УДК 519.711/.72

МАТРИЧНЫЕ АЛГОРИТМЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ И ОБМЕНА КЛЮЧАМИ ШИФРОВАНИЯ

Белецкий А.Я., Белецкий А.А., Стеценко Д.А.
Национальный авиационный университет, Киев

Разработаны алгоритмы обмена ключами шифрования между абонентами компьютерной сети и криптографической защиты информации, передаваемой по открытым каналам связи. В основу алгоритмов положен модифицированный асимметричный протокол Диффи-Хэллмана (DH). Суть модификации сводится к замене больших простых чисел алгоритма DH гарантированно невырожденными n – полными двоичными матрицами высокого порядка. Предлагаются методы синтеза таких матриц. Обсуждены способы противодействия атакам на алгоритм шифрования.

Ключевые слова: *примитивные двоичные матрицы, криптографический алгоритм, шифрование данных.*

Введение и постановка задачи

В работах [1,2] предлагается строить блочные криптографические шифры на основе обратимых матриц над полем *GF*(2). Если $\boldsymbol{X}$, $\boldsymbol{Y}$ – векторы, представляющие соответственно открытый и зашифрованный текст, а $\boldsymbol{M}$ - шифрующая матрица, то зашифрование задается уравнением $\boldsymbol{Y} = \boldsymbol{M} \cdot \boldsymbol{X}$, а расшифрование – уравнением $\boldsymbol{X} = \boldsymbol{M}^{-1} \cdot \boldsymbol{Y}$. Для обмена сеансовыми ключами в системе авторы предлагают использовать протокол Диффи – Хэллмана (DH) [3] в циклической группе матриц $\langle \boldsymbol{M} \rangle$, причем матрица считается общедоступной. Предполагается, что пользователь $\mathcal{A}$ вырабатывает случайный показатель x, вычисляет матрицу $\boldsymbol{M}^x$ и посылает ее пользователю $\mathcal{B}$. В свою очередь пользователь $\mathcal{B}$ вырабатывает случайный показатель y, вычисляет матрицу $\boldsymbol{M}^y$ и посылает ее пользователю $\mathcal{A}$. Затем оба пользователя возводят полученные матрицы в свои степени и получают общую матрицу (ключ шифрования) $\boldsymbol{M}^{xy} = \boldsymbol{M}^{yx}$. Поскольку мощность группы, образующим элементом которой являются невырожденные двоичные матрицы $\boldsymbol{M}$ (рекомендуемый порядок должен быть не менее чем 100), велико, то вычисление ключа, как утверждают авторы (кстати, без доказательства), имеет переборную сложность.

Целью данной статьи является разработка протоколов обмена ключами шифрования, осуществляемая по открытым каналам связи и синтез матричных алгоритмов криптографической защиты информации. В основу алгоритмов положен модифицированный асимметричный протокол Диффи-Хэллмана (DH). Суть модификации сводится к замене больших простых чисел алгоритма DH невырожденными n – полными двоичными матрицами высокого порядка, последовательность степеней которых в кольце вычетов по mod 2 образует циклическую группу максимальной длины. В основу синтеза таких матриц положен метод обобщенных преобразований Грея [4], являющийся расширением классических кодов Грея [5].

Очевидно, что одной из важных проблем, которая возникает в ходе реализации матричных алгоритмов DH, состоит в формировании шифрующих матриц $\boldsymbol{M}$. Матрицы $\boldsymbol{M}$ должны быть невырожденными, что естественно. К ним также предъявляется еще такое требование. Порядок циклической группы, образуемой степенями $\boldsymbol{M}$ в кольце вычетов по mod 2, должен быть по возможности максимальным. Или, другими словами, последовательность элементов указанной группы, которую для простоты мы будем называть $\boldsymbol{M}$ – группой, должна обладать свойствами m-последовательности.

Обобщенные преобразования Грея

В известной (классической) схеме [5] процесс формирования прямых и обратных кодов Грея (КГ) развивается по направлению слева направо. По этой причине, а также в силу того, что можно построить систему преобразования, подобную кодам Грея, но по направлению формирования справа налево, классические коды Грея названы нами *левосторонними*.

Обозначим разряды двоичного числа, представленного в позиционном коде, через $x_{n-1}, x_{n-2}, ..., x_1, x_0$ (старший разряд слева), а разряды того же числа, выраженного в коде Грея, через $y_{n-1}, y_{n-2}, ..., y_1, y_0$, где n – число разрядов в кодовых векторах $\boldsymbol{x}$ и $\boldsymbol{y}$.

