ПРОБЛЕМА ФАКТОРИЗАЦИИ И КРИПТОГРАФИЧЕСКАЯ СИСТЕМА RSA

1 Проблема целочисленной факторизации

Безопасность многих криптосистем с открытым ключом базируется на трудности *проблемы факторизации* составного числа: пусть n – составное число, необходимо найти простое число p, $p|n$. Все известные алгоритмы факторизации (при подходяще выбранных составных числах) субэкспоненциальны.

1.1 *Po*-метод

Выбирается легко вычислимое отображение кольца Z_n в себя, например, описываемое полиномом $f(x) = x^2 + 1$.

Далее выбирается некоторый элемент $x_0 \in Z_n$ и выполняются итерации, в которых вычисляется последовательность $x_0, x_1, \ldots x_j,\ j = 1, 2, \ldots, x_j = f(x_{j-1})$

В каждой итерации проверяется, не сравнима ли разность текущего элемента последовательности с некоторым предыдущим элементом x_k по модулю некоторого делителя числа n. Для этого вычисляют НОД$(x_j - x_k, n)$ для каждого $k,\ 0 \le k \le j-1$. Если результат отличен от 1, то он и есть искомый делитель числа n.

Пример. Пусть $n = 91,\ x_0 = 1,\ f(x) = x^2 + 1$.

$x_1 = 2$, НОД$((x_1 - x_0, n) = 1$;

$x_2 = 5$, НОД(4,91)=НОД(3,91)=1;

$x_3 = 26$ НОД(25,91)=НОД(24,91)=1; НОД(21,91)=$7 \to 7|91$.

Здесь каждый элемент x_k участвует в вычислении многих НОД, а можно модифицировать метод так, чтобы он участвовал в вычислении единственного НОД.

Заметим, что если $x_{k'} \equiv x_{j'} (\mathrm{mod}\ r)$, то $k-j = k'-j' \to x_k \equiv x_j (\mathrm{mod}\ r)$. Чтобы убедиться в этом достаточно применить к элементам $x_{k'}$ и $x_{j'}$ преобразование $k - k'$ раз (мы полагаем, что $k' \le k$).

Последовательно вычисляем (или используем ранее вычисленное) x_k. Пусть k есть $h+1$-разрядное двоичное число и пусть уже вычислено $x_j,\ j = 2^{h+1} - 1$ – наибольшее h-разрядное двоичное число. Вычисляем НОД$(x_k - x_j, n)$, если он не равен 1, то он и есть искомый делитель числа n, иначе, переходим к следующему числу k.

Пример. Пусть $n = 91,\ f(x) = x^2+1,\ x_0 = 1$. Вычисляем $x_1 = 2,\ x_2 = 5,\ x_3 = 26,\ x_4 = 40$; НОД$(x_2 - x_1, 91) = 1$, НОД$(x_3 - x_1, 91) = 1$, НОД$(x_4 - x_3, 91) = 7$.

Ро-метод быстро находит малые множители.

2 Метод Ферма. Факторные базы

Теорема 1. *Пусть n – натуральное число. Существует взаимно-однозначное соответствие между факторизациями n в виде $n = ab, p \geq q > 2$, и представлениями числа n в виде $t^2 - s^2$, где s и t – неотрицательные целые числа, удовлетворяющие уравнениям*

$$t = \frac{p+q}{2},\ s = \frac{p-q}{2}, p = t + s,\ q = t - s.$$

Метод Ферма: начиная с $\lfloor\sqrt{n}\rfloor + 1$ найти наименьшее t, для которого $t^2 - n$ есть полный квадрат s^2 и вычислить множитель $p = t + s$.

Пример. $n = 200819$. Анализируем $t - \lfloor\sqrt{200819}\rfloor + 1 = 449$, $449^2 - 200819 = 782$ не есть полный квадрат. Далее пробуем $t = 450$: $450^2 - 200819 = 41^2$. Нашелся множитель $p = t+s = 450+41 = 491$. При этом $= t-s = 450-41 = 409$.

Метод работает долго, если $|p - q|$ велико. В такой ситуации полезно использовать малые k и вместо $\lfloor\sqrt{n}\rfloor + 1$, $\lfloor\sqrt{n}\rfloor + 2$, ... вычислять $\lfloor\sqrt{kn}\rfloor + 1$, $\lfloor\sqrt{kn}\rfloor + 2$, ..., пока не получим t, для которого $t^2 = kn = s^2$ для некоторого целого s. Тогда $(t + s)(t - s) = kn$, т.е. $t + s,\ t - s \in \{kp, kq, p, q\}$ и $t + s$ имеет с n общий нетривиальный делитель. Его можно найти как НОД$(t+s, n) \in \{p, q\}$.

