УДК 004.056.55

СПОСОБ ЗАЩИТЫ ДАННЫХ ПРИ ПЕРЕДАЧЕ ОТВЕТСТВЕННОЙ ИНФОРМАЦИИ ПО ОТКРЫТЫМ КАНАЛАМ

Волынская А.В.

Уральский государственный университет путей сообщения, Екатеринбург, e-mail: anna-volinskaya@mail.ru

В известных алгоритмах шифрования данных с закрытым ключом применяется операция сложения по модулю два элементов передаваемого сообщения с элементами псевдослучайной последовательности, выполняющей роль ключа шифра. Известно также, что для повышения криптостойкости следует применять более сложный алгоритм шифрования-расшифрования. В качестве такого алгоритма предлагается применить операцию математической свертки. При этом для перехвата и расшифрования методом перебора необходимо найти не просто псевдослучайную последовательность, а обратную матрицу большой размерности, что требует на много порядков большего времени. В статье приведены результаты моделирования алгоритма, которые подтверждают его корректность. Практическая значимость состоит в возможности защиты от перехвата при передаче по открытым каналам сравнительно небольших, но ценных сообщений.

Ключевые слова: шифрование сообщений, закрытый ключ, свертка, обратная матрица, моделирование

DATA PROTECTION METHOD BY TRANSMISSION OF RESPONSIBLE INFORMATION ON OPEN CHANNELS

Volynskaya A.V.

Ural State University of railway transport, Ekaterinburg, e-mail: anna-volinskaya@mail.ru

In the famous data encryption algorithms with private key addition operation on the module two of elements of the transferred message with elements of the pseudorandom sequence executing a cipher key role is applied. It is known also, that it is necessary to apply more difficult algorithm of encoding deciphering to increase of cryptofirmness. As such algorithm we suggest to apply operation of a mathematical convolution. At the same time for interception and deciphering the method of search needs to be found not just pseudorandom sequence, but a reciprocal matrix of big dimensionality that requires on many orders of bigger time. Results of simulation of algorithm which confirm its correctness are given in article. The practical significance consists in a possibility of protection against interception by transmission through open channels of rather small, but valuable messages.

Keywords: encoding of messages, private key, convolution, reciprocal matrix, simulation

Защита данных от несанкционированного доступа с целью ознакомления, искажения (подмены) или уничтожения – проблема, которую нельзя решить в принципе, но можно ослабить, придумывая все более изощренные методы шифрования. При этом криптостойкость шифра оценивается из экономических соображений: если раскрытие шифра «стоит» больше, чем сама зашифрованная информация, то шифр считается достаточно надежным.

В работах автора [1, 2, 3] приведены результаты исследований по повышению помехоустойчивости каналов связи путем применения алгоритма линейно-параметрической модуляции. При этом сигнал $x(t)$ на выходе модулятора и в канале имеет вид последовательности фрагментов псевдослучайного сигнала, каждый из которых представляет собой результат свертки $s(t)$ и сигнала-переносчика $y(t)$ и может быть выражен в матричной форме

$$[x] = [y][s]$$

или
$$\begin{bmatrix} x_1^{(i)} \\ x_2^{(i)} \\ . \\ . \\ x_n^{(i)} \end{bmatrix} = [y] \begin{bmatrix} s_1^i \\ s_2^i \\ . \\ . \\ s_n^i \end{bmatrix}, \quad i = 1, 2, ..., m. \qquad (1)$$

Матрица $[y]$ квадратная n-го порядка, все строки ее получены из первой путем циклических перестановок.

Для выделения полезного сигнала на приемной стороне принятый сигнал $x(t)$ на фоне аддитивной помехи $n(t)$ должен быть подвергнут линейному преобразованию вида

$$z(t) = \int_0^T \int_0^T y(t-\theta-\tau)s(\tau)g(\theta)d\tau\, d\theta + \int_0^T n(t-\theta)g(\theta)d\theta, \qquad (2)$$

где $g(t)$ – импульсная характеристика демодулятора.

