Повышение эффективности децентрализованных алгоритмов обеспечения безопасности

Александр Мартынов, Дмитрий Николаев, Виктор Фомченко (Нижегородская обл.)

Предложены подходы к повышению эффективности децентрализованных алгоритмов обеспечения безопасности на основе алгоритма RSA. Проведено их сравнение с характеристиками алгоритма RSA. Выполнен анализ возможных воздействий, основанных на неправильном использовании алгоритма, а также воздействий, использующих метод факторизации параметра преобразования.

Введение

На сегодняшний день децентрализованные алгоритмы обеспечения безопасности, использующие асимметричное преобразование, т.е. преобразование с открытым и конфиденциальным параметрами, находят всё более широкое применение. Такие алгоритмы используются для реализации электронной цифровой подписи, распределения сессионных параметров и во многих других случаях.

Одним из наиболее часто используемых децентрализованных алгоритмов является алгоритм преобразования с открытым параметром RSA. Поскольку данный алгоритм используется повсеместно, то и аналитическим воздействиям он подвергается также очень часто. Следовательно, разработка модификаций данного алгоритма с целью использования более коротких параметров при той же криптографической стойкости либо улучшения его криптографических характеристик является актуальной задачей [1].

Целью работы являлась разработка модификаций алгоритма RSA с более качественными характеристиками и практическая реализация данных модификаций.

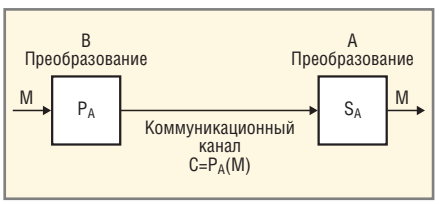

Рис. 1. Обобщённая схема преобразования и восстановления данных с использованием алгоритма RSA

Алгоритм RSA

В основу алгоритма с открытым параметром RSA положена задача умножения и разложения простых чисел на множители, которая является вычислительно однонаправленной задачей [2] (см. рис. 1).

Предположим, сторона B хочет послать стороне A сообщение M. Сообщением являются целые числа, лежащие от 0 до $n-1$, т.е $M \in D = Z_n$.

Алгоритм:

- взять открытый параметр (e, n) стороны A;
- взять исходный текст M;
- передать сообщение:

$$P_A(M) = M^e. \qquad (1)$$

Алгоритм:

- принять сообщение C;
- применить конфиденциальный параметр (d, n) для восстановления сообщения:

$$S_A(C) = C^d. \qquad (2)$$

Уравнения (1) и (2), на которых основана схема RSA, определяют взаимно обратные преобразования множества Z_n.

Доказательство.

Действительно, $\forall M \in Z_n$, $P(S(M)) = S(P(M)) = M^{ed} \bmod n$. Докажем, что $M^{ed} \equiv M (\mathrm{mod}\, p)$ $\forall M$.

Возможны два случая. Первый, когда $M \neq 0 (\mathrm{mod}\, p)$, тогда, поскольку числа e и d являются взаимно обратными относительно умножения по модулю, $\varphi(n) = (p-1)(q-1)$, т.е. $ed = 1 + k(p-1)(q-1)$ для некоторого целого k, следовательно,

$$M^{ed} \equiv M(M^{p-1})^{k(q-1)} (\mathrm{mod}\, p) \equiv \equiv M(1)^{k(q-1)} (\mathrm{mod}\, p) \equiv M (\mathrm{mod}\, p),$$

где второе тождество следует из теоремы Ферма.

И второй случай, когда $M \equiv 0 (\mathrm{mod}\, p)$, тогда $M^{ed} \equiv M (\mathrm{mod}\, p)$.

Таким образом, при всех M выполняется равенство $M^{ed} \equiv M (\mathrm{mod}\, p)$.

Аналогично можно показать, что $M^{ed} \equiv M (\mathrm{mod}\, q)$ $\forall$M. Таким образом, из Китайской теоремы об остатках следует, что $M^{ed} \equiv M (\mathrm{mod}\, n)$ $\forall$M.

Поскольку генерация параметров происходит значительно реже операций, реализующих преобразования, а также создание и проверку цифровой подписи, задача вычисления $a = b^e \bmod n$ представляет основную вычислительную сложность. Эта задача может быть решена с помощью алгоритма быстрого возведения в степень. Таким образом, для вычисления $M^e \bmod n$ требуется $O(\ln e)$ операций умножения по модулю.