Пример. Пусть $n = 141467$. Методом Ферма потребуется попробовать 38 значений t. Но если взять $k = 3$, то $t = \lfloor\sqrt{3 \cdot 141467}\rfloor + 1 = 652, \ldots, t = \lfloor\sqrt{3 \cdot 141467}\rfloor + 4 = 655$, $655^2 - 3 \cdot 141467 = 68^2$, НОД(655+68,141467)=241.

Дальнейшее обобщение метода Ферма приводит к методу факторных баз. В его основе следующая идея:

если удалось найти два числа t и s такие, что $t \not\equiv s \pmod n$ и $t^2 \equiv s^2 \pmod n$, то НОД$(s + t, n)$ есть нетривиальный делитель числа n.

Пример. Пусть $n = 4633$, заметим, что $118^2 \equiv 5^2 \pmod{4633} \rightarrow$ НОД(118+5,4633)=41|4633.

Вероятность удачного выбора мала и необходима большая свобода в выборе двух несравнимы по модулю n чисел, квадраты которых оказываются по модулю n сравнимыми. Для этого строят факторные базы и так называемые B-числа, связанные с понятием наименьшего абсолютного вычета по модулю n.

---

[0]Алгоритм вычисления целой части квадратного корня целого числа"

ВХОД: Неотрицательное натуральное число n.

ВЫХОД: Целая часть корня квадратного из n.

1. Присвоить $= n$, $Y = \frac{X+1}{2}$.
2. Если $X = 0$, вернуть 0.
3. Если $X = 1$ или $X = 2$, вернуть 1.
4. Иначе, пока X не равен Y и $Y - X$ не равно 1.
   4.1. Присвоить $X = Y$.
   4.2. Присвоить $Y = [(X + [n/(X)])/2]$.
5. Вернуть X.

Наименьшим абсолютным вычетом числа a по модулю n называется целое число в интервале от $-n/2$ до $n/2$, сравнимое с a по модулю n.

Факторной базой называется множество $B = \{p_1, \ldots, p_h, \}$ состоящее из простых чисел, кроме числа p_1, которое может быть равно -1. Квадрат числа b есть *B-число*, если наименьший абсолютный вычет числа b^2 по модулю n можно записать как произведение $\Pi_{i=1}^{h} p_i^{e_i}$ чисел из B.

Каждому B-числу b^2 можно сопоставить двоичный вектор $\varepsilon(b) = (\alpha_1, \alpha_2, \ldots \alpha_i, \ldots, \alpha_h)$, элементы α_i которого равны $e_i \bmod 2$, где e_i есть число сомножителей p_i в абсолютном вычете числа b^2 по модулю n, а также вектор $e(b) = (e_1, \ldots, e_n)$

Теперь числа t и s такие, что $t \not\equiv s (\mathrm{mod}\ n)$ и $t^2 \equiv s^2 \pmod{n}$, можно подобрать как

$$t = \Pi_{i \in \{1,\ldots,h\}} b_i,$$

$$\sum_{i \in \{1,\ldots,h\}} \varepsilon(b_i) = 0.$$

(произведение положительных квадратных корней b_i из B-чисел b_i^2, сумма двоичных векторов $\varepsilon(b)$ которых равна нулю). Число s можно получить как произведение $\Pi_{i=1}^{h} p_i^{e_i/2}$ степеней $p_i^{e_i/2}$ соответствующих элементов базы B.

Пример. Пусть $n = 4633$, возьмем факторную базу $B = \{-1, 2, 3, 5\}$. Квадраты чисел 68,69 и 96 суть B-числа: $68^2 \equiv -9 \pmod{4633}$, $-9 = -1^1 \cdot 2^0 \cdot 3^2 \cdot 5^0$;
$69^2 \equiv 128 \pmod{4633}$, $128 = -1^0 \cdot 2^7 \cdot 3^0 \cdot 5^0$
$96^2 \equiv -50 \pmod{4633}$, $-50 = -1^1 \cdot 2^1 \cdot 3^0 \cdot 5^2$;
$e(68) = (1, 0, 2, 0)$; $e(69) = (0, 7, 0, 0)$; $e(96) = (1, 1, 0, 2)$; $e = (2, 8, 2, 2)$.

Найдем $\varepsilon(68) = (1, 0, 0, 0)$, $\varepsilon(69) = (0, 1, 0, 0)$, $\varepsilon(96) = (1, 1, 0, 0)$.

Эти три вектора имеют нулевую сумму. Поэтому возьмем $t = 68 \cdot 69 \cdot 96$; $t \bmod 4533 = 1031$.

Соответственно вычислим $s = (-1) \cdot 2^4 \cdot 3 \cdot 5 = -240$. НОД(1031+240, 4533)=41.

Дальнейшим развитием был метод квадратичного решета Померанца.

Затем Ленстра разработал методы эллиптических кривых и числового поля.