Модем, у которого импульсная характеристика демодулятора и несущее колебание выбраны из условия минимизации среднеквадратичного отклонения сигнала $z(t)$ на выходе от модулирующего колебания $s(t)$, назовем адаптированным к помехам в канале. У адаптированного модема характеристика демодулятора определяется выражением

$$g(t) = \frac{K_0}{2\pi} \int_{-\infty}^{+\infty} \sqrt{N_m - N(\omega)} e^{-j\psi(\omega)} e^{j\omega t} d\omega, \quad (3)$$

где K_0 – постоянное число; $N(\omega)$ – энергетический спектр помех в канале; N_m – постоянное число, превышающее пиковое значение $N(\omega)$; $\Psi(\omega)$ – произвольно выбранный фазовый спектр, а несущее колебание связано с импульсной характеристикой демодулятора матричным соотношением

$$[y] = [g]^{-1}, \quad (4)$$

где матрица $[g]$ построена из отсчетных значений импульсной характеристики демодулятора на периоде T путем циклических перестановок.

Отсчетные значения импульсной характеристики $g(t)$ могут быть найдены по ее преобразованию Фурье

$$G(j\omega) = K_0 \sqrt{N_m - N(\omega)}\, e^{-j\Psi(\omega)} \quad (5)$$

с помощью следующих формул:

$$g_\nu = \frac{2}{T}\left[\frac{A_0}{2} + (-1)^\nu \frac{A_{FT}}{2} + \sum_{k=1}^{FT-1}\left(A_k \cos\frac{2\pi k\nu}{2FT} + B_k \sin\frac{2\pi k\nu}{2FT}\right)\right], \quad (6)$$

$$\nu = 1, 2, 3, ..., 2FT,$$

где A и B связаны с $G(j\omega)$ соотношением

$$G\left(j\frac{2\pi k}{T}\right) = A_k - jB_k. \quad (7)$$

Первая строка матрицы $[y]$, полученной из соотношения (5), представляет собой отсчетные значения псевдослучайного сигнала на периоде T.

Проходя через демодулятор с импульсной характеристикой $g(t)$, сигнальная составляющая $x(t)$ принятого колебания, учитывая (4), преобразуется в модулирующее колебание

$$\begin{bmatrix} s_1^{(i)} \\ s_2^{(i)} \\ . \\ s_n^{(i)} \end{bmatrix} = [g] \begin{bmatrix} x_1^{(i)} \\ x_2^{(i)} \\ . \\ x_n^{(i)} \end{bmatrix}, \quad i = 1, 2, ..., m. \quad (8)$$

Приведенный алгоритм модуляции позволяет повысить помехоустойчивость и помехозащищенность при передаче сигналов. Покажем, что его можно применить и для шифрования сообщений, причем существенно повысить криптостойкость по сравнению с известными методами.

Один из методов шифрования основан на использовании псевдослучайных чисел [4]:

$$T_{i+1} := (a \cdot T_i + b) \bmod c, \quad (9)$$

где T_i – предыдущее псевдослучайное число, T_{i+1} – следующее псевдослучайное число, а коэффициенты *a, b, c* постоянны и известны. Обычно последовательность псевдослучайных чисел имеет период *c*.

Шифруемое сообщение представляется в виде последовательности слов $S_0, S_1, \ldots$, каждое длины N, которые складываются по модулю 2 со словами псевдослучайной последовательности $T_0, T_1, \ldots$, то есть

$$C_i := S_i \oplus T_i. \quad (10)$$

Последовательность $T_0, T_1, \ldots$ называют *гаммой* шифра. Расшифрование сводится к сложению шифрованной последовательности с гаммой шифра:

$$S_i := C_i \oplus T_i. \quad (11)$$

Ключом шифра является начальное значение T_0, которое известно отправителю и получателю сообщения, то есть шифр относится к классу *симметричных*. Дешифровать сообщение можно только подбором ключа, при этом с увеличением N экспоненциально увеличивается криптостойкость шифра.

Метод считается простым и эффективным, однако если злоумышленнику известна хотя бы часть исходного сообщения, что на практике вполне возможно (многие текстовые редакторы помещают в начало файла документа одну и ту же служебную информацию), то все сообщение может быть легко дешифровано. Пусть известно одно исходное слово S_i, тогда

$$T_i := C_i \oplus S_i, \quad (12)$$

и далее вся правая часть гаммы шифра определяется по указанной формуле датчика псевдослучайных чисел.

