ПРОБЛЕМЫ ДЕШИФРОВАНИЯ В КРИПТОСИСТЕМЕ РАБИНА

Болтак С. В. , Деренчук В.И.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Ярмолик В.Н. – д.т.н., профессор

В работе рассматривается алгоритм шифрования Рабина и предлагается способ выбора верного корня из четырёх, полученных при дешифровании.

Шифр Рабина относится к криптосистемам с открытым ключом или как ещё их называют - асимметричным криптосистемам. Алгоритмы получили такое название, так как в отличие от классических, шифрование осуществляется одним ключом, обычно его называют открытым или публичным, а дешифрование другим, секретным или закрытым ключом. Данный алгоритм явился результатом переосмысления криптосистемы RSA и был опубликован в 1979 году Майклом О. Рабином как часть цифровой подписи [1]. В своей работе Рабин впервые привёл доказательство стойкости криптосистем с открытым ключом, которая эквивалентна неразрешимости задачи факторизации числа N. В системе Рабина шифрование происходит быстрее чем в других алгоритмах с открытым ключом, поэтому её можно эффективно использовать во многих прикладных приложениях.

Для генерации пары открытый - закрытый ключ необходимо выполнить следующие шаги:

1. Выбрать два случайных простых числа p и q. При этом $p \approx q$ и $p \equiv q \equiv 3 \bmod 4$.
2. Вычислить $n = p \cdot q$.
3. Выбрать случайное число $b < n$.

Открытый ключ - n и b, закрытый - числа p и q.

Прежде чем шифровать сообщение M, его необходимо разбить на блоки $m_1, m_2, m_3.$, $(0 \le m_i \le n-1)$. Процедура шифрования имеет следующий вид:

$$c_i = m_i(m_i + b) \bmod n. \quad (1)$$

Для того, чтобы расшифровать сообщение, необходимо решить квадратное уравнение вида $m_i^2 + b \cdot m_i - c_i = 0 \pmod n$. Для извлечение квадратного корня из дискриминанта используется китайская теорема об остатках. В результате вычисляются четыре результата, что является проблемой криптосистемы Рабина, так как неизвестно, какой из четырёх результатов соответствует исходному сообщению. Особенно, если исходное сообщение - это поток случайных битов.

Один из вариантов решения проблемы - добавление к сообщению известного заголовка перед шифрованием. Ещё один способ выбрать правильный корень - например, продублировать последние биты сообщения. С высокой долей вероятности только один из четырёх корней будет содержать продублированные биты [2]. Однако, добавлять избыточность придётся для каждого шифруемого блока.

Способ выбора корректного корня, предлагаемый в данной работе, подходит для расшифровки файлов с любым содержимым. Это может быть как текстовое сообщение так и любой случайный поток битов. Предлагается рассматривать шифруемое сообщение как поток байтов. Байт может принимать значения от 0 до 255, то есть шифруются числа в этом промежутке. При дешифровании при больших p и q только один из четырёх корней будет лежать в данном диапазоне (таблица 1).

Таблица 1 – Поиск корректного корня в криптосистеме Рабина.

№	p, q, b	Искомые корни
1	p = 523, q = 3 b = 1	1551, **17**, 540, 1028
2	p = 5003, q = 5227 b = 1234	26149430, **17**, 495314, 25654133
3	p = 523, q = 3 b = 2	**17**, 1550, 1550, **17**

Как видно из таблицы, в нужном диапазоне могут лежать два одинаковых числа. В таком случае выбирается первый найденный. Предлагаемый способ без добавления избыточности обеспечивает выбор верного корня для любого потока случайных битов.

Список использованных источников:

1. Rabin, M. O. Digitalized signatures and public-key function as intractable as factorization / M. O. Rabin - Massachusetts institute of technology laboratory for computer science, Cambridge, 1979.

2. Menezes, A. P. Handbook of applied cryptography / A. P. Menezes, S. Vanstone - CRC Press, 1996.

3. Ярмолик, С. В. Криптография и охрана коммерческой информации: методическое пособие / С. В. ярмолик, В. Н. Ярмолик - Минск, БГУИР, 2010 - 32 с.