3 Криптосистемы с открытым ключом

Криптосистемы с открытым ключом устроены таким образом, что зашифрование осуществляется с использованием публикуемого (через сервер авторизации) ключа k_3, а расшифрование производится с использованием секретного ключа k_p. При этом обеспечивается тождество

$$D_{k_p}(E_{k_3}(x)) = x.$$

Преобразования зашифрования E_{k_3} осуществляется за полиномиальное время. Преобразование расшифрования E_{k_p} также требует полиномиального времени, но при условии использования секретного ключа k_p.

Что же касается процесса дешифрования без знания k_p, то его осуществление связывается с решением трудной задачи теории чисел или теории других алгебраических структур, для которой неизвестны в настоящее время быстрые алгоритмы. Ключ k_p является "лазейкой,"с помощью которой легальный получатель может осуществить расшифрование.

Функции, используемые для зашифрования и обладающие тем свойством, что вычисление обратного преобразования не может быть осуществлено за полиномиальное время, получили название односторонних функций. Существование таких функций не доказано математически и основано на оценке самых быстрых известных алгоритмов для трудных задач.

Односторонние функции, имеющие "лазейки,"то есть допускающие полиномиальное инвертирование при использовании дополнительной секретной информации называются криптографическими.

Существование таких функций также не доказано, хотя криптография с открытым ключом основана на использовании ряда числовых или алгебраических функций в качестве криптографических.

Примерами таких функций являются модульное возведение в степень в конечном поле, умножение целых чисел и другие.

В отличие от симметричных классических систем ключ k_p при достаточно больших размерах не может быть вычислен по ключу k_3 за полиномиальное время (при современном уровне алгоритмической базы теории чисел и теории других алгебраических структур).

Принципиальная же возможность установления связи между k_3 и k_p имеется, в частности, она просто реализуется при малых параметрах. Поэтому в этом классе криптосистем отсутствуют совершенные (принципиально не вскрываемые) криптосистемы.

Криптосистемы с открытым ключом, обеспечивая возможность передачи ключа второму абоненту без использования закрытого канала (авторизация передачи осуществляется существенно проще, чем обеспечение конфиденциальности), обладают примерно в 1500 раз меньшим быстродействием. чем симметричные криптосистемы. Поэтому криптосистемы с открытым ключом используют, как правило, для передачи коротких сообщений, в частности, ключевой информации для симметричных криптосистем. Криптосистемы с открытым ключом на самом деле не являются безопасными, если не приняты специальные меры, гарантирующие их безопасность.

4 Криптосистема RSA.

Описываемая ниже система RSA ($Rivest - Shamir - Adleman$) основана на трудной проблеме разложения числа на простые множители, хотя не существует доказательства трудной разрешимости этой проблемы, как и доказательства того факта, что невозможен криптоанализ RSA без факторизации, а существу-

ют лишь эмпирические подтверждения этих фактов.

Абонент A системы RSA для обеспечения возможности передачи ему секретной информации на открытом ключе выбирает два случайных больших простых числа p и q и вычисляют значение функции Эйлера $\varphi(p \cdot q) = (p-1)(q-1)$ от их произведения $n = p \cdot q$. Далее абонент выбирает число e, $e > 1$, такое, что $(e, \varphi(n)) = 1$, и после этого вычисляют число d, обратное по модулю $\varphi(n)$ к этому числу e :

$$e \cdot d \equiv 1 \pmod{\varphi(n)}.$$

Числа n, e и d называются *модулем, экспонентой шифрования и расшифрования* соответственно. Числа n и e образуют *открытый ключ шифрования* и публикуются через центр сертификации открытых ключей.[1]. Остальные числа $p, q, \varphi(n)$ и d составляют секретную *лазейку* и сохраняются как секрет абонента A. (Эти числа взаимосвязаны и, зная одно из них, можно найти все остальные).

Любой отправитель B, получив от центра сертификации сертификат открытого ключа абонента A, имеет возможность зашифровать и безопасно передать абоненту A секретное сообщение в виде числа m, $0 < m < n$. (Более длинные сообщения предварительно разбиваются на блоки, последовательно шифруемые и передаваемые абоненту A). Алгоритм E_A зашифрования абонентом B имеющегося сообщения для абонента A заключаются в возведении в степень e по модулю n (то есть в кольце Z_n):

$$c = E_A(m) = m^e \bmod n,$$

где m и c – исходное открытое сообщение (шифрвеличина) и криптотекст (шифробозначение) соответственно.

Расшифрование осуществляется получателем A по алгоритму расшифрования D_A с использованием известного только ему секретного ключа d возведением шифробозначения c в степень d по модулю n :

$$m = D_A(c) = c^d \bmod n.$$

Каждый абонент сети имеет возможность вычислить и сертифицировать свой открытый ключ. Существенно, что простые числа p и q должны выбираться абонентами независимо друг от друга.

