УДК 003.26.09
DOI: 10.33764/2618-981X-2019-7-59-61

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ ШИФРОВАНИЯ ТЕКСТОВОЙ ИНФОРМАЦИИ НА БАЗЕ МОДИФИЦИРОВАННОГО АЛГОРИТМА РИХАРДА ЗОРГЕ

Евгений Александрович Долгочуб
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, обучающийся, тел. (913)932-07-05, e-mail: evgeniidolg@mail.ru

Петр Юрьевич Бугаков
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, кандидат технических наук, доцент кафедры прикладной информатики и информационных систем, тел. (383)343-18-53, e-mail: peter-bugakov@ya.ru

В работе рассматривается алгоритм шифрования Рихарда Зорге и его последующая модификация. Производится грубая оценка криптографической стойкости модифицированного алгоритма. Описываются основные аспекты проекта.

Ключевые слова: алгоритм шифрования, программное обеспечение, Рихард Зорге, C++.

SOFTWARE FOR THE ENCRYPTION OF TEXT DATA BASED ON THE MODIFIED ALGORITHM OF RICHARD ZORGE

Evgeniy A. Dolgochub
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Student, phone: (913)932-07-05, e-mail: evgeniidolg@mail.ru

Petr Yu. Bugakov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Ph. D., Associate Professor, Department of Applied Informatics and Information Systems phone: (383)343-18-53, e-mail: peter-bugakov@yandex.ru

The paper deals with the encryption algorithm of Richard Sorge and its subsequent modification. Made a rough evaluation of the cryptographic strength of the modified al-gorithm. The main aspects of the project are described.

Key words: encryption algorithm, software, Richard Zorge, C++.

Люди всегда нуждались, нуждаются и будут нуждаться в конфиденциальной переписке, поэтому разработка методов шифрования никогда не стоит на месте. С раскрытием одних шифров придумывались более сложные. Требования к защите конфиденциальной информации возросли многократно.

Целью работы является модификация и программная реализация алгоритма шифрования Рихарда Зорге. Область применения разрабатываемой программы весьма обширна, но в первую очередь она предназначена для тех, кто заинтересован в конфиденциальности своей переписки и сохранности важных документов.

Для начала, рассмотрим принцип работы симметричного алгоритма шифрования Рихарда Зорге [1–6]. Создавалась сетка, в которую записывался английский алфавит в определённом порядке. Сообщение разбивалось на группы по 4 буквы и каждой букве присваивались десятичные номера. В результате образовывалась числовая последовательность, на которую накладывалась гамма из немецкого статического ежегодника 1939 года. После этого сообщение отправлялось получателю. Стоит отметить, что все сообщения, которые передал советский разведчик, остались непрочитанными.

Перейдём непосредственно к модификации алгоритма. Для шифрования используется алфавит, состоящий из букв латиницы и кириллицы верхнего и нижнего регистров, цифр от 0 до 9 и специальных символов. В алгоритм вводятся 8 ключевых переменных, значение которых пользователь может ввести сам. С использованием этих переменных вычисляются 200 возможных вариантов гамм. Далее генерируется массив M, состоящий из псевдослучайных чисел от 0 до 199. Смещение индексов гамм определяется значением элемента массива M, стоящего под номером N, где N – это константное значение в интервале от 1 до 10, выбираемое пользователем.

Передачу копий программы и временных файлов с заданным массивом псевдослучайных чисел планируется осуществлять на миниатюрных флэш-накопителях. Для того, чтобы начать шифровать информацию, необходимо выставить все нужные параметры. Пока параметры не будут изменены пользователем, программа функционирует в автоматическом режиме.

В программе задействован набор защитных протоколов:

– «Очистка», предназначенный для удаления исходного и зашифрованного текста;

– «Профилактика», который предполагает удаление из временного файла всех использованных гамм и значений, а также сброс всех настроек программы;

– «Протокол Lockdown», который полностью удаляет временные файлы и программу, а также делает невозможным обнаружение признаков её использования на устройстве пользователя.

При шифровании текста каждый символ отделяется пробелом. Пробелы в исходном тесте шифруются отдельно по такому же принципу. Это позволяет сложить предложение, не разрушив его структуру. Программа позволяет шифровать и дешифровать любую текстовую информацию на латинице и кириллице.

В результате работы была выполнена модификация алгоритма шифрования Рихарда Зорге, написана программа на языке C++ в среде программирования Visual Studio [7]. Апробация программы показала высокую криптостойкость модифицированного алгоритма. Для его взлома необходимо узнать начальные данные и восстановить временный файл с массивом псевдослучайных чисел. В случае подбора исходных настроек программы злоумышленнику придётся перебрать $6{,}86*10^{33}$ вариантов без учёта подбора массива псевдослучайных чисел во временном файле.

Криптостойкость модифицированного алгоритма Рихарда Зорге способна обеспечить безопасную передачу данных по открытым каналам связи, а разработанная на его основе программа может использоваться коммерческими организациями и физическими лицами для защиты данных, представленных в текстовой форме.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Сигх С. – Книга шифров. Тайная история шифров и их расшифровки [Текст]. – М.: Аст, Астрель, 2006. 447 с.

2. Бауэр Ф. Расшифрованные секреты. Методы и принципы криптологии [Текст]. – М.: Мир, 2007. 550 с.

3. Мао В. Современная криптография. Теория и практика [Текст]. – М.: Вильямс, 2005. 763 с.

4. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии [Текст]. – М.: Гелиос АРВ, 2001. 479 с.

5. Блог Лаборатории Касперского - Рихард Зорге и книжный шифр - информационная безопасность времен Второй мировой [Электронный ресурс]. – Режим доступа : https://www.kaspersky.ru/blog/ww2-zorge-book-cipher/7724/

6. Синельников А.В. Шифры советской разведки. – Новосибирск, 2009. – 40 с.

7. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си [Текст]. – М.: Триумф, 2003. 806 с.