Один из путей повышения криптостойкости подобных шифров – применение вместо суммирования по модулю два более сложной (но обратимой) операции для вычисления шифровки [5].

Шифрованное сообщение получают, свертывая (convolution) слова исходного сообщения с гаммой шифра, которую находят либо по алгоритму (9), либо другим способом

$$C_i := S_i * T_i, \qquad (13)$$

где * – знак математической свертки.

Двоичное сообщение S, подлежащее шифрованию, разобьем на пакеты s^1, s^2, ..., s^i, ..., s^L; здесь индексом обозначен номер пакета. Каждый пакет содержит N двоичных символов $s_1^i, s_2^i, ..., s_n^i, ..., s_N^i$. Гамма также может быть представлена последовательностью двоичных символов t_1, t_2, …, t_n, …, t_N. Тогда алгоритм шифрования можно записать следующим образом

$$c^i(n) = \oplus \sum_{j=1}^{N} s_j^i \, t_{j-n}, \qquad (14)$$

Раскроем выражение (14) в виде системы уравнений

$$c_1^i = t_n s_1^i \oplus t_{n-1} s_2^i \oplus .... \oplus t_1 s_n^i;$$
$$c_2^i = t_1 s_1^i \oplus t_n s_2^i \oplus ... \oplus t_2 s_n^i;$$
$$.....;$$
$$c_N^i = t_{n-1} s_1^i \oplus t_{n-2} s_2^i \oplus .... \oplus t_n s_n^i,$$
$$i = 1, 2, ..., L. \qquad (15)$$

Запишем систему уравнений в матричной форме

$$\begin{bmatrix} c_1^i \\ c_2^i \\ ... \\ c_N^i \end{bmatrix} = [t] \begin{bmatrix} s_1^i \\ s_1^i \\ ... \\ s_1^i \end{bmatrix}, \quad i = 1, 2, ..., L. \qquad (16)$$

Матрица $[t]$ квадратная N-го порядка, все строки ее образуются из первой путем циклических перестановок. Можно показать [14], что столбцы матрицы $[t]$ линейно независимы, поэтому она невырождена (определитель не равен нулю), а значит, имеет обратную матрицу

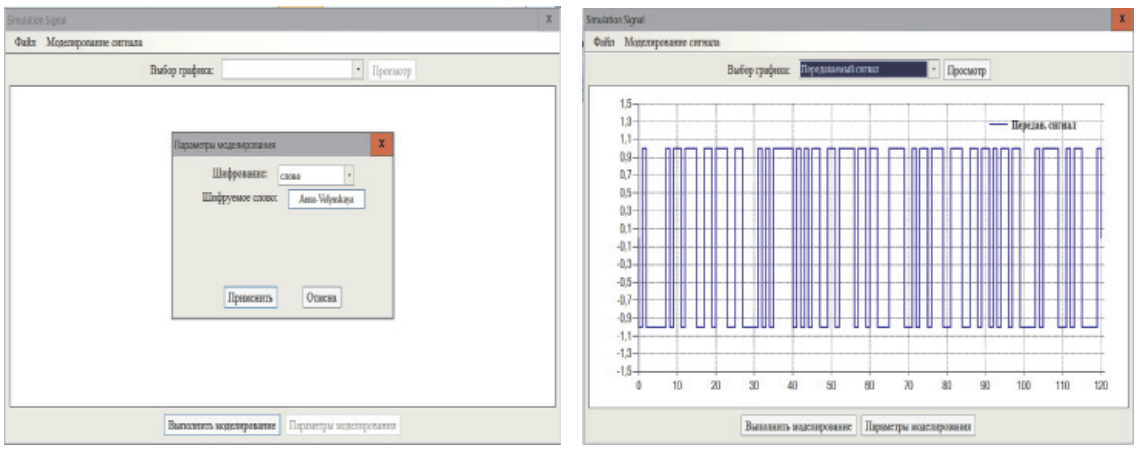
$$[y] = [t]^{-1}. \qquad (17)$$

Для расшифрования следует осуществить свертку принятого сообщения с обратной матрицей; назовем эту процедуру разверткой (deconvolution):

$$\begin{bmatrix} s_1^i \\ s_2^i \\ ... \\ s_N^i \end{bmatrix} = [y] \begin{bmatrix} c_1^i \\ c_1^i \\ ... \\ c_1^i \end{bmatrix}, \quad i = 1, 2, ..., L. \qquad (18)$$

