УДК 681.322

МНОГОАЛФАВИТНЫЙ БЛОЧНЫЙ ШИФР СО СКРЫТОЙ НУМЕРАЦИЕЙ БЛОКОВ

А. П. Алексеев,
канд. техн. наук, доцент
М. И. Макаров,
аспирант
Поволжский государственный университет телекоммуникаций и информатики

Рассматривается шифр многоалфавитной замены, основанный на интегральном преобразовании, работа которого строится таким образом, чтобы выходное распределение чисел криптограммы было равномерным. В шифре используется дробление криптограммы на блоки, скрытая нумерация каждого блока и пересылка блоков по нескольким каналам связи.

Ключевые слова *— криптография, стеганография, адаптивный многоалфавитный шифр, пространственно-временной метод распыления информации.*

Введение

Шифры одноалфавитной замены не являются криптостойкими. Значительно надежнее шифры многоалфавитной замены. В этих шифрах каждому символу открытого текста ставится в соответствие не один, а несколько символов алфавита замены. Многоалфавитные шифры замены повышают криптостойкость. Тем не менее существует возможность взлома и многоалфавитных шифров, которые продолжают наследовать статистическую картину распределения частоты появления символов открытого текста.

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

Для увеличения криптостойкости шифра предлагается с помощью многоалфавитной замены и интегральных преобразований обеспечить равномерное распределение числовых данных криптограммы, разбить криптограмму на блоки различной длины, скрытно пронумеровать блоки и передать их по разным каналам связи.

Разработка шифра многоалфавитной замены

Основная идея построения шифра заключается в формировании криптограммы в виде равномерной смеси вещественных чисел.

Равномерность распределения вещественных чисел в криптограмме достигается тем, что в процессе шифрования ведется анализ получающегося распределения чисел шифрограммы. С этой целью непрерывно строится гистограмма распределения. При этом очередные элементы шифровки формируются таким образом, чтобы они попали в те места распределения, где наблюдаются провалы (глобальные минимумы). Возможность изменять (варьировать) положение очередного элемента криптограммы на числовой оси имеется благодаря тому, что при шифровании используются многоалфавитная замена и интегральное преобразование [1].

Алгоритм шифрования таков, что осуществляется непрерывный анализ выходного распределения и выполняется такая коррекция (адаптация) шифра, при которой обеспечивается приближение формируемых чисел к равномерному закону распределения.

Многоалфавитное шифрование предполагает, что каждый символ открытого текста многократно встречается в таблице замен на различных участках числовой оси. В табл. 1 приведен фрагмент некоторой упрощенной таблицы многоалфавитной замены (ТМЗ). При этом считается, что буква «е» встречается в открытом тексте чаще, а буква «д» — реже других. По этой причине для буквы «е» выделено 6 интервалов многоалфавитной замены, а для буквы «д» — только 2.

Рассмотрим, как осуществляется шифрование с помощью ТМЗ. Предположим, что нужно

■ ***Таблица 1***. *Фрагмент ТМЗ*

Интервалы замены в алфавите открытого текста					
а	б	в	г	д	е
[5...6)	[2...3)	[4...5)	[3...4)	[1...2)	[6...7)
[8...9)	[10...11)	[11...12)	[7...8)	[9...10)	[12...13)
[13...14)	[14...15)	[17...18)	[15...16)	–	[16...17)
[18...19)	–	[21....22)	[20...21)	–	[19...20)
[23...24)	–	–	–	–	[22...23)
–	–	–	–	–	[24...25)

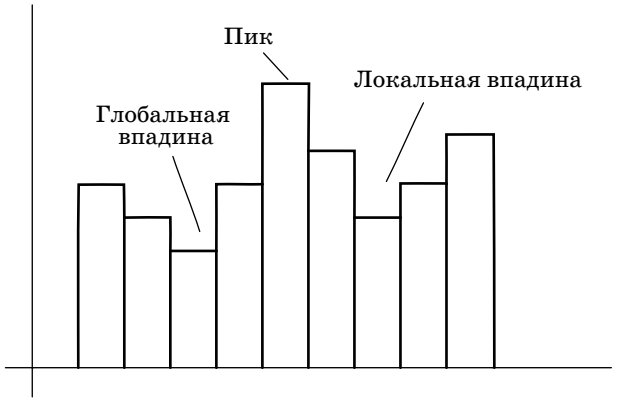
зашифровать фразу «где абба». Шифровку можно создать бесконечным числом способов. При этом каждую букву допустимо заменять любым вещественным числом из указанных интервалов. Приведем две криптограммы для указанной фразы:

1) 15,33 — 9,101 — 22,99 — 18,06 — 14,57 — 2,331 — 5,064;

2) 7,105 — 1,102 — 12,98 — 8,473 — 10,16 — 14,91 — 23,26.

