Раздел III
ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ И УПРАВЛЯЮЩИЕ СИСТЕМЫ (ПО ОТРАСЛЯМ), ИНФОРМАЦИОННЫЕ ПРОЦЕССЫ И РЕСУРСЫ

III. DATA MEASURING AND CONTROL SYSTEMS (BY BRANCHES), INFORMATION PROCESSES AND RESOURCES

УДК 004.056.53

К ВОПРОСУ О ПОВЫШЕНИИ ЭФФЕКТИВНОСТИ РАБОТЫ БАЗОВЫХ АЛГОРИТМОВ СИСТЕМЫ С ОТКРЫТЫМ КЛЮЧОМ

Е.К. Герасимова

Ключевые слова и фразы: защита информации; класс вероятностных алгоритмов; необратимые функции; программно-аппаратные средства; псевдослучайные числа; шифрование.

Аннотация: Дан анализ математических методов преобразования информации и их применения к шифрованию данных; разработке и реализации программного продукта, демонстрирующего работу этих алгоритмов при передаче данных. Актуальность данной разработки обусловлена постоянно повышающимся интересом к вопросам защиты информации, и в частности, анализу работы и применения криптосистемы RSA; сложностью теоретико-числовых алгоритмов и отсутствием достаточно эффективных методов их решения, лежащих в основе RSA.

1. Введение

Рассмотрим современные методы построения криптосистемы с открытым ключом, т.е. системы, которая не требует передачи ключа принимающему сообщение и даже сохранения в тайне самого метода шифрования.

Математическая идея построения одной из подобных систем, а именно системы с открытым ключом RSA, состоит в следующем. Процесс шифрования заключается в нахождении в кольце классов вычетов степеней тех чисел, которые биективно соответствуют элементам текста. Процесс дешифрования происходит аналогично, с той лишь разницей, что объектами возведений в степень являются числа, полученные в результате шифрования. Реализация этой идеи осуществляется поэтапно:

– выбирают два больших простых числа p, q;

– вычисляют их произведение $n = p \cdot q$;

– определяют нечетное целое число e, взаимно простое с числом

$$k = \varphi(n),$$

где $\varphi(\cdot)$ – функция Эйлера;

– определяют целое число d, являющееся обратным к элементу e в кольце Z_k;

– возводят в степень e элементы исходного текста (при шифровании);

– возводят в степень d элементы зашифрованного текста (при дешифровании).

Возведение в степень происходит в кольце Z_n, при этом число e называют открытым ключом, число d – закрытым ключом [3].

Суть состоит в том, что каждым адресатом информационной системы (**ИС**) генерируются два ключа e и d, связанные между собой по установленному правилу. Открытый ключ публикуется и доступен любому, кто желает послать сообщение адресату. Закрытый ключ сохраняется в тайне.

Исходный текст шифруется открытым ключом адресата и передается ему. Зашифрованный текст, в принципе, не может быть расшифрован тем же открытым ключом. Дешифрование сообщения возможно только с использованием закрытого ключа, который известен только самому адресату.

Иногда нет необходимости зашифровывать передаваемое сообщение, но нужно его скрепить электронной подписью. В этом случае текст шифруется закрытым ключом отправителя, и полученная цепочка символов прикрепляется к документу. Получатель с помощью открытого ключа отправителя расшифровывает подпись и сверяет ее с текстом.

2. Современные методы построения криптосистемы с открытым ключом

Все чаще теоретические исследования переходят в плоскость практической реализации. И становится очевидным, что за внешней простотой выстроенной схемы скрыты сложные алгоритмические и, как следствие, – сложные математические задачи:

– как проверить число на простоту;

– как построить простое число из заданного интервала;

– как проводить вычисления с большими числами;

– как вычислять огромные степени больших чисел;

– предложить быстрые алгоритмы для модулярной арифметики.

Задачи проверки на простоту и построения простого числа обычно решаются с использованием решета Эратосфена, критерия Вильсона. Но для больших чисел применение подобных методов практически лишено смысла.

В теории чисел показано, что вероятность того, что число порядка n будет простым, составляет $1/\ln n$. Следовательно, с увеличением n вероятность того, что найдено именно простое число уменьшается.

Хотя более двух тысяч лет назад Евклидом было доказано существование бесконечного множества простых чисел, все же на данный момент времени количество практически найденных простых чисел конечно, хотя тем не менее велико.

