УДК 003.26 + 51-7

ЭЛЕМЕНТЫ БОЛЬШИХ ПОРЯДКОВ В ЛИНЕЙНЫХ ГРУППАХ И МОДИФИКАЦИЯ СИСТЕМЫ ЭЛЬ-ГАМАЛЯ

Н.Д. Зюляркина

В данной работе описывается криптосистема с открытым ключом, являющаяся модификацией системы Эль-Гамаля.

Ключевые слова: Криптосистема с открытым ключом, группа, порождающий элемент.

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

Криптографическая система с открытым ключом (или асимметричное шифрование, асимметричный шифр) – система шифрования, при которой открытый ключ передается 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.

Большое распространение в настоящее время получили криптосистемы, основанные на задаче нахождения дискретного логарифма. К ним можно отнести схему распределения ключей Диффи – Хеллмана, схему Эль-Гамаля, цифровую подпись Шнорра и т.д. Классическое описание этих систем предполагает использование мультипликативных групп конечных полей простого порядка. Но развитие технических средств сделало системы, использующие традиционные ключи, более уязвимыми. 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.

Задача нахождения дискретного логарифма и элементы больших порядков

Пусть G − циклическая группа порядка n, порожденная элементом g, а x − элемент из G. Назовем элемент m из Z_n *логарифмом x по основанию g* если выполняется равенство $g^m=x$. Если G имеет бесконечный порядок, то m выбирается из множества целых чисел.

Задачей дискретного логарифмирования назовем нахождение m по известным g и x. Сложность этой задачи связана с видом группы G. Если в качестве G взять множество целых чисел с операцией сложения, а элемент g выбрать равным 1, то, очевидно, указанная задача будет решаться тривиально, так как m=x. Но ситуация кардинально меняется, если в качестве G взять специальным образом выбранную матричную группу.

Пример 1. Рассмотрим общую линейную группу $GL_n(R)$ и выберем в ней элемент $g=\begin{pmatrix} -14 & -9 \\ 25 & 16 \end{pmatrix}$. Пусть G=<g>. Можно показать, что g имеет бесконечный порядок и, следовательно, G изоморфна группе целых чисел. Но задача нахождения дискретного логарифма в этой группе уже далеко не так проста как для Z. Ведь уже далеко не очевидно, что решением уравнения $g^m=\begin{pmatrix} -224 & -135 \\ 375 & 226 \end{pmatrix}$ будет m=15.

Для того чтобы задача о нахождении дискретного логарифма была трудно разрешимой, нужно подобрать подходящую группу, а в ней подходящий элемент. Необходимым условием подбора элемента является большое значение его порядка, так как для элементов малых порядков дискретный логарифм можно найти с помощью перебора. Но это условие не является достаточным, что следует из примера G=Z. Группами, в которых есть элементы с указанными свойствами, являются мультипликативные группы конечных полей, группы точек эллиптических кривых и линейные (матричные) группы. Отметим, что решение задачи нахождения дискретного логарифма для мультипликативных групп конечных полей можно найти с помощью метода «Шаг младенца − шаг великана» и метода исчисления порядка, которые более эффективны, чем метод перебора. Метод «Шаг младенца − шаг великана» является универсальным и применим к любой конечной циклической группе. Но при большом значении порядка группы он не дает существенного выигрыша во времени по сравнению с методом перебора. Метод исчисления порядка является более быстрым, но он специфичен и не переносится на случай матричных групп.

Модификация криптосистемы Эль-Гамаля с использованием линейных групп

Схема Эль-Гамаля – криптосистема с открытым ключом, основанная на трудности вычисления дискретных логарифмов в конечном поле, включающая в себя алгоритм шифрования и алгоритм цифровой подписи. Она

лежит в основе стандартов электронной цифровой подписи в США (DSA) и России (ГОСТ Р 34.10-94). Опишем классический вариант данной схемы.

Генерация ключей

1. Генерируется случайное простое число p.

2. Выбирается случайный примитивный элемент x поля Z_p.

3. Выбирается случайное целое число a такое, что $2 \le a \le p-2$.

4. Вычисляется x^a.

Открытым ключом является тройка (p,x,x^a), а секретным ключом – число a.

Алгоритм шифрования

1. Исходный текст представляется в виде последовательности элементов из Z_p.

