УДК 681.327

МАТЕМАТИЧЕСКИЕ МЕТОДЫ ФОРМИРОВАНИЯ МНОГОАЛФАВИТНЫХ ШИФРОВ ЗАМЕНЫ

Алексеев А.П.

В статье рассматривается шифр многоалфавитной замены, основанный на интегральном преобразовании.

Постановка задачи

Шифры одноалфавитной замены (например, квадрат Полибия) не являются криптостойкими. Значительно надежнее шифры многоалфавитной замены (например, шифр Виженера). В этих шифрах каждому символу открытого текста ставится в соответствие не один, а несколько символов алфавита замены [1].

Представляет интерес разработка и совершенствование криптостойких шифров многоалфавитной замены. Для создания таких шифров может быть использован различный математический аппарат, например, интегральное исчисление.

Разработка шифра многоалфавитной замены

В предлагаемом шифре каждый символ (буква, знак препинания, цифра) заменяется двумя вещественными числами. Эти два числа являются верхним и нижним пределами определенного интеграла. Значение интеграла используется для того, чтобы на приемной стороне по таблице замен определить, какому символу открытого текста соответствует вычисленное значение интеграла. Предполагается, что вид подынтегральной функции и конфигурация таблицы замен известны только доверенным лицам на передающей и приемной сторонах. В каждом сеансе связи таблица замен и подынтегральная функция определяются секретным ключом.

Рассмотрим порядок шифрования с помощью предлагаемого метода.

В данном сеансе связи из множества возможных видов выбирают некоторый конкретный вид подынтегральной функции:

$$I = \int_a^b f(x)dx . \qquad (1)$$

С помощью таблицы замен ставят в соответствие каждому символу алфавита открытого текста s_i определенный интервал вещественных чисел $[c_i; d_i)$.

Для шифрования некоторого символа s_i генерируют случайное число I_i из интервала $[c_i; d_i)$. Затем из некоторого допустимого интервала $[k; m]$ генерируют еще одно случайное число, например, a_i (нижний предел интегрирования). С помощью формулы Ньютона-Лейбница

$$\int_a^b f(x)\,dx = F(b) - F(a) \qquad (2)$$

по известным значениям интеграла I_i и нижнего предела a_i вычисляют значение верхнего предела b_i.

По открытому каналу связи передают два числа a_i и b_i. На приемной стороне числа a_i и b_i используют для вычисления интеграла I_i. Так как вид подынтегральной функции на приемной стороне известен, то вычисление определенного интеграла не представляет труда. Полученное значение I_i используется для определения с помощью таблицы замен принятого символа s_i.

Поясним идею с помощью конкретного примера.

Пусть для шифрования (в соответствии с некоторым ключом) выбрана подынтегральная функция $f(x) = x^2$, то есть

$$I = \int_a^b x^2 dx . \qquad (3)$$

Далее формируют таблицу замен. При этом каждому символу открытого текста в соответствии с ключом ставят в соответствие своё значение интервала вещественных чисел. Приведем фрагмент подобной таблицы (см. таблицу 1). Затем шифруют открытый текст.

Предположим, что нужно зашифровать символ «В». Вначале в соответствии с таблицей замен формируют случайное вещественное число из интервала $[c; d)$. Из таблицы 1 видно, что символ «В» может быть зашифрован любым вещественным числом из интервала [2; 3).

Допустим, что сгенерировано число $I = 2{,}5$. Затем генерируют некоторое случайное число (нижний предел интегрирования). Пусть таким числом будет $a = 3{,}2$.

Формула Ньютона-Лейбница (2) позволяет по известным значениям интеграла *I* и нижнего предела *a* вычислить верхний предел интегрирования. Для интеграла вида (3) верхний предел *b* вычисляют по формуле:

$$b = \sqrt[3]{3 \cdot I + a^3}\ . \qquad (4)$$

Подставляя значение интеграла I и нижнего предела a в (4), получают $b = 3{,}428$.

Таким образом, в линию предают два вещественных числа: 3,2 и 3,428, которые представляют собой замену символа «В».

На приемной стороне эти два числа используют для вычисления интеграла (3). Полученное число $I = 2{,}5$ позволяет по таблице замен определить значение принятого символа (буквы). Очевидно, что в данном случае это будет символ «В».

Таблица 1.

Символы текста, s_i	А	Б	В	Г	Д	Е	…
Интервалы замен, $[c;d)$	[0; 1)	[1; 2)	[2; 3)	[4; 5)	[5; 6)	[6; 7)	…

Замечания об округлении чисел

Объем шифрограммы и время ее передачи по каналу связи тесно связаны с разрядностью передаваемых чисел. Естественно, что разрядность чисел желательно уменьшать (не снижая криптостойкость). В этом случае потребуется выполнить разумное округление чисел. Из-за сделанных округлений в процессе шифрования могут произойти ошибки двух видов: принимаемый символ может быть воспринят (опознан на приеме), как соседний слева символ или как соседний справа символ (речь идет о таблице замен).