Например, количество простых чисел для ключа длиной 512 бит приблизительно составляет 10^{150}.

Сложность вычислений с большими числами состоит в том, что стандартное математическое обеспечение не позволяет перемножать, к примеру, числа размером по 65 десятичных знаков. Приходится использовать аппарат длинной арифметики, модулярной. Например, методы Карацубы и Офмана, Шенгане-Штрассена. Если используется ключ длиной k бит, то для операций по открытому ключу требуется $O(k^2)$ операций, по закрытому ключу – $O(k^3)$ операций, а для генерации новых ключей требуется $O(k^4)$ операций [2].

Не стоит использовать неслучайные ключи с целью легкости их запоминания. В серьезных ИС используются специальные аппаратные и программные методы генерации случайных ключей. Как правило, используют датчики псевдослучайных чисел (**ПСЧ**). Однако степень случайности их генерации должна быть достаточно высокой. Идеальными генераторами являются устройства на основе «натуральных» случайных процессов. Например, появились серийные образцы генерации ключей на основе белого радиошума. Другим случайным математическим объектом являются десятичные знаки иррациональных чисел, например π или e, которые вычисляются с помощью стандартных математических методов.

В ИС со средними требованиями защищенности вполне приемлемы программные генераторы ключей, которые вычисляют ПСЧ как сложную функцию от текущего времени и (или) числа, введенного пользователем.

Анализ современного состояния исследований в этом направлении требует отдельного обзора. «Борьба» ведется вокруг вопросов эффективности реализации алгоритмов на конкретной вычислительной базе.

Стоит сказать, что для некоторых задач, лежащих в основе преобразования информации, эффективные алгоритмы при шифровании вообще неизвестны. Иногда в таких случаях все же можно предположить последовательность действий, которая, «если повезет», быстро приводит к требуемому результату. Существует класс так называемых вероятностных алгоритмов, которые дают правильный результат, но имеют вероятностную оценку времени работы. Такие алгоритмы, если подобран удачный параметр, на практике работают достаточно эффективно, хотя и не имеют хороших оценок сложности.

3. Надежность системы RSA

Криптографические системы с открытым ключом используют так называемые необратимые или односторонние функции, обладающие тем свойством, что при заданном значении аргумента относительно просто вычислить значение функции, однако если известно значение функции, то нет простого пути для вычисления значения аргумента.

Множество классов необратимых функций и порождает все разнообразие систем с открытым ключом. Однако не всякая необратимая функция годится для использования в реальных информационных системах. При этом под необратимостью понимается практическая невозможность вычислить обратное значение, используя современные вычислительные средства за обозримый интервал времени.

Поэтому чтобы гарантировать надежную защиту информации, к системам с открытым ключом (**СОК**) предъявляются два важных и очевидных требования.

1. Преобразование исходного текста должно быть необратимым и исключать его восстановление на основе открытого ключа.

2. Определение закрытого ключа на основе открытого, также должно быть невозможным на современном технологическом уровне. При этом желательна точная нижняя оценка сложности (количества операций) раскрытия шифра.

Стойкость системы RSA основывается на секретности закрытого ключа. В системе RSA используется тот факт, что нахождение больших простых чисел в вычислительном отношении осуществляется легко, но разложение на множители произведения двух таких чисел практически невыполнимо. Доказано (теорема Рабина), что раскрытие шифра RSA эквивалентно такому разложению. Поэтому для любой длины ключа можно дать нижнюю оценку числа операций для раскрытия шифра, а с учетом производительности современных компьютеров оценить и необходимое на это время.

Надо отметить, что усовершенствование вычислительного оборудования само по себе не уменьшит стойкость криптосистемы RSA, если ключи будут иметь достаточную длину. Фактически же, совершенствование оборудования увеличивает стойкость криптосистемы.

Время выполнения наилучших из известных алгоритмов разложения при $n = 10^{100}$, на сегодняшний день, выходит за пределы современных технологических возможностей.

Возможность гарантированно оценить защищенность алгоритма RSA стала одной из причин популярности этой системы на фоне десятков других. Поэтому алгоритм RSA используется в банковских компьютерных сетях, особенно для работы с удаленными клиентами, при обслуживание кредитных карточек.

