УДК 004

Криптография. Методы шифрования данных

Цветков Николай Витальевич
Ярославский государственный педагогический университет им.К.Д.Ушинского
магистрант

Аннотация
Данная работа посвящена знакомству с основами криптографии и, в частности, с методами шифрования информации. Главная задача данной работы - познакомить пользователя с простейшими методами шифрования информации. В данной работе, во–первых, были подобраны наиболее известные методы шифрования информации, во–вторых, выполнена реализация данных алгоритмов на языке программирования C#. Результатом работы является демонстрационно-обучающая программа, которая предусматривает пошаговое изучение каждого алгоритма шифрования, а также шифратор и дешифратор.
Ключевые слова: криптография, шифрование, безопасность, алгоритмы шифрования

Cryptography. Data encryption methods

Tsvetkov Nikolay Vitalievich
Yaroslavl State Pedagogical University after K.D.Ushinsky
Undergraduate student

Abstract
This work is devoted to familiarity with the basics of cryptography and, in particular, with the methods of information encryption. The main task of this work is to acquaint the user with the simplest methods of information encryption. In this work, firstly, the most known methods of information encryption were selected, and secondly, the implementation of these algorithms in the C#programming language was performed.
The result of the work is a demonstration and training program, which provides a step-by-step study of each encryption algorithm, as well as an encoder and decoder.
Keywords: cryptography, encryption, security, encryption algorithms

На протяжении долгих столетий человечество нуждалось в шифровании любого рода информации. Общение человека – узко избирательно, и то, что мы сообщаем одним, стараемся тщательно скрыть от других. Чем оживленнее в обществе велась переписка, тем больше ощущалась потребность в ее шифровании. Возникали шифры, сначала

простейшие, а затем и более совершенные, вплоть до современных шифров, которые способны расшифровать только компьютеры.

Из потребности шифровать информацию возникла целая наука – криптография. Стоит сказать, что ранее, криптография была востребована лишь в интересах государства, но с появлением интернета, методы шифрования заинтересовали и простых пользователей. Для того что бы правильно действовать на просторах интернета, нужно иметь представление об основах криптографии.

Данная статья посвящена знакомству с основами криптографии и в частности с методами шифрования информации. Любой человек сталкивается с шифрованием данных практически каждый день, поскольку работа в интернете предусматривает шифрование информации в огромных количествах с целью вашей безопасности. Главная задача – познакомить с простейшими методами шифрования информации, доступными для любого человека.

В данной работе, в–первых, были подобраны наиболее известные простейшие методы шифрования информации, во–вторых, выполнена оценка сложности каждого алгоритма, в–третьих, проведен анализ на стойкость к взлому каждого из шифров, в-четвертых, выполнена реализация данных алгоритмов на одном из языков программирования.

Результатом проведенной работы является демонстрационно-обучающее приложение (рисунок 1).