Рис. 1 поясняет, как могут возникнуть ошибки из-за неверного округления. На приеме буква «Б» может быть принята как буква «А», либо как буква «В». Округление значения интеграла I при шифровании не требуется, так как оно не передается по каналу связи. Поэтому разрядность этого числа может быть любой.

Округление первого сгенерированного предела интегрирования на передающей стороне не может сказаться на надежности дешифрации, так как по его значению вычисляется зависимый второй предел интегрирования. По этой причине первый сгенерированный предел можно округлять без всяких ограничений. Округление же зависимого предела (второго) должно происходить по определенным правилам.

Если интеграл генерируется в левой половине интервала замен, то предел округляется так, чтобы значение интеграла увеличивалось (чтобы на приеме не попасть в левый соседний интервал замен). Если интеграл сгенерирован в правой половине интервала замен, то округление ведется в сторону уменьшения вычисленного значения интеграла.

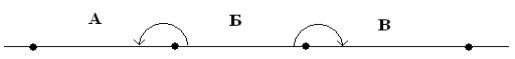

Рис. 1. Возможные ошибки на приемной стороне

Покажем, как с помощью рассмотренного метода может быть зашифрована фраза «ГДЕ АББА» (см. таблицу 2).

Прокомментируем полученные результаты. Следует обратить внимание на тот факт, что дважды встретившиеся в открытом тексте символы «А» и «Б» были зашифрованы разными парами вещественных чисел. Например, первая буква «А» зашифрована парой чисел (6,36; 6,363), а вторая буква «А» – числами (1,5; 1,81).

Таблица 2.

Текст	Г	Д	Е	А	Б	Б	А
I	4,3	5,11	6,8	0,12	1,4	1,785	0,85
a	3,98	12,3	0,11	6,36	2,43	8,2	1,5
b	4,235	12,334	2,732	6,363	2,647	8,226	1,81

Повторим шифрование, взяв прежнюю таблицу замен и новую подынтегральную функцию: $f(x) = e^x$. В этом случае верхний предел b вычисляется по формуле:

$$b = \ln(e^a + I)\,.$$

Результат шифрования приведен в таблице 3.

Сложность криптоанализа полученных шифровок состоит в том, что противник не знает, каков вид использованной таблицы замен, и какая использована подынтегральная функция. В реальной таблице замен символы располагаются в псевдослучайном порядке (не в алфавитном порядке). Кроме того, символы открытого текста (в том числе и одинаковые) в передаваемом сообщении не шифруется одинаковыми числами. Это

Таблица 3.

Текст	Г	Д	Е	А	Б	Б	А
I	4,85	5,82	6,07	0,52	1,59	1,03	0,45
a	0,6	1,2	2,1	1,85	2,43	4,71	0,824
b	1,898	2,213	2,656	1,929	2,561	4,719	1,004

обеспечивается генерацией в процессе шифрования каждого символа двух случайных чисел (значение интеграла и одного из пределов интегрирования). Заметим, что при генерации случайных чисел целесообразно использовать генераторы с равномерным распределением.

Не всякая подынтегральная функция может быть с одинаковым успехом использована при шифровании. Так тригонометрические функции вносят ограничения на значения подынтегральной функции и пределов интегрирования. Эти ограничения делают такую криптографическую систему сложно реализуемой.

В таблице 4 приведены примеры простейших подынтегральных функций и определены границы их использования для шифрования.

Таблица 4.

Подынт. функция $f(x)$	Вычисление нижнего предела a по известным I и b	Ограничения по b	Вычисление верхнего предела b по известным I и a	Ограничения по a
x	$a=\sqrt{b^2-2\cdot I}$	$b^2-2\cdot I\ge 0$	$b=\sqrt{2\cdot I+a^2}$	$2\cdot I+a^2\ge 0$
x^2	$a=\sqrt[3]{b^3-3\cdot I}$	-	$b=\sqrt[3]{3\cdot I+a^3}$	-
x^3	$a=\sqrt[4]{b^4-4\cdot I}$	$b^4-4\cdot I\ge 0$	$b=\sqrt[4]{4\cdot I+a^4}$	$4\cdot I+a^4\ge 0$
x^4	$a=\sqrt[5]{b^5-5\cdot I}$	-	$b=\sqrt[5]{5\cdot I+a^5}$	-
$\sin x$	$a=arc\ \cos(\cos b+I)$	$\lvert\cos b+I\rvert\le 1$	$b=arc\ \cos(\cos a-I)$	$\lvert\cos a-I\rvert\le 1$
$1/x$	$a=\exp(\ln\lvert b\rvert-I)$	$b>0$	$b=\exp(I+\ln\lvert a\rvert)$	$a>0$
C^x	$a=\log_c(C^b-I\cdot\ln C)$	$C^b>I\cdot\ln C$	$b=\log_C(I\cdot\ln C+C^a)$	$I\cdot\ln C+C^a>0$
e^x	$a=\ln(e^b-I)$	$e^b>I$	$b=\ln(e^a+I)$	$I>-e^a$