Процесс преобразования вектора $\boldsymbol{x}$ в вектор $\boldsymbol{y}$ (классический код Грея) на примере четырехбитных кодовых комбинаций показан на рис. 1. На этом рисунке отрезки дуги символизируют операцию суммирования по mod 2.

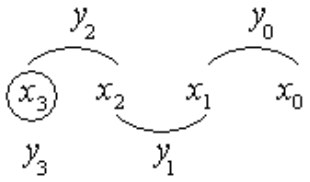

Рис. 1. Схема формирования классических кодов Грея

Правило преобразования компонент вектора $\boldsymbol{x}$ в компоненты вектора $\boldsymbol{y}$ достаточно простое и имеет вид:

$$y_i = x_{i+1} \overset{2}{\oplus} x_i, \quad i = \overline{n-1, 0}, \quad x_n = 0, \tag{1}$$

где $\overset{2}{\oplus}$ – операция поразрядного сложения по mod 2, которую для операндов a и b мы будем записывать и в такой форме $c = (a+b)_2$.

Изложение материала по кодовым преобразованиям целесообразно вести, опираясь на структурные схемы формирования кодов. Такой подход к пояснению сути алгоритма кодирования удобен тем, что делает материал не только более понятным для инженеров, но существенно упрощает задачу математического описания процедуры кодирования.

Для того чтобы придать структурным схемам законченную форму, ограничим (без потери общности) порядок системы уравнений (1), полагая $n = 4$. Тогда

$$\begin{aligned} y_3 &= x_3; \\ y_2 &= (x_3 + x_2)_2; \\ y_1 &= (x_2 + x_1)_2; \\ y_0 &= (x_1 + x_0)_2. \end{aligned} \tag{2}$$

Структурная схема, соответствующая алгоритму преобразования (2), показана на рис. 2.

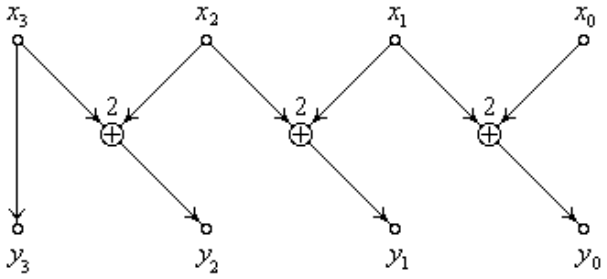

Рис. 2. Структурная схема алгоритма формирования прямого двоичного кода Грея левостороннего

Преобразование (2) можно представить в матричной форме:

$$\boldsymbol{y} = \left(\boldsymbol{x}\, \boldsymbol{M}_{\overset{\circ}{\rightarrow}} \right)_2 ,$$

где $\boldsymbol{x}$ и $\boldsymbol{y}$ – вектор-строки двоичного позиционного кода и его изображения по коду Грея прямому левостороннему соответственно, а $\boldsymbol{M}_{\overset{\circ}{\rightarrow}}$ – квадратная матрица прямого левостороннего преобразования Грея *n*-го порядка. В частности, для системы уравнений (2) матрица $\boldsymbol{M}_{\overset{\circ}{\rightarrow}}$ имеет вид:

$$\boldsymbol{M}_{\overset{\circ}{\rightarrow}} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} .$$

К *обратному* левостороннему (классическому) преобразованию Грея приходим, решая обычными алгебраическими приемами систему модульных уравнений (2) относительно разрядов x_i исходной кодовой комбинации $\boldsymbol{x}$. В частности, из соотношений (2) имеем:

$$\begin{aligned} x_3 &= y_3 ; \\ x_2 &= (y_3 + y_2)_2 ; \\ x_1 &= (y_3 + y_2 + y_1)_2 ; \\ x_0 &= (y_3 + y_2 + y_1 + y_0)_2 . \end{aligned} \qquad (3)$$

В системе уравнений (3) учтено, что $(-1)_2 = 1$.

Преобразованию (3) отвечает структурная схема, показанная на рис. 3.

