресурс. - Режим доступа: www/ http://nature.web.ru/db/msg.html?mid=1157083&uri=node14.html-2(3):Односторонние функции.
8. Попов И.Ю. Квантовый компьютер и квантовые алгоритмы. Учебное пособие / И.Ю. Попов - СПб.: СПбГИТМО, 2007. - 88 с.