RSA CRYPTANALYSIS

Sinochkin D.V. (Russian Federation)
Email: Sinochkin432@scientifictext.ru

Sinochkin Denis Vadimovich – Student,
DEPARTMENT OF INFORMATICS AND COMPUTER SCIENCE,
DON STATE TECHNICAL UNIVERSITY, ROSTOV-ON-DON

Abstract: *this article is devoted to methods of cryptoanazil RSA cipher. The article describes the basic concepts used in cryptography, and also considers the very purpose of data encryption. Two main methods for hacking a cryptosystem are described: factorization and discrete logarithm, including their advantages and disadvantages. Two of the most simple RSA hacking techniques are considered, the necessary parameters for complicating cryptanalysis are indicated; the complexity of each algorithm is shown.*
Keywords: *cryptanalysis RSA, RSA, cipher, factorization, discrete logarithm.*

КРИПТОАНАЛИЗ RSA

Синочкин Д.В. (Российская Федерация)

Синочкин Денис Вадимович – студент,
факультет информатики и вычислительной техники,
Донской государственный технический университет, г. Ростов-на-Дону

Аннотация: *данная статья посвящена методам криптоаназила шифра RSA. В статье описаны основные понятия, используемые в криптографии, а также рассмотрена сама цель шифрования данных. Описаны два основных метода взлома криптосистемы: факторизация и дискретное логарифмирование, в том числе их преимущества и недостатки. Рассмотрены два наиболее простые в реализации метода взлома RSA, указаны необходимые параметры для того, чтобы злоумышленнику потребовалось больше времени и вычислительных ресурсов; приведена сложность каждого алгоритмов.*
Ключевые слова: *криптоанализ RSA, RSA, шифр, факторизация, дискретное логарифмирование.*

Введение. Шифрование - преобразование информации в невосприимчивый формат в целях сокрытия от неавторизованных лиц с предоставлением авторизованным пользователям доступа к ней [3, стр. 9]. Секретность данных основана не на тайном алгоритме, а на том, что ключ шифрования известен только доверенным лицам. Ключ – важнейший компонент шифра, отвечающий за выбор преобразования, применяемого для зашифрования конкретного сообщения [2, стр. 58].

В современном мире криптография находит множество различных применений: для передачи информации, она используется в сотовой связи, платном цифровом телевидении, при подключении к Wi-Fi и на транспорте для защиты билетов от подделок, и в банковских операциях, для электронного документооборота.

Обязательным этапом создания шифра считается изучение его уязвимости к различным известным атакам – криптоанализу [2].

Цель шифрования данных. Шифрование изначально использовалось только для передачи конфиденциальной информации. Однако впоследствии шифровать информацию начали с целью её хранения в ненадёжных источниках. Шифрование информации с целью её хранения применяется и сейчас, это позволяет избежать необходимости в физически защищённом хранилище. Шифрование направлено на достижение четырех основных целей:

1. Статическая защита информации, хранящейся на жестком диске компьютера или дискетах (шифрование файлов, фрагментов файлов или всего дискового пространства), исключает или серьезно затрудняет доступ к информации лицам, не владеющим паролем (ключом), т.е. защищает данные от постороннего доступа в отсутствие владельца информации.

2. Разделение прав и контроль доступа к данным. Пользователь может владеть своими личными данными, не доступными другим пользователям.

3. Защита отправляемых (передаваемых) данных через третьи лица, в том числе по электронной почте или в рамках локальной сети.

4. Идентификация подлинности (аутентификация) и контроль целостности переданных через третьи лица документов.

Атаки на RSA. Факторизация. Факторизацией натурального числа называется его разложение в произведение простых множителей. Существование и единственность (с точностью до порядка следования множителей) такого разложения следует из основной теоремы арифметики. В отличие от задачи распознавания простоты числа, факторизация предположительно является вычислительно сложной задачей. В настоящее время неизвестно, существует ли эффективный не квантовый алгоритм факторизации целых чисел. Однако доказательства того, что не существует решения этой задачи за полиномиальное время, также нет. Для больших чисел задача факторизации является вычислительно сложной и лежит в основе широко используемых алгоритмов.

Последние исследования показали, что решить задачу RSA может оказаться легче, чем разложить N на множители, но есть основания предполагать, что в общем случае задача RSA и задача разложения на множители имеют одинаковую сложность. Поэтому наиболее естественным способом решение задачи RSA является разложение N на множители. Самые эффективные алгоритмы фаторизации принадлежат к двум категориям. Первая – время выполнения зависит от размера N, числа, которое нужно разложить на множители, а зависимость от множителя p более слабая. Вторая – время выполнения зависит от размера p. Алгоритмы из обеих категорий эффективны и имеют большое значение. Тем не менее, для атаки на RSA с конкретным значением N только некоторые из них оказываются эффективными.