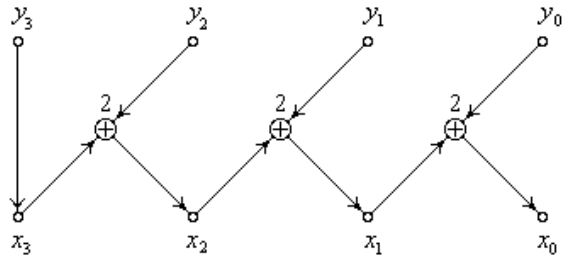

Рис. 3. Структурная схема алгоритма формирования обратного двоичного кода Грея левостороннего

Обратные левосторонние преобразования Грея двоичных кодовых комбинаций (как и прямые преобразования) можно представить в матричной форме

$$\boldsymbol{x} = \left(\boldsymbol{y}\, \boldsymbol{M}_{\overset{\circ}{\rightarrow}} \right)_2 ,$$

где $\boldsymbol{y}$ и $\boldsymbol{x}$ есть вектор-строки двоичного позиционного кода и его обратного преобразования по коду Грея левостороннему соответственно, а $\boldsymbol{M}_{\overset{\circ}{\rightarrow}}$ – квадратная матрица преобразования, порядок которой совпадает с порядком векторов $\boldsymbol{x}$ и $\boldsymbol{y}$.

Системе уравнений (3) отвечает матрица обратного левостороннего преобразования Грея

$$\boldsymbol{M}_{\overset{\circ}{\rightarrow}} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Рассмотренные алгоритмы преобразования двоичных кодовых комбинаций из пространства оригиналов в пространство изображений (коды Грея), в равной степени, как и алгоритмы преобразования двоичных кодовых комбинаций из пространства изображений в исходный позиционный код, соответствуют классической трактовке формирования прямого и обратного кодов Грея, достаточно хорошо изученных и описанных в многочисленных научных публикациях и технической литературе. Вместе с тем, не было обращено внимание на возможность генерации кодов, подобных классическим (левосторонним) прямым и обратным кодам Грея, процесс формирования которых выполняется от младших разрядов кода к старшим, т.е. развивается по направлению справа налево. В таком классе преобразований Грея, который назван *правосторонним*, при прямом и обратном преобразованиях сохраняется неизменным значение младшего (правого) разряда преобразуемого числа.

К структурным схемам алгоритмов формирования правосторонних кодов Грея приходим, развернув на 180° вокруг центральной вертикальной оси соответствующие структурные схемы левосторонних кодов, показанных на рис. 2 и 3.

Правосторонние преобразования Грея так же можно представить в матричных формах, а именно

$$\boldsymbol{y} = \left(\boldsymbol{x}\, \boldsymbol{M}_{\overset{\circ}{\leftarrow}} \right)_2 \quad \text{и} \quad \boldsymbol{x} = \left(\boldsymbol{y}\, \boldsymbol{M}_{\overset{\circ}{\leftarrow}} \right)_2,$$

причем

$$\boldsymbol{M}_{\overset{\circ}{\leftarrow}} = \boldsymbol{M}^{T}_{\overset{\circ}{\rightarrow}}; \qquad \boldsymbol{M}_{\overset{\circ}{\leftarrow}} = \boldsymbol{M}^{T}_{\overset{\circ}{\rightarrow}}.$$

Введем для основных операторов (матриц) преобразований Грея символьное обозначение $\boldsymbol{g}_i$, полагая, что индексы $i = 2, 3, 4$ и 5 отвечают прямым (2, 4) и обратным (3, 5) лево- (2, 3) и правосторонним (4, 5) кодам. Дополнив перечисленную совокупность операторов операторами сохранения исходной комбинации $\boldsymbol{g}_0$ и инверсной перестановки $\boldsymbol{g}_1$, приходим к полной группе (табл.1) *простых операторов Грея.* В дальнейшем для простоты обозначения операторов вместо символов кодов будем использовать также их цифровые индексы.

Таблица 1. Полная группа простых операторов Грея

Обозначение оператора	Выполняемая операция
e (или 0)	Сохранение исходной комбинации
1	Инверсная перестановка
2	Прямое кодирование по Грею левостороннее
3	Обратное кодирование по Грею левостороннее
4	Прямое кодирование по Грею правостороннее
5	Обратное кодирование по Грею правостороннее

Оператор $\boldsymbol{g}_0$ представляет собой единичную матрицу $n-$го порядка, а $\boldsymbol{g}_1$ - матрицу инверсной перестановки.

Из элементов полной группы простых операторов Грея, представленных в табл. 1, можно сформировать так называемые *составные коды Грея* (СКГ), образуемые произведением простых (элементарных) кодов Грея.