4. Проблема реализации методов защиты информации

Эта проблема имеет два аспекта:

– разработку средств, реализующих криптографические алгоритмы;

– методику использования этих средств.

Каждый из криптографических методов могут быть реализованы либо программным, либо аппаратным способом.

Возможность программной реализации обуславливается тем, что все методы криптографического преобразования формальны и могут быть представлены в виде конечной алгоритмической процедуры.

При аппаратной реализации все процедуры шифрования и дешифрования выполняются специальными электронными схемами. Наибольшее распространение получили модули, реализующие комбинированные методы.

Основным достоинством программных методов реализации защиты является их гибкость, т.е. возможность быстрого изменения алгоритмов шифрования.

Основным же недостатком программной реализации является существенно меньшее быстродействие по сравнению с аппаратными средствами (примерно в 10 раз) [1].

В последнее время стали появляться комбинированные средства шифрования, так называемые программно-аппаратные средства. В этом случае в компьютере используется своеобразный «криптографический сопроцессор» – вычислительное устройство, ориентированное на выполнение криптографических операций (сложение по модулю, сдвиг и т.д.). Меняя программное обеспечения для такого устройства, можно выбирать тот или иной метод шифрования. Такой метод объединяет в себе достоинства программных и аппаратных методов.

В рамках исследования была создана программа, предназначенная для демонстрации возможностей криптосистемы RSA. В ней реализованы базовые алгоритмы схемы RSA, основанные на современных методах решения сложных теоретико-числовых задач.

Для формирования ключей выполняются следующие шаги:

– генерируются два нечетных случайных числа p, q;

– последовательно проходят проверку полученные числа на простоту с помощью двух алгоритмов – Рабина и перебора делителей; если p, q не прошли проверки, то – возврат на первый шаг; успешно прошли оба алгоритма, то они перемножаются методом Карацубы;

– вычисляется значение функции Эйлера $\varphi(p \cdot q) = (p-1)(q-1)$;

– генерируется случайное нечетно натуральное число $e < \varphi(p \cdot q)$;

– проверяется взаимная простота e и $\varphi(p \cdot q)$ (на основе алгоритма Евклида); если $\text{НОД}(e, \varphi(p \cdot q)) \neq 1$, то e генерируется заново; если $\text{НОД}(e, \varphi(p \cdot q)) = 1$, то это число e фиксируем (открытый ключ);

– для нахождения закрытого ключа d в программе реализуется алгоритм отыскания целочисленного решения уравнения $d \cdot e - k \cdot \varphi(p \cdot q) = 1$.

Перед шифрованием устанавливается взаимно однозначное соответствие между символами исходного сообщения и международным стандартом кодовых таблиц UTF 16.

Алгоритм возведения: 1) кода в степень e в кольце классов вычетов Z_n , где $n = p \cdot q$ (при шифровании); 2) элементов зашифрованного сообщения в степень d в кольце Z_n (при дешифровании); реализуется на основе дихотомического метода, с использованием представления показателя степени в двоичной системе счисления, что позволяет существенно сократить число производимых операций.

Выполняемый тест Рабина является вероятностным. Это означает, что он использует датчик случайных чисел и, таким образом, работает недетерминировано. Для входного целого числа n тест Рабина может выдать один из следующих двух ответов: число является составным; не знаю.

В случае первого ответа число n действительно является составным, тест Рабина предъявляет доказательство этого факта. Второй ответ может быть выдан как для простого, так и для составного числа n. Однако для любого составного числа n вероятность второго ответа не превышает 1/4. Ценность теста Рабина состоит именно в неравенстве, ограничивающем сверху вероятность второго ответа для произвольного составного числа n.

Таким образом, если мы применим 100 раз тест Рабина к числу n и получим 100 ответов «не знаю», то можно с большой вероятностью утверждать, что число n простое. Более точно, вероятность получения ста ответов «не знаю» для составного числа n не превышает $(1/4)^{100}$, т.е. практически равна нулю. Тем не менее, тест Рабина не предъявляет доказательства того, что число n простое.

Существует алгоритм, доказывающий простоту, со сложностью $O(\ln^3 n)$, согласно которому необходимо провести тест Рабина со всеми числами $2 \le m < 70\ln^2 n$, а затем проверить, не является ли n степенью простого числа. Однако его правильность зависит от недоказанной в настоящее время гипотезы Римана.

