ЛЕКЦИЯ 5

КРИПТОГРАФИЯ С ОТКРЫТЫМ КЛЮЧОМ

Продемонстрируем, как изложенные выше факты из теории чисел используются в современной криптографии с открытым ключом. Кстати, заметим, что фактически новый подход в современной криптографии использует результаты теории чисел, которые были доказаны до 1760года. Идея криптографии с открытыми ключами была опубликована в 1976году в работе Диффи и Хеллмана «Новые направления в криптографии». Эта идея базируется на построении функции F, при помощи которой, зная значение аргумента x, можно эффективно вычислить

$$y = F(x).$$

В то же время по значению y невозможно за приемлемый промежуток времени решить обратную задачу, т. е. по y определить аргумент x. Функции с такими свойствами называются односторонними.

Определение. Функция F: $X \to Y$ называется односторонней, если она обладает двумя свойствами:

- существует полиномиальный алгоритм вычисления значения $y = F(x)$;
- не существует полиномиального алгоритма для решения обратной задачи, т. е. определения значения x по y.

Решение обратной задачи для односторонней функции одинаково невыполнимо как для санкционированного, так и несанкционированного решения. Для разрешения данной коллизии Диффи и Хеллман ввели понятие односторонней функции с секретом (*one-way trapdoor function*).

Определение. Функция

$$FK : X \to Y,$$

которая зависит от параметра K, называется

односторонней с секретом K, если она обладает тремя свойствами

- при любом параметре K существует полиномиальный алгоритм вычисления значения

$$y = FK(x);$$

- при неизвестном K не существует полиномиального алгоритма для решения обратной задачи, т. е. определения значения x по y;
- при известном K существует полиномиальный алгоритм для решения обратной задачи, т. е. определения значения x по y.

Решение обратной задачи для односторонней функции с секретом становится выполнимой для санкционированного решения, но невыполнимо для несанкционированного решения.

Для практических целей в криптографии при построении функций, которые исполняют роль односторонних, используют сложные задачи из теории чисел, например, следующие:

- Разложить на множители число n.
- Определить, является ли число n простым.
- Найти простое число больше n.
- Найти число x из уравнения

$$x^2 \equiv a \bmod n.$$

- Найти число x из уравнения

$$ax \equiv b \bmod n.$$

В последнее время развиваются криптографические методы с открытыми ключами, которые базируются на теории эллиптических кривых. Суть криптографии с открытым ключом заключается в следующем. В криптографической системе существуют два разных ключа. Расшифровать и зашифровать может только тот, кто владеет этими двумя ключами. При таком подходе

можно разрабатывать различные схемы использования открытых ключей, например, следующие:

■ есть пользователь, который владеет двумя ключами;

■ нет пользователей, которые владеют одновременно двумя ключами.

В зависимости от разработанной схемы можно выполнять различные криптографические процедуры: аутентификацию, электронную подпись, формирование общего ключа, криптографические протоколы. Данные процедуры в свою очередь решают различные задачи, связанные с обменом информацией и т. д. В предложенных выше схемах с открытыми ключами в качестве примера их использования будут предлагаться алгоритмы цифровой подписи и аутентификации. Определим данные понятия.

Аутентификация – процедура (функция) проверки подлинности. Аутентификация может относиться ко всем аспектам взаимодействия при передаче информации – сеансу связи, передаваемому сообщению, источнику сообщения и т. д.

Электронная цифровая подпись (**ЭЦП**) – процедура, которая обеспечивает невозможность отказа от переданного и подписанного сообщения.

Справедливости ради следует заметить, что первые результаты по криптографии с открытым ключом были ранее получены британскими учеными, но они не были опубликованы [4].

Криптосистема *RSA*

Алгоритм *RSA* является первым алгоритмом шифрования с открытым ключом. Название системы *RSA* происходит от первых букв фамилий ее авторов – Р. Ривест, А. Шамир и Л. Адлеман. Система базируется на следующих фактах:

■ при известных числах d и b вычисление числа a из сравнения

$$a \equiv b^d \bmod n$$

по составному модулю n – это простая задача;

■ вычисление неизвестного числа b при известных числах d и a из сравнения по составному модулю n

$$a \equiv b^d \bmod n$$

является трудной задачей;

■ если известно, что p и q простые числа и $n = pq$, то вычислить n легко, а найти разложение n на простые множители трудно;

■ если известно разложение $n = pq$ на простые множители, то задача вычисления числа b из уравнения

$$A \equiv b^d \bmod n$$

выполнима.

Теоретической основой криптосистемы *RSA* является теорема Эйлера из теории чисел. Напомним ее.

