УДК 004.056.5 + 003.26:004.056
ББК Х401.114

Животова А. Е., Зюляркина Н. Д., Костыгина Ю. О.

МОДИФИКАЦИЯ КРИПТОСИСТЕМЫ С ОТКРЫТЫМ КЛЮЧОМ НА ОСНОВЕ «ЗАДАЧИ О РЮКЗАКЕ»

В работе рассмотрены достоинства и недостатки криптосистем с открытым ключом, основой для которых является классическая формулировка «задачи о рюкзаке». Предложена идея модификации рюкзачной схемы, связанная с вычислениями в группах и использующая для построения рюкзака специально подобранные порождающие множества группы, которые обеспечивают однозначное представление заданного элемента. Приведен пример использования мультипликативного рюкзака, построенного при помощи прямого произведения диагональных подгрупп в общей линейной группе над конечным полем и замаскированного под рюкзак произвольного вида посредством внутреннего автоморфизма этой группы.

Ключевые слова: *криптосистема с открытым ключом, рюкзачная схема, группа, порождающий элемент.*

Zhivotova A. E., Ziuliarkina N. D., Kostygina Y. O.

MODIFICATION OF THE CRYPTOSYSTEM WITH PUBLIC KEY ON THE BASIS OF KNAPSACK PROBLEM

The article dwells on advantages and disadvantages of the cryptosystem with a public key based on the knapsack problem. The author proposes the idea of the modification of the knapsack scheme connected with the calculations in groups. For construction of a knapsack the scheme uses specifically matching groups which produce multitudes and provide single-valued representation of a stated element. The author gives an example of the usage of a multiplicative knapsack created with the help of direct product of diagonal subgroups of the general linear group over a finite field and disguised as a knapsack of general form by the inner automorphism of the group.

Keywords: *cryptosystem with public key, knapsack scheme, group, generating element.*

Начало асимметричным шифрам было положено в 1976 г. в работе У. Диффи и М. Хеллмана «Новые направления в современной криптографии»[1].

Криптографическая система с открытым ключом (или асимметричное шифрование, асимметричный шифр) — система шифрования, при которой открытый ключ передаётся по открытому каналу и используется для шифрования сообщения. Для расшифровки сообщения используется секретный ключ. Криптографические системы с открытым ключом в настоящее время широко применяются в различных сетевых протоколах и стандартах цифровой подписи.

Для построения криптосистемы с открытым ключом выбирается класс задач, для которого в произвольном случае не известен эффективный алгоритм решения, и в этом классе выделяется подзадача, для которой такой алгоритм существует. Выбранную задачу маскируют под задачу общего вида и на основе ее выбирают ключ шифрования. В качестве секретного ключа используется информация, позволяющая перевести выбранную задачу в исходный вид.

Наиболее распространенными в настоящее время являются криптосистемы, основанные на задаче факторизации (RSA) и задаче нахождения дискретного логарифма (схема Эль-Гамаля). Но усовершенствование технических средств требует постоянного изменения параметров систем, основанных на задаче факторизации, что приводит к определенным сложностям при их использовании. Ввиду этого актуальность приобретают методы построения асимметричных криптосистем, которые не используют задачи, связанные с факторизацией. В связи с этим особенно активно изучаются способы, основанные на вычислениях в специально подобранных группах. Отметим в качестве примера группы точек эллиптических кривых, которые используются в обобщенной схеме Эль-Гамаля, применяемой в стандартах цифровой подписи. К достоинствам этих групп следует отнести наличие элементов большого порядка и сложность нахождения дискретного логарифма.

К задачам, не связанным с проблемой факторизации, относится и задача об укладке рюкзака, являющаяся NP-полной. На ее основе был разработан ряд криптосистем, отличающихся простотой реализации. Но в ходе их анализа были выявлены существенные недостатки, делающие эти системы уязвимыми для различного вида криптографических атак. В настоящее время системы этого класса не получили широкого распространения, но ведется работа по их модификации, которая позволит улучшить их надежность. Одним из способов такой модификации является использование специальных порождающих множеств в конечных группах для создания рюкзачной схемы.