В предлагаемом шифре после многоалфавитной замены осуществляется интегральное преобразование каждого полученного числа. Это дает возможность один из пределов интегрирования выбирать по случайному закону [2]. При этом нужно находить очередной предел интегрирования таким образом, чтобы формируемое число криптограммы попало в зону наибольшего провала (в зону глобальной впадины) на гистограмме.

Для шифрования адаптивным (подстраиваемым) шифром необходимо постоянно решать такую задачу: по найденному числу в выходном распределении выбирать такое значение предела интегрирования, которое обязательно попадет в заданный интервал гистограммы. Эту идею иллюстрирует рис. 1. После зашифрования очередного символа гистограмма достраивается (пополняется). На гистограмме выделяется максимальное значение (пик), минимальное значение (глобальная впадина) и провалы (локальные впадины). Формирование криптограммы ведется так, чтобы с максимально возможной степенью выровнять имеющееся выходное распределение.



■ ***Рис. 1***. *Гистограмма выходного распределения*

Предположим, что наибольший провал на гистограмме наблюдается в интервале чисел $[c_i, c_{i+1}]$. Пусть при этом для интегрального преобразования используется некоторая подынтегральная функция $f(x)$:

$$I = \int_a^b f(x)\mathrm{d}x.$$

Для того чтобы уменьшить глубину глобальной впадины на гистограмме, генерируют случайное число a из интервала $[c_i, c_{i+1}]$. По ТМЗ определяется значение интеграла I, которое соответствует шифруемому символу. По известному значению нижнего предела интегрирования a и величине интеграла I находят значение верхнего предела интегрирования b:

$$b = \varphi(a, I).$$

Полученные числа a и b передают в линию. Эти числа являются элементами криптограммы (шифровкой). Заметим, что пределы интегрирования можно формировать и в обратном порядке: сначала выбирать b, а потом вычислять a.

На приемной стороне известны вид использованного интегрального преобразования (подынтегральная функция) и конфигурация ТМЗ. Эти два элемента определяются секретным сеансовым ключом. Поэтому процесс дешифрации криптограммы не вызывает затруднений. Он сводится к вычислению определенного интеграла по известным значениям нижнего и верхнего пределов интегрирования и определению принятого символа по ТМЗ.

Таким образом, сформированная величина a обязательно попадет в зону глобального минимума гистограммы, а верхний предел интегрирования b случайно окажется в одной из зон гистограммы.

Величину b в процессе шифрования также можно приблизить к одной из локальных впадин на гистограмме (эта величина даже может попасть в зону глобальной впадины). Для этого нужно произвести расчеты верхнего предела интегрирования b при имеющемся значении нижнего предела интегрирования a, поочередно выбирая допустимые значения интеграла I из ТМЗ. При расчете верхнего предела интегрирования b желательно не допустить попадания этого числа в зону пика гистограммы. Все другие результаты расчетов являются приемлемыми.

Число интервалов k на гистограмме, предназначенной для контроля выходного распределения, можно примерно оценить по формуле Стержесса:

$$k \approx 1 + 3{,}32 \lg n, \qquad (1)$$

где n — число элементов (вещественных чисел) в криптограмме.

Зависимость числа интервалов в гистограмме k от длины (числа символов) зашифрованного текста n следующая:

n	100	1000	10 000	100 000	1 000 000
k	7,64	10,96	14,28	17,6	20,92

С учетом того, что при шифровании каждый символ открытого текста s заменяется двумя вещественными числами ($n = 2s$), при длине открытого текста (сообщения) $s = 500$ символов число интервалов k на гистограмме оценивается числом 10,96 (это значение округляется до целого числа 11).

На передающей стороне ТМЗ служит для замены символа открытого текста на некоторое вещественное число. Это число эквивалентно значению определенного интеграла, для которого определяются значения верхнего и нижнего пределов интегрирования. На приемной стороне ТМЗ используется для определения значения принятого символа по величине определенного интеграла, вычисленного с помощью полученных значений верхнего и нижнего пределов интегрирования. ТМЗ является элементом секретного ключа.

Рассмотрим порядок формирования ТМЗ.

1. Вначале нужно определить длину открытого текста, подлежащего шифрованию. Пусть $S_{\max} = 50\,000$ символов. Тогда число вещественных чисел, из которых будет состоять криптограмма, $n = 100\,000$.

