ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 23 МАТЕМАТИКИ Выпуск 3
2016

Д. В. Гусева, С. В. Яковлев (Ставрополь, СКФУ). **Метод шифрования на основе тригонометрической функции двух аргументов.**

Предлагаемый алгоритм шифрования основан на методе гаммирования и использует тригонометрическую функцию двух аргументов.

Пусть XoY — *плоскость открытого текста*, где по осям Ox и Oy расставляются символы алфавита исходного сообщения согласно таблице кодов ASCII. Каждому символу соответствует середина единичного отрезка.

По оси Oz расположим символы алфавита, используемого в зашифрованном сообщении согласно таблице кодов ASCII.

Взаимосвязь значений символов открытого и закрытого текстов можно описать системой уравнений:

$$\begin{cases} Z = X, \\ X = Y, \end{cases}$$

где $Z = X$ — равенство, показывающее зависимость между значениями Z и значениями на плоскости XoY; $X = Y$ — равенство, определяющее равномерное и одинаковое распределение символов на плоскости открытого текста.

Аналитические формулы, используемые при шифровании сообщения открытого текста будут иметь вид:

$$\begin{cases} Z_1 = X_i + 256 \times (\cos(x_0 + \Delta x \times N) \times \sin(y_0 + \Delta y \times N)) + 256, \\ Z_2 = X_i + 256 \times (\cos(x_0 + \Delta x \times N) \times \sin(y_0 + \Delta y \times N)), \\ Z_3 = X_i + 256 \times (\cos(x_0 + \Delta x \times N) \times \sin(y_0 + \Delta y \times N)) - 256, \end{cases}$$

где X_i — середина отрезка шифруемого символа по осям Ox и Oy соответственно; i — порядковый номер символа в алфавите открытого текста $(i \in [0; 255])$; x_0, y_0 — начальные фазы по осям Ox и Oy соответственно $(x_0, y_0 \in [-\infty; \infty])$; Δx и Δy — числа, определяющие величину смещения по Ox и Oy соответственно, причем $\Delta x \in [-\infty; \infty]$ и $\Delta y \in [-\infty; \infty]$; N — целое число, определяющее порядковый номер символа в шифруемом сообщении.

В нашем случае гамма определяется выражением

$$256 \times (\cos(x_0 + \Delta x \times N) \times \sin(y_0 + \Delta y \times N)) \pm 256.$$

Секретными параметрами рассматриваемого алгоритма шифрования в данном случае будут значения $\Delta x, \Delta y, x_0, y_0$.

После выполнения вычислений из трех значений Z_1, Z_2, Z_3 выбираем значение $Z \in [0; 256]$. Округлив выбранное значение Z до ближайшего целого в меньшую сторону, получим значение, которое соответствует символу сообщения закрытого текста поступающего в канал связи.

Допустим, что канал связи идеален и на приемной стороне мы принимаем сигнал полностью соответствующий переданному символу. Прибавляем к значению полученного символа 0,5 для того, чтобы попасть середину отрезка.

Аналитические формулы, используемые при дешифровании сообщения закрытого текста будут иметь вид:

$$\begin{cases} XY_1 = Z^* - 256 \times (\cos(x_0 + \Delta x \times N) \times \sin(y_0 + \Delta y \times N)) + 256, \\ XY_2 = Z^* - 256 \times (\cos(x_0 + \Delta x \times N) \times \sin(y_0 + \Delta y \times N)), \\ XY_3 = Z^* - 256 \times (\cos(x_0 + \Delta x \times N) \times \sin(y_0 + \Delta y \times N)) - 256, \end{cases}$$

где Z^* — значение середины отрезка на оси Oz соответствующее полученному символу $(Z^* \in [0; 256])$.

После выполнения вычислений из трех значений XY_1, XY_2, XY_3 выбираем значение соответствующее условию $XY \in [0; 256]$ и определяем, какому интервалу принадлежит декодированный символ на плоскости XoY.

Рассмотренные этапы кодирования и декодирования символов итерационно применяются ко всем элементам передаваемого сообщения.

СПИСОК ЛИТЕРАТУРЫ

1. *Сизов В. П.* Алгоритм защиты информации на основе тригонометрических функций. Дисс. на соискание уч. ст. канд. техн. наук: 05.13.19. Пермь: 2012, 156 с.