1. Криптосистемы на основе задачи о рюкзаке

Задача о рюкзаке. Имеется упорядоченный набор чисел $(a_1,a_2,...a_n)$ (этот набор называют рюкзаком или рюкзачным вектором) и число m. Требуется указать такой бинарный вектор $(x_1,x_2,...x_n)$, для которого выполняется равенство

$$x_1\ a_1+x_2\ a_2+...+x_n\ a_n=m.$$

В общем случае для данной задачи нет эффективного алгоритма решения и приходится применять полный перебор для нахождения требуемого вектора или доказательства отсутствия решения. Кроме того, в общей постановке задача о рюкзаке может иметь несколько различных решений. Но если рюкзак является сверхрастущим, то решение в случае его существования единственно и существует эффективный алгоритм его нахождения.

Рюкзак с положительными элементами $(a_1,\ a_2,\ ...,\ a_n)$ будем называть сверхрастущим, если $a_2>a_1,\ a_3>a_j+a_2,...,a_n>a_1+a_2+...+a_{n-1}$.

На основе задачи о рюкзаке разработан ряд криптографических систем. Первой из них была система Меркля — Хеллмана, описание которой приведено ниже.

Генерация ключей:

1. Выбирается некоторый сверхрастущий рюкзак.
2. Выбирается число k $(k > a_1+a_2+\ldots+a_n)$.
3. Выбирается число c, взаимно простое с k.
4. Формируется рюкзак-ловушка $(b_1,b_2,\ldots b_n)=c(a_1,a_2,\ldots a_n)\ (\mathrm{mod}\ k)$, который и является открытым ключом.
5. Числа c и k являются секретными ключами.

Алгоритм шифрования:

1. Открытый текст представляется в виде двоичной последовательности.
2. Последовательность разбивается на блоки длины n.

3. Каждый блок $(x_1,x_2,\dots x_n)$ заменяется на число m, вычисленное по правилу $\sum_{i=1}^{n} a_i x_i = m$.

Алгоритм дешифровки:

1. Находится исходный сверхрастущий рюкзак: $(a_1,a_2,\dots,a_n)=c^{-1}(b_1,b_2,\dots b_n) \pmod k$.
2. Для каждого элемента m шифр текста вычисляется элемент $m'=c^{-1}m$.
3. Для вычисленного m' решается задача о рюкзаке для рюкзака $(a_1,a_2,\dots,a_n)$ и находится блок открытого текста $(x_1,x_2,\dots,x_n)$.

Пример 1. Используется латинский алфавит, в котором каждая буква представлена пятиразрядной двоичной записью своего номера. Рюкзак-ловушка B=(182, 128, 192, 175, 50, 100) получен из сверхрастущего рюкзака A путем умножения на c=91 и приведением по модулю n=300. Сообщение Y=(232, 178, 502) получено шифрованием на основе рюкзака B. Восстановить исходный рюкзак A и, используя его, расшифровать сообщение Y.

Решение:

1) Найдем $c^{-1} \pmod{300}$: $c^{-1}=91^{-1}=211$.

2) Восстановим исходный рюкзак: $A=211B \pmod{300} =211(182, 128, 192, 175, 50, 100) \pmod{300} = (2, 8, 12, 25, 50, 100)$.

3) Преобразуем сообщение Y: $Y \to Z = 211Y \pmod{300} = 211(232, 178, 502) \pmod{300} = (52, 58, 22)$.

4) Решим задачу о рюкзаке для каждого элемента сообщения Z:

$$52=50+2 \to (1, 0, 0, 0, 1, 0),$$
$$58=50+8 \to (0, 1, 0, 0, 1, 0),$$
$$22=12+10=12+8+2 \to (1, 1, 1, 0, 0, 0).$$

5) Запишем полученные двоичные векторы в единую последовательность, которую разобьем на блоки длины 5: $(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \to (1, 0, 0, 0, 1), (0, 0, 1, 0, 0), (1, 0, 1, 1, 1), (0, 0, 0)$. Последний блок из трех элементов исключим из рассмотрения.