2. По формуле (1) следует оценить число необходимых интервалов на гистограмме. Для выбранного значения $S_{\max}$ число интервалов $k = 17{,}6$.

3. Определить общее число интервалов в ТМЗ t, которое должно быть на один-два порядка больше числа k. Кроме того, число интервалов в ТМЗ должно быть в 3–4 раза больше числа символов в алфавите открытого текста. Таким образом, число интервалов в ТМЗ лежит в пределах 176–1760. Примем $t = 1000$.

4. Найти сумму нормированных частот символов открытого текста

$$sg = \sum_{i=1}^{r} g_i,$$

где r — число символов в алфавите открытого текста ($r = 256$ при использовании всех символов таблицы СР-1251 и $r = 33$ при использовании только русских строчных или заглавных букв); g_i — нормированная частота.

Нормированные частоты появления символов в открытом тексте g_i получают путем деления абсолютных частот на наименьшее значение абсолютной частоты.

5. Вычислить число интервалов замен для каждого i-го символа алфавита открытого текста

$$t_i = \frac{g_i t}{\sum_{i=1}^{r} g_i}.$$

Для примера вычислим число интервалов замен для букв «а» и «б»:

$$t_{\text{а}} = \frac{619 \cdot 1000}{7939} = 78; \quad t_{\text{б}} = \frac{105 \cdot 1000}{7939} = 13.$$

6. Задать диапазон (ширину) гистограммы и ее положение на числовой оси. Это означает, что задаются значения $a_{\min}$ и $b_{\max}$ (для случаев, когда определенный интеграл принимает только положительные значения). Задать ширину и положение на числовой оси ТМЗ, т. е. определить значения $I_{\min}$ и $I_{\max}$. Перечисленные величины связаны между собой, и соотношения между ними зависят от вида подынтегральной функции:

$$I_{\max} = \varphi(a_{\min}, b_{\max}); \; I_{\min} \approx 0.$$

Например, для подынтегральной функции $f(x) = x^4$ правая граница для ТМЗ вычисляется по формуле

$$I_{\max} = \frac{b_{\max}^5 - a_{\min}^5}{5}.$$

Вычислить ширину одного интервала замен

$$\Delta = \frac{I_{\max} - I_{\min}}{t}.$$

Пусть $\Delta = 0{,}1$.

7. Составить ТМЗ, в которой ширина каждого интервала замен равна Δ, а общее число интервалов замен равно t. Все интервалы замен образуют непрерывный интервал чисел шириной Δt. Для рассматриваемого случая $\Delta t = 0{,}1 \cdot 1000 = 100$. Каждому интервалу замен ставят в соответствие один из символов алфавита открытого текста. При этом число интервалов замен для буквы «а» равно $t_{\text{а}}$, для буквы «б» равно $t_{\text{б}}$ и т. д. Интервалы замен для каждого символа располагаются на числовой оси в случайном порядке.

Конфигурация ТМЗ является одним из элементов секретного ключа. Вторым элементом ключа является вид подынтегральной функции. Заметим, что криптоанализ рассматриваемого шифра усложняется еще за счет того, что выбираемое из ТМЗ число и один из пределов интегрирования выбираются по случайному закону.

Примеры шифрования с помощью адаптивного многоалфавитного шифра.

Предположим, что в текущий момент времени необходимо зашифровать букву «в». В качестве

первого ключевого элемента используется табл. 1. Вторым элементом секретного ключа является вид подынтегральной функции. Пусть $f(x) = x^4$.

Предположим, что на гистограмме, сформированной на предыдущих шагах шифрования, наблюдается глобальная впадина в диапазоне чисел [6...10).

Для зашифрования буквы «в» по случайному закону из табл. 1 выбирается один из четырех интервалов замен. Допустим, что выбран интервал 3, т. е. (17...18]. Из этого интервала генерируется случайное число, например $I = 17{,}58$.

Для заполнения провала на гистограмме генерируется случайное число a из интервала [6...10). Пусть $a = 8{,}02$. С учетом формулы Ньютона—Лейбница для выбранной подынтегральной функции получаем

$$b = \sqrt[5]{5I + a^5}.$$

Расчет верхнего предела интегрирования дает значение $b = 8{,}024$. Таким образом, оба числа a и b попали в зону глобальной впадины. «Рассеяние» (отличие, отклонение) пределов интегрирования в рассмотренном случае небольшое.

В качестве подынтегральной функции желательно выбрать функцию, у которой с изменением аргумента существенно меняются амплитуда и частота колебаний.

При выборе вида подынтегральной функции $f(x)$ и нахождении первообразной $F(x)$ можно воспользоваться следующими соображениями.