Таким образом, каждый абонент сети

[1]При этом абонент проходит аутентификацию некриптографического характера, предъявляет открытый ключ и криптографическим методом доказывает, что владеет соответствующим ему секретным ключом. При этом возможно использование протокола доказательства с нулевым разглашением секрета. Центр сертификации публикует открытый ключ данного абонента в составе сертификата открытого ключа за своей цифровой подписью, ключ проверки которой известен всем абонентам компьютерной сети. Использование сертифицированного открытого ключа гарантирует, что зашифрованная на этом ключе информация может быть расшифрована только владельцем соответствующего секретного ключа, имя которого указывается в сертификате открытого ключа

1. Выбирает большие простые числа p и q, примерно одного размера.

2. Вычисляет $n = pq$, $\varphi(n) = (p-1)(q-1)$ выбирает e, НОД$(e, \varphi(n)) = 1$, вычисляет $d = e^{-1} \bmod n$.

3. Объявляет через центр сертификации открытым ключом (n, e), секретным ключом является пара (p, q).

Абонент B зашифровывает сообщение m для стороны A, выполняя следующие действия:

1. Получить из центра сертификации сертификат открытого ключа стороны A и проверить цифровую подпись центра.

2. Представить сообщение m как целое в пределах $0, 1, \ldots, n-1$.

3. Вычислить $c = m^e \bmod n$.

4. Послать шифртекст c стороне A.

Абонент A расшифровывает сообщение, используя свой открытый ключ: $m = c^d \bmod n$.

Корректность процедур зашифрования и расшифрования мотивируется следующей леммой.

Лемма. *Пусть*

$$c \equiv m^e \pmod{n},$$

тогда

$$m \equiv c^d \pmod{n},$$

то есть, если расшифрование однозначно, то

$$m = c^d \bmod n.$$

Доказательство. Для любого целого m и любого простого p справедливо сравнение

$$m^p \equiv m (\bmod\ p).$$

Действительно, это сравнение равносильно сравнению

$$m^p - m \equiv 0 (\bmod\ p)$$

которое, в свою очередь, эквивалентно сравнению

$$m(m^{p-1} - 1) \equiv 0 (\bmod\ p).$$

Если НОД$(m, p) = p$, то есть p делит m, то $m \equiv 0 (\bmod\ p)$, а в случае НОД$(m, p) = 1$ по малой теорема Ферма $m^{p-1} - 1 \equiv 0 (\bmod\ p)$. Таким образом, указанные сравнения выполняются.

Заметим, что поскольку $e \cdot d \equiv 1 \pmod{\varphi(n)}$, имеется такое число j, что $e \cdot d = j \cdot \varphi(n) + 1$ и, следовательно,

$$m^{e \cdot d} = m^{j \cdot \varphi(n) + 1}.$$

Таким образом,

$$c^d = (m^e)^d = m^{ed} = m^{j\cdot\varphi(n)+1} = m^{j(p-1)(q-1)+1} =$$

$$m^{j\cdot p\cdot(q-1)} \cdot m^{-j\cdot q+j+1} = (m^p)^{j\cdot(q-1)} \cdot m^{-j\cdot q+j+1}.$$

С учетом доказанного выше сравнения $m^p \equiv m(\mathrm{mod}\ p)$ получаем сравнение [1]

$$(m^p)^{j\cdot(q-1)} \cdot m^{-j\cdot q+j+1} \equiv m^{j\cdot(q-1)} \cdot m^{-j\cdot q+j+1} \equiv m\ (\mathrm{mod}\ p).$$

То есть,

$$c^d \equiv m\ (\mathrm{mod}\ p) \qquad (4.1)$$

Аналогично получим, что

$$c^d \equiv m(\mathrm{mod}\ q). \qquad (4.2)$$

Поскольку p и q – простые числа, то по китайской теореме об остатках[2]) с учетом (4.1) и (4.2) получаем что

$$c^d \equiv m(\mathrm{mod}\ n).$$

(В рассматриваемом случае имеется система сравнений

$$x \equiv m \bmod p,$$

$$x \equiv m \bmod q,$$

где $x = c^d$. По китайской теореме об остатках

$$x = (m \cdot p^{-1} \bmod q \cdot p + m \cdot q^{-1} \bmod p \cdot q) \bmod n =$$

$$x = m \cdot (p^{-1} \bmod q \cdot p + q^{-1} \bmod p \cdot q) \bmod n =$$

$$m \cdot 1 \bmod n = m \bmod n.$$

Выше в круглых скобках имеем НОД(p,q)=1).

---

[2] Любое целое число, не превосходящее произведения взаимно простых натуральных чисел $m_1, m_2, \ldots, m_t$, можно однозначно восстановить по Китайской теореме об остатках, если известны его вычеты по этим модулям.