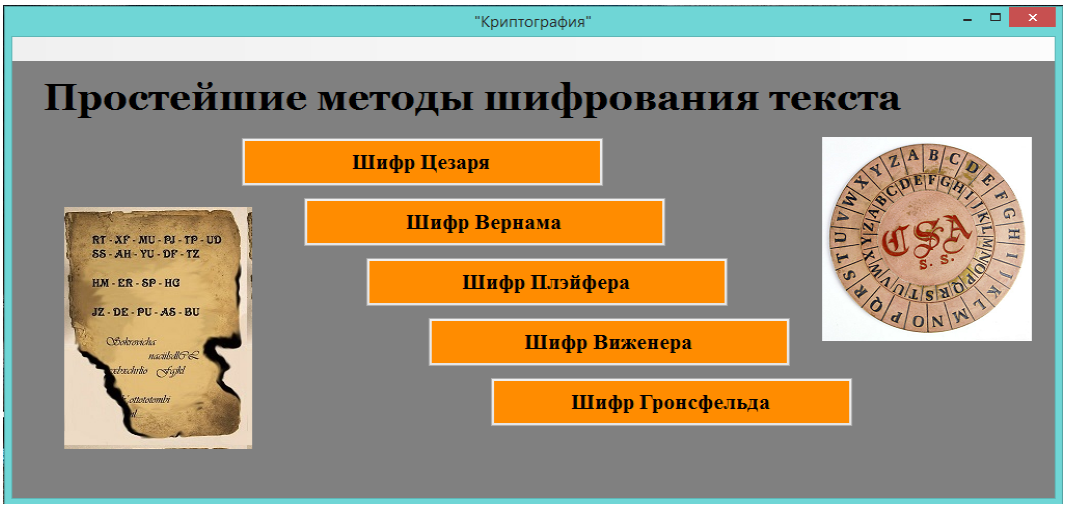

Рисунок 1. Демонстрационно-обучающая программа

В приложении реализовано пять алгоритмов, основанных на симметричном шифровании: Шифр Цезаря; Шифр Вернама; Шифр Плэйфера; Шифр Виженера; Шифр Гронсфельда.

Приложение предусматривает пошаговое изучение каждого алгоритма шифрования, а также шифратор и дешифратор, соответствующий требованиям шифра.

Первым, одним из самых широко известных методов шифрования возник шифр Цезаря, названный в честь римского императора Гая Юлия

Цезаря. Император использовал его в личных военных целях для секретной переписки со своими генералами.

Шифр Цезаря – это шифр замены, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций правее него в алфавите.

Неизвестно, насколько эффективным шифр Цезаря был в то время, но, вероятно, он был безопасен, благодаря тому, что большинство врагов Цезаря были неграмотными, и многие предполагали, что сообщения были написаны на неизвестном иностранном языке. Даже позднее, в 1915 году, шифр Цезаря находил применение: российская армия использовала его как замену для более сложных шифров, которые оказались слишком сложными для войск.

Шифр Цезаря активно используется и в современных алгоритмах шифрования, но не как полноценный метод шифрования, а лишь как часть алгоритма [2].

