В. И. Вербицкая

СИСТЕМАТИЗАЦИЯ АЛГОРИТМОВ ШИФРОВАНИЯ ДАННЫХ

Рассматриваются алгоритмы шифрования, примеры криптоалгоритмов и их систематизация.

Введение

Потребность в защите информации в условиях передачи данных по глобальной сети и потенциально высокой вероятности ее взлома или перехвата, требует новых подходов к шифрованию информации устойчивыми методами.

I. Описание алгоритмов шифрования

Алгоритмы шифрования делятся на три категории: бесключевые, одноключевые и двухключевые (рис.1).

Рис. 1 – Алгоритмы шифрования

Каждая из систем шифрования имеет практические сферы применения, они все разные по уровню криптоустойчивости. Однако, все методы развиваются за счет большой востребованности в защите информации на разных уровнях работы с информацией.

II. Анализ криптоалгоритмов

Современные алгоритмы шифрования разрабатываются таким образом, чтобы взломщик имел как можно меньше шансов отыскать секретный ключ, с помощью которого были зашифрованы данные. Одноключевое шифрование обеспечивает гарантированную криптостойкость при использовании ключей достаточно большого размера, однако, существует необходимость передачи конфиденциальной информации, когда и отправитель, и получатель имеют ключи лишь малого размера. Использование таких ключей непосредственно в алгоритмах одноключевого шифрования позволяет нарушителю определить эти ключи методом перебора.Одноключевые системы используются как самостоятельное средство для защиты информации, как средство распределения ключей и аутентификации пользователей, широко применяются для сокрытия конфиденциальной информации и обладают высокой скоростью передачи данных.

Для решения данной проблемы необходимо использовать алгоритмы бесключевого шифрования, которые обеспечивают необходимый уровень устойчивости. Недостатками бесключевого алгоритма являются невозможность обеспечить аутентификацию сообщений и сложность управления ключами в большой сети, и для применения алгоритма необходимо решить проблему надёжной передачи ключей каждой из сторон по секретному каналу.

Более надежной системой шифрования является двухключевая система шифрования, которая генерирует два ключа, связанные друг с другом определенным способом – открытый и закрытый ключ. Такой подход обладает повышенной надежностью за счет того, что знание открытого ключа не позволяет определить закрытый ключ, также только одной стороне известен ключ дешифрования, который нужно держать в секрете. В данный алгоритм сложнее внести изменения и он имеет более длинные ключи. Двухключевая криптосистема чаще всего предназначена для авторизации и обеспечения юридической значимости электронных документов при обмене между пользователями.

III. Выводы

Существует огромное число качественных алгоритмов шифрования, однако это не исключает возможности несанкционированного доступа к данным. Поэтому криптография является важной дисциплиной современного мира.

1. Камский, В. А. Защита личной информации в Интернете, смартфоне и компьютере / В. А. Камский // – 2017. – С. 15-18.
2. Романьков, В. А. Введение в криптографию / В. А. Романьков // – 2012. – С. 130-134.

Вербицкая Вероника Игоревна, студент 1 курса факультета информационных технологий и управления БГУИРа, veron.itgame@gmail.com.

Научный руководитель: Шатилова Ольга Олеговна, старший преподаватель кафедры вычислительных методов и программирования БГУИР, магистр технических наук, o.shatilova@bsuir.by.