Представим подынтегральную функцию в виде

$$f(x) = \omega'(x)\sin\omega(x). \qquad (2)$$

Тогда с учетом известного соотношения

$$F'(x) = f(x)$$

для подынтегральной функции (2) получим

$$F(x) = -\cos\omega(x).$$

В качестве $\omega(x)$ можно использовать большой класс функций, например

$$\omega(x) = Ax + C\sin Bx.$$

Тогда

$$f(x) = (A + BC\cos Bx)\sin(Ax + C\sin Bx).$$

В этом случае первообразная определяется выражением

$$F(x) = -\cos(Ax + C\sin Bx).$$

Понятно, что первообразная должна быть использована при вычислении нижнего и верхнего пределов интегрирования, которые являются элементами шифра. Коэффициенты A, B и C можно использовать в качестве элементов ключа рассмотренного шифра.

Пространственно-временное распыление информации

Процедура дробления криптограммы на несколько блоков и передачи их по нескольким каналам связи создает перед криптоаналитиками дополнительный барьер защиты. Очевидно, что помимо традиционных проблем с атакой на шифр возникают проблемы с перехватом (или поиском мест хранения) всех сообщений и выстраиванием их в нужном порядке.

Под каналами связи будем понимать не только традиционные каналы связи (радио, радиорелейные, спутниковые, кабельные, почтовые), но и передачу информации с помощью мультимедийных контейнеров (графики, текста, звука, видео), при этом сама криптограмма может быть стеганографически скрыта в указанных контейнерах. Передачу можно осуществлять с помощью электронной почты, мессенджеров, чатов, SMS, MMS, web-страниц, микроблогов, файлообменных сетей.

Предлагается передачу блоков криптограммы осуществлять не последовательно и не непрерывно, а в порядке, который определяет генератор псевдослучайных чисел. При этом он определяет, какой из множества блоков криптограммы передается, по какому каналу и в какой момент времени. Таким образом, сформированная псевдослучайная последовательность становится элементом секретного ключа. Помимо информационных блоков по каналам связи можно передавать маскирующие (дезинформирующие) блоки.

Каждый информационный блок на передаче получает порядковый номер, с помощью которого сообщение на приеме восстанавливается в исходной последовательности, вне зависимости от порядка и времени поступления блоков в канал связи. В данном шифре стеганограммой будет являться порядковый номер блока криптограммы.

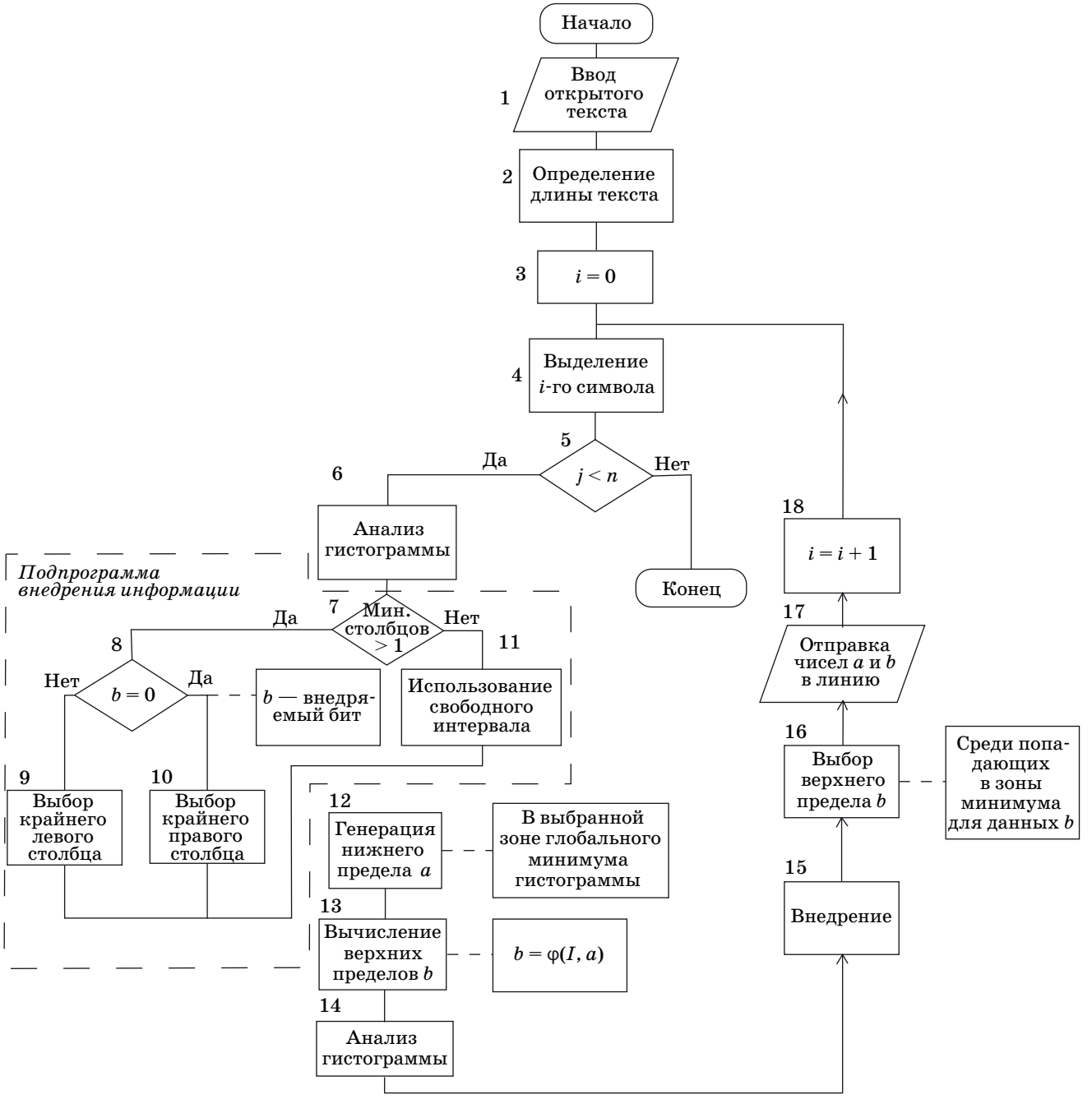
Естественно, что номера блоков должны оставаться скрытыми от противника. Скрытая нумерация блоков может осуществляться криптографическими или стеганографическими способами. В первом случае блок криптограммы должен содержать порядковый номер этого блока. Номер блока должен быть зашифрован тем же ключом, что и вся криптограмма. Известны технические решения, в которых номер блока шифруется шифром, который отличается от основного.