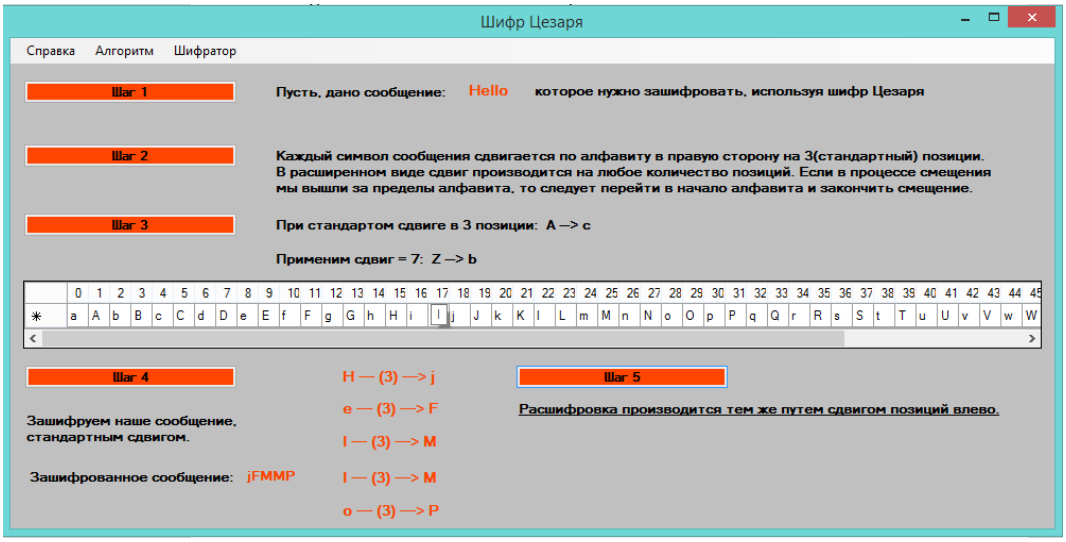

Рисунок 2. Пошаговое изучение шифра Цезаря

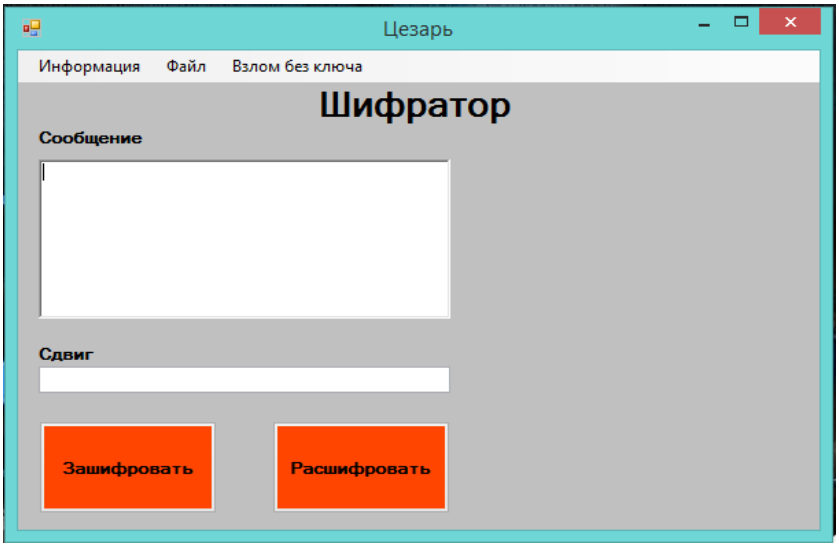

Рисунок 3. Шифратор/дешифратор шифра Цезаря

Другой, более сложный шифр, был назван в честь телеграфиста компании AT&T Гильберта Вернама, который изобрел его в 1917 году, а в

1919 запатентовал систему автоматического шифрования телеграфных сообщений. Шифр является разновидностью криптосистемы одноразовых блокнотов, в котором используется булева функция «Исключающее ИЛИ». Каждый символ в сообщении преобразовывался побитовым XOR (Исключающее ИЛИ) с ключом бумажной ленты.[2]

Шифр Вернама является примером системы с абсолютной криптографической стойкостью, но при этом он считается одной из простейших криптосистем.

В настоящее время шифрование Вернама используется достаточно редко. Тем не менее, совершенно стойкие шифры типа Вернама всё же нашли практическое применение. Так, например, англичане и американцы использовали шифры типа Вернама во время второй мировой войны.