Аналитически СКГ можно представить соотношением

$$\boldsymbol{G} = \prod_{j=1}^{k} \boldsymbol{g}_j ,$$

где $\boldsymbol{g}_j -$ простой КГ, выбираемый из полной группы $\{\overline{\boldsymbol{g}_0, \boldsymbol{g}_5}\}$, а $k -$ порядок СКГ.

Как простые, так и составные коды Грея обладают рядом замечательных свойств. Во-первых, отвечающие им матрицы преобразования являются невырожденными и в силу этого оказываются обратимыми. И, во-вторых, существуют достаточно простые алгоритмы обращения СКГ.

Синтез *n*-полных матриц

Перейдем теперь непосредственно к задаче синтеза невырожденных *n*-полных матриц $\boldsymbol{M}$. Как показали результаты компьютерных расчетов, интересными свойствами обладают матрицы, отвечающие СКГ типа $1\boldsymbol{g}$, где $\boldsymbol{g} = \overline{2,5}$. Замечательная особенность таких матриц состоит в том, что порядок L_n циклических групп, порождаемых операторами $1\boldsymbol{g}$, за небольшим исключением (названных нами артефактом), определяется соотношением:

$$L_n = 2^m - 1, \qquad m \le n, \tag{4}$$

где $n -$ порядок матрицы.

Более того, существуют такие значения порядка n, для которых элементы групп, порождаемые степенями матриц $\boldsymbol{M}$, составляют последовательность максимальной длины, равную $2^n - 1$. Такие матрицы названы нами *$n-$полными матрицами.*

Одним из важнейших результатов, к которому мы приходим на основании анализа свойств матриц, порождаемых СКГ $1\boldsymbol{g}$, состоит в том, что период цикла группы $1\boldsymbol{g}$, представляет собою *степенную величину*. Это обстоятельство, во-первых, дает нам возможность существенно сократить затраты машинного времени, необходимые для вычисления оценок L_n. И, во-вторых, наталкивает на мысль, о целесообразности поиска других выражений для СКГ (отличных от $1\boldsymbol{g}$), которые порождают *n*-полные матрицы $\boldsymbol{M}$. И такие СКГ были найдены. Часть из них, для примера, представлена в табл. 2.

Таблица 2. Составные коды Грея, доставляющие двоичным матрицам свойство n-полноты

Порядок матрицы (n)			
32	64	128	256
2244424	22533435	2425535	22533435
2442224	22534335	2433534	22534335
12242253	24334225	2435334	24334225
12242443	25224334	22524224	25224334
12252242	222524424	22533334	2222535224

Пусть $\boldsymbol{M}$ есть *n*-полная двоичная матрица, отвечающая СКГ $\boldsymbol{G}$. Относительно *n*-полных матриц $\boldsymbol{M}$ легко доказать (методом непосредственной проверки) следующее положение.

Утверждение. *n-полнота матриц $\boldsymbol{M}$ инвариантна к группам линейных преобразований $\boldsymbol{\Omega}$ над СКГ $\boldsymbol{G}$ и преобразований $\boldsymbol{Q}$ над строками и столбцами матриц $\boldsymbol{M}$.*

В состав $\boldsymbol{\Omega}$ **–** группы входят такие операторы линейных преобразований над $\boldsymbol{G}$: циклического сдвига, обращения (*I*), инверсии (*R*) и сопряжения (*C*), а также произвольные комбинации этих операторов.

Кратко поясним суть преобразований, входящих в $\boldsymbol{\Omega}$ группу. Введем (табл. 3) символику для операторов $\boldsymbol{\Omega}$ – группы преобразований. Стрелки оператора циклического сдвига указывают направление прокрутки СКГ $\boldsymbol{G}$, а нижний индекс k - задает число разрядов прокрутки. Например, $\overleftarrow{1}_3$ означает, что СКГ подвергается циклическому сдвигу по часовой стрелке на три разряда (символа) кода. Если $k=1$, то нижний индекс цифрового символа оператора циклического сдвига будем для простоты опускать.