Доказательство.

Представим e в двоичной системе счисления:

- $e = e_k \times 2^k + e_{k-1} \times 2^{k-1} + \ldots + e_1 \times 2 + e_0$, где $e_k = 1$, $e \in \{0, 1\}$;
- положим $M_0 = 1$;
- вычислим $M_i = M_{i-1}^2 M^{e_{k-i}}$ для $i = 1, \ldots, k$;
- найденное M_k и будет искомым значением M.

Поскольку каждое вычисление на шаге 2 требует не более трёх умножений по модулю n и этот шаг выполняется $k \le \log_2 e$ раз, то сложность алгоритма может быть оценена величиной $O(\ln e)$.

Чтобы проанализировать время выполнения операций с открытым и конфиденциальным параметрами, предположим, что открытый параметр (e, n) и конфиденциальный параметр (d, n) удовлетворяют соотношениям $\log_2 e = O(1)$, $\log_2 d \le \beta$. Тогда в процессах их применения будут выполнены соответственно $O(1)$ и $O(\beta)$ умножений по модулю.

Таким образом, время выполнения операций возрастает с увеличением количества ненулевых битов в двоичном представлении открытой экспоненты e. Чтобы увеличить скорость преобразования, значение e часто вы-

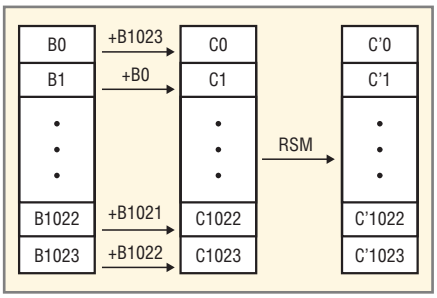

Рис. 2. Схема работы первой модификации алгоритма RSA

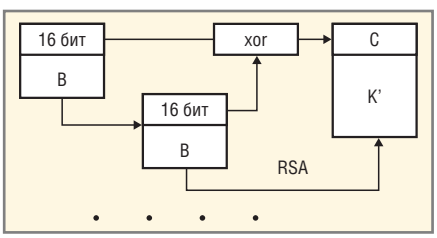

Рис. 3. Схема работы второй модификации алгоритма RSA

бирают равным 17, 257 или 65537 – простым числам, двоичное представление которых содержит лишь две единицы: $17 = 0 \times 11$, $257 = 0 \times 101$, $65537 = 0 \times 10001$ (простые числа Ферма).

По эвристическим оценкам, длина конфиденциальной экспоненты d, нетривиальным образом зависящей от открытой экспоненты e и модуля n, с большой вероятностью близка к длине n. Поэтому восстановление данных идёт медленнее, чем преобразование, а проверка подписи быстрее, чем сама подпись.

Размер параметра в алгоритме RSA связан с размером модуля n. Два числа p и q, произведением которых является модуль, должны иметь приблизительно одинаковую длину, поскольку в этом случае найти сомножители (факторы) сложнее, чем в случае, когда длина чисел значительно отличается.

Например, если предполагается использовать 768-битный модуль, то каждое число должно иметь длину приблизительно 384 бита. Если два числа чрезвычайно близки друг к другу или их разность близка к некоторому предопределенному значению, то возникает потенциальная угроза безопасности, однако такая вероятность – близость двух случайно выбранных чисел – незначительна.

Время преобразования файла объемом 700 Мб

Алгоритм	Время преобразования, с
RSA	215
Модификация № 1	270
Модификация № 2	165

Возьмём $M = (p + q)/2$. При $p < q$ имеем $0 \le M - n^{1/2} \le (q - p)^{2/8p}$. Поскольку $p = M(\pm(m^2 - n)^{1/2})$, то значения p и q можно легко найти, если разность $(p - q)$ достаточно мала.

Оптимальный размер модуля определяется требованиями безопасности: модуль большего размера обеспечивает большую безопасность, но замедляет работу алгоритма RSA. Длина модуля выбирается, в первую очередь, на основе значимости защищаемых данных и необходимой стойкости защищённых данных и, во вторую очередь, на основе оценки возможных угроз.

В математической основе предложенных модификаций лежит алгоритм преобразования RSA по 32-битному параметру. В дополнение к преобразованию блоков данных путём возведения в степень используются дополнительные меры для улучшения характеристик текста, а также для ускорения преобразования файлов [1].

