УДК 621,391.1 (075.8)

«ЗОЛОТЫЕ» МАТРИЦЫ И НОВЫЙ МЕТОД КРИПТОГРАФИИ

А.П. Стахов, доктор технических наук, профессор
e-mail: goldenmuseum@rogers.com

1. «Золотая» криптография

Суть «золотой» криптографии состоит в следующем. В качестве «криптографического ключа» используется некоторое значение переменной x. Это означает, что количество «криптографических ключей» для данного метода теоретически бесконечно. Метод может быть применен для криптографической защиты так называемых «дискретных сигналов», представляющих последовательность «отсчетов» некоторой непрерывной функции:

$$a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, \ldots \quad (1)$$

Шифрация сообщения состоит в последовательном представлении четверок «отсчетов» типа a_1, a_2, a_3, a_4 из (1) в виде квадратной матрицы:

$$M = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \quad (2)$$

и последующем ее умножении на прямую «золотую» матрицу. При этом образуется «кодовая матрица» E

$$M \times Q(2x) = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \times \begin{pmatrix} cFs(2x+1) & sFs(2x) \\ sFs(2x) & cFs(2x-1) \end{pmatrix} = \begin{pmatrix} e_{11} & e_{12} \\ e_{21} & e_{22} \end{pmatrix} = E(x), \quad (3)$$

которая представляет собой «зашифрованное сообщение», передаваемое затем по «каналу связи».

Дешифрация зашифрованного сообщения, полученного из «канала связи», состоит в умножении «кодовой матрицы» (3) на инверсную матрицу.

Между детерминантами исходной матрицы (2) и «кодовой матрицы» (3) существует следующая связь:

$$\mathrm{Det}\ E = \mathrm{Det}\ M, \qquad (4)$$

что непосредственно вытекает из свойства (5).

2. Преимущества «золотой» криптографии

Предложенный метод принадлежит к так называемой «симметричной» криптографии, то есть для его реализации «криптографический ключ» должен быть известен «получателю» зашифрованного сообщения. Для передачи «криптографического ключа» предлагается использовать существующие «асимметричные» криптографические системы, то есть «криптографическая способность» данного метода определяется «криптографической способностью» соответствующей «асимметричной» системы, используемой для передачи криптографического ключа.

Основным достоинством «золотой» криптографии является простота алгоритма шифрации-дешифрации, что обеспечивает высокую скорость шифрации-дешифрации и позволяет использовать метод для криптографической защиты «дискретных сигналов», работающих в реальном масштабе времени (телефонные, измерительные и другие телекоммуникационные системы). При этом частая смена «криптографического ключа», выбираемого по случайному закону, неизвестному «передатчику» и «приемнику» и передаваемого с помощью «асимметричных» систем, обеспечивает достаточно высокий уровень криптографической защиты. Еще одним достоинством метода является возможность контроля процесса шифрации и дешифрации, что основывается на уникальном математическом тождестве (4), связывающем детерминанты исходной матрицы (2) и «кодовой матрицы» (3).

Таким образом, с помощью предложенного метода можно создавать простые с точки зрения технической реализации, быстродействующие и высоконадежные криптографические системы, предназначенные для защиты информационных систем, работающих в реальном масштабе времени.