Таблица 3. Символическое обозначение операторов преобразования

Обозначение оператора	Тип преобразования
$\overrightarrow{1}_k$, $\overleftarrow{1}_k$	Циклический сдвиг
I_f	Обращение полное
I_d	Обращение поразрядное
R	Инверсия
C	Сопряжение

Преобразование типа «обращение» соответствует вычислению обратного СКГ. «Инверсия» означает запись операторов СКГ в порядке, обратному последовательности простых операторов в исходном СКГ. И, наконец, преобразованиям типа «сопряжение» отвечают вычисления простого $\boldsymbol{g}^*$ или составного $\boldsymbol{G}^*$ операторов, сопряженных операторам $\boldsymbol{g}$ или $\boldsymbol{G}$, которые определяются соотношениями:

$$\boldsymbol{g}^* = 1 \cdot \boldsymbol{g} \cdot 1; \quad \boldsymbol{G}^* = 1 \cdot \boldsymbol{G} \cdot 1.$$

Будем называть преобразования, представленные в табл. 3, $\boldsymbol{\Omega}$ – преобразованиями. Обозначим через F составной оператор преобразования из $\boldsymbol{\Omega}$ – группы линейных преобразований. Например, $F = \overrightarrow{1}_k \cdot R \cdot C$ или $F = R \cdot I$ и т.д.

Предположим, что некая n-полная матрица $\boldsymbol{M}$ порядка n = 256 образована составным кодом Грея $\boldsymbol{G} = 25224334$. Фактически СКГ отвечает произведению (в кольце вычетов по mod 2) двоичных матриц n-го порядка. Это означает, что правила преобразования СКГ $\boldsymbol{G}$ совпадают с общими правилами преобразования над произведением матриц. Сведем в табл. 4 результаты простых и некоторых составных преобразований F над этим произведением.

Таблица 4. Примеры преобразований

Простой оператор преобразования	Результат преобразования	Составной оператор преобразования (F)	Результат преобразования
$\overleftarrow{1}_2$	22433425	$\overrightarrow{1}_3 C$	55244342
I_f	52253343	$\overleftarrow{1}_3 I_d C$	53443525
I_d	34335225	$I_f C R$	52553443
R	43342252	$R \overrightarrow{1}_3 C I_d$	52534435
C	25524434	$I_f \overleftarrow{1}_5 R$	35225343

Табл. 4 в какой-то мере иллюстрирует многообразие линейных операторов $\boldsymbol{\Omega}$ – преобразований, сохраняющих свойство n-полноты матриц $\boldsymbol{M}$.

$\boldsymbol{Q}$ – группу линейных преобразований над n-полными матрицами $\boldsymbol{M}$ составляют операторы «дружной перестановки» строк и столбцов матрицы, частным случаем которых являются операторы «дружного циклического сдвига» строк и столбцов матрицы $\boldsymbol{M}$.

Проиллюстрируем «дружную перестановку» строк и столбцов на примере матрицы $\boldsymbol{M}$ шестого порядка, сформированной СКГ $\boldsymbol{G}$ = 12435. Для удобства отобразим исходную матрицу в виде табл. 5. Выбрав «дружную перестановку» $\pi = 204153$, приходим к матрице, показанной в табл. 6. Исходная матрица, как и матрица, образованная «дружной перестановкой» ее строк и столбцов (не имеет значение, как организована дружная перестановка: сначала по столбцам, а потом по строкам, или наоборот), являются образующими элементами циклических групп одинакового порядка.

Таблица 5. Исходная матрица

		0	1	2	3	4	5
0		1	1	1	1	1	0
1		0	0	0	0	1	0
2		0	0	0	1	0	0
3		0	0	1	0	0	0
4		0	1	0	0	0	0
5		1	1	0	1	0	1

Таблица 6. «Дружная перестановка» строк и столбцов исходной матрицы

		2	0	4	1	5	3
2		0	0	0	0	0	1
0		1	1	1	1	0	1
4		0	0	0	1	0	0
1		0	0	1	0	0	0
5		0	1	0	1	1	1
3		1	0	0	0	0	0

«Дружный циклический сдвиг» строк и столбцов матриц сводится к циклической прокрутке столбцов по часовой стрелке на заданное число разрядов, а затем к циклической прокрутке строк матрицы сверху вниз на тоже число разрядов (или наоборот, сначала прокручиваются строки, а затем столбцы матрицы).

Оператор дружного циклического сдвига строк и столбцов матрицы $\boldsymbol{M}$ является ничем иным, как оператором формирования подобной матрицы $\boldsymbol{M}_p$, определяемый соотношением

$$\boldsymbol{M}_p = \boldsymbol{P} \cdot \boldsymbol{M} \cdot \boldsymbol{P}^{-1},$$

где $\boldsymbol{P}$ – матрица перестановки.

