ЛИНЕЙКАЯ КОНСТРУКЦИЯ КОДА ДЛЯ СИСТЕМЫ РАСПРЕДЕЛЕНИЯ СИММЕТРИЧНЫХ КЛЮЧЕЙ

Ву Вьет Хынг, магистрант

Белорусский государственный университет информатики и радиоэлектроники,
Институт информационных технологий,
г. Минск, Республика Беларусь

Митюхин А.И. – доцент

Рассматривается конструкция формирования кодовых последовательностей на основе линейных дискретных функций Адамара. Результатом является повышение уровня защиты передаваемых данных посредством использования сеансовых ключей.

Для надежной работы симметричных криптосистем подобных DES, AES с числом n пользователей необходимо иметь доверенную систему управления секретными ключами. Основная проблема управления – это значительная величина ключей. Например, для ИИТ БГУИР с 1000 студентами нужно создать

$$K = \frac{n(n-1)}{2} \approx 500000 \text{ ключей.}$$

С большим количеством уже используемых в информационной системе ключей возможна преднамеренная компрометация ключа. Для устранения проблемы распределения ключей предлагается шифрование длинного сообщения осуществлять с использованием кодовых конструкций (схем). При этом возникает задача выбора базового кода, на основе которого осуществляется скрытность структуры ключа. В работе в качестве базового кода предлагается использовать линейный код Адамара. Код строится с помощью порождающей матрицы Адамара вида Сильвестра. Матрица Сильвестра определяется кронекеровским произведением

$$\mathbf{H}_{2^n} = \mathbf{H}_{2^{n-1}} \times \mathbf{H}_2,$$

где $\mathbf{H}_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, $\{1,\ -1\} \in GF(2)$.

Пример. Пусть открытое сообщение есть слово $m = ИИТ$. Разобъем m на блоки M_1, M_2, M_3. Согласно теории информации блок M_i описывает дискретный источник без памяти [1]. На выходе такого источника формируется целое число. Используем стандартное соответствие между символами источников и двоичным 8-битовым кодом ASCII. Сообщению $m = ИИТ$ соответствуют целые десятичные и двоичные числа ASCII-кода. Получаем

$$I \to M_1 = M_2 \to (0\ 1\ 0\ 0\ 1\ 0\ 0\ 1) \to 73_{10},$$
$$T \to M_3 \to (0\ 1\ 0\ 1\ 0\ 1\ 0\ 0) \to 84_{10}.$$

Шифрование выполним с использованием алгоритма гаммирования и кодовых слов матрицы $\mathbf{H}_{2^3}$. Для удобства вычисления криптограммы используем двоичную матрицу Адамара. В качестве кодовых слов (ключей) выберем две произвольные строки матрицы $\mathbf{H}_{2^3}$: $h_1 = (0\ 1\ 0\ 1\ 0\ 1\ 0\ 1)$, $h_2(0\ 0\ 1\ 1\ 0\ 0\ 1\ 1)$. Результат гаммирования на полем $GF(2)$ имеет вид $C = (0\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ 0)$. По защищённому каналу связи вместо слова $m = ИИТ$ передается десятичное число 1842278_{10}. Эффективность защиты данных существенно возрастает с увеличением порядка матрицы Адамара. Достоинством предложенного метода защиты данных является сравнительно малые вычислительные затраты потокового шифрования.

Вывод. Предложенная конструкция ключа может применяться для обеспечения конфиденциальности на сеансовом принципе организации связи. Раскрытие сеансового ключа не является катастрофой всей криптосистемы.

Список использованных источников:

1. Compressing the geospatial data of testing grounds / *A. Mitsiukhin* / WSEAS Transactionson Environmentand Development, ISSN: 1790-5079 E-ISSN: 2224-3496 Volume 19, 2023, Art. #125. Pages: 1386-1391DOI: 10.37394/232015.2023.19.