Китайская теорема об остатках. *Если модули m_i взаимно просты, то система сравнений*

$$x \equiv a_i\ (\mathrm{mod}\ m_1),\quad i = 1,\ \ldots,\ k,$$

имеет в интервале $[0, m-1]$, $m = m_1 \cdot m_2 \cdot \ldots \cdot m_t$ единственное решение x вида

$$x = \Sigma_{i=1}^{t} a_i \cdot N_i \cdot\ M_i(\mathrm{mod}\quad m),$$

где $M_i = \frac{m}{m_i}, N_i = (M_i)^{-1}(\mathrm{mod}\quad m_i), i = 1, \ldots, t.$

Таблица 1: Поиск нетривиального квадратного корня из 1.

s'	$2^{s'} \cdot 105$	$9^{2^{s'} \cdot 1575} \mod 9017$	$3^{2^{s'} \cdot 1575} \mod 9017$
4	25200	1	1
3	12600	1	1
2	6300	1	1
1	3150	1	1
0	1575	1	4190

Пример . Пусть выбраны простые числа $p = 73,\ q = 127$. Тогда $n = 9271,\ \varphi(n) = 72 \cdot 126 = 9072$. Выберем $e = 17$, тогда $d = 1601$. Оригинальный текст запишем, заменяя русские буквы их двузначными алфавитными номерами, начиная с 10, пробелы заменим на 42. Тогда неоднозначность расшифрования четырехзначных блоков исключается, так как модуль $n = 9271$ превышает наибольшее возможное число 4242, представляющее блок.

Упражнение 1. Покажите, что знание $\varphi(n)$ позволяет факторизовать $n = pq$. Указание. Решить систему уравнений

$$pq = n; (p-1)(q-1) = \varphi(n).$$

Упражнение 2. Покажите, что знание экспоненты расшифрования d позволяет факторизовать $n = pq$.

Указание. Знание d позволяет найти нетривиальный квадратный корень u из 1:

Пусть $ed - 1 = 2^s \cdot t$, где t нечетное.

Возьмем произвольное $w \in Z_n^*$ и для $s',\ 0 \le s' \le s$ вычислим $w^{2s' \cdot t} \mod n$. Если окажется, что для некоторого s' это число не равно ± 1, а $w^{2^{s'+1} \cdot t} \mod n = 1$, то $u = w^{2^{s'} \cdot t} \mod n$ и есть искомый квадратный корень. Теперь можно найти множитель числа n. Действительно, поскольку $u^2 \equiv 1 \pmod n$, число n делит $u^2 - 1$, но n не делит ни $(u+1)$, ни $u - 1$, значит $(u-1, n)|n$, как и $(u+1, n)|n$). В книге Саломаа показано, что вероятности успешного выбора числа w не менее $1/2$. Например, пусть $p = 127,\ q = 71$; $n = 9017,\ \varphi(n) = 8400$;

$e = 11;\ d = 2291;\ ed = 25201,\ ed - 1 = 25200 = 2^4 \cdot 1575$.

Выберем $w = 9$, что не позволит найти нетривиальный корень из 1, а затем выберем $w = 3$ и получим этот корень (см. Табл.2.) Получен нетривиальный корень $u = 4190$ из 1 по mod n.

Теперь найдем множитель (4190+1,9017)=(4191,9017)= 127 числа n

Упражнение 3. Покажите, что при одинаковых модулях n один участник В сети может узнать экспоненту расшифрования другого участника А, даже не прибегая к факторизации модуля.

Указание. Можно было бы сначала разложить n по предыдущему упражнению, но зная e_B, d_B, а также e_A можно найти b, такое, $e_A \cdot b \mod \varphi(n) = 1$

и использовать b в качестве экспоненты расшифрования d_A участника B и не прибегая к факторизации модуля n.

Такое b можно было бы найти посредством расширенного алгоритма Евклида из линейного соотношения

$$\alpha \cdot x + b \cdot e_A = 1,$$

где b положительно, если сначала найти α, которое кратно $\varphi(n)$ и взаимно просто с e_A. Такое число можно найти как $(e_B \cdot d_B - 1)/t$, где t – наибольшее число, делящее $(e_B \cdot d_B - 1)$ и имеющее с e_A нетривиальный (не равный e_A) множитель. Заметим, что $(e_B \cdot d_B - 1) = k \cdot \varphi(n)$, и, следовательно, $(e_B \cdot d_B - 1)/t = k\varphi(n)/t$ – целое, так как t делит $(e_B \cdot d_B - 1) = k \cdot \varphi(n)$. Число $\alpha = k\varphi(n)/t$ определим по итеративной схеме следующим образом.

