УДК 004.056.55

АЛГОРИТМЫ ШИФРОВАНИЯ

И.А. Грязнов

Научный руководитель – **М.И. Озерова**, доцент

Владимирский государственный университет

Описаны основы шифрования. Представлен алгоритм шифрования, разработанный автором данной статьи. Проведено зашифровывание и расшифровывание с помощью этого алгоритма.

Ключевые слова: *шифрование, алгоритм, безопасность*

Encryption Algorithms

I.A. Gryaznov

Scientific Supervisor – **M.I. Ozerova**, Associate Professor

Vladimir state university

Bases of encryption are described. Encryption Algorithm developed by the author of this article is represented. This algorithm was used to encrypt and decrypt some data.

Keywords: *encryption, algorithm, security*

Шифрование - обратимое преобразование информации в целях сокрытия от неавторизованных лиц. Шифрование в основном происходит с помощью ключа, доступ к которому предоставляется авторизированным пользователям. Злоумышленники же, перехватив сообщение, но не имею ключа, не смогут воспользоваться им. Одни из первых методов шифрования были разработаны еще в Древнем Египте. Они заключались в замене одних букв алфавита на другие по определенным математическим правилам. И конечно среди самых известных алгоритмов шифрования – метод Цезаря. С развитием технологий безопасность информации становилась все важнее, а шифрование все изощреннее. Важную роль в исходе Второй Мировой Войны сыграло расшифровывание кодов «Энигмы» британским ученым Аланом Тьюрингом. Также большой вклад в данную область был внесен Клодом Шенноном, описавшим в своей статье "Теория связи в секретных

системах" 1949 г. теоретическую и практическую стойкость алгоритмов шифрования

Современный мир невозможно представить без шифрования. Все больше и больше информации «оцифровывается» и хранится на компьютерах в базах данных. Среди этих данных множество конфиденциальных таких как: личные данные клиента (его прописка, номер паспорта и т.д); всевозможные пароли; номера банковских карт, счетов, договоров; ключи активации программного обеспечения; секретные военные данные и многое другое. С развитием вычислительных сетей физического ограничения доступа к информации стало недостаточно, поэтому вся секретная информация должна быть зашифрована.

В наше время шифрование является частью науки криптография и обеспечивает три состояния безопасности информации: конфиденциальность (для скрытия информации от неавторизованных пользователей), целостность (для предотвращения изменения информации), идентифицируемость (для аутентификации источника информации). Различают 3 алгоритма шифрования:

1. Симметричное шифрование. Его суть заключается в том, что для зашифровки и расшифровки применяется один и тот же ключ. Однако главной проблемой данных методов является проблема безопасной передачи ключа авторизированным пользователям. В свою очередь, симметричные алгоритмы подразделяются на блочное и поточное шифрование. В первом случае данные разделяются на блоки фиксированной длины, которая равна длине ключа шифрования, затем сегменты шифруется отдельно (для большей надежности каждый блок можно шифровать собственным методом зависимым, например, от результата шифрования предыдущего). Поточное шифрование является частным случаем блочного, когда длина нашего блока равна 1 биту. Важной проблемой этих методов является передача ключа, по которому проводится шифровка/расшифровка данных. В ходе передачи ключ может быть перехвачен злоумышленниками, и тогда алгоритм шифрования станет бесполезен. Следующая же группа методов лишена этого недостатка.

2. Ассиметричное шифрование. В его основе лежит использование 2 ключе – открытого и закрытого. Открытый используется для шифровки информации и не скрывается. Расшифровка же происходит с помощью закрытого ключа, доступного только авторизированным пользователям. Вычисление же секретного

ключа из открытого практически не представляется возможным и потребует огромного количества времени.

