УДК 004.724.4(045)

КУЛАКОВ Ю.А.,
КОГАН А.В.,
ПИРОГОВ А.А.

АЛГОРИТМ РАЗДЕЛЕНИЯ И СБОРКИ СЕКРЕТНОГО СООБЩЕНИЯ ДЛЯ МНОГОПУТЕВОЙ МАРШРУТИЗАЦИИ В БЕСПРОВОДНЫХ СЕТЯХ

Предложен алгоритм разделения и сборки секретного сообщения для многопутевой маршрутизации в мобильных сетях. Разбиение сообщения осуществляется на основе использования периодических функций типа y = cos(x) и уравнения «волны». Разработана программа и приведен пример моделирования процесса безопасной многопутевой передачи информации.

The algorithm of division and build a secret message for secure multipath routing. Partition is based on the use of periodic functions of y = cos (x) and the equation of the "wave". The program is an example of modeling and process secure multipath transmission.

1. Введение

В настоящее время актуальным вопросом является безопасность передачи информации в беспроводных сетях. Это связано с тем, что прослушивание передающей беспроводной среды не составляет особого труда. Кроме того, существующие методы повышения безопасности ориентированы в основном на сети фиксированной структуры. В то же время целый ряд беспроводных технологий позволяют обеспечивать высокую мобильность узлов, для которых известные методы защиты информации, используемые в сетях со статической структурой, требуют значительных накладных расходов, а возможно и не применимы вообще [1].

В данной работе предложен способ передачи информации на основе многопутевой маршрутизации с использованием процедуры разделения и сборки секретного сообщения.

2. Обзор существующих решений

До настоящего времени в большинстве случаев решения задачи разделения и сборки секретного сообщения ранее была предложена схема интерполяционных полиномов Лагранжа (схема разделения секрета Шамира). Данная схема позволяет создать (t, n)-пороговое разделение секрета для любых t, n. Основная идея схемы Шамира базируется на том, что полином степени t – 1 может быть однозначно восстановлен по его значениям в t различных точках.

Основной недостаток непосредственного применения схемы – отсутствие способа верификации отдельных ключей, передаваемых участникам, а также возможности проверки достоверности любого их поднабора размера l (для предотвращения подмены отдельных частей секрета).

3. Описание алгоритма

Предлагаемый в настоящей работе алгоритм разделения и сборки секретного сообщения характеризуется тем, что вычисления производятся с определённой точностью, на основе периодических тригонометрических функций. Данные функции имеют постоянную амплитуду, определены и непрерывны на всем промежутке $x \in (-\infty, +\infty)$. Особенность алгоритма заключается в том, что при увеличении точности вычислений период гаммирования может достигать сколь угодно большого значения.

При реализации данного алгоритма использовались периодическая функция y = cos(x) и уравнение «волны» [2]. Особенность данной периодической функции в том, что ее период выражен иррациональным числом, а значению, например, y = 0,5 соответствует бесконечное количество значений x. То есть, при y = 0,5 x принимает значения:

$$\frac{\pi}{3}; \frac{7\pi}{3}; \frac{13\pi}{3} \ \ldots$$

и т. д. до бесконечности, как положительных, так и отрицательных значений.

Применяя уравнение волны y = cos (x + N * Δx), где:

N – целое число, в данном случае определяющее порядковый номер шифруемого символа (0-256);

Δx – приращение функции, задаваемое в секретном ключе (любое число);

x – значение, взятое из открытого текста (0-256).

Отсюда следует, что при y = 0,5 * x может принимать любое значение от $-\infty$ до $+\infty$ (рис.1).