Обозначим $g_0 = e_B d_B - 1,\ h_0 = (g_0, e_A)$, и определим индуктивно, для $i, i \geq 1$,

$$g_i = g_{i-1}/h_{i-1},\ h_i = (g_i, e_A).$$

Для $h_i \geq 2$ имеем $g_{i+1} \leq g_i/2$, поэтому $h_i = 1$ будет найдено за линейное число шагов, на каждом из которых используется алгоритм Евклида. Возьмем $\alpha = g_i$. По построению, $\alpha = k\varphi(n)/t$, где $t = h_1 h_2 \cdots h_i$ – максимальный нетривиальный множитель e_A, делящий также $e_B d_B - 1$. Пусть, например,$p = 31,\ q = 29,\ n = 899, \varphi(899) = 840$; $e_B = 11; d_B = 611$; $e_A = 13$. Найдем d_A, не используя секретные параметры.
Возьмем $g_0 = e_B d_B - 1 = 6720;\ h_0 = (6720, 13) = 1, h_0 = 1,\ i = 1 \to t = 1$;
Таким образом, $\alpha = g_0 = 6720$.
Вычислим $d_A = b$ по расширенному алгоритму Евклида из линейного соотношения

$$6720 \cdot x + b \cdot 13 = 1,$$

где 6720 есть значение α, а 13 – значение e_A, получаем $d_A = b = 517$. Проверим, что $e_A \times d_A \bmod 840 = 1$.

5 Особенности выбора параметров

Выбираемые простые числа p и q должны быть случайными и достаточно большими, но они не должны быть близкими друг к другу (различие длин их двоичных записей должно составлять несколько битов). В противном случае, если $(p-q)/2$ $(p > q)$ мало, то есть $(p+q)/2$ лишь немного превышает $\sqrt{n}$ легко найти оба эти числа: учитывая, что

$$\frac{(p+q)^2}{4} - n = \frac{(p-q)^2}{4},$$

то есть левая часть равенства образует полный квадрат, перебирая целые числа $x > \sqrt{n}$, найдем число x, такое, что $x^2 - n$ есть полный квадрат: $x^2 - n = y^2$. Тогда $p = x + y,\ q = x - y$.

Пример [2]. Если $n = 97343$, вычислим $\sqrt{n} = 311.988\ldots$. Сразу получаем $y^2 = 312^2 - n = 1$, откуда $p = 313,\ q = 311$.

Следующей рекомендацией является то, что НОД$(p-1, q-1)$ не должен быть большим (иначе НОК u этих чисел мало по сравнению с $\varphi(n)$ и любая инверсия числа e по модулю u будет работать как экспонента расшифрования и d легче найти простой проверкой, чем пытаться разложить n на множители, затем найти $\varphi(n)$ и вычислить d как обратное к e по модулю $\varphi\ (n)$.)

В частности, опасными являются также случаи, когда одно из чисел, например, $p-1$ делит другое $q-1$. Тогда экспоненту расшифрования можно найти среди инверсий экспоненты шифрования e по модулю $q-1$.

Пример 1.[2]. Пусть $n = 11041,\ p = 181, q = 61\ e = 4013,\ d = 6677$. Любая инверсия числа 4013 по модулю 180 может быть использована как экспонента расшифрования, так как НОК$(p-1, q-1) = 180$. Отсюда получаем $d' = 17$.

2. Пусть $p = 7,\ q = 127, \varphi = 756\ e = 5,\ d = 605$. Тогда $n = 889,\ p-1 = 6|q-1 = 126$, НОК(6,126)=126, $d' = 5^{-1} \bmod 126 = 101$.

$$m^{5\cdot 101} \equiv m \bmod 889.$$

Далее, в разложении $\varphi(n)$ на множители должны присутствовать не очень маленькие простые числа. Иначе перебором с большой вероятностью можно найти $\varphi(n)$ (см. [2]).

Две последние отмеченные неприятности можно преодолеть, если использовать только *безопасные* простые числа. Простое число p безопасно по определению, если $(p-1)/2$ также является простым числом. Примеры безопасных простых чисел: 83, 107, 10^{100}-166517 [2].

Еще одним методом криптографической атаки является метод "последовательного расшифрования "путем многократного шифрования: процесс начинается с полученного криптотекста c_0 и продолжается вычислением текстов $c_i \equiv c_{i-1}^e (\bmod\ n)$ до тех пор, пока не будет получен осмысленный текст. Вероятность успеха такой криптографической атаки мала, если числа $p-1,\ q-1,$ $p+1,\ q+1$ имеют большие множители $p',\ q'$ и, более того, числа $p'-1,\ q'-1$ также имеют большие простые множители. Такие простые числа называются *строгими.*

После выбора p и q выбирают d и e. Оба эти числа должны быть большими. При этом определенные экспоненты шифрования недопустимы. Например, если $e-1$ является кратным обоих чисел $p-1$ и $q-1$, то $E(m) = m$, что следует из теоремы Эйлера. В частности, особенно плохим является выбор $e = \varphi(n)/2 + 1$.