2. Каждый элемент m открытого текста шифруется следующим образом:

a) выбирается сессионный ключ r – случайное целое число, такое, что $1<r<p-1$.

b) вычисляются числа x^r и $m(x^a)^r$.

Пара чисел $(x^r, m(x^a)^r)$ является шифр-текстом, соответствующим m.

Алгоритм расшифровки

1. Шифр-текст разбивается на пары (c, b).

2. По каждой паре восстанавливается элемент открытого текста по формуле $m=(c^a)^{-1}b$.

Теперь дадим описание модификации данной схемы, использующей линейные группы.

Генерация ключей

1. Выбирается линейная группа $G=GL_n(K)$, где K − некоторое коммутативное кольцо с единицей (например, кольцо вычетов).

2. Выбирается случайный элемент x группы G большого порядка p.

3. Выбирается случайное целое число a такое, что $2 \le a \le p-1$.

4. Вычисляется x^a.

Открытым ключом является тройка (G,x,x^a), а секретным ключом – число a.

Алгоритм шифрования

1. Исходный текст представляется в виде последовательности элементов из $M_n(K)$.

2. Каждый элемент m открытого текста шифруется следующим образом:

a) выбирается сессионный ключ r – случайное целое число, такое, что $1<r<p$.

b) вычисляются элементы x^r и $m(x^a)^r$.

Пара чисел $(x^r, m(x^a)^r)$ является шифр-текстом, соответствующим m.

Алгоритм расшифровки

1. Шифр-текст разбивается на пары (c, b).

2. По каждой паре восстанавливается элемент открытого текста по формуле $m=b(c^a)^{-1}$.

Пример 2. Пусть открытым ключом в описанной модификации является набор ($GL_2(137)$, $\begin{pmatrix} 4 & 9 \\ 136 & 135 \end{pmatrix}$, $\begin{pmatrix} 124 & 95 \\ 96 & 15 \end{pmatrix}$), а секретный ключ a=41. Зашифруем сообщение $m=\begin{pmatrix} 2 & 5 \\ 8 & 9 \end{pmatrix}$:

a) выберем сеансовый ключ r=83;

b) вычислим $x^r=\begin{pmatrix} 113 & 62 \\ 54 & 26 \end{pmatrix}$ и $m(x^a)^r=\begin{pmatrix} 117 & 76 \\ 89 & 115 \end{pmatrix}$.

Зашифрованный текст представим матрицей $\begin{pmatrix} 113 & 62 & 117 & 76 \\ 54 & 26 & 89 & 115 \end{pmatrix}$.

Для расшифровки данного сообщения выполним следующие действия:

a) разобьем полученное сообщение на две матрицы $b=\begin{pmatrix} 113 & 62 \\ 54 & 26 \end{pmatrix}$ и $c=\begin{pmatrix} 117 & 76 \\ 89 & 115 \end{pmatrix}$;

b) используя секретный ключ a=83, найдем исходное сообщение по формуле $m=bc^{-83}$.

В данном примере элемент $\begin{pmatrix} 4 & 9 \\ 136 & 135 \end{pmatrix}$ имеет в группе $GL_2(137)$ порядок равный 136.

Элементы больших порядков в линейных группах

Для выбора ключа в описанной модификации нужно иметь в своем распоряжении матрицу достаточно большого порядка. Поэтому особую важность представляет информация о порядках элементов в линейных группах и способах построения элементов заданного порядка. Если рассматривается группа $GL_n(Z_m)$, то с помощью китайской теоремы об остатках ситуацию можно свести к рассмотрению групп $GL_n(Z_q)$, где q является примерным числом. Для усложнения задачи дискретного логарифмирования можно преобразовывать элемент **x** с помощью сопряжения.

Пример 3. Элемент $x=\begin{pmatrix} 4 & 9 \\ 136 & 135 \end{pmatrix}$ в группе $GL_2(137)$ из предыдущего примера был получен как $y^h=h^{-1}yh$, где $h=\begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}$, $y=\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Элемент y имеет порядок 136 и задача дискретного логарифмирования для него эквивалентна задаче нахождения дискретного логарифма в поле порядка 137. Легко заметить, что задача дискретного логарифмирования для элемента x является более сложной.

Библиографический список

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

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