Анализ таблицы 4 показывает, что при использовании подынтегральных функций $f(x)=x^2$ и $f(x)=x^4$ нет ограничений на выбор пределов интегрирования. В некоторых случаях ограничения могут быть не жесткими, например, для $f(x)=1/x$ значения пределов интегрирования должны быть положительными числами. Ограничения могут быть и достаточно жесткими. Так для подынтегральной функции $f(x)=x^3$ генерация двух случайных чисел становится зависимой. После генерации значения интеграла I верхний предел интегрирования должен генерироваться с учетом ограничения $b\ge\sqrt[4]{4\cdot I}$.

Как известно [2], наиболее сложно произвести криптоанализ тех шифров, которые формируют равновероятную смесь чисел.

Для формирования шифрограммы с распределением чисел, близким к равномерному закону распределения, предлагается воспользоваться следующим алгоритмом.

Таблица 5.

Символы	a_1	a_2	a_3	...	a_n
Частоты	p_1	p_2	p_3	...	p_n

1. На основании статистического анализа открытого текста составляется таблица частот появления символов открытого текста.

2. Определяется минимальное значение частоты $p_{\min}$ и выполняется нормирование

$$g_i=\frac{p_i}{p_{\min}}.$$

В результате такого преобразования нормированные частоты будут лежать в пределах $g_i\ge 1$. Величина g_i показывает, во сколько раз частота

появления данного символа больше, чем частота появления наиболее редко встречающегося символа в текстах, подвергнутых статистической обработке.

3. Задается (выбирается) ширина интервала замен для символа с наименьшей частотой появления:

$$\Delta_{\min} = d - c .$$

4. Вычисляется ширина интервалов замен для остальных символов открытого текста

$$\Delta_i = g_i \Delta_{\min} . \qquad (5)$$

5. Составляется таблица замен, в которой ширина интервала замен вычисляется по формуле (5), а положение интервала замен на числовой оси определяется сеансовым ключом. При этом все интервалы замен должны образовать непрерывную числовую последовательность. Границы интервалов замен будут, как правило, не целыми, а вещественными числами.

Рассмотрим пример определения ширины интервала замен для каждого символа.

Таблица 6.

Буква	p_i	Буква	p_i	Буква	p_i	Буква	p_i
О	0.09	В	0.038	З	0.016	Ж	0.007
Е,Ё	0.072	Л	0.035	Ы	0.016	Ш	0.006
А	0.062	К	0.028	Б	0.014	Ю	0.006
И	0.062	М	0.026	Ь,Ъ	0.014	Ц	0.004
Н	0.053	Д	0.025	Г	0.013	Щ	0.003
Т	0.053	П	0.023	Ч	0.012	Э	0.003
С	0.045	У	0.021	Й	0.01	Ф	0.002
Р	0.04	Я	0.018	Х	0.009		

Пусть частот таблица 6 задана: из нее видно, что реже всего встречается буква «Ф». Частота появления этой буквы $p_{\min} = 0{,}002$. После нормирования (вычисление $g_i = p_i / p_{\min}$) таблица 7 частот будет иметь вид

Таблица 7.

Буква	g_i	Буква	g_i	Буква	g_i	Буква	g_i
О	45	В	19	З	8	Ж	3,5
Е,Ё	36	Л	17,5	Ы	8	Ш	3
А	31	К	14	Б	7	Ю	3
И	31	М	13	Ь,Ъ	7	Ц	2
Н	26,5	Д	12,5	Г	6,5	Щ	1,5
Т	26,5	П	11,5	Ч	6	Э	1,5
С	22,5	У	10,5	Й	5	Ф	1
Р	20	Я	9	Х	4,5		

Затем необходимо задать интервал замены для буквы «Ф». Выберем, например, $\Delta_{\min} = 2$. Далее вычисляется ширина интервалов замен для остальных символов открытого текста $\Delta_i = 2g_i$. В новом сеансе связи выбирается другое значение $\Delta_{\min}$. Например, $\Delta_{\min} = 1{,}731$.