Целесообразность применения в криптографии и в других приложениях матриц, отвечающих составным кодам Грея, объясняется рядом замечательных свойств, которыми они обладают. Во-первых, матрицы, порождаемые СКГ любого порядка, чрезвычайно просто генерировать. Во-вторых, такие матрицы являются гарантированно невырожденными. В-третьих, для них легко вычисляются обратные матрицы. В-четвертых, как установлено на основании компьютерного моделирования, для произвольных порядков n матриц существуют такие СКГ, которые доставляют соответствующим матрицам свойство n- полноты. Это свойство проявляется в том, что порядок циклических групп, формируемых этими матрицами, достигает максимального значения, равного $2^n - 1$. И, наконец, в-пятых, если некоторая матрица $\boldsymbol{M}$ является n-полной, то это свойство сохраняется инвариантным к группам линейных $\boldsymbol{Q}$ – преобразований над строками и столбцами матриц $\boldsymbol{M}$ и $\boldsymbol{\Omega}$ – преобразований над СКГ $\boldsymbol{G}$.

Однонаправленная матричная функция

В данном разделе работы рассматривается задача осуществления однонаправленной функции на матрицах с целью построения алгоритма обмена криптографическими ключами по открытому каналу связи. По замыслу эти построения должны выполнять те же задачи, которые реализованы в известном протоколе Диффи-Хэллмана [3]. Идея эта, как отмечено в [6], не новая и была применена в ином исполнении еще в работе [7]. Интересное предложение относительно создания однонаправленной функции высказано [6].

Изложенный ниже протокол обмена ключами между абонентами открытой сети Алисой и Бобом опирается на алгоритм, приведенный в данной работе.

Суть протокола состоит в следующем. Пусть $\boldsymbol{M}$ – невырожденная n-полная матрица высокого порядка и $\boldsymbol{k}$ – двоичная вектор-строка длины n. Матрица $\boldsymbol{M}$, как и вектор $\boldsymbol{k}$, предполагаются открытыми. Алиса вырабатывает случайный показатель x, порядок которого не превышает n, вычисляет матрицу $\boldsymbol{M}^x$ и посылает Бобу вектор $\boldsymbol{a} = \boldsymbol{k} \cdot \boldsymbol{M}^x$. Боб, в свою очередь, также вырабатывает случайный показатель $ó$, вычисляет матрицу $\boldsymbol{M}^{ó}$ и посылает Алисе вектор $\boldsymbol{b} = \boldsymbol{k} \cdot \boldsymbol{M}^y$. Затем оба абонента умножают полученные векторы на свои матрицы в соответствующих степенях и получают общих ключ шифрования

$$\boldsymbol{K} = \boldsymbol{b} \cdot \boldsymbol{M}^x = \boldsymbol{k} \cdot \boldsymbol{M}^{y+x} \equiv \boldsymbol{a} \cdot \boldsymbol{M}^y = \boldsymbol{k} \cdot \boldsymbol{M}^{x+y}. \quad (5)$$

Ключ $\boldsymbol{K}$, образованный соотношением (5), подвержен атаке «человек посередине» и может быть взломан (подменен) [8]. Угрозу подмены ключа шифрования (5) можно ослабить, используя маскирующие матрицы. С этой целью Алиса формирует матрицу-маску $\boldsymbol{W}$ и по закрытому каналу передает Бобу обратную маску $\boldsymbol{W}^{-1}$. При наличии у абонентов указанных матриц векторы $\boldsymbol{a}$ и $\boldsymbol{b}$ подвергаются дополнительным преобразованиям (маскированию), в результате которых Боб получает вектор $\boldsymbol{a}_w = \boldsymbol{a} \cdot \boldsymbol{W}$, а Алиса – вектор $\boldsymbol{b}_w = \boldsymbol{b} \cdot \boldsymbol{W}$. Снимая маски, абоненты восстанавливают векторы $\boldsymbol{a}$ и $\boldsymbol{b}$, а затем преобразованием (5) образуют общий ключ шифрования $\boldsymbol{K}$.