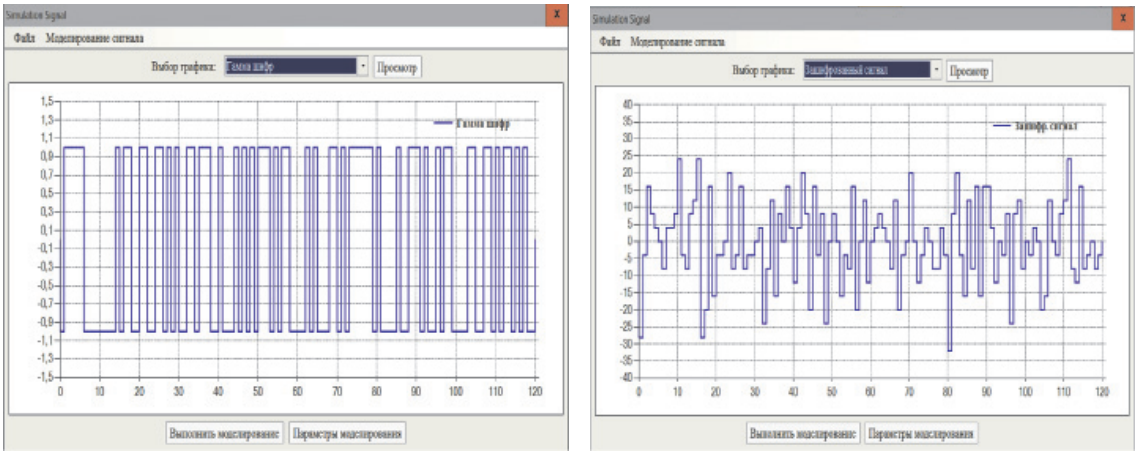
Для проверки корректности алгоритма проведено компьютерное моделирование в программной среде Visual Studio 2012. На рис. 1–3 приведены диалоговые окна моделирования процесса шифрования – расшифрования.

Сначала вводится текстовое сообщение, например, «Anna_Volynskaya», подлежащее шифрованию (рис. 1, а). Затем оно переводится в двоичную форму одним из известных кодов, например МТК-2 и представляется двоичным сигналом (рис. 1, б).



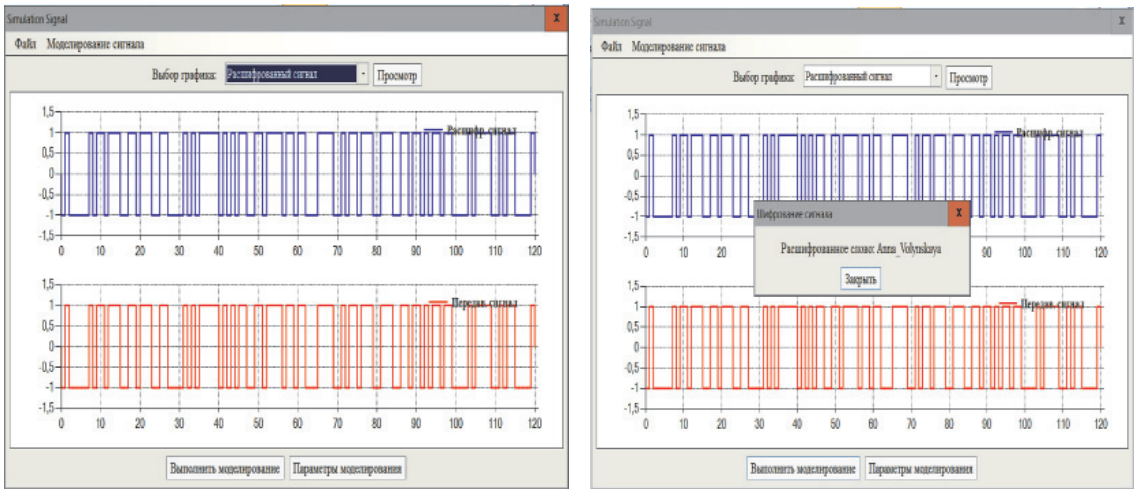
а б

Рис. 1.
а – ввод текстового сообщения, подлежащего шифрованию;
б – двоичный сигнал (код) передаваемого сообщения