Для реализации шифра с пространственно-временным распылением информации необходимо выполнить две операции: разбить криптограмму на блоки и скрытно пронумеровать эти блоки.

Стеганографическое внедрение информации

Одно из направлений современной стеганографии занимается исследованием внедрения информации в криптограммы [3–6]. За основу разрабатываемого шифра был взят адаптивный многоалфавитный шифр с интегральным преобразованием [2].

Номер каждого блока криптограммы представляют в двоичной системе счисления. При сокрытии считывается внедряемый бит двоичного числа, и если он равен 1, то при шифровании выбирается столбец, ближайший к началу гистограммы (если допустимо, то используется крайний левый столбец). Если внедряемый бит равен 0, то выбирается столбец гистограммы (точнее, интервал) с максимальным удалением от начала числовой оси (крайний правый столбец). Если отсутствует выбор среди столбцов (т. е. остается единственный допустимый интервал гистограммы), то внедрение стеганограммы переносится на следующие шаги алгоритма (рис. 2). На прием-



■ ***Рис. 2.*** *Блок-схема алгоритма внедрения информации*

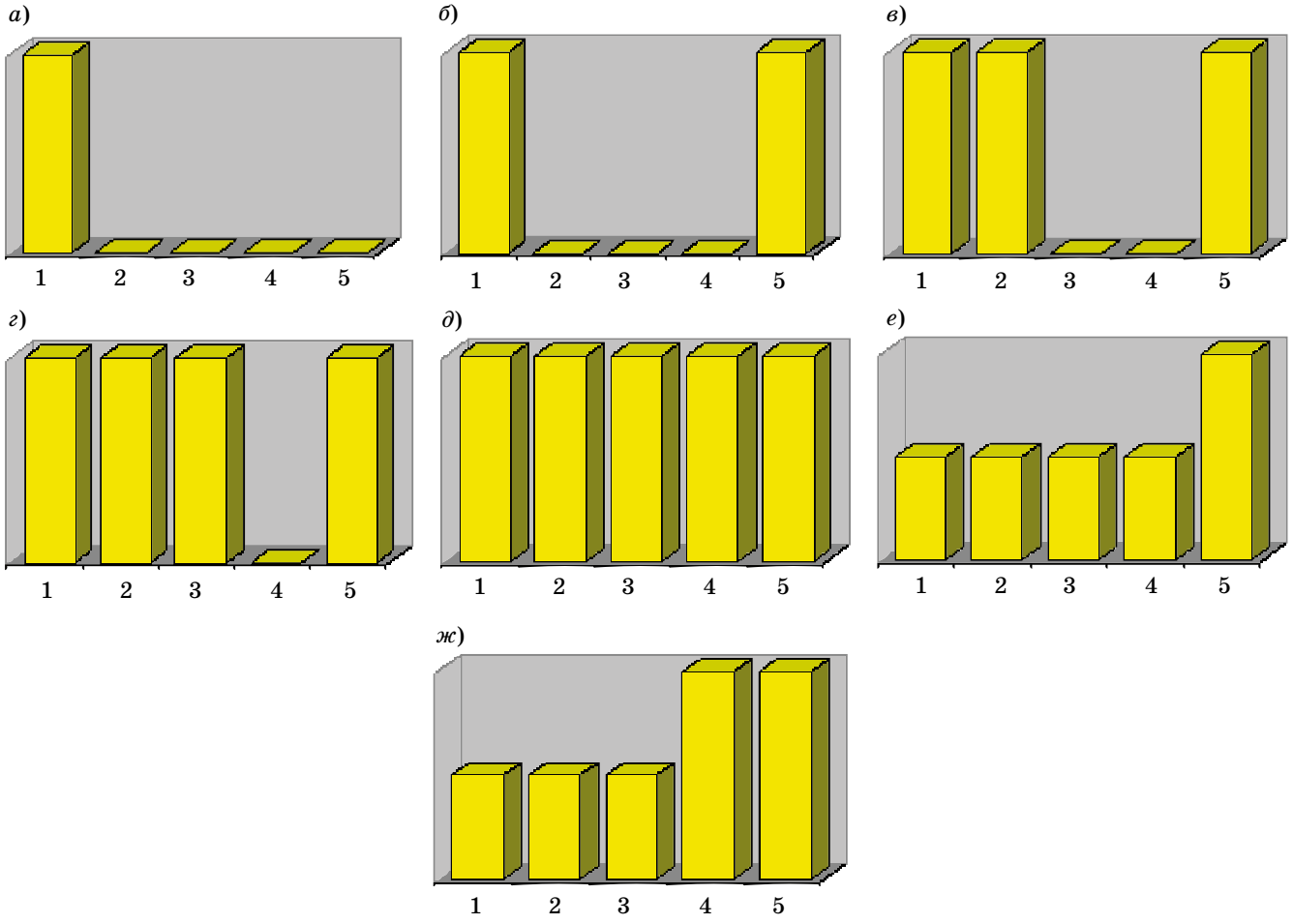
ной стороне после расшифрования переданного сообщения по полученным нижним и верхним пределам интегрирования и вычисленным значениям интеграла производится поэтапное восстановление (реконструкция) гистограммы. При этом на приеме необходимо восстановить последовательность заполнения гистограммы, реализованную на передающей стороне.

Рассмотрим **пример**, в котором таблица многоалфавитной замены составлена так, что при заданной подынтегральной функции, например x^4, выбор предела интегрирования может осуществляться из всех интервалов гистограммы. Допустим, что число интервалов (столбцов гистограммы) пять. Пусть очередному блоку криптограммы требуется присвоить порядковый десятичный номер 44 (двоичное число 101100).