Теорема (Эйлера). Для любых натуральных и взаимно простых чисел n и a справедливо равенство

$$a^{\varphi(n)} \equiv 1 \bmod n.$$

Здесь $\varphi(n)$ есть функция Эйлера – количество взаимно простых с n натуральных чисел от 1 до n.

Из теории чисел известно, что если p и q простые числа, а $n = pq$, то

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

Кроме того, из теоремы Эйлера следует, что если некоторое число e взаимно просто с $\varphi(n)$, то уравнение

$$de \equiv 1 \bmod \varphi(n),$$

или иначе

$$de = k\,\varphi(n) + 1,$$

однозначно разрешается относительно d. Решение легко определяется расширенным алгоритмом Евклида.

Итак, если известно, что

$$de \equiv 1 \bmod \varphi(n),$$

а x – передаваемая информация, то справедливо равенство

$$(x^e)^d \bmod n \equiv (x^{k\varphi(n)+1}) \bmod n \equiv$$
$$\equiv (x^{\varphi(n)})^k x \bmod n \equiv x.$$

Фактически, последнее соотношение является основой для формулировки системы *RSA*.

Формирование системы *RSA*

1. Выбираем два различных простых числа p и q.
2. Вычисляем $n = pq$ и

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

3. Выбираем число e, взаимно простое с $\varphi(n)$.
4. Вычисляем число d из уравнения

$$de \equiv 1 \ mod \ \varphi(n).$$

5. Определяем открытые ключи e и n.
6. Определяем закрытые ключи d, p, q и $\varphi(n)$.

Алгоритм шифрования

1. Дан текст сообщения M.

Шифротекст C вычисляется по формуле

$$C = E_k(M) = M^e \bmod n.$$

Алгоритм дешифрования

1. Дан шифротекст C.
2. Текст сообщения M вычисляется по формуле

$$M = D_k(C) = C^d \bmod n = (M^e)^d \bmod n = M.$$

Цифровая подпись

1. Есть абонент A и текст для подписи M.
2. Определяются закрытые ключи системы RSA, а именно d, p, q и $\varphi(n)$.
3. Определяются открытые ключи e и n.
4. Закрытым ключом вычисляется

$$C = M^d \bmod n.$$

Сообщение C рассматривается как подпись абонента A, потому что закрытый ключ d известен только ему.

5. Проверка подписанного документа вычисляется по формуле

$$C^e = (M^d)^e \bmod n = M,$$

используя открытый ключ e.

Замечание. Схема подписи усложняется, если абоненты A и B имеют систему RSA с эксклюзивными модулями n_A и n_B соответственно. Если абонент A желает свое подписанное сообщение

$$C = M^d \bmod n_A$$

зашифровать открытым ключом абонента B, т. е. вычислить

$$C_1 = C^{e\beta} \bmod n_B,$$

чтобы M было доступно только абоненту B, то значение

$$C1^{d_B} \bmod n_B$$

не всегда будет равно сообщению

$$C = M^{d} \bmod n_A.$$

Для этого необходимо выполнение неравенства $n_A < n_B$. Чтобы в подобном режиме пересылки информации разрешить представленную коллизию, пользователям надо договориться о некотором пороге T и создавать два набора параметров – один с модулем меньшим T, другой с модулем большим T. В этом случае отправитель использует свой меньший модуль для подписи, а больший модуль получателя – для шифрования [5].

Пример [6]. Зашифруем аббревиатуру *RSA*. Пусть $p = 17$ и $q = 31$. Тогда $n = pq = 527$, причем имеет место

$$\varphi(n) = (p - 1)(q - 1) = 480.$$

Выберем число $e = 7$, взаимно простое с $\varphi(n)$. Решая уравнение

$$de \equiv 1 \bmod \varphi(n)$$

относительно d с помощью алгоритма Евклида, найдем число $d = 343$. Поскольку $-137 = 343 \bmod 480$, то выполняется равенство $d = 343$. Проверка:

$$7 \bullet 343 = 2401 \equiv 1 \bmod 480.$$

Представим сообщение *RSA* в виде последовательности чисел, содержащихся в интервале [0, 526]. Для этого буквы *R*, *S* и *A* закодируем пятимерными двоичными векторами, воспользовавшись двоичной записью их порядковых номеров в английском алфавите

$$R = 18 = (10010),\ S = 19 = (10011),$$
$$A = 1 = (00001).$$

Тогда

$$RSA = (100101001100001).$$

Укладываясь в заданный интервал [0, 526], получаем представление кода

$$RSA = (100101001), (100001) = (M_1 = 297, M_2 = 33).$$

Далее последовательно шифруем M_1 и M_2

$$C_1 = E_к(M_1) = M_1^e \equiv 2977 \bmod 527 = 474.$$

При этом мы воспользовались тем, что

$$297\ 7 = ((297\ 2)3\ 297) \bmod 527 =$$
$$= (200\ 3\ (\bmod 527)\ 297) \bmod 527,$$
$$C_2 = E_к\ (M_2) = M_2^e \equiv 33^7 \bmod 527 = 407.$$

В итоге получаем шифртекст $y_1 = 474$ и $y_2 = 407$.