Экспонента зашифрования может быть малой, например, можно выбрать и $e = 3$. Но тогда необходимо "подсаливать"сообщение, чтобы избежать возможности простого (не модульного) извлечения кубического корня. Кроме того нельзя передавать одинаковые сообщения разным абонентам (по китайской теореме об остатках создаются условия для немодульного кубического корня).

Далее, нельзя использовать общий модуль, варьируя для абонентов сети только экспоненты e и d. Знание одной такой пары позволяет факторизовать n, применяя известный вероятностный алгоритм (см. упражнение 2), а также, зная открытый ключ другого участника по своей паре ключей найти секретный ключ этого другого участника даже и не прибегая к факторизации (см. упражнение 3).

Заметим также, что в каждой криптосистеме RSA некоторые блоки исходного сообщения при зашифровании не изменяются (переходят сами в себя). Существуют по крайней мере четыре блока, таких, что $E(m) = m,\ (m, n) = 1$ [2]. Такие исходные блоки можно вычислить заранее и предупредить или запретить их использование в реальной работе.

Пример [2]. Пусть $n = 55,\ p = 5,\ q = 11$. Имеем $\varphi(n) = 40$, выберем $e = 7,\ d = 23$. Нетрудно проверить, что $(m, 55) = 1,\ m^7 \equiv m$ (mod 55 для чисел $m \in \{1,\ 21,\ 34,\ 54\}$.

6 Работа RSA с составными псевдопростыми числами

Вероятность прохождения теста на простоту составным числом мала, но эта возможность должна быть исследована. Она либо практически не сказывается на безопасности RSA либо приводит к нарушению функционирования, которое выявляется при испытаниях,

Пусть $p = p_1 \cdot p_2$, где p_1 и p_2, как и q – простые числа. Тогда вместо функции Эйлера $\varphi(n) = (p_1 - 1) \cdot (p_2 - 1) \cdot (q - 1)$ в алгоритме RSA используется ложная функция $\varphi_1 = (p - 1) \cdot (q - 1)$. Обозначим u=НОК$((p_1 - 1), (p_2 - 1), (q - 1))$. Пусть также $(m, n) = 1$. Тогда по теореме Эйлера справедливы сравнения

$$m^{p_1-1} \equiv 1(\text{mod } p_1), m^{p_2-1} \equiv 1(\text{mod } p_2), m^{q-1} \equiv 1(\text{mod } q),$$

и сравнение $m^u \equiv 1$ имеет место для всех трёх модулей. Отсюда следует, что

$$m^u \equiv 1(\text{mod } n).$$

По определению, u делит $\varphi(n)$.

Если при этом u делит также $\varphi_1(n)$, то

$$m^{\varphi_1(n)+1} \equiv m(\text{mod } n),$$

откуда следует, что зашифрование и расшифрование выполняются так, как если бы p было простым числом.

Пример. [2] Пусть $p = 91 = 7 \cdot 13$, $q = 41$. Тогда

$$n = 3731,\ \varphi_1 = 3600,\ \varphi = 2880.$$

НОК(6,12,40)=120 делит число $\varphi_1(n) = 3600$.

Из этого следует, что если $(e, \varphi_1(n)) = 1$, то и $(e, \varphi(n)) = 1$. То есть по ложной функции $\varphi_1(n)$ можно вычислять d, для которого по-прежнему будет выполняться равенство $D(E(m)) = m$. Это не влияет на безопасность системы, кроме того, что наименьшее общее кратное будет значительно меньше $\varphi(n)$.

Если же u не делит $\varphi_1(n)$, то в большинстве случаев $D(E(m)) \neq m$, и это немедленно будет замечено при испытаниях.

Пример. [2] Пусть $p = 391 = 17 \cdot 23,\ q = 281$. Тогда

$$n = 109871,\ \varphi_1(n) = 109200,\ \varphi(n) = 98560.$$

В этом случае $u = 6160$, и u не делит $\varphi_1(n)$.

Если при этом выбрать $e = 19$ и вычислить $d = 45979$, для исходного текста $m = 8$ получим

$$m^{ed} = 95548 \pmod{109871.}$$

7 Электронная подпись в системе RSA

Протокол электронной подписи реализуется по принципам RSA следующим образом

1)Для передачи сообщения x банку B клиент A вычисляет

$$y = E_B(D_A(x)) = \{x^{d_A} \bmod n_A\}^{e_B} \bmod n_B$$

и пересылает результат к B.

2)В банке B вычисляют

$$D_B(y) = \{y^{d_B} \bmod n_B\} = x^{d_A} \bmod n_A = D_A(x);$$

$$x = E_A(y) = E_A(D_A(x)) = y^{e_A} \bmod n_A.$$

В упрощенном варианте сообщение x передается в открытом виде и сопровождается подписью $D_A(x) = x^{d_A} \bmod n$.