Дальнейшее усложнение рассмотренного алгоритма шифрования может быть осуществлено следующим образом. Найденная ширина интервала замен каждого символа дробится на n частей:

$$\Delta_i = \Delta_{i1} + \Delta_{i2} + \ldots + \Delta_{in} .$$

Затем все дробленые интервалы Δ_{ij} всех символов тасуются (переставляются, перемешиваются) таким образом, чтобы образовать непрерывную числовую последовательность. Другими словами: каждой букве открытого текста ставится в соответствие не один, а несколько интервалов замен (как бы каждая буква равномерно распыляется по числовой оси).

Еще один прием дальнейшего увеличения криптостойкости заключается в том, что шифровку передают не парами чисел (которые соответствуют одному зашифрованному символу), а в разбивку: например, 4 верхних предела – 4 нижних; 3 верхних, 3 – нижних; 6 верхних, 6 – нижних и т.д. Порядок передачи верхних и нижних пределов определяется сеансовым ключом.

Вероятно, наиболее подходящими для шифрования будут подынтегральные периодические функции с изменяющейся амплитудой и частотой. Такие функции позволяют формировать на-

иболее разнообразные значения интегралов на разных участках числовой оси.

Выводы

Предложен метод шифрования, основанный на замене символов открытого текста двумя вещественными числами. Одно из чисел генерируется с помощью датчика случайных чисел. Особенностью шифра является использование интегральных преобразований для получения второго числа. Другой особенностью описанного шифра является формирование таблицы замен, в которой символы распылены по числовой оси. Криптоанализ усложняется благодаря генерации двух случайных чисел (значения интеграла и одного из пределов). Секретный ключ определяет форму таблицы замен и вид подынтегральной функции.

Литература

1. Алексеев А.П. Информатика 2007. М.: СОЛОН-ПРЕСС, 2007. – 608 с.
2. Бабаш А.В., Шанкин Г.П. Криптография. М.: СОЛОН-Р, 2002. – 512 с.

ТЕХНОЛОГИИ ТЕЛЕКОММУНИКАЦИЙ

УДК 621.392

БЕСПРОВОДНЫЕ MESH-СЕТИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Легков К.Е., Федоров А.Е.

В настоящее время наиболее распространенной технологией беспроводного доступа, которая повсеместно применяется для передачи большого количества трафика различного вида, является стандарт беспроводных локальных сетей IEEE 802.11. Одним из самых перспективных направлений развития технологии Wi-Fi стали mesh-сети, описываемые в стандарте IEEE 802.11s. В статье рассмотрена возможность применения данного стандарта для сил специального назначения и работа одного из известных алгоритмов назначения каналов в сетях IEEE 802.11s – Hyacinth с централизованным способом назначения каналов.

Перспективный класс широкополосных беспроводных сетей передачи мультимедийной информации – mesh-сети, которые являются одним из направлений развития технологии Wi-Fi [1] и описываются в стандарте IEEE 802.11s [2]. Одним из главных принципов построения mesh-сети является принцип самоорганизации архитектуры, обеспечивающий такие возможности, как реализацию топологии сети «каждый с каждым»; устойчивость сети при отказе отдельных компонентов; масштабируемость сети; динамическую маршрутизацию трафика; контроль состояния сети и т.д. Mesh-технология становится особенно необходимой при отсутствии проводной инфраструктуры для соединения станций.

Эти положительные качества неуклонно подводят к вопросу о применении таких технологий для обеспечения управления в силовых структурах при выполнении специальных задач. Благодаря низким ценам на оборудование Wi-Fi, а также легкости в установке, возможно его массовое применение и в организациях специального назначения. Границу автоматизации, как общепринятого способа повышения эффективности функционирования любой системы, можно довести до отдельного сотрудника. Такой процесс давно происходит в армиях и организациях специального назначения ведущих государств мира, в частности в США. В комплект оснащения для каждого сотрудника могут входить вычислительный комплекс, набор датчиков, видео- и инфракрасные камеры, шлем со встроенным монитором, отображающим цифровую карту и местонахождение своих и чужих подразделений, и устройство беспроводной связи. Технология передачи мультимедийных данных в условиях единого информационного пространства мест проведения операций должна функционировать по особым правилам.

Останавливаясь на mesh-сетях IEEE 802.11s [2], необходимо отметить, что данная спецификация рекомендует применять станции (узлы), содержащие несколько радиоинтерфейсов. Это позволяет одновременно использовать несколько частотных каналов для передачи информации. Общаясь с каждым из своих соседей, узел использует конкретный интерфейс (интерфейсы). Каждый интерфейс использует определенный канал. Механизмы назначения каналов (и другие механизмы функционирования) влияют на производительность сети, которая к тому же зависит от особенностей трафика. В системах управления специального назначения особенности трафика проявляются в его направлении, приоритетах, пульсации и др. С достаточной степенью