Задача дискретного логарифмирования. Дискретное логарифмирование — задача обращения функции g^x в некоторой конечной мультипликативной группе G. Наиболее часто задачу дискретного логарифмирования рассматривают в мультипликативной группе кольца вычетов или конечного поля, а также в группе точек эллиптической кривой над конечным полем. Эффективные алгоритмы для решения задачи дискретного логарифмирования в общем случае неизвестны. Задача нахождения дискретного логарифма лежит в основе вычислительной теории чисел, вычислительной алгебры и имеет большое значение для криптографии с открытым ключом. Задачу дискретного логарифмирования можно сформулировать как

$$\left\{ n \in Z_{>1}^{+}, x, y, k \in Z^{+}, y \equiv x^{k} (\mathrm{mod}\, n) \right\} \xrightarrow{\text{найти}} \{k\}. \qquad (1)$$

Как известно это вычислительно трудная задача, и безопасность некоторых хорошо известных криптосистем, таких как схема обмена ключами Диффи-Хелмана-Меркла, схема Эль-Гамаля, основываются на этом. Имея эффективный алгоритм дискретного логарифмирования, нарушитель может создать свой открытый текст M и использовать откытую информацию (e,N) для того, чтобы создать собственный шифротекст C, а затем с помощью алгоритма дискретного логарифмирования вычислить

$$d \equiv \log_{M^e} M (\mathrm{mod}\, N). \qquad (2)$$

Атака методом (p-1)-алгоритмом Полларда. Простые числа p и q в системе RSA необходимо также выбирать, исходя из тех соображений, чтобы p±1, q±1 имели по крайней мере один простой делитель, больший 10^{20}, в противном случае p можно эффективно найти, используя (p-1)-алгоритм Полларда.

Пусть N > 1 составное число. Следующий алгоритм с некоторой вероятностью возвращает нетривиальный делитель N.

1. Случайно выбрать a Є Z_n. Выбрать положительное целое k=НОК(1,2, …, B), для соответствующей границы B.
2. Вычислить $a_k \equiv a^k (\mathrm{mod}\ N)$.
3. Вычислить f=НОД(a_k-1,N).
4. Если 1<f<N, то f – делитель N, вывести f и перейти к шагу 6.
5. Иначе перейти к шагу 2 и выбрать новое a и k.
6. Завершить алгоритм.

Сложность алгоритма составляет O(B log B $(\log N)^2$) [1], так что алгоритм эффективен только при малом B.

Атака малых и больших шагов. Данная задача вычислительно трудная, и безопасность некоторых хорошо известных криптосистем основываются на этом.

Алгоритм заключается в следующем:

1. Вычислить s=√n.
2. Вычислить первую последовательность S, состоящую из пар (ya^r,r), r=1,2,…,s-1.
3. Вычислить последовательность T, состоящую из пар (a^{ts},ts), t=0,1,…,s
4. Найти соответствие пар и вычислить x=ts-rx, являющееся требуемым значением d.

Алгоритму необходима таблица с O(n) [1] записями. Для вычисления дискретного логарифма требуется O(√nlogn) [1] операций и память для O(√n) [1] элементов группы. Если порядок группы будет больше 10^{40}, алгоритм станет неэффективным.

Заключение. Деятельность практически любой российской компании сегодня связана с хранением и обработкой персональных данных различных категорий, к защите которых законодательством РФ выдвигается ряд требований. Для их выполнения руководство компании, прежде всего, сталкивается с необходимостью формирования модели угроз персональным данным и разработки на ее основе системы защиты персональных данных, в состав которой должно входить средство криптографической защиты информации.

Для того чтобы прочитать зашифрованную информацию, принимающей стороне необходимы ключ и дешифратор (устройство, реализующее алгоритм расшифровывания). Однако, с развитием криптоанализа, появились методики, позволяющие дешифровать закрытый текст без ключа. Они основаны на математическом анализе переданных данных.

Список литературы / References

1. *Сонг Ян*. Криптоанализ RSA. М.: Ижевск: НИЦ «Регулярная и хаотическая динамика», 2011. 312 с.
2. *Рябко Б.Я.* Криптографические методы защиты информации. // Учебное пособие для вузов, 2-е изд. М.: Горячая линия - Телеком, 2012. 229 с.
3. *Алферов А.П.* Основы криптографии: учебное пособие. М.: Гелиос АРВ, 2002. 480 с.

Список литературы на английском языке / References in English

1. *Song Yang*. Cryptanalytic Attacks on RSA. M.: Izhevsk: NIC «Reguljarnaja i haoticheskaja dinamika», 2011. 312 p.
2. *Rjabko B.Ja*. Cryptographic methods of information protection. // Textbook manual for universities, 2 ed. M.: Gorjachaja linija - Telecom, 2012. 229 p.
3. *Alferov A.P*. Fundamentals of cryptography. // A tutorial. M.: Helios ARV, 2002. 480 p.