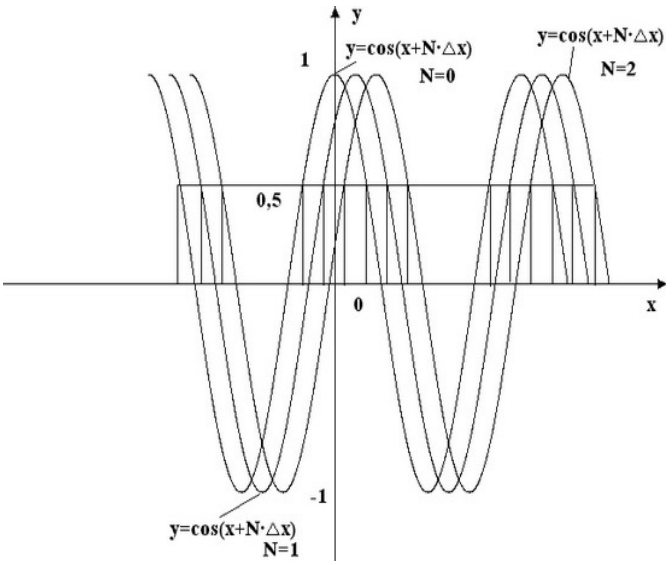

Рис. 1. График функции y = cos (x).

Пример реализации:

По координатной оси x расставляются символы из открытого текста в любом порядке. Каждому символу соответствует свой порядковый номер, например, от 1 до 256. По оси y расставляются символы, используемые в шифротексте в любом таком же или другом порядке. Им так же присваиваются порядковые номера, например от 1 до 256. Три линейные функции описываются как: Y_1, Y_2, Y_3 (рис. 2).

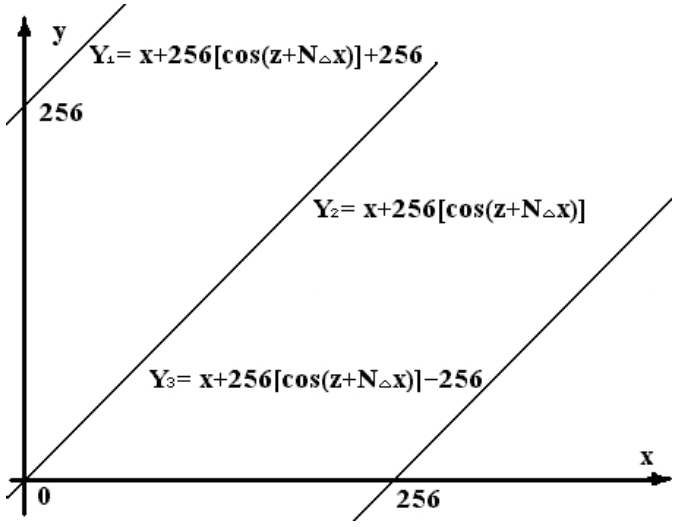

Рис. 3. Линейные функции Y_1, Y_2, Y_3.

$Y_1 = x + 256 * [\cos(z + N * \Delta x)] + 256;$

$Y_2 = x + 256 * [\cos(z + N * \Delta x)];$

$Y_3 = x + 256 * [\cos(z + N * \Delta x)] – 256;$

где:

x – порядковый номер символа из открытого текста;

z – любое число (-∞ до +∞);

N – номер по счету шифруемого символа из открытого текста;

Δx – любое число (-∞ ÷ +∞);

Для примера зашифруем букву А. А – открытый текст. В данном примере секретными являются числа Δx и z. Все остальные параметры не являются секретом. Кроме того, количество секретных параметров можно сделать бесконечное множество.

Знак А занимает промежуток (0÷1) по оси x, знак Б – (1÷2), В – (2÷3) и т.д.. Имея три формулы, подставляем значение 0,5 – середину промежутка (0÷1) – буква А (для буквы Б это значение соответствует 1,5, для В – 2,5 и т.д.).

Пусть, z = 0. Шифруется первый по счету знак из открытого текста, тогда N = 1. Δx = 32.

