А.М. Атаян, В.С. Дзигоева
Финансовый университет при Правительстве Российской Федерации,
г. Владикавказ, Россия

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ: РЮКЗАЧНЫЕ КРИПТОСИСТЕМЫ

Защита информации в условиях глобализации является одной из важнейших задач обеспечения безопасности. В статье рассматриваются математические методы построения стойких криптосистем. Для повышения надежности криптосистем предлагается использовать рюкзачную криптосистему Чора-Райвеста, которая использует наборы, состоящие из элементов конечного поля.

Ключевые слова: криптография, рюкзачные криптосистемы, шифрование, дешифрование, открытый ключ, закрытый ключ

Information security in globalization conditions is one of the most important tasks of safety ensuring. The article deals with mathematical methods of resistant cryptosystems creation. It is offered to use Chor-Rivest knapsack cryptosystem for reliability increase of cryptosystems. It uses the sets which consist of finite field elements.

Key words: cryptography, knapsack cryptosystem, encryption, decryption, public key, private key.

Одним из технико-технологических факторов глобализации сегодня является Интернет. Однако важнейшим условием его широкого применения было и остается обеспечение адекватного уровня безопасности всех сетевых транзакций. Понятие «безопасность информации» можно определить как состояние устойчивости информации к случайным или преднамеренным воздействиям, исключающее недопустимые риски ее уничтожения, искажения и раскрытия, которые приводят к материальному ущербу владельца или пользователя информации.

Решить проблемы безопасности призвана криптография – наука об обеспечении безопасности данных. Криптография представляет собой совокупность методов преобразования данных, направленных на то, чтобы сделать эти данные бесполезными для несанкционированного доступа. Такие преобразования позволяют решить две главные проблемы защиты данных: проблемы конфиденциальности (путем лишения противника возможности извлечь информацию из канала связи) и проблему целостности (путем лишения противника возможности изменить сообщение так, чтобы изменился его смысл, или ввести ложную информацию в канал связи). Проблемы конфиденциальности и целостности информации тесно связаны между собой, поэтому методы решения одной из них часто применимы для решения другой.

Поэтому одной из основных задач криптографии является разработка стойких криптосистем.

Существуют симметричные криптосистемы и криптосистемы с открытым ключом [4, с.15]. В симметричных криптосистемах ключ и алгоритм шифрования известны только адресату и отправителю. В основе криптосистемы с открытым ключом лежит односторонняя функция f, такая, что значение f (x) легковычислимо по x (вычисление осуществимо с вре-

менной сложностью, являющейся полиномом низкой степени относительно размера входа задачи); но решение уравнения y=f(x) при неизвестном x трудновычислимо (т.е. в настоящее время неизвестен полиномиальный алгоритм решения уравнения).

Особый интерес представляют рюкзачные криптосистемы, которые основаны на так называемой задаче о рюкзаке.

Пусть задан набор a_i, если это возможно, сумма которых равна k. В простейшем случае k указывает размер рюкзака, а каждое из чисел a_i – размер предмета, который может быть упакован в рюкзак. Если числовой набор невелик, то эта задача может быть решена простым перебором всех подмножеств. Если же в наборе, например, 300 элементов, то такой перебор подмножеств невозможен.

Однако существуют наборы, для которых задача о рюкзаке решается просто независимо от количества элементов. Это так называемые быстрорастущие наборы, в которых каждый элемент больше суммы всех предыдущих. Для решения задачи с таким набором достаточно просмотреть его справа налево. Если последнее число набора a_n больше числа k, то мы переходим к предпоследнему числу, если же нет, то оно служит одним из искомых слагаемых. Это следует из того факта, что все оставшиеся числа в сумме дают число, меньшее k. Далее мы повторяем процедуру для $k_1 = k - a_n$ и т.д. Заметим, что в случае быстрорастущих наборов разложение k в сумму a_i однозначно, что важно в контексте криптосистем.

Заметим также, что криптосистема должна быть построена таким образом, чтобы задача легко решалась легальным получателем, владеющим секретной лазейкой, и была трудновычислима для криптоаналитика, знающего открытый ключ – рюкзачный набор.

Опишем рюкзачную криптосистему Меркля – Хеллмана, основанную на быстрорастущих наборах [1].

Пусть $A = (a_1, a_2, \dots, a_n),\ a_i \in N,\quad i = \overline{1,n}$, быстрорастущий набор, т.е. $a_s > a_1 + \cdots + a_{s-1},\quad s = \overline{2,n}$. И пусть выбрано целое число m такое, что $m > \sum_1^n a_i$, и число t взаимно простое с m. Умножим каждое число набора на t и обозначим через b_i наименьший положительный остаток $b_i \equiv t \cdot a_i \pmod m$.

В результате мы получим набор $B = (b_1, b_2, \dots, b_n)$, который будет служить открытым ключом. Секретной лазейкой при этом будут m, t.

Процесс шифрования происходит следующим образом. Сначала исходное сообщение кодируется и разбивается на n-разрядные блоки. При необходимости последний блок дополняется в конце нулями.

Каждый такой блок C шифруется числом. Процесс дешифрования легальным получателем осуществляется следующим образом. Так как согласно выбору t и m взаимно простые, то существует элемент t^{-1}, обратный к t по модулю m, т.е. $t \cdot t^{-1} \equiv 1 \pmod m$. С помощью элемента t^{-1} легальный получатель восстанавливает быстрорастущий набор A: $a_i \equiv b_i \cdot t^{-1} \pmod m, i = \overline{1,n}$. Далее он вычисляет наименьший положительный остаток и решают задачу о рюкзаке, определяемую набором A и числом c. Далее по соответствующему двоичному набору восстанавливает исходное сообщение.