Отметим такие особенности алгоритма маскирования ключа. «Человек посередине» в условиях отсутствия сведения относительно маскирующих матриц не в состоянии прочесть информацию, которой обмениваются Алиса и Боб, в силу того, что сформированный им ключ шифрования отличается от ключей шифрования, образуемых Алисой и Бобом. В самом деле, пусть □ и **ß –** векторы, которые соответственно получают Боб и Алиса от «человека посередине». В результате предписанных преобразований Алиса образует ключ $\hat{\boldsymbol{E}}_a =$ $\boldsymbol{ß} \cdot \boldsymbol{W} \cdot \boldsymbol{M}^x$**,** а Боб – ключ $\boldsymbol{K}_b = \square \cdot \boldsymbol{W}^{-1} \cdot \boldsymbol{M}^y$**.** Совершенно очевидно, что $\hat{\boldsymbol{E}}_a \neq \boldsymbol{K}_b$. Поэтому, как Алиса, так и Боб оказываются не в состоянии расшифровать полученную ими от партнера информацию, что является свидетельством присутствия в канале передачи информации «человека посередине».

Матричный алгоритм шифрования информации

Структурная схема алгоритма формирования секретной матрицы шифрования для абонентов Алиса и Боб отображена на рис. 4.

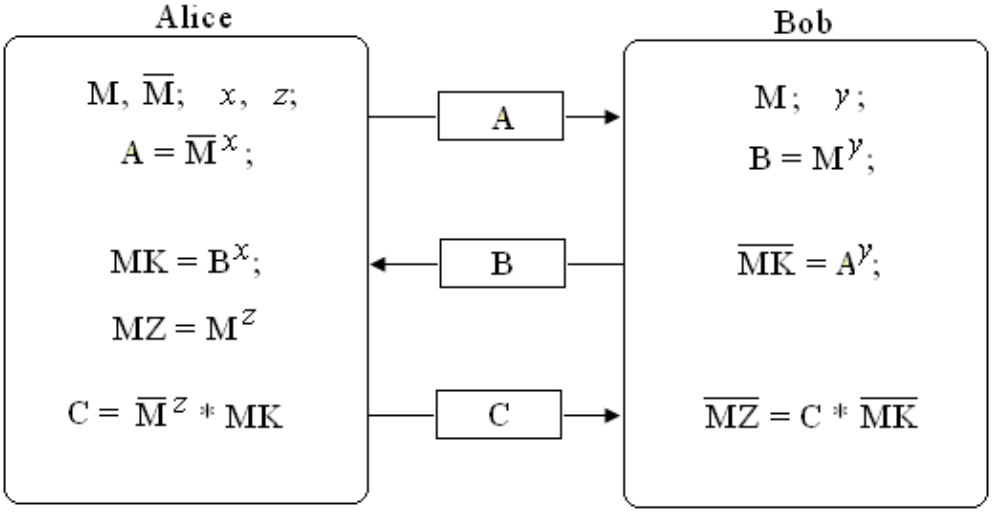

Рис. 4. Структурная схема алгоритма формирования секретной матрицы шифрования

Ниже приведено краткое описание протокола обмена ключами шифрования между абонентами A и B.

1. Предварительно абоненты договариваются о выборе некоторой n-полной матрицы M порядка n, которой соответствует обратная матрица $\overline{M}$. В результате «дружной перестановки» $\boldsymbol{\pi}$ их строк и столбцов образуются матрицы $\mathbf{M}$ и $\overline{\mathbf{M}}$.

2. Абонент A вырабатывает случайный показатель x, вычисляет матрицу $\mathbf{A} = \overline{\mathbf{M}}^{x}$ и посылает ее пользователю B.

3. Абонент B вырабатывает случайный показатель y, вычисляет матрицу $\mathbf{B} = \mathbf{M}^{y}$ и посылает ее пользователю A.

4. Абоненты A и B возводят полученные матрицы в свои показатели, формируя на стороне Алисы матрицу зашифрования $\mathbf{MK}$, а на стороне Боба – матрицу расшифрования $\overline{\mathbf{MK}}$.

Как указано в [9], подобный матричный шифр подвержен атаке «человек посередине» [8]. Кроме того, для известных M показатель y матрицы $\mathbf{M}^{y}$ может быть вычислен с помощью китайской теоремы об остатках [10]. Следовательно, при любых $\boldsymbol{\pi}$ шифр легко взламывается.

Приведем далее некоторые методы устранения атаки «человек посередине». Радикальным, но экономически не всегда целесообразным (финансово затратным) можно рассматривать способ, который состоит в организации защищенного канала обмена между абонентами сети исходными матрицами M и $\overline{M}$ (или соответствующим им СКГ G и $\overline{G}$).