Подставив цифры, получим формулы следующего вида:

$Y_1 = 0,5 + 256 * [\cos(0 + 1 * 32)] + 256 = 437,6;$

$Y_2 = 0,5 + 256 * [\cos(0 + 1 * 32)] = 217,6;$

$Y_3 = 0,5 + 256 * [\cos(0 + 1 * 32)] - 256 = 38,39;$

Из трех значений Y_1, Y_2, Y_3 выбираем Y_2, так как значение Y_2 попало в промежуток от 0 до 256. И округляем значение Y_2 до большего целого $Y_2 = 218$.

В итоге, открытый текст 0,5 был зашифрован и получил значение 218.

Для расшифровки применяются те же формулы, подставляя уже известное значение 218. Из каждого известного значения необходимо вычесть 0,5 для того, что бы в формулу подставлялось значение из середины отрезка, которому принадлежит данный знак:

$x_1 = 217,5 - 256 * [\cos(0 + 1 * 32)] – 256 = - 255,6;$

$x_2 = 217,5 - 256 * [\cos(0 + 1 * 32)] = 0,4;$

$x_3 = 217,5 - 256 * [\cos(0 + 1 * 32)] + 256 = 265,4.$

Из трех значений Y_1, Y_2, Y_3 выбираем Y_2, так как значение Y_2 попало в промежуток (0÷1).

Преимущества алгоритма:

Данный алгоритм прост в реализации. Особенностью алгоритма является то, что шифротекст представлен в виде иррациональных чисел. В самом процессе шифрования учувствуют промежутки, в которые попадают эти иррациональные числа. Произвести аналитический взлом шифра возможно только точно зная число, а оно иррациональное, то есть бесконечно, и его невозможно вычислить. Соответственно при расшифровании уже участвуют совершенно случайные числа, а не те, которые получили в процессе шифрования.

4. Моделирование процесса безопасной многопутевой маршрутизации

В рамках данной работы была разработана программа моделирования процесса безопасной многопутевой передачи информации.

На первом шаге моделирования (Такт: 0) с помощью модифицированного алгоритма Дейкстры осуществляется поиск множества непересекающихся путей, для каждого из которых вычисляется значение SLi, характеризующее надежность доставки информации по каждому из выбранных путей. Пути и степень их надежности, а также опции вершин отображаются в сервисном окне (рис. 3), при данной топологии сети формируется 3 маршрута с различной надежностью.

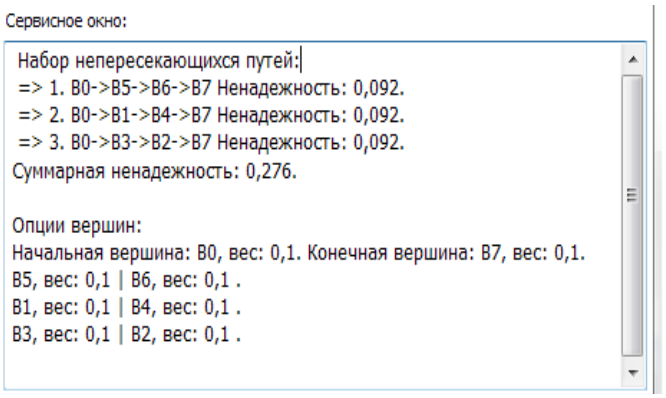

Рис. 3. Сервисное окно программы

На втором шаге осуществляется разбиение исходного сообщения на пары символов (с дополнением символов «0» в начало сообщения в случае несоответствия длины сообщения с требованиями алгоритмов разбиения/сборки сообщения). Далее полученные пары символов преобразуются в соответствии с предложенным алгоритмом (рис 4.). В данном примере исходное сообщение FB7EC5 разбивается на три пакета и шифруется с использованием периодической функции y = cos (x + N * Δx) (рис. 5). Необходимые значения параметров z и Δx задаются в настройках программы, z = 1, Δx = 30. Исходные части сообщения: FB7EC5. В итоге функции шифрования будут иметь следующий вид:

$Y_1 = (251 + 0,5) + 256 * (\cos(1 + 1 * 30))$;
$Y_1 = 485,67$ [+ / - 256] => 229,67;
После округления $Y_1 = 230$;
$Y_2 = (126 + 0,5) + 256 * (\cos(1 + 2 * 30))$;
$Y_2 = 60,43$ [+ / - 256] => 60,43;
После округления Y2 = 61;
$Y_3 = (197 + 0,5) + 256 * (\cos(1 + 3 * 30))$;
$Y_3 = - 57,06$ [+ / - 256] => 198,94;
После округления $Y_3 = 199$.