В обоих вариантах, однако, активный противник может прислать подписанное как бы абонентом A, но по содержанию неизвестное противнику сообщение: Таким сообщением может $x = E_A(c)$, сопровождаемое "подписью"$c = E_A(c)^d \bmod n = e^{ed} \bmod n$. Абонент A не сможет формально отказаться от того, что это не его сообщение и не его подпись, так как "подпись"c могла бы быть получена из "сообщения"$E_A(c)$, по мнению абонента B. Единственным аргументом в защиту A в этом случае является то, что с большой вероятностью "сообщение"$E_A(c)$ является бессмысленным (если оно содержит достаточно много символов). Например невозможно будет использовать этот аргумент,

если сообщение состоит из одного бинарного символа. Случай передачи подписанного засекреченного сообщения не более устойчив к подобному вмешательству активного противника, что выявляется аналогичным анализом. Таким образом, например, при передаче сообщений банку надо условиться о некоторой структуре таких сообщений, при которой, случайное сообщение с очень малой вероятностью соответствовало бы такой структуре. В частности, ни инверсия осмысленного (соответствующего такой структуре) сообщения, ни произведение осмысленных сообщений не должны быть осмысленными, иначе перехватчик, зная подписи $s_1 = D_A(c_1),\ s_2 = D_A(c_2)$ сможет получить подписи

$$D_A(c_1 \cdot c_2) = s_1 \cdot s_1 \bmod n_A, \quad D_A(c_1^{-1}) = s_1^{-1} \bmod n_A.$$

нарушение этого принципа позволяет применить метод адаптивной атаки по шифртексту. (См. [4, стр. 288-289]).

Один из вариантов этого метода следующий. Пусть криптоаналитик перехватил $c = m^e$ и желает узнать m.

Он может выбрать случайное число x и получить $y = x^e \bmod n$. Он возьмет также $r = x^{-1} \bmod n$.

Далее он просит отправителя криптограммы c подписать сообщение yc и получает $(yc)^d \equiv x^{ed}m^{ed} \equiv xm \pmod n$. Теперь он может узнать $m \equiv rxm \equiv x^{-1}xm \pmod n$.)

Пример . Пусть выбраны простые числа $p = 73,\ q = 127$. Тогда $n = 9271$. Пусть опубликовано $e = 17$ и перехвачена криптограмма 2306.

Пусть случайно выбрано $x = 2218$ и вычислено $y = x^{17} \bmod 9271 = 5489$, $r = x^{-1} \bmod 9271 = 790$.

Далее вычисляем $y \cdot c \bmod n = 5489 \cdot 2306 = \bmod 9271 = 2719$. Получаем подпись $s = 2719^d \bmod 9271 = 7515$.

Снимаем маску $m = s \cdot r \bmod n = 7515 \cdot 790 \bmod 9271 = 3410$.

Этот метод атака основан на *мультипликативном свойстве* RSA:

если $m = m_1 m_2$, то $c = m^e = m_1^e m_2^e = c_1 c_2 \bmod n$.

На этом свойстве основана атака встречей по середине (meet-in-the-middle attack).

Пример. Пусть $c = m^e \pmod{\text{n}}$ и атакующему известно, что $m < 2^l$. С не исчезающей вероятностью m является составным числом, таким, что

$$m = m_1 m_2,\ m_1 < 2^{l/2},\ m_2 < 2^{l/2}.$$

При этом по мультипликативному свойству RSA

$$m^e = m_1^e m_2^e, .$$

Атакующий создает отсортированную базу данных

$$\{1^e, 2^e, 3^e, \ldots, (2^{l/2})^e\} \bmod n.$$

Затем он пытается найти в этой базе элемент i^e, такой, что

$$c/i^e \equiv j^e \ (\bmod n).$$

8 Контрольные вопросы

1. Как обеспечить безопасность зашифрования при использовании малой экспоненты зашифрования?

2. Почему недопустимо использование одинаковых модулей при выборе параметров криптосистем RSA различными абонентами компьютерной сети?

3. Каковы последствия использования составного числа вместо простого при формировании параметров криптосистемы RSA.

4. Каковы ограничения на выбор простых чисел p и q при формировании параметров криптосистемы RSA?

5. В чем состоят предостережения при использовании цифровой подписи RSA?

Литература

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. – М.: Гелиос АРВ. 2001.

2. Саломаа А. Криптография с открытым ключом. – М: Мир, 1996.

3. Коутинхо С. Введение в теорию чисел. Алгоритм RSA. М.: Постмаркет. 2001.

4. Menezes A, van P. Oorschot, Vanstone S. Handbook of Applied Cryptography. CRC Press. 1997.