В первоначальном состоянии гистограммы (в момент начала шифрования) все интервалы гистограммы пустые. Так как первый бит (старший бит числа) скрываемой стеганограммы равен 1, то выбирается предел интегрирования из интервала столбца *1* гистограммы (крайний левый столбец, рис. 3, *а*).

Далее производится предварительный расчет второго предела интегрирования для всех возможных значений интеграла для данной шифруемой буквы. В этом примере ТМЗ составлена так, что предел интегрирования может попасть в любой столбец. На данном этапе идет выбор между интервалами (столбцами) *2, 3, 4* и *5*. Так как второй бит скрываемой стеганограммы равен 0, то выбирается число (предел интегрирования) из столбца *5* (крайний правый столбец, рис. 3, *б*).

Рассмотрим процесс шифрования второй буквы открытого текста. Интервал выбирается среди столбцов с номерами *2, 3* и *4*. Так как нужно скрыть бит со значением 1 (третий бит), то выбирается столбец *2* (крайний левый среди минимально заполненных, рис. 3, *в*). Для значения второго предела интегрирования выбирается область определения среди столбцов *3* и *4*. При сокрытии четвертого бита стеганограммы, который равен 1, выбирается *3*-й диапазон (крайний левый среди минимально заполненных, рис. 3, *г*). Следующий этап — выбор интервала для первого предела интегрирования третьей буквы. В этой ситуации выбора нет, так как есть только один



■ ***Рис. 3.*** *Этапы (а—ж) построения гистограммы*

допустимый интервал — *4*-й, откуда и выбирается очередной предел интегрирования. В подобных случаях (когда нет выбора между двумя допустимыми столбцами) скрыть очередной бит стеганограммы невозможно. В такой ситуации сокрытие информации не происходит, а идет штатное формирование криптограммы (рис. 3, *д*).