После шифрования исходного сообщения формируются соответствующие пакеты, которые будут отправлены узлу-адресату по разным маршрутам, которые были найдены ранее:

T=0 Пакет №0 с содержимым:
1|230 сформирован.
T=0 Пакет №1 с содержимым:
2|61 сформирован.
T=0 Пакет №2 с содержимым:
3|199 сформирован.

После того как узлу-получателю пришли все части исходного сообщения, происходит обратная сборка их в исходное сообщение. В итоге функции расшифровании будут иметь следующий вид:

$x_1 = (230 - 0,5) – 256 * (\cos(1 + 1 * 30))$;
$x_1 = - 4,67$ [+ / - 256] => 251,33;
После округления $x_1 = 251$;
$x_2 = (61 - 0,5) – 256 * (\cos(1 + 2 * 30))$;
$x_2 = 126,57$ [+ / - 256] => 126,57;
После округления $x_2 = 126$;
$x_3 = (199 - 0,5) – 256 * (\cos(1 + 3 * 30))$;
$x_3 = 453,06$ [+ / - 256] => 197,06;
После округления $x_3 = 197$;

Исходное сообщение: FB7EC5.

Выводы

Алгоритм разбиения и сборки исходного сообщения на основе тригонометрических функций cos и sin удобен и просто в реализации. Особенность этих функций в том, что они непрерывны и определены на всем промежутке от минус бесконечности до плюс бесконечности на оси x. А на оси y они принимают значения от -1 до 1, причем и на том и на другом промежутке они могут принимать любые значения в этих промежутках. Над этими функциями возможно производить фактически любые математические действия.

Отличительная особенность алгоритма – при увеличении точности вычислений период гаммирования может достигнуть сколь угодно большого значения.

В отличии от предложенной ранее модифицированной схемы Шамира, данный алгоритм позволяет участникам протокола еще до момента восстановления полного сообщения с уверенностью сказать, является ли их часть подлинной.