а б

Рис. 2.
а – гамма шифра – двоичный псевдослучайный сигнал;
б – зашифрованное сообщение – шумоподобный сигнал



а б

Рис. 3.
а – расшифрованный сигнал в сравнении с передаваемым;
б – расшифрованное сообщение

Гамма шифра, заранее полученная с помощью датчика случайных двоичных чисел и известная получателю сообщения, приведена в форме двоичного сигнала (рис. 2, а). Далее проводится операция свертки по алгоритму (14), в результате чего получается шумоподобный сигнал (рис. 2, б), который может быть передан непосредственно получателю в форме последовательности десятичных (или по другому основанию) чисел, соответствующих его значениям.

Для расшифрования сообщения получатель проводит свертку полученного сигнала с сигналом, полученным из гаммы шифра обращением матриц по формуле (17), в результате получает расшифрованный сигнал (рис. 3, а). Затем этот двоичный сигнал декодируется и получается исходное сообщение (рис. 3, б).

Результаты моделирования подтверждают корректность алгоритма. Способ может быть использован в системах с закрытым ключом для передачи сравнительно небольших, но важных сообщений. Длина фрагментов передаваемого сообщения ограничена временем и вычислительной

устойчивостью процедуры нахождения обратной матрицы. В наших исследованиях применялись сообщения длиной до 500 двоичных разрядов.

Криптостойкость данного способа шифрования обусловлена необходимостью подбора обратной матрицы для расшифрования путем перебора. При этом каждый ее вариант требуется подвергнуть свертке с зашифрованным сигналом, что многократно замедляет процесс подбора и делает его практически бесполезным.

Список литературы

1. Волынская А.В., Сергеев Б.С. Предпосылки применения псевдослучайных сигналов-переносчиков в каналах телемеханики железнодорожного транспорта // Транспорт: наука, техника, управление: Научный информационный сборник РАН ВИНИТИ. – 2011. – Вып. 6. – С. 39–41.

2. Волынская А.В. Пробные эксперименты по изучению спектральных и статистических характеристик электромагнитных помех в каналах телемеханики железнодорожного транспорта // Семинар докторантов УрГУПС: сб. науч. докл. / под науч. ред. С.П. Баутина. – Екатеринбург: Изд-во УрГУПС, 2012. – С. 29–40.

3. Волынская А.В. Интеллектуальный канал телемеханики // Транспорт: наука, техника, управление: Научный информационный сборник РАН ВИНИТИ, 2013. – Вып. 4. – С. 13–16.

4. Дискретная математика для программистов / Ф.А. Новиков. – СПб.: Питер, 2001. – 181с.

5. Beker H. and Piper F. Cipher Sistems. John Wiley & Sons, Inc. – New York, 1982.

References

1. Volynskaya A.V., Sergeev B.S. *Transport: nauka, tehnika, upravlenie – nauchnyi informatsionnyi sbornik RAN VINITI*, 2011, vyp. 6, pp. 39–41.

2. Volynskaya A.V. *Seminar doktorantov UrGUPS* (Seminar of doctoral candidates of UrGUPS). Ekaterinburg, 2012, pp. 29–40.

3. Volynskaya A.V. *Transport: nauka, tehnika, upravlenie – nauchnyi informatsionnyi sbornik RAN VINITI*, 2013, vyp. 4, pp. 13–16.

4. Diskretnaya matematika dlya programmistov/ F.A. Novikov. SPb: Piter, 2001, 181p.

5. Beker H. and Piper F. Cipher Sistems. John Wiley & Sons, Inc., New York, 1982.