Модификация № 1

Алгоритм работает следующим образом (см. рис. 2). Из файла, открытого в бинарном режиме, читаются 1024 блока по 16 бит (либо меньше в случае, если конец файла достигнут). Далее происходит перемешивание блоков с помощью побитовой операции «исключающее ИЛИ» (обозначим её символом ^): B1 = B1^B0, B2 = = B2^B1...B1023 = B1023^B1022, B0 = = B0^B1023. Затем каждый блок преобразуется по алгоритму RSA (в результате каждый блок из 16 бит преобразуется в блок данных из 32 бит, т.к. основание равно 32 битам), и результат записывается в новый файл.

Восстановление полученного файла происходит аналогичным образом, но в обратном порядке: из файла читаются 1024 блока данных по 4 бита, каждый блок восстанавливается конфиденциальным параметром RSA, в результате чего каждый блок преобразуется в 2-битный. Затем блоки перемешиваются в обратном порядке. В итоге получаем исходный файл.

Данный алгоритм работает дольше, чем RSA, но, вследствие перемешивания блоков данных, возможно, текст имеет более приемлемые характеристики, чем при преобразовании обычным RSA.

Модификация № 2

Алгоритм работает следующим образом (см. рис. 3). Из файла в двоичном режиме читаются блоки данных по 16 бит. Далее из считанного блока данных формируется основа параметра длиной 8 бит (берутся первые 4 бита и последние 4 бита). Полный параметр формируется из основы её дублированием (если основа параметра $k1$, то полный параметр представляет собой число $k1k1$, или $k1*256 + k1$). Далее идёт преобразование считанного блока данных с помощью операции «исключающее ИЛИ» (если прочитанный блок – X, а $k1k1$ – параметр, то блок S формируется как $S = X\hat{}k1k1$). Но, помимо записи в файл текста, идёт добавочная запись преобразованного по алгоритму RSA параметра $k1$. И, таким образом, преобразуются каждые считанные 16 бит данных.

Восстановление происходит в обратном порядке: считывается блок данных в 16 бит и параметр. Параметр декодируется по алгоритму RSA, и по полученному параметру находится исходный блок данных ($S\hat{}k1k1 = (X\hat{}k1k1)\hat{}k1k1 = X$). Операция повторяется для каждого считанного блока данных.

Данный алгоритм работает быстрее RSA, т.к. все операции занимают мало вычислительного времени, а непосредственно при преобразовании параметра в степень открытой (конфиденциальной) экспоненты возводится число не в 16 бит длиной, а только в 8 бит.

На основе реализованной программы было произведено сравнение времени преобразования файла большого объёма (порядка 700 Мб) тремя алгоритмами (RSA и его модификациям). Результаты представлены в таблице.

Как видно из таблицы, вторая модификация работает быстрее, чем алгоритм RSA, в то время как первая работает медленнее. Но первый алгоритм обеспечивает перемешивание блоков данных и, возможно, улучшает статистические характеристики текста. Проведённый анализ показал целесообразность дальнейшего исследования предложенных алгоритмов. В случае неудовлетворительных результатов возможно изменение предложенных алгоритмов.

Заключение

Были разработаны две модификации алгоритма RSA с параметрическими последовательностями в 32 бита, которые реализованы в программном обеспечении, преобразующем файлы

системы. Разработанные методы сравнивались по временной трудоёмкости (результаты представлены в таблице). По результатам сравнения, вторая модификация работает быстрее алгоритма RSA.

На основании проделанной работы можно сделать следующие выводы:

- алгоритм RSA подвержен множеству внешних воздействий, и для обеспечения конфиденциальности передаваемой информации необходимо использовать параметрическую информацию большого объёма;
- не во всех приложениях (аппаратных или программных) возможно использование параметров порядка 1024 бит и более, поэтому для решения подобных задач были разработаны модификации алгоритма RSA;
- при сравнении по временной трудоёмкости разработанные алгоритмы сопоставимы с RSA (вторая модификация работает быстрее), но для более глубокого анализа необходимо осуществить дальнейшие исследования их криптографических характеристик.

Литература

1. *Мартынов А.П., Фомченко В.Н.* Криптография и электроника. Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2006.
2. *Фомичев В.М.* Дискретная математика и криптология. ДИАЛОГ-МИФИ, 2003.