6) Сопоставим каждому полученному блоку число, для которого этот блок является двоичной записью, и найдем соответствующую букву латинского алфавита:

$$(1, 0, 0, 0, 1) \to 17 \to R,$$
$$(0, 0, 1, 0, 0) \to 4 \to E,$$
$$(1, 0, 1, 1, 1) \to 23 \to X.$$

Кроме системы Меркля — Хеллмана отметим систему Грэма — Шамира, в которой также используется сверхрастущий рюкзак. Но маскировка его под рюкзак общего вида производится не с помощью приведения по модулю, а с использованием вектора случайного шума. В системе Мории — Касахары используется мультипликативный способ шифрования и формирования секретного ключа. Система Хора — Ривеста основана на вычислениях в конечных полях, а система Накаше — Штерна является гибридом системы Меркля — Хеллмана и алгоритма Полига — Хеллмана. Описание некоторых из этих схем можно найти в работе[2].

2. Модификация рюкзачных криптосистем с использованием конечных групп

Пусть G — группа, $g_1\ g_2, \dots,g_n$ — её элементы, такие, что для любого вектора $(x_1, x_2, \dots ,x_n)$, $x_i \in Z_{mi}$, $m_i=|g_i|$ элемент $g=g_1^{x1}g_2^{x2}\dots g_n^{xn}$ имеет единственное представление в указанном виде. Будем предполагать, что существует эффективный алгоритм, позволяющий по данному элементу g находить вектор $(x_1, x_2, \dots ,x_n)$, $x_i \in Z_{mi}$, $m_i=|g_i|$, для которого выполняется равенство $g=g_1^{x1}g_2^{x2}\dots g_n^{xn}$. Тогда можно рассмотреть следующую рюкзачную криптосистему, основанную на вычислениях в данной группе G.

Генерация ключей:

1. Выбирается рюкзак $(g_1\ g_2, \dots,g_n)$, для которого выполняются описанные ранее условия.
2. Выбирается маскирующий изоморфизм f из группы G в группу G'.
3. Формируется рюкзак-ловушка $(b_1,b_2,\dots b_n)=(f(g_1), f(g_2),\dots,f(g_n))$, который и является открытым ключом.
4. Отображение f является секретным ключом.

Алгоритм шифрования:

1. Открытый текст представляется в виде последовательности
$(x_1, x_2, \dots ,x_n)$, $x_i \in Z_{mi}$, $m_i=|g_i|$.
2. Каждый блок $(x_1, x_2, \dots ,x_n)$ заменяется на элемент b, вычисленный по правилу: $b= b_1^{x1}b_2^{x2}\dots b_n^{xn}$.

Алгоритм дешифровки:

1. Находится исходный рюкзак $(g_1,g_2,\dots,g_n)=f^{-1}(b_1,b_2,\dots,b_n)$.
2. Для элемента b шифр текста вычисляется элемент $g=f^{-1}(b)$. Для вычисленного g решается задача о рюкзаке для рюкзака $(g_1,g_2,\dots,g_n)$ и находится блок открытого текста $(x_1,x_2,\dots,x_n)$.

3. Для удобства вычислений элементы g_1, $g_2, \ldots, g_n$ можно выбрать так, чтобы они имели одинаковый порядок m. В этом случае исходный текст можно считать последовательностью элементов из Z_m и при шифровании разбивать его на блоки длины n.

Пример 2. Рассмотрим общую линейную группу $G = GL_3(7)$ и выберем в ней элементы a, b и c:

$$a=\begin{pmatrix}3&0&0\\0&1&0\\0&0&1\end{pmatrix},\quad b=\begin{pmatrix}1&0&0\\0&5&0\\0&0&1\end{pmatrix},\quad c=\begin{pmatrix}1&0&0\\0&1&0\\0&0&3\end{pmatrix}.$$

Заметим, что $\langle a, b, c\rangle$ является прямым произведением подгрупп $\langle a\rangle$, $\langle b\rangle$ и $\langle c\rangle$, каждая из которых имеет порядок 6. Кроме того, по виду элемента $g=a^k b^s c^t$ набор (k, s, t) элементов из Z_6 легко восстанавливается. Следовательно, условия, накладываемые на элементы g_1 $g_2, \ldots, g_n$, будут выполняться.

