ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 54.057, 681.518.22

МЕТОД РАСШИРЕНИЯ КЛЮЧА ДЛЯ КОДИРОВАНИЯ ИНФОРМАЦИИ, ПЕРЕДАВАЕМОЙ ПО КАНАЛУ СВЯЗИ

Н.И. КОРСУНОВ[1]
В.В. МУРОМЦЕВ[1]
А.И. ТИТОВ[2]

[1]Белгородский государственный университет

[2]Белгородский государственный технологический университет им. В.Г. Шухова

e-mail:korsunov@bsu.edu.ru

Рассмотрен метод расширения ключа, который может быть использован при построении алгоритмов шифрования информации, передаваемой по каналу связи. Метод основан на использовании ключа, расширяемого на основе самокорректирующих кодов.

Ключевые слова: код, информация, канал связи, самокорректирующиеся коды.

Предполагается, что сообщения передаются по открытому каналу связи, доступному для просмотра некоторым другим лицам, отличным от получателя. При кодировании передаваемого сообщения предполагается, что у лица, передающего сообщение, и лица их принимающего есть некоторый противник, который может перехватывать сообщения и анализировать их. Для обеспечения недоступности передаваемой информации используются алгоритмы, основанные на общих принципах кодирования: рассеивание и перемешивание. Рассеивание заключается в распространении влияния одного символа открытого текста на много символов шифрованного текста, что позволяет скрыть статистические свойства открытого текста. Перемешивание состоит в использовании преобразований, которые исключают восстановление взаимосвязи открытого и шифрованного текстов.

Распространенный способ достижения хорошего рассеивания состоит в использовании нескольких шифров, которые могут быть реализованы в виде некоторой последовательности простых шифров, каждый из которых вносит вклад в результирующий текст, образуемый рассеиванием и перемешиванием. В качестве простых шифров чаще всего используют простые подстановки, перестановки, а также методы аналитического преобразования, гаммирования и комбинированного шифрования [1, 2].

В зависимости от формы передаваемой информации используют различные методы кодирования.

При аналоговой форме представления информации защиту осуществляют одним из следующих методов.

1. Наложение защитного шума. Используют генератор псевдослучайных чисел, что приводит при подавлении шума к остаточным признакам сигнала, по которым сигнал может быть восстановлен в приемлемом качестве.

2. Временные преобразования. Осуществляется перемешиванием отрезков, временной инверсией. При этом необходим блок для запоминания некоторой части сигнала, и защищенность сигнала зависит от длины элементарных отрезков. А так как при значительном уменьшении длины отрезка возникают трудности хранения сигнала, то для шифрования сигналов такие методы малопригодны. При перемешивании блоков возникают в местах их стыковки существенные наложения, и сигнал восстанавливается очень грубо.

3. Частотные преобразования связаны с инверсией спектра, перестановкой полос спектра. При этом используются взаимнооднозначные преобразования спектра по какому-либо закону, что уменьшает стойкость защиты и ухудшает качественные показатели восстановления сигнала.

Более эффективно строится защита информации в цифровом канале связи, основанном на построении соотношений между открытым кодом, шифрованным кодом и ключом.

При использовании ГОСТ 28147-89 открытый текст разбивается на две половины. Младшие A и старшие B биты и организуется циклический процесс, в котором на i-ом цикле

$$A_{i+1}=B_i+f(A_i,K_i),\ B_{i+1}=A_i,$$

где K_i – ключ, разделенный на восемь подключей по 32 бита, $f(A_i,K_i)=A_i+K_i$ по модулю 232.

Несмотря на эффективность реализации и высокое быстродействие код может быть вскрыт с помощью дифференциального криптоанализа, формирования целевой функции от известного открытого текста, соответствующего шифрованного текста и искомого значения ключа при нахождении экстремума этой целевой функции, соответствующего истинному значению ключа [3].

При использовании других алгоритмов необходимо, чтобы избыточные группы битов открытого текста были полностью зашифрованы в шифрованном тексте, длина шифрованного текста равнялась длине открытого текста, подстановки и перестановки, используемые в алгоритмах, были некоммукативны и определялись входными данными и ключом [4].

Если в этих методах используются детерминированные преобразования, то необходимо в алгоритме использовать элемент случайности. Один из алгоритмов [4] содержит внешний и внутренний циклы. Внутренний цикл превращает открытый текст в шифрованный, повторяясь для каждого байта открытого текста. Итерация внутреннего цикла оперирует с трехбайтовым окном данных, смещаемом на один байт в каждой итерации. На каждой итерации два байта циклически сдвигаются на переменное число позиций, а над содержимым последнего байта выполняется сложение по модулю два с некоторыми битами ключа. Это делает процесс обратимым, так как каждый байт данных влияет на два байта слева от себя и на один байт справа.