Этот алгоритм, опираясь на недоказанный факт, в принципе может «соврать» в отношении доказательства простоты, хотя если тест Рабина говорит, что число составное, значит, так оно и есть. На практике он работает неплохо. В программе реализуется вероятностный алгоритм Рабина с 20 раундами (*Rounds*). Вероятность ошибки (то, что составное число будет названо простым) меньше $4^{(-Rounds)}$.

Метод умножения многозначных чисел, более эффективный, чем общеизвестный, предложил в 1962 году А.А. Карацуба. Обычный прием умножения двух $2n$-значных чисел легко сводится к четырем умножениям n-значных чисел, метод Карацубы позволяет обойтись только тремя умножениями n-значных чисел. Если записать $2n$-значное число в виде $A_n + 10^n B_n$, то легко проверить тождество

$$(A_n + 10^n B_n)(C_n + 10^n D_n) =$$

$$= A_n C_n (10^n + 1) + (D_n - C_n)(A_n - B_n)10^n + B_n D_n (10^{2n} + 10^n),$$

в правой части которого перемножить n-значные числа нужно лишь три раза.

При реализации алгоритма решения уравнения $de - k\varphi(pq) = 1$ относительно d и k число $\dfrac{e}{\varphi(pq)}$ обращается в конечную цепную дробь при помощи алгоритма Евклида, и d есть знаменатель предпоследней подходящей дроби.

В алгоритме, реализующем дихотомический метод возведения в степень, показатели степени представляются как $n = d_0 + d_1 2 + d_2 2^2 + ... + d_k 2^{k-1}$, при возведении некоторого числа m в степень n выполняется ряд последовательных умножений. Предварительно вычисляются степени 1, m, m^2, m^4,..., $m^{2^{k-1}}$, при этом достаточно выполнить $(k-1)$ умножений (возведений в квадрат). Затем некото-

рые из них перемножаются. Их не более $(k-1)$. Итак, для вычисления степени m^n потребуется не более $2(k-1)=2\lceil \log_2 n \rceil$ умножений (см. [4]).

Результатом работы созданной программы являются зашифрованные и расшифрованные сообщения.

Созданная программа позволяет продемонстрировать невозможность правильного дешифрования сообщения без знания закрытого ключа, т.е. в случае, когда дешифрование производит постороннее лицо. А также, в программе предусмотрена возможность открытия необходимых текстов, сообщений из файла, что удобно при передаче информации.

Пользователь сам может менять как числа p, q, так и открытый и закрытый ключи по своему усмотрению, генерировать их автоматически или вводить вручную. Только потом он должен опубликовать новый открытый ключ. Это позволяет добиваться бóльшей криптостойкости.

Возможными направлениями продолжения работы можно рассматривать расширение функциональности системы в части увеличения детализации управления элементами алгоритма шифрования, нахождение более эффективных методов построения, реализации и оценки оперативности базовых алгоритмов системы RSA.

Список литературы

1. Баричев, С. Криптография без секретов / С. Баричев. – М. : Горячая линия – Телеком, 2001. – 42 с.

2. Василенко, О.Н. Теоретико-числовые алгоритмы в криптографии / О.Н. Василенко. – М. : МЦНМО, 2003. – 328 с.

3. Нечаев, В.И. Элементы криптографии (Основы теории защиты информации) / В.И. Нечаев. – М. : Высшая школа, 1999. – 112 с.

4. Ноден, П. Алгебраическая алгоритмика / П. Ноден, К. Китте. – М. : Мир, 1999. – 720 с.

TO QUESTION ABOUT INCREASING OF EFFICIENCY OF WORKING BASE ALGORITHMS OF SYSTEM WITH OPEN SWITCH

E.K. Gerasimova

Key words and phrases: protection of information; class of probabilistic algorithms; inconvertible functions; fireware facilities; pseudorandom numbers; cryptooperation.

Abstract: The purpose of this study consists in analysis mathematical methods of the transformation to information and their using to cryptooperation data; the development and realization of the program product, demonstrating work these algorithms at data transmission. Urgency of this development is conditioned constantly increasing interest to questions of protection to information, and in particular, analysis of the work and use cryptosystem RSA; difficulty theorist-numeric algorithm and absence it is enough efficient methods of their decision, being the basis of RSA.