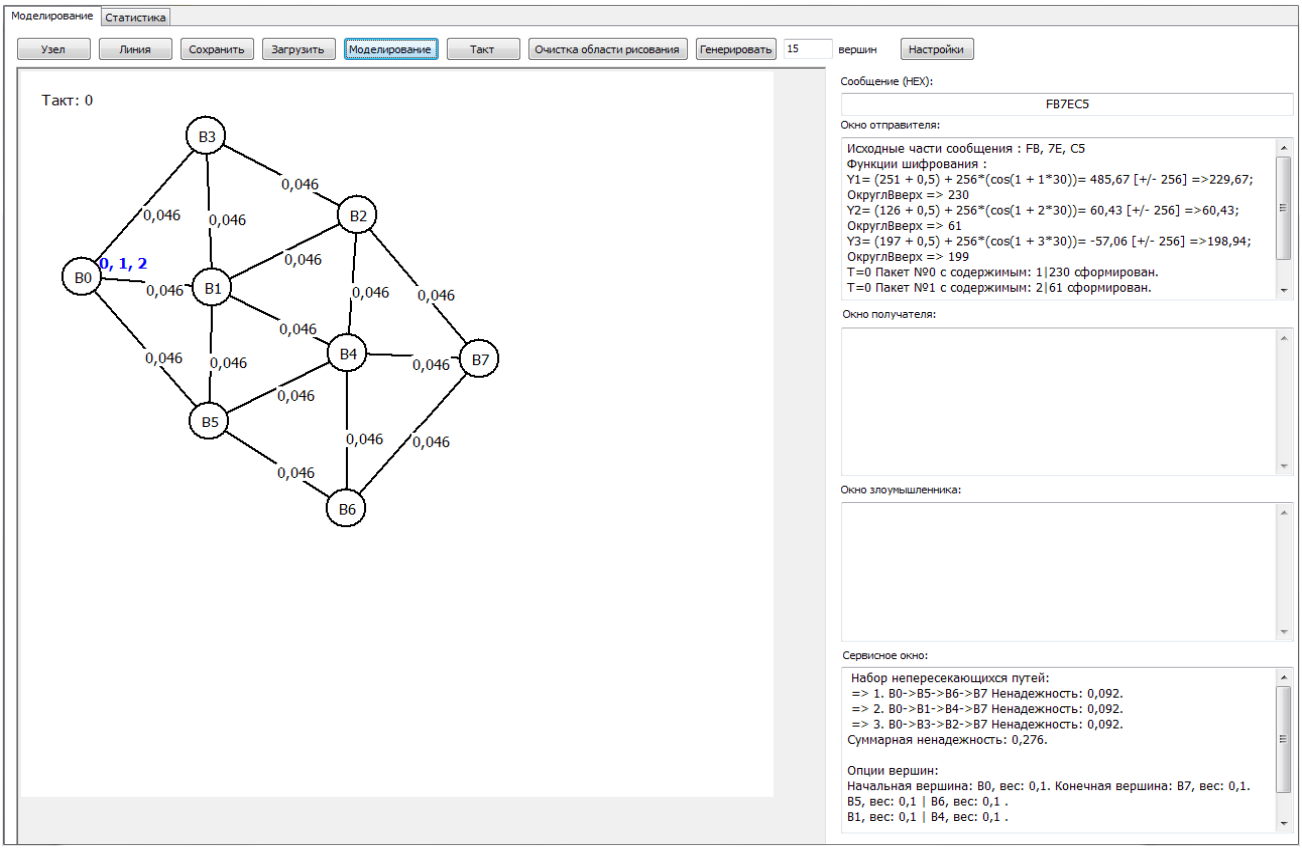

Рис. 4. Поиск набора непересекающихся путей, разбиение исходного сообщения на части и шифрование