В качестве маскирующего изоморфизма рассмотрим сопряжение посредством элемента x:

$$x=\begin{pmatrix}2&3&1\\1&4&2\\2&5&6\end{pmatrix}.\text{ Заметим что } x^{-1}=\begin{pmatrix}0&3&6\\1&2&5\\5&2&1\end{pmatrix}.$$

Вычислим набор (a^x, b^x, c^x), который будет являться открытым ключом:

$$a^x=x^{-1}ax=\begin{pmatrix}1&0&0\\4&0&2\\6&2&4\end{pmatrix},\qquad b^x=x^{-1}bx=\begin{pmatrix}6&6&3\\1&5&2\\1&4&3\end{pmatrix},$$

$$c^x=x^{-1}cx=\begin{pmatrix}4&4&2\\6&2&4\\4&3&6\end{pmatrix}.$$

Зашифруем в данной системе сообщение $(1, 5, 2)$:

$$(1,5,2) \rightarrow b=a^x (b^x)^5 (c^x)^2 = \begin{pmatrix}5&5&6\\4&6&5\\5&2&4\end{pmatrix}.$$

Для дешифровки сообщения b найдем элемент g:

$$g=xbx^{-1}=\begin{pmatrix}3&0&0\\0&3&0\\0&0&2\end{pmatrix}.$$

Поскольку $3^1=3$, $5^5=3$, $3^2=2$, $g= a^1b^5c^2$ и открытый текст имеет вид $(1, 5, 2)$.

Рассмотренная модификация опирается на мультипликативный рюкзак, поэтому представляется достаточно надежной ввиду того, что для подобных схем неизвестны эффективные способы взлома.

Примечания

[1] Diffie, W. New Directions in Cryptography / W. Diffie, M. E. Hellman // IEEE Transactions on Information Theory. — 1977. — V. T. 1—22. — P. 644—654.

[2] Саломаа, А. Криптография с открытым ключом = Public-Key Cryptography / А. Саломаа. — Springer-Verlag, 1990. — С. 102—150.

References

[1] Diffie W, Hellman M.E. New Directions in Cryptography. // IEEE Transactions on Information Theory ,V. TI-22,1977, pp 644-654.

[2] Salomaa A. Kriptografiya s otkrytym klyuchom [Public-Key Cryptography]. — Springer-Verlag Publ., 1990. — p. 102-150.

Животова Анастасия Евгениевна, студент кафедры «Безопасность информационных систем» Приборостроительного факультета ФГОБУ ВПО «Южно-Уральский государственный университет» (национальный исследовательский университет). E-mail: nastiazhiv@mail.ru

Зюляркина Наталья Дмитриевна, кандидат физ.-мат. наук, доцент кафедры безопасности информационных систем ФГБОУ ВПО «Южно-Уральский государственный университет» (национальный исследовательский университет). E-mail: toddeath@yandex.ru

Костыгина Юлия Олеговна, студент кафедры «Безопасность информационных систем» Приборостроительного факультета ФГОБУ ВПО «Южно-Уральский государственный университет» (национальный исследовательский университет). E-mail: kostygina250@mail.ru

Anastasia Yevgenievna Zhivotova, student of the Department of Information System Security of the Faculty of Instrument Design of the South Ural State University (National Research University). E-mail: nastiazhiv@mail.ru

Natalia Dmitrievna Ziuliarkina, cand. Sc. Physics and Mathematics, associated professor of Department of Information System Security of the South Ural State University (National Research University). E-mail: toddeath@yandex.ru

Kostygina Yulia Olegovna, student of the Department of Information System Security of the Faculty of Instrument Design of the South Ural State University (National Research University). E-mail: kostygina250@mail.ru