При расшифровывании нужно выполнить определенную последовательность действий. Вычислить

$$D_k\ (C_1)^{343} = (C_1)^{343} \bmod 527.$$

Отметим, что при возведении в степень удобно воспользоваться тем, что

$$343 = 256 + 64 + 16 + 4 + 2 + 1.$$

На основании этого представления получаем

$$474\ 2 \equiv 174 \bmod 527,\ 474\ 4 \bmod 527 \equiv 237,$$
$$474\ 8 \bmod 527 \equiv 307,\ 474\ 16 \bmod 527 \equiv 443,$$
$$474\ 32 \bmod 527 \equiv 205,\ 474\ 64 \bmod 527 \equiv 392,$$
$$474\ 128 \bmod 527) \equiv 307,\ 474\ 256 \bmod 527 \equiv 443,$$

в силу чего имеет место

$$474^{343} \bmod 527 \equiv$$
$$\equiv (443 \bullet 392 \bullet 443 \bullet 237 \bullet 174 \bullet 474) \bmod 527 \equiv 297.$$

Аналогично

$$407^{343} \bmod 527 \equiv 33.$$

Возвращаясь к буквенной записи, получаем после расшифровывания *RSA*.

Следуя [6], проанализируем вопрос о стойкости системы *RSA*. Можно показать, что сложность нахождения секретного ключа системы *RSA* определяется сложностью разложения числа n на простые множители. В связи с этим нужно выбирать числа p и q таким образом, чтобы задача разложения числа n была достаточно сложна в вычислительном плане. Для этого рекомендуются выполнять следующие требования:

1) числа p и q должны быть достаточно большими, не слишком сильно отличаться друг от друга и в то же время быть не очень близкими друг другу;

2) числа p и q должны быть такими, чтобы наибольший общий делитель чисел $(p - 1)$ и $(q - 1)$ был небольшим; желательно, чтобы наибольший общий делитель имел вид $(p - 1, q - 1) = 2$;

3) числа p и q должны быть сильно простыми числами.

Определение [7]**.** Простое число p называется **сильно простым**, если выполняются условия:

$$p \equiv 1 \bmod r,$$
$$p \equiv s - 1 \bmod s,$$
$$r \equiv 1 \bmod t,$$

где p, r, s, t – большие простые числа.

Когда не выполнено хотя бы одно из указанных условий, имеются эффективные алгоритмы разложения n на простые множители (см., например [8 – 9]).

В настоящее время самые большие простые числа вида $n = p \cdot q$, которые удается разложить на множители известными методами, содержат в своей записи 140 десятичных знака. Поэтому согласно указанным рекомендациям числа p и q в системе *RSA* должны содержать не менее 100 десятичных знаков.

Следует подчеркнуть необходимость соблюдения осторожности в выборе модуля *RSA* (числа *n*) для каждого из корреспондентов сети. Читатель может самостоятельно убедиться в том, что, зная одну из трех величин p, q или $\varphi(n)$, можно легко найти секретный ключ *RSA*. Известно также, что, зная секретную экспоненту расшифровывания d, можно легко разложить модуль n на множители. В этом случае удается построить вероятностный алгоритм разложения n. Отсюда следует, что каждый корреспондент сети, в которой для шифрования используется система *RSA*, должен иметь свой уникальный модуль.

В самом деле, если в сети используется единый для всех модуль n, то такая организация связи не обеспечивает конфиденциальности, несмотря на то, что базовая система *RSA* может быть стойкой. Другими словами, говорят о несостоятельности протокола с общим модулем. Несостоятельность следует из того, что знание произвольной пары экспонент (e_i, d_i) позволяет, как было отмечено, разложить n на множители. Поэтому любой корреспондент данной сети имеет возможность найти секретный ключ любого другого корреспондента. Более того, это можно сделать даже без разложения n на множители (см., например [8]).

Как отмечалось ранее, системы шифрования с открытыми ключами работают сравнительно медленно. Для повышения скорости шифрования *RSA* на практике используют малую экспоненту зашифровывания e [6].