3. Бесключевые алгоритмы шифрования. Как следует из названия не предполагают использование ключей. Среди этих методов очень часто применяются Хэш-функции, использующиеся, например, для проверки целостности данных при передаче или же для быстрого поиска в базах данных (системе не придется просматривать всю базу, а по хэш-коду будет вычислен раздел, в котором необходимо провести поиск). Популярность этот метод заслужил за счет своей простоты и низкой потребности ресурсов

Для оценки качества алгоритма шифрования используют понятие криптографической стойкости - свойство криптографического шифра противостоять криптоанализу, то есть анализу, направленному на изучение шифра с целью его дешифрования. Различают абсолютно стойкие и достаточно стойкие системы.

Ниже приведен один из возможных симметричных алгоритмов сортировки, придуманный автором данной статьи.

Алгоритм шифровки:

Для удобства обозначим: исходная строка - S1, зашифрованная строка - S2 = «»

1. Рассчитывается исходная длина входной строки S1, если она нечетна, прибавляем к ней символ « »;
2. Берутся первый с начала и первый с конца S1 символы, последний прибавляется к S2 слева, первый справа;
3. Берутся второй с начала и второй с конца S1 символы, последний прибавляется к S2 справа, первый слева
4. Берутся третий с начала и третий с конца S1 символы, последний прибавляется к S2 слева, первый справа;
5. Продолжать, пока не дойдем до середины S1

Алгоритм расшифровки

Расшифровка идет по тому же принципу, что и шифрование за двумя исключениями –

1. Не требуется проверка на четность строки;
2. Если величина равная длине расшифрованной строки, поделенной на 2 является четной, то результат получится «перевернутым». В этом случае будет необходимо выполнить реверс.

Рассмотрим данный алгоритм шифровки на простой исходной строке S1 = «Гитара»

1. Длина строки = 6 – четна, преобразование не требуется
2. Берем первый сначала «Г» и первый с конца «а» символы. «а» прибавляем к S2 слева, «Г» справа. Получим S2 = «аГ»
3. Берем второй сначала «и» и второй с конца «р» символы. «р» прибавляем к S2 справа, «и» слева. Получим S2 = «иаГр»
4. Берем третий с начала «т» и третий с конца «а» символы. «а» прибавляем к S2 слева, «т» справа. Получим S2 = «аиаГрт». Шифровка окончена.

Теперь расшифруем S1 = «аиаГрт»

1. Берем первый с начала «а» и первый с конца «т» символы. «т» прибавляем к S2 слева, «а» справа. Получим S2 = «та»
2. Берем второй с начала «и» и второй с конца «р» символы. «р» прибавляем к S2 справа, «и» слева. Получим S2 = «итар»
3. Берем третий с начала «а» и третий с конца «Г» символы. «Г» прибавляем к S2 слева, «а» справа. Получим S2 = «Гитара». Расшифровка закончена.

Возможно данный метод не впечатляет при шифровке строк, состоящих из 1 слова, но при увеличении строки, ее «усложнении» различными знаками препинания и прочими символами, при шифровке целых предложений, а то и текстов, узнать исходные данные просто невозможно.

Например, исходная строка: «I don’t believe that luck is a coincidence. I believe it’s the result of tireless preparation, hours and hours perfecting your craft. Being willing to go harder and further than the next man. For me, luck is no coincidence». Превращается в нечто неузнаваемое: «psruehtdna sourhc,aott repnr isllnr tofg lasdrreatdsftr hvritea he nedtcminc aos ec lutkhi voicei c’don eIcdenitnbol enest ac lu,kmir F .oan ixence.tInbhl eeetiu’ nh eeruhtoo tigeielswpgeiaBa.ifnr oury gni cofre »

Данный алгоритм не претендует на мировое господство и не стремиться хватать звезд с неба, но вполне сгодиться для личного пользования и сохранения конфиденциальности какой-либо информации.

СПИСОК ЛИТЕРАТУРЫ

1. Э. Мэйволд. Безопасность сетей. — 2006. — 528 с. — ISBN 978-5-9570-0046-9
2. Мао В. Современная криптография: Теория и практика — М.: Вильямс, 2005. — 768 с. — ISBN 978-5-8459-0847-6

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