ПРИМЕНЕНИЕ ОБОБЩЕННЫХ МАТРИЦ ФИБОНАЧЧИ ПРИ КОДИРОВАНИИ ИНФОРМАЦИИ

С.С. Бывшев, И.Н. Лущакова

БГУИР, П Бровки 6, 220027 Минск, Беларусь
IrinaLushchakova@yandex.ru

В докладе обсуждаются принципы построения криптосистемы, использующей при кодировании информации матрицы специального вида — обобщенные матрицы Фибоначчи.

Определение 1. [1]. Матрицей Фибоначчи называется $n \times n$-матрица $A = (a_{ij})$, у которой $a_{11} = 1$, $a_{n1} = 1$, $a_{i,i+1} = 1$, $1 \leqslant i \leqslant n-1$, а все остальные элементы $a_{ij} = 0$.

Будем рассматривать $n \times n$-матрицы более общего вида, которые получаются из перестановочных матриц (т. е. матриц размерности $n \times n$ с элементами 0 и 1, в каждой строке и каждом столбце которых содержится ровно одна единица) с помощью изменения точно одного элемента $a_{ij} = 0$ на $a_{ij} = 1$. Назовем такие матрицы обобщенными матрицами Фибоначчи. Нетрудно заметить, что умножение некоторой $n \times n$- матрицы B слева на обобщенную матрицу Фибоначчи приводит к элементарным преобразованиям строк матрицы B (а именно, перестановке строк и прибавлению к одной строке другой). Умножение матрицы B справа на обобщенную матрицу Фибоначчи приводит к соответствующим элементарным преобразованиям столбцов матрицы B.

В [1] было предложено использовать матрицы Фибоначчи для кодирования информации. В настоящей работе рассматривается один из возможных подходов к практической реализации этой идеи.

Вначале устанавливается взаимнооднозначное соответствие между используемым алфавитом мощности m и множеством целых чисел $Z_m = \{0, 1, 2, \ldots, m-1\}$. Зашифрованный текст записывается в столбцы матриц размерности $n \times n$, которые являются шифрвеличинами для криптосистемы, аналогичной системе Хилла [2, 3]. Далее шифрвеличины (матрицы) умножаются по модулю m слева или (и) справа на некоторые степени обобщенных матриц Фибоначчи, причем обобщенные матрицы Фибоначчи являются обратимыми над кольцом Z_m. Обобщенные матрицы Фибоначчи будем генерировать из единичной матрицы с помощью перестановки l соседних столбцов, которая определяется так называемой базовой перестановкой, и указания расположения дополнительной "суммирующей" единицы.

На этапе предварительного распределения ключей стороны оговаривают первоначальные значения следующих параметров: размерность n кодирующей матрицы; базовая перестановка чисел $\{1, 2, \ldots, l\}$, $2 \leqslant l \leqslant n$ (отдельная для каждого пользователя); позиция подматрицы, определяемой базовой перестановкой, в матрице кодирования; положение "суммирующей" единицы; степени кодирующей матрицы при умножении справа и слева. При каждом сеансе связи меняется только часть параметров, так что при перехвате невозможно восстановить кодирующую матрицу. Большое количество независимых параметров позволяет при каждом сеансе связи получить уникальный ключ, причем передаваемые параметры просты и не требуют большого объема памяти.

Демонстрационная программа, выполненная в среде DELPHI 7.0, реализует описанную криптосистему.

Литература

1. *Стахов А.П.* Компьютеры Фибоначчи и новая теория кодирования: история, теория, перспективы // Перспективные информационные технологии и интеллектуальные системы. 2004. № 2(18). С.17-30.

2. *Конопелько В.К., Липницкий В.А., Дворников В.Д. и др.* Теория прикладного кодирования: Учебн. пособие.Т.1. Мн.: БГУИР, 2004.

3. *Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.П.* Основы криптографии. М.: Гелиос АРВ, 2002.