УДК 004.056.5

ОБЗОР СОВРЕМЕННЫХ МЕТОДОВ ШИФРОВАНИЯ

Смирнов П.П., студент 3 курса экономического факультета
ФГБОУ ВО Ульяновский ГАУ
Замальдинова Ю. М., студентка 3 курса факультета физико-математического и технологического образования
ФГБОУ ВО Ульяновского ГПУ
Научный руководитель – Голубев С.В.,
кандидат экономических наук, доцент
ФГБОУ ВО Ульяновский ГАУ

Ключевые слова: *шифрование, алгоритмы, ключ, шифр.*

В статье рассмотрены современные методы и алгоритмы шифрования данных, их преимущества и недостатки.

В настоящее время актуальна защита личной информации. В эпоху «цифровой жизни» встает важный вопрос обеспечения защиты данных путем сокрытия информации от лиц, для которых она не предназначена. В наше время успех любого вида деятельности все сильней зависит от знания какой-либо ценной информации и от отсутствия ее у конкурентов. Поэтому особое внимание уделяется защите информации. Для того чтобы решить столь серьезную проблему, были разработаны специальные алгоритмы шифрования.

Шифрование — изменение информации с помощью ключа в особый, скрытный формат в целях обезопасить от злоумышленников и понятный для пользователя, которому она предназначена [1]. Шифрование позволяет избежать таких рисков информационной безопасности: кража, распространение информации, подделка под оригинал. В данное время существует множество различных способов шифрования. При сравнительном анализе алгоритмов шифрования необходимо учитывать следующие характеристики: практическую стойкость шифра, ресурсоемкость и энергоемкость, скорость работы.

Алгоритмы шифрования устроены таким образом, что для вскрытия требуется перебор по ключевому пространству, поэтому надежность шифра определяется длиной ключа. Основные способы шифрования: симметричное, асимметричное, хеширование.

Симметричное шифрование — это способ шифрования данных, при котором один и тот же ключ используется и для кодирования, и для восстановления информации [2]. До 1970-х годов, когда появились первые асимметричные шифры, оно использовалось, как единственный криптографический метод шифрования.

В целом симметричным считается любой шифр, использующий один и тот же секретный ключ для шифрования и расшифровки.

Допустим, если алгоритм предполагает замену букв числами, то и у отправителя сообщения, и у его получателя должен быть один и тот же способ сопоставления букв и чисел: первый с ее помощью зашифровывает сообщение, а второй его расшифровывает.

К сожалению, такие простейшие шифры легко поддаются взлому — например, зная частотность разных букв в языке, можно соотносить самые часто встречающиеся буквы с самыми многочисленными числами или символами в коде, пока не удастся получить осмысленные слова. С использованием современных технологий такая задача стала наилегчайшей, так как занимает мало времени. Исходя из этого, использование подобных алгоритмов утратило всякий смысл [3].

Чтобы решить эту проблему программисты начали использовать асимметричное шифрование. В данном способе создаются случайным образом два математически связанных ключа. Один – это приватный ключ, доступ к которому имеете только вы. Второй – открытый, который является доступным для всех пользователей. Публичный ключ используется для шифрования информации и может передаваться по незащищенным путям. Приватный ключ используется для расшифровки отправленных данных, зашифрованных открытым ключом [4]. Открытый и закрытый ключи — это очень длинные числа, которые связаны друг с другом, но так, что, зная одно, почти невозможно вычислить второе. Асимметричное шифрование используют, главным образом, для защиты информации при ее передаче.

Хеширование, в отличие от симметричного и асимметричного шифрования, является односторонней функцией. Можно сгенерировать хеш из некоторых данных, но не существует способа, чтобы обратить этот процесс. Это можно назвать недостатком и делает хеширование не очень удобным способом хранения данных. Но данный метод отлично подходит для проверки целостности данных. Идеальная функция хеширования создает уникальные

значения для различных путей. Одинаковый ввод всегда будет производить одинаковый хеш. Поэтому данный способ удобно использовать для проверки целостности данных [5 - 7].

Исходя из вышеприведенной информации следует, что существует много различных и надежных способов шифрования данных. Но стоит отметить, что не всегда их использование может обеспечить полную защиту данных и исключить возможность несанкционированного доступа к ней.

Библиографический список:

1. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайдер. — М.: Триумф, 2003. — 121 с.

2. Сингх, С. Книга шифров. Тайная история шифров и их расшифровки / С. Сингх. — М.: Аст, Астрель, 2006. — 447 с. – Режим доступа: http://kriptografea.narod.ru/TDES.html.

3. Иванов, К. К. Алгоритмы шифрования данных / К. К. Иванов, Р. Н. Юрченко, А. С. Ярмонов // Молодой ученый. — 2016. — № 29 (133). — С. 18-20. — Режим доступа: https://moluch.ru/archive/133/37180/.

4. Нагиева, А. Ф. Корпоративные сети и проблемы безопасности / А.Ф. Нагиева // Молодой ученый: Международный научный журнал. – Казань, 2016. – № 29 (133). – С. 34–36.

5. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей / В.Ф. Шаньгин. – М.: ИД «форум» — инфра-м, 2011. – 201 с.

6. Солнцева, О.В. Анализ статистических данных в пакете Statistica 5.5 / О.В. Солнцева, А.В. Севастьянов.- Ульяновск, 2004. Часть I

7. Круглова, Э.В. Оценка регулирующего воздействия как механизм поиска баланса между экономической и социальной эффективностью (на примере государственного регулирования рынка алкогольной продукции в Ульяновской области)/ Э.В. Круглова, М.Г. Светуньков, И.В. Шелаганова // Современная конкуренция. - 2014. - № 1 (43). - С. 71-79.

OVERVIEW OF MODERN ENCRYPTION METHODS

Smirnov P.P.,
Zamaldinova Yu.M.

Key words: *encryption, algorithms, key, cipher.*

This article discusses modern methods and algorithms for data encryption, their advantages and disadvantages.