Второй способ защиты основан на использовании вспомогательных матриц $\mathbf{MZ}$ и $\overline{\mathbf{MZ}}$, алгоритм формирования которых показан на рис. 4. Посредством данных матриц, которые назовем «трансформирующими матрицами», решается одна из важных задач шифрования, согласно которой не должно быть легко устанавливаемой зависимости между последовательно используемыми ключами. Передача информации от Алисы к Бобу может быть построена по следующей схеме. В самом начале сеанса связи по каналу передается какая-либо открытая информация. Затем, через некоторое число фрагментов передаваемых данных (о котором Алиса и Боб заранее договариваются), Алиса пересылает Бобу матрицу $\overline{\mathbf{MZ}}$ и оба абонента модифицируют (трансформируют) свои матрицы, переходя к матрице зашифрования $\mathbf{MK} = \mathbf{MK} * \mathbf{MZ}$ и матрице расшифрования $\overline{\mathbf{MK}} = \overline{\mathbf{MZ}} * \overline{\mathbf{MK}}$. Если на линии присутствует «человек посередине», то Боб не сможет правильно расшифровать переданную ему Алисой «контрольную фразу» и на этом сеанс связи прерывается.

И, наконец, в качестве третьего варианта защиты канала связи можно использовать метод «маскирующих матриц», рассмотренный в предыдущем разделе (Однонаправленные матричные функции).

Выводы:

1. Метод обобщенных кодов Грея предоставляет возможность построить достаточно простые алгоритмы синтеза n-полных невырожденных шифрующих двоичных матриц произвольного порядка n.
2. Свойство инвариантности порядка циклических групп, порождаемых шифрующими матрицами, к установленным линейным преобразованиям операторов СКГ или к «дружным перестановкам» строк и столбцов матриц шифрования, существенно расширяет множество матриц, которые могут быть использованы в матричных алгоритмах шифрования информации.
3. Атаку типа «человек посередине» на криптографический протокол Диффи-Хэллмана, которой подвержены также рассмотренные в статье его матричные аналоги, можно не только ослабить, но и устранить, применяя трансформирующие или маскирующие матрицы.
4. Предлагаемые протокол обмена криптографическими ключами и матричный алгоритм шифрования имеют хорошую перспективу применения в системах передачи данных по

открытым компьютерным сетям, обеспечивая необходимый уровень защиты информации от несанкционированного доступа.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Ерош И.Л. Адресная передача сообщений с использованием матриц над полем GF(2) / Ерош И.Л., Скуратов В.В. // Проблемы информационной безопасности. Компьютерные системы. 2004, №1. – С. 72-78.
2. Ерош И.Л. Скоростное шифрование разнородных сообщений / Ерош И.Л., Сергеев М.Б // Проблемы информационной безопасности. 2004. № 1. С. 72 – 78.
3. Diffie W., Hellman M.E., *"New Directions in Cryptography"*, IEEE Transactions on Information Theory, v. IT-22, no. 6, November 1976, 644-654.
4. Белецкий А.Я. Преобразования Грея. Монография в 2-х томах / Белецкий А.Я., Белецкий А.А., Белецкий Е.А. Т.1. Основы теории. – К.: Кн. изд-во НАУ, 2007. – 506 с., Т.2. Прикладные аспекты. – К.: Кн. изд-во НАУ, 2007. – 644 с.
5. Gray F. Pulse code communication. – Pat USA, № 2632058, 1953.
6. Мегрелишвили Р.П. Однонаправленная матричная функция – быстродействующий аналог протокола Диффи-Хэллмана. / Мегрелишвили Р.П., Челидзе М.А., Бесиашвили Г.М. – Збірник матеріалів 7-й МК «Інтернет-Освіта-Наука-2010». – Вінниця: ВНТУ, 2010. – С. 341-344.
7. Hill L.S. Cryptography in an Algebraic Alphabet. American Mathematical Montly, v. 36, Jun 1929, pp. 306-312.
8. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: «ТРИУМФ», 2003. – 816 с.
9. Ростовцев А.Г. О матричном шифровании (критика криптосистемы Ероша и Скуратова) www.ssl.stu.neva.ru/psw/crypto/rostovtsev/Erosh_Skuratov.pdf
10. Смарт Н. Криптография – М.: «Техносфера», 2005. – 528 с.