При шифровании весь ключ подвергается операции сложения по модулю два со случайной константой, а затем циклически смещается влево на три бита младшего байта. Смысл случайной константы состоит в превращении ключа в псевдослучайную последовательность.

К недостаткам реализации данного кодирования информации следует отнести: выполнение только линейных операций циклического сдвига и сложения по модулю два, а также неизменность четности всех битов шифрованного и открытого текстов, вследствие чего, обладая открытым и шифрованным текстами можно предсказать четность

шифрованного текста для любого открытого. А так как четность шифрованного текста зависит только от ключа, его определение не представляет трудностей.

В предлагаемом методе кодирования информации при передаче по каналу связи предлагается использовать превращение ключа в псевдослучайную последовательность K_i с последующим сложением с исходным кодом A_i по модулю два для получения шифрованного кода

$$B_i = A_i \oplus K_i, \quad (1)$$

но при этом проводить расширение полей шифрованного кода B_i и ключа K_i за счет введения циклических кодов, задеваемых порождающими матрицами кода W_i, связанными с обнаружением и исправлением ошибок в передаваемом сообщении. Построение этих матриц связано с длиной кодовой последовательности и кратностью исправляемой ошибки. Число двоичных разрядов проверочной матрицы определяется по формуле $n>=2t+1$, где t – кратность исправляемых ошибок. При этом контрольные коды можно образовывать всевозможными перестановками строк в матрице W_i. Это повышает надежность защиты шифрованного текста в связи с большим количеством возможных перестановок, которые можно обнаруживать только прямым перебором.

Предлагаемый метод включает выполнение следующих действий.

1. Случайным образом задать ключ K_i и, пользуясь (1) по известному коду A_i, сформировать шифрованный код B_i

2. Задать матрицу W_{i1}, W_{2i}, используя которые сформировать расширенные векторы кодов

$$K_i = W_{i1}K_i, \; B_i = W_{2i}B_i, \quad (2)$$

которые и передать по каналу связи.

W_{i1} – представляет некоторое конечное число матриц, для которых существуют обратные матрицы.

Последние представляют блоки закрытых ключей и могут передаваться простым шифрованным адресом при передаче информации от передатчика к приемнику. Не исключен выбор конкретной матрицы W_{kr} случайным образом из заданного множества.

В выражении (2) используются в отличие от известных методов шифрования значения ключей K_i шифрованного кода B_i, образованных наложением шумов h_i^1 h_i^2 на сформированные ранее в соответствии с (1) значения K_i, B_i, т.е.

$$K_i^* = K_i \oplus h_i^1, \; B_i^* = B_i \oplus h_i^2.$$

На приемной стороне по шифрованному адресу выбирается необходимая обратная матрица W^{-1}_{ji}, которая при использовании циклических кодов при передаче позволяет по значениям K_i^* и B_i^* восстановить значения K_i и B_i.

А так как при шифровании используется (1), то дешифрование осуществляется в соответствии с выражением $A_i = B_i \oplus K_i$.

При реализации передачи необходимо каждый шифрованный блок снабжать кодами начала и конца и вводить дополнительные поля, определяющие требуемые обратные матрицы W_{ji}, шифрованные зашумленные данные и ключ.

Предлагаемый метод защиты информации при передаче по каналам связи не позволяет исходному тексту и шифрованному тексту восстанавливать ключ, т.к. помимо превращения ключа в псевдослучайную последовательность производится расширение длины ключа и шифрованного текста с последующим зашумлением значений ключа и шифрованного текста.

Литература

1. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации. – М.: Горячая линия-Телеком, 2005. – 229 с.

2. Корсунов Н.И., Титов А.И., Глушак А.В. Повышение эффективности зашиты информации модификацией шифра Вижинера // Научные ведомости БелГУ. –2010. № 7 (78) вып. 14. – С. 171-175.

3. Игнатьев В.В. Информационная безопасность современного коммерческого предприятия – Старый Оскол: ООО ТНТ, 2005. – 448 с.
4. Панасенко С.П. Алгоритмы шифрования: спец. спр. – СПб.: БХВ-Петербург, 2009. – 576 с.

THE COMPUTERIZED SYSTEM OF MEASUREMENT OF DIELECTRIC PROPERTIES OF FIRM BODIES

N.I. KORSUNOV[1]
V.V. MUROMTSEV[1]
A.I. TITOV[2]

[1] *Belgorod State University*

[2] *Belgorod State Technological Universitythem V.G. Shukhov*

e-mail:korsunov@bsu.edu.ru

Presents a method of expanding the key, which can be used in the construction of encryption of information transmitted over a communication channel. The method is based on the use of key enhanced through self-correcting codes.

Key words: a code, the information, a communication channel, self-correcting codes.