Затем выбирается второй предел интегрирования для третьей буквы. Сейчас интервалов с минимальным заполнением пять — *1, 2, 3, 4* и *5*. Теперь требуется скрыть пятый бит стеганограммы, равный 0. Выбирается крайний правый столбец — *5*-й (рис. 3, *е*). Далее выбирается первый предел интегрирования для четвертой буквы из интервалов с номерами *1, 2, 3* и *4*. Так как требуется скрыть бит, равный 0, то выбирается *4*-й интервал (крайний правый допустимый, рис. 3, *ж*).

Разбиение криптограммы на отдельные блоки

Разбиение криптограммы на блоки происходит в тех местах алгоритма (в те моменты времени), когда при шифровании все столбцы гистограммы имеют одинаковую высоту.

Таким образом, каждый блок криптограммы на приеме можно расшифровывать отдельно, задав все начальные значения гистограммы нулевыми. Это приведет к верному расшифрованию каждого блока криптограммы и правильному извлечению скрытого номера блока.

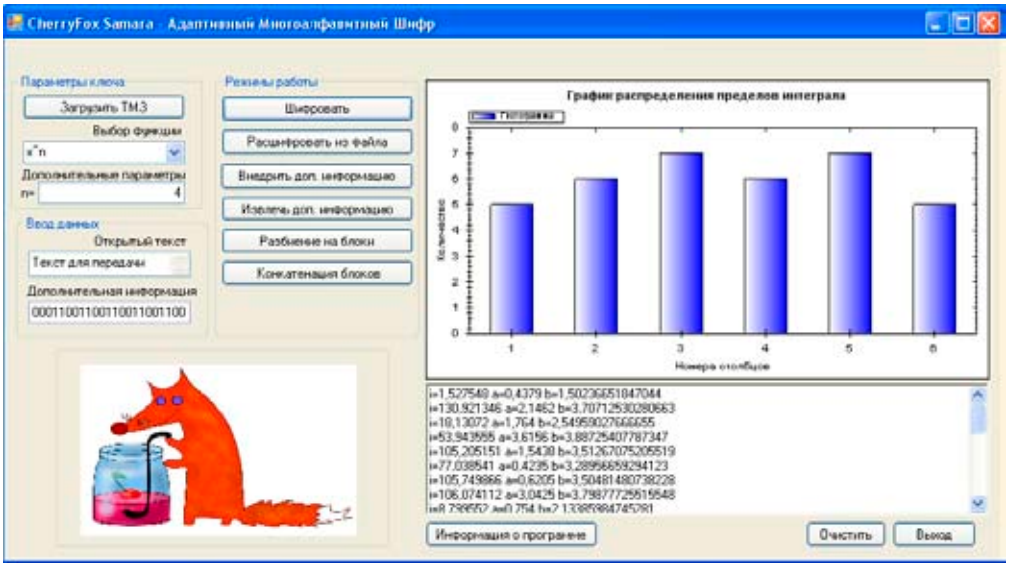
Разбиение на блоки позволяет осуществить раздельную передачу шифра по различным (нескольким) каналам связи, в произвольном порядке и в псевдослучайные моменты времени. Передачу информационных блоков можно перемежать передачей маскирующих блоков. Таким образом увеличивается безопасность передаваемой информации. Перед криптоаналитиком помимо основной задачи по взлому и перехвату шифра возникают дополнительные препятствия, такие как разделение маскирующих блоков и блоков, содержащих криптограмму (информационных), определение (пеленгация) каналов связи и определение времени передачи блоков. В качестве каналов связи могут выступать глобальная сеть Internet, беспроводные локальные сети Wi-Fi, сети сотовой связи (пересылка по MMS). Стеганографическое сокрытие блоков шифра в мультимедиа-контейнерах усложняет задачу на тот случай, если канал связи будет запеленгован.

Проверка рассмотренного способа шифрования с разбиением на блоки была осуществлена с помощью разработанной программы *CherryFox Samara* (рис. 4). Криптограмма объемом 10 КБ была разбита на 8 блоков. Пересылка блоков криптограммы осуществлялась с помощью мессенджера ICQ, размещением на HTML-странице, по электронной почте и размещением на FTP-сервере. На приемной стороне блоки были получены в произвольном порядке и расшифрованы без ошибок.

