УДК 004.94

СИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ

Студент гр. 11307123 Дайлида А. В.
кандидат техн. наук, доцент Бокуть Л. В.
Белорусский национальный технический университет, Минск, Беларусь

Симметричные криптосистемы – это криптосистемы, использующие алгоритмы симметричного шифрования, то есть это способ шифрования данных с одним криптографическим ключом как для кодирования, так и для декодирования информации [1]. В свою очередь алгоритмы симметричного шифрования подразделяются на потоковые и блочные.

Потоковое шифрование основано на замене каждого бита информации. Замещающий бит генерируется на основе ключа. На сегодняшний день актуальными остаются следующее алгоритмы потокового шифрования: HC-256, RC4, WAKE, Salsa20, SEAL.

Блочное шифрование основано на шифровании данных блоками одинаковой длины (например, 64, 128 бит). Если длина сообщения не кратна размеру блока, то система дополняет последний блок определенным набором символов, называемым дополнением. Актуальные блочные алгоритмы: Blowfish, RC5, NUSH, Twofish, AES, ГОСТ 28147-89, DES [2].

Одним из самых известных и легких симметричных потоковых шифров является шифр Цезаря. Его суть заключалась в сдвиге букв алфавита на некоторое количество. Сам Цезарь чаще всего использовал сдвиг на 3 вправо (А-Г, Б-Д…).

В истории можно выделить также метод шифрования информации «Решетка Кардано». Его суть заключалась в наложении на лист шифрованного текста дощечки с прорезями, в которых можно было прочесть истинное сообщение. Однако такой метод трудоемок для шифрования в силу того, что нужно придумать отвлекающий текст с частями исходного сообщения [3].

Наиболее распространенным и известным компьютерным алгоритмом шифрования является блочный алгоритм DEA, лежащий в основе DES (стандарт шифрования данных в США). Его суть заключается в последовательном преобразовании 64-битовых блоков:

$$У, Ф_1, Ф_2, ..., Ф_{16}, У^{-1}, \quad (1)$$

где У – заданная подстановка; $Ф_i = V_iT$ – преобразование Файстеля:

$$T(L, R) = (R, L) – перестановка левой и правой частей;$$

$$V_i = V(L_i, R_i) = (L_i, R_i \oplus F(R_{i-1}, K_i)); \quad L_0R_0; \quad L_i = R_{i-1}; \quad R_i = L_{i-1} \oplus F(R_{i-1}, K_i), (i = 1, ... ,16),$$

где K_i – ключи, получаемые на основе 56-битового секретного ключа K; F – функция раунда.

Дешифрование реализуется на основе преобразований (1) и с помощью ключа K, такого, что ключи K_i генерируются в обратном порядке. Стоит заметить, что оригинальный алгоритм DEA был разработан для применения в виде микросхем, из-за чего программный код показывает себя очень медленным [4].

При сравнении симметричных и асимметричных криптосистем можно выделить достоинства и недостатки первых. К достоинствам симметричных криптосистем относятся простота и скорость шифрования, возможность использования коротких ключей со сравнительно высокой стойкостью, а к их недостаткам можно отнести сложность безопасной передачи ключа получателю шифра, а также плохая масштабируемость систем шифрования.

Литература

1. Энциклопедия Касперского [Электронный ресурс]. – Режим доступа: https://encyclopedia.kaspersky.ru/glossary/symmetric-encryption/. – Дата доступа: 08.03.2024.

2. Гатчин, Ю. А. Основы криптографических алгоритмов. / Ю. А. Гатчин, А. Г. Коробейников. – СПб.: СПбГИТМО (ТУ), 2002. – 142 с.

3. Singh, S. The Code Book. Histoire des codes secrets: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, De l'Égypte des pharaons à l'ordinateur quantique / S. Singh. – New York City: Doubleday, Knopf Doubleday Publishing Group, 1999. – 416 p.

4. Лекция кандидата техн. наук, доцента Ливак Е. Н. [Электронный ресурс]. – Режим доступа: https://mf.grsu.by/UchProc/livak/b_protect/zok_2.htm. – Дата доступа: 10.03.2024.