В начале 80-х гг. данный тип рюкзачных криптосистем был вскрыт Шамиром, предложившим алгоритм, решающий задачу о рюкзаке с такими наборами за полиномиальное время. Алгоритм основан на том факте, что не обязательно для криптоаналитика нахождение истинных значений множителя t и модуля m. Достаточно найти любые t' и m', такие, что умножение чисел открытого ключа B на $(t')^{-1}$ приводит к быстрорастущему набору [2, с.145-152].

Несмотря на то, что А. Шамир показал, что система Меркля-Хеллмана является ненадежной, попытки ее усовершенствования до сих пор не прекращаются, о чем свидетельствуют работы Р. Гудмана, Э. Маколи, Б. Чора, Р. Райвеста, В.О. Осипяна, В.В. Подколзина. Более полный обзор работ в области анализа системы Меркля-Хеллмана и ее развития дан Б. Шнайером [3].

В своей работе мы хотим рассмотреть рюкзачную систему, которая до сих пор пользуется доверием и не поддается вскрытию. Это рюкзачная криптосистема, предложенная Чором и Райвестом, использующая наборы, состоящие из элементов конечного поля.

Пусть $k = F_{p^h}$ – конечное поле из p^h элементов, θ – образующая мультипликативной группы k^* поля k, α – алгебраический элемент степени h над полем F_p. Если $\theta^m = \beta$, то будем писать $\log_\theta \beta = m$. Такие логарифмы называются дискретными логарифмами.

Вычислим $\alpha_i = \log_\theta(\alpha + i - 1), 1 \le i \le p$. Перемешаем α_i с помощью случайно выбранной перестановки π из p элементов и добавим по модулю $p^h - 1$ к результату произвольно выбранное число $d, 0 \le d \le p^h - 2$. Обозначим через $B = (b_1, \dots b_p)$ полученный вектор.

Открытый ключ составляют B, p, h. Секретной лазейкой служат α, θ, π, d.

Исходное сообщение кодируется двоичными наборами C длины p, содержащими h единиц. Вектор C, рассматриваемый как вектор-столбец, зашифровывается как наименьший положительный остаток от $B \cdot C (mod\ p^h - 1)$.

Дешифрование для легального получателя, знающего секретную лазейку, выполняется следующим образом. Из числа криптотекста вычитается число $h \cdot d$ по модулю $(p^h - 1)$, получается число y. Тем самым нейтрализуется добавление случайного шума d. В поле k вычисляется θ^y.

С целью пояснения дальнейших действий заметим, что согласно выбору α – алгебраический элемент степени h над полем F_p. Следовательно, α служит корнем неприводимого над полем F_p многочлена $f(x)$ степени h, т.е $f(\alpha) = 0$, и любой элемент представим в виде многочлена от α степени, не превосходящей $h - 1$. В частности, θ^y представим в таком виде.

Продолжим описание процесса дешифрования. Составляется многочлен степени h: $s(\alpha) = f(\alpha) + \theta^y$. Так как многочлен $s(\alpha)$ представляет собой степень $\theta^y = \theta^{\alpha_{i_1} + \dots + \alpha_{i_r}}$, он разлагается на линейные сомножители, $s(\alpha) = (\alpha + i_1 - 1) \cdot \dots \cdot (\alpha + i_r - 1)$. Линейные множители могут быть найдены подстановкой 0,1,…p-1.

Числа $i_1, \dots, i_r$ указывают на позиции единиц. Места для единиц в закодированном исходном тексте определяются после применения обратной перестановки π^{-1} к числам $i_1, \dots, i_r$.

В описанной криптосистеме используются наборы длины p , содержащие ровно h единиц. Ясно, что в результате кодирования число единиц в каждом наборе, в общем говоря, не всегда равно h . Но этого можно добиться, используя следующую лемму.

Лемма. Пусть $h \geq 3, h < n$. Тогда существует вложение множества всех двоичных наборов длины $[\log_2 \binom{n}{h}]$ во множество всех двоичных наборов длины n , содержащих ровно h единиц.

Напомним, что в случае криптосистем с модульным умножением быстрорастущие наборы обеспечивали однозначность дешифрования. В описанной криптосистеме Чора-Райвеста это условие обеспечивается следующей леммой.

Лемма. Пусть p – простое число, $h \geq 2$ - целое число. Тогда найдется рюкзачный вектор $A = (\alpha_1, \ldots \alpha_p)$, удовлетворяющий следующим условиям:

1. Числа α_i удовлетворяют неравенству $1 \leq \alpha_i \leq p^h - 1, i = \overline{1,p}$;
2. Пусть $x_i, y_i, \quad i = \overline{1,p}$ - неотрицательные целые числа такие, что $(x_1, \ldots, x_p) \neq (y_1, \ldots, y_p), \sum_i x_i = \sum_i y_i = h$. Тогда $\sum_i x_i \cdot \alpha_i \neq \sum_i y_i \cdot \alpha_i$.

Набор A , состоящий из $\alpha_i = \log_\theta(\alpha + i - 1)$, используемый в криптосистеме Чора-Райвеста, удовлетворяет всем условиям леммы, следовательно, обеспечивает однозначность процесса дешифрования.

ЛИТЕРАТУРА

1. *Ralph C. Merkle, Martin E. Hellman*. Hiding Information and Signatures in Trapdoor Knapsacks. IEEE Transactions on Information Theory, vol. IT-24, 1978.
2. *Shamir A. A* polynomial time algorithm for breaking. The basic Merkle-Hellman cryptosystem // Proc. of the 23rd FOCS Symposium. 1982.
3. *Шнайер Б*. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2002. 816 с.
4. *Ященко В.В*. Введение в криптографию. М.:МЦНМО – ЧеРО, 1999. 272 с.