Новости мира News of the World Новости мира

Гибкий OLED-дисплей Sony накручивается на карандаш

Представители корпорации Sony на проходящем в эти дни в американском Сиэтле Международном симпозиуме SID 2010 (Society for Information Display) обнародовали информацию о перспективной разработке в области OLED-дисплеев. Продемонстрированный прототип представляет собой гибкую панель с диагональю 4,1 дюйма, разрешением 432 × 240 точек, контрастностью 1000 : 1, яркостью более 100 кд/м², и способностью отображать до 16 млн. цветов.

На первый взгляд кажется, что ничего революционного компания не продемонстрировала, ведь гибкие OLED-дисплеи известны нам ещё с 2007 г. Однако после просмотра видеоролика становится понятно, вокруг чего весь шум о новинке Sony.

Производитель сообщает, что показанный прототип можно скрутить в трубочку диаметром до 4 мм при сохранении его полной функциональности. В структуре панели применены тонкоплёночные органические транзисторы нового типа, размещённые на гибкой подложке, при этом толщина панели не превышает 80 нм. Для того чтобы поднять качество OLED-дисплеев на новый уровень, специалисты Sony разработали новый органический полупроводниковый материал, который является PXX-производным (peri-Xanthenoxanthene). В отличие от применявшихся ранее пентаценовых органических полупроводников, новый материал гораздо лучше противостоит воздействию кислорода, влаги, тепла и солнечного света и обладает в восемь раз лучшими модуляционными характеристиками. Впечатляющие показатели гибкости стали возможны благодаря тому, что необходимость в «жёстких» управляющих микросхемах отпала. Инженеры компании сообщают о том, что дисплей сохраняет возможность отображать видео даже после 1000 циклов сворачивания-растяжения.

Немаловажным является и то обстоятельство, что на производство гибких OLED-дисплеев Sony расходуется гораздо меньше энергоресурсов, что в свою очередь снижает количество выбросов в атмосферу. Это стало возможным благодаря применению органических диэлектриков, которые входят в структуру OLED-матрицы: в отличие от традиционных высокотемпературных полупроводниковых вакуумных процессов с применением кремния, производство новейших органических диэлектриков проходит при нормальных условиях, без воздействия высоких температур и давления.

В планы Sony входит работа по дальнейшему совершенствованию технологии производства органических дисплеев, результатом которой станет начало серийного выпуска гибких OLED-панелей для индустрии мобильных устройств, игровых консолей, телевизоров и т.д.

http://www.sony.net/

STMicroelectronics планирует перейти на 20-нм техпроцесс в 2012 г.

Швейцарская компания STMicroelectronics планирует перейти на 20-нм техпроцесс в четвёртом квартале 2012 г. Об этом сообщил её главный технолог Джин-Марк Чери (Jean-Marc Chery) в рамках ежегодного дня аналитики. Он не уточнил, будет ли STMicroelectronics лично разрабатывать новый технологический процесс на своей фабрике, которая находится во французском городе Кролле, неподалеку от Гренобля, или же обратится за помощью к сторонней исследовательской компании.

Эксперты предполагают, что первой в мире 20-нм техпроцесс освоит компания GlobalFoundries на фабрике в немецком городе Дрезден. Но возможно, новая технология будет разработана на заводе GlobalFoundries в Нью-Йорке, который в данный момент строится. Данное достижение стало бы хорошим началом работы нового подразделения GlobalFoundries.

В данный момент GlobalFoundries на дрезденской фабрике работает над освоение 22-нм техпроцесса, производство чипов на его основе будет первым заданием фабрики в Нью-Йорке.

http://www.eet.com/

Спрос на ЖК-панели достигнет минимума в июне

Согласно источникам из среды тайваньских производителей жидкокристаллических дисплеев, совокупный спрос и объёмы поставок TFT-LCD-панелей в текущем месяце достигнут нижнего предела. Сложившаяся ситуация связывается с низким спросом на рынках США и Китая, а также долговым кризисом в Европе.

Ожидается, что в июне цены на жидкокристаллические панели для мониторов упадут в среднем на $1–2.

Слабый спрос во втором квартале 2010 г. помог сократить дефицит поставок компонентов для LCD-панелей. Тем не менее, нехватка этих компонентов может вновь стать острой проблемой во второй половине года, когда начнётся пик сезона. Производственные мощности поставщиков компонентов для LCD до сих пор не могут полностью удовлетворить спрос.

http://www.digitimes.com/