Характеристики разработанного метода

Оценка скоростей шифрования предлагаемого шифра и наиболее известных шифров осуществлялась на ЭВМ со следующими характеристиками: Windows XP SP2, процессор Celeron, тактовая частота 1,6 ГГц, ОЗУ 3 ГБ.

Результаты испытаний представлены в табл. 2.



■ ***Рис. 4.*** *Интерфейс программы CherryFox Samara*

■ ***Таблица 2.*** *Сравнительная характеристика шифров*

Процесс	AES (МБ)	ГОСТ 28147-89 (МБ)	Адаптивный шифр (КБ)	С внедрением (Б/с)
Шифрование	11,5	6,25	15,1	208
Расшифрование	11,8	7,69	32	162

Адаптивный многоалфавитный шифр использовал ТМЗ с 1280 интервалами для 256 символов кодовой таблицы СР-1251 и подынтегральной функцией x^2.

В криптограмме каждый символ открытого текста заменяется двумя пределами интегрирования, представленными одним разрядом целой части, а после запятой — тремя (для верхнего) и четырьмя (для нижнего). Таким образом, расширение шифртекста по отношению к открытому тексту осуществляется в 9 раз.

Имеются способы, позволяющие существенно сжать получающуюся криптограмму. В пределе эти способы могут обеспечить расширение криптограммы по сравнению с исходным текстом лишь в 2 раза.

Достоинством шифра является стойкость к перебору числа возможных ключей. В данном способе шифрования ключевыми элементами являются таблица многоалфавитной замены и вид подынтегральной функции. Представляет интерес оценка числа различных конфигураций ТМЗ (другими словами, оценка числа ключей).

Пусть имеется алфавит символов открытого текста, состоящий из m символов. Таблица многоалфавитной замены должна удовлетворять следующим требованиям: число интервалов должно быть больше числа символов $n > m$, все интервалы должны быть размещены таким образом, чтобы образовать непрерывную числовую ось и чтобы любому символу открытого текста не соответствовали никакие два смежных интервала ТМЗ.

Обозначим число всевозможных различных способов формирования (конфигураций) ТМЗ символом A_n^m. В ходе исследования была доказана справедливость рекуррентной формулы

$$A_{n+1}^m = (m-1)A_n^m + mA_n^{m-1}.$$

Таким образом, для 256 символов (например, кодовая таблица СР-1251) с 1000 интервалов в ТМЗ число комбинаций составит $1{,}74 \cdot 10^{2404}$. Проведенные расчеты говорят о большом числе ключей, которые могут быть использованы в этом шифре. Заметим, что расчеты произведены для одной подынтегральной функции. Понятно, что число ключей линейно возрастает с увеличением числа подынтегральных функций.

Заключение

Разработанный шифр создает перед криптоаналитиками дополнительный барьер, состоящий в необходимости перехвата всех блоков криптограммы, передаваемых по разным каналам связи. Проведенная экспериментальная проверка пересылки блоков криптограммы по нескольким каналам подтверждает эффективность предлагаемой идеи.

Один из вариантов реализации рассмотренного способа шифрования сводился к размещению пронумерованных блоков шифрограммы на нескольких серверах (или сайтах). Принимающая сторона после скачивания всех файлов отбирала по номерам файлы (блоки), необходимые для восстановления (синтеза) исходного сообщения.

Литература

1. **Алексеев А. П.** Математические методы формирования многоалфавитных шифров замены // Инфокоммуникационные технологии. 2009. Т. 7. № 2. С. 21–25.
2. **Алексеев А. П., Блатов И. А., Макаров М. И., Похлебаев В. А.** Многоалфавитный адаптивный шифр, основанный на интегральных преобразованиях // Инфокоммуникационные технологии. 2010. Т. 8. № 1. С. 70–75.
3. **Simmons G. J.** Subliminal Channels: Past and Present // European Transactions on Telecommunications. Aug. 1994. Vol. 4. N 4. P. 459–473.
4. **Simmons G. J.** The Subliminal Channels of the U. S. Digital Signature Algorithm (DSA) // State and Progress of Research in Cryptography: Proc. of the Third Symp. Rome: Fondazone Ugo Bordoni, 1993. P. 35–54.
5. **Шнайер Б.** Прикладная криптография. — М.: ТРИУМФ, 2002. — 816 с.
6. **Белим С. В., Федосеев А. М.** Исследование скрытых каналов передачи информации в алгоритме цифровой подписи ГОСТ Р 34.10-2001 // Изв. Челябинского научного центра. 2007. Вып. 2(36). С. 17–19.