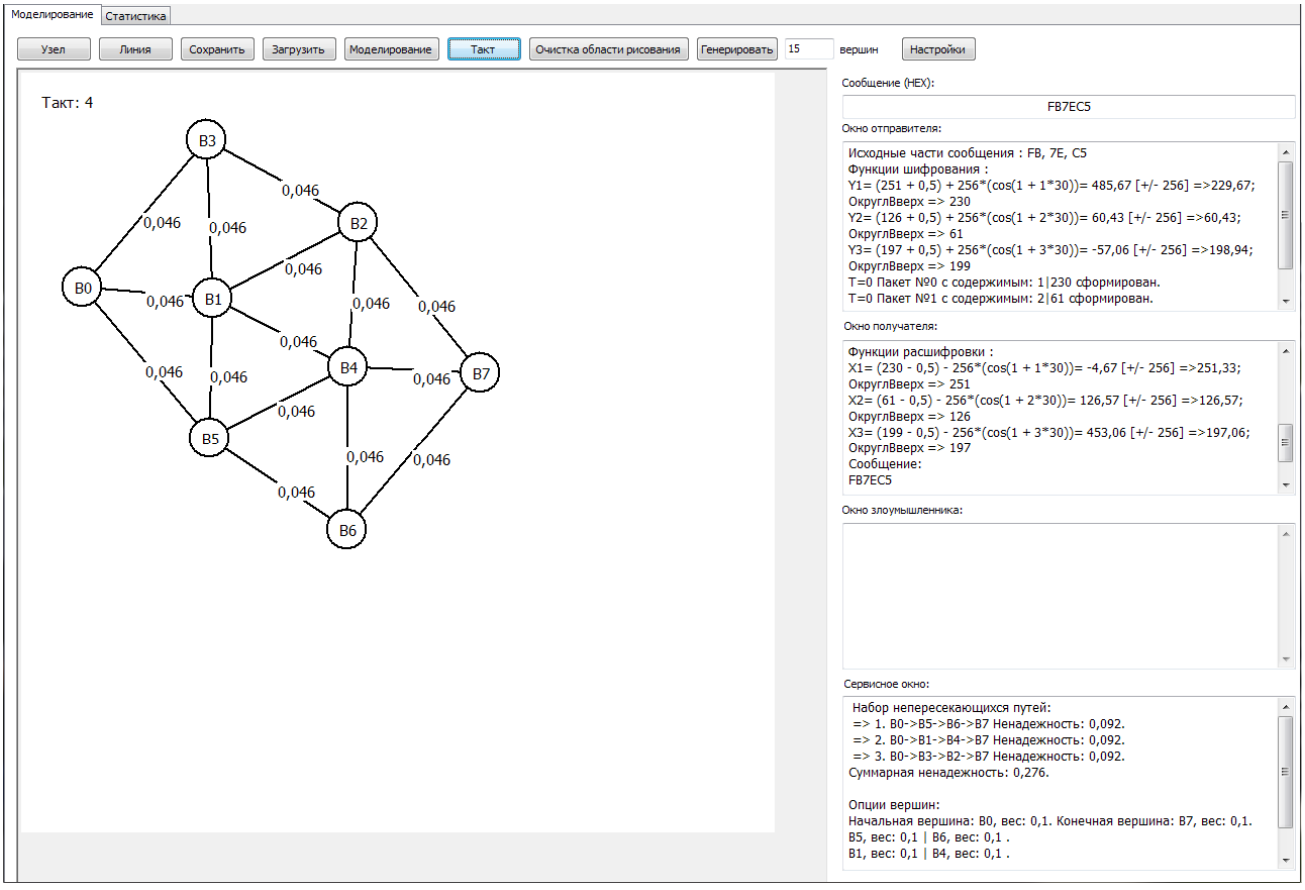

Рис. 5. Сборка частей исходного сообщения и дешифрование

А для того, что бы прочитать сообщение полностью, злоумышленнику необходимо не просто перехватить все части исходного сообщения, но и так же знать значения параметров z и Δx, что осуществить весьма не просто.

Список литературы

1. Кулаков Ю.А. Разработка и моделирование процесса безопасной многопутевой передачи информации в мобильных сетях / Ю.А. Кулаков, А.В. Коган, А.А. Пирогов // Вісник Национального техн. Ун -ту України «КПІ». Інформатика, управління та обчислювальна техніка: зб. наук. праць. – К.: Век+, 2011. – № 54. – С. 145-149.
2. Сизов В. П. «Новый алгоритм шифрования». // Сайт ITSec.Ru – 2007. [Электронный ресурс]. URL: http://www.itsec.ru/articles2/Inf_security/novy-alg-shifrov . – название с экрана.
3. Кулаков Ю.А. Повышение уровня безопасности передачи информации в мобильных сетях / Кулаков Ю.А., Максименко Е.В., Рущак О.А.// Вісник Національного техн. ун -ту України "КПИ": Інформатика, управління та обчислювальна техніка. – К.: ТОВ "ВЕК+", 2007. – Вип. 47. – С.297-304.
4. Кулаков Ю. А. Многопутевая маршрутизация в беспроводных сетях./ Ю. А. Кулаков, А. В. Левчук // Проблеми інформатизації та управління: Зб. наук. пр. – К.: Вид-во Нац. авіац. ун-ту «НАУ-друк», Вып. 4 (26), 2010. – С.142-147.
5. Marti S. Mitigating routing misbehavior in mobile ad hoc networks/ Marti S., Giuli T., Lai K., Baker M. // The 6th annual ACM/IEEE International Conference on Mobile Computing and Networking (Mobi-Com'OO) – 2000 – Boston(MA, USA) – P.255-265.