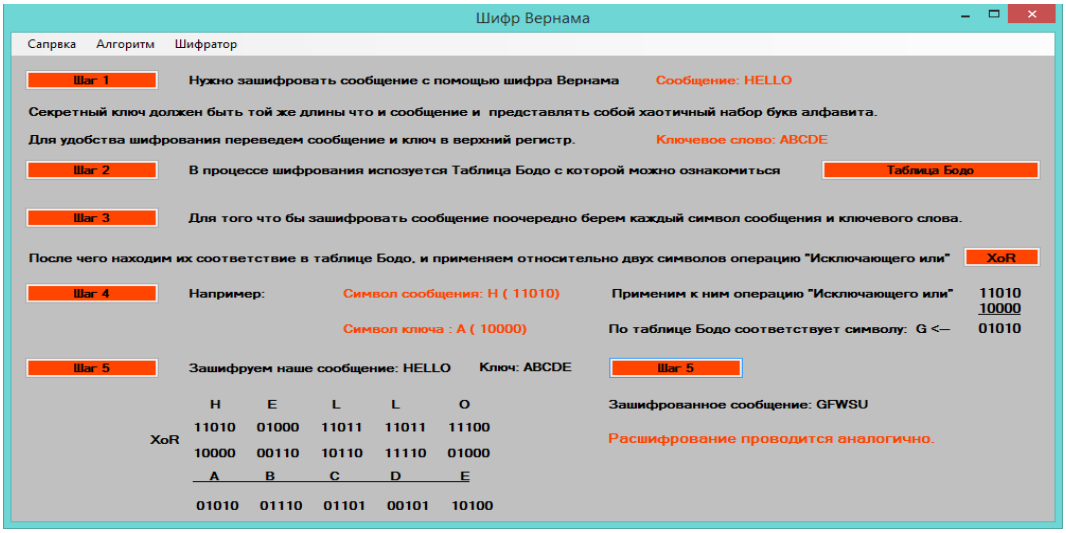

Рисунок 4. Пошаговое изучение шифра Вернама

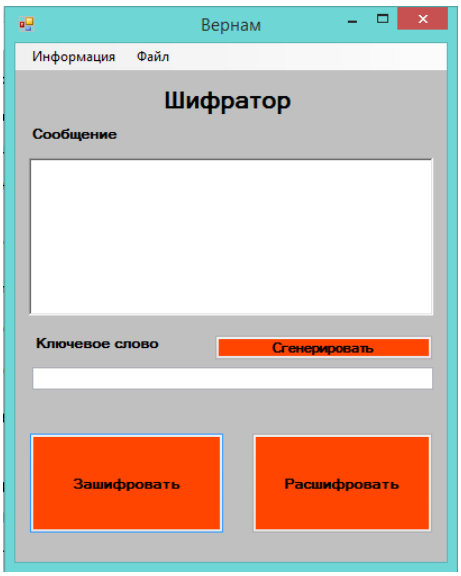

Рисунок 5. Шифратор/дешифратор шифра Вернама

Первым «биграммным» шифром стал шифр Плейфера. Ручная симметричная техника шифрования, в которой впервые использована замена биграмм, то есть шифровались одновременно 2 символа сообщения.[2]

Шифр изобретен в 1854 году английским физиком Чарльзом Уитстоном, но назван именем лорда Лайона Плейфера, который внёс большой вклад в продвижение использования данной системы шифрования в государственной службе.

Использование шифра Плейфера в настоящее время является нецелесообразным, поскольку современные компьютеры могут легко взломать шифр в течение нескольких секунд. Первый изданный алгоритм взлома шифра Плейфера был описан только в 1914 году. Немецкая армия, ВВС и полиция использовали двойную систему шифрования Плейфера во второй мировой войне.

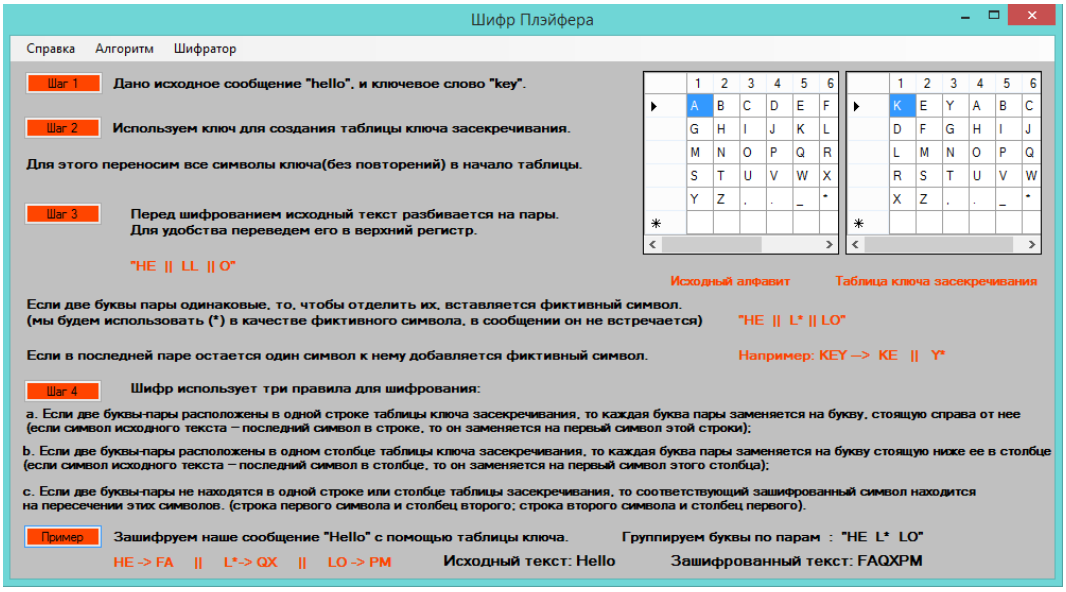

Рисунок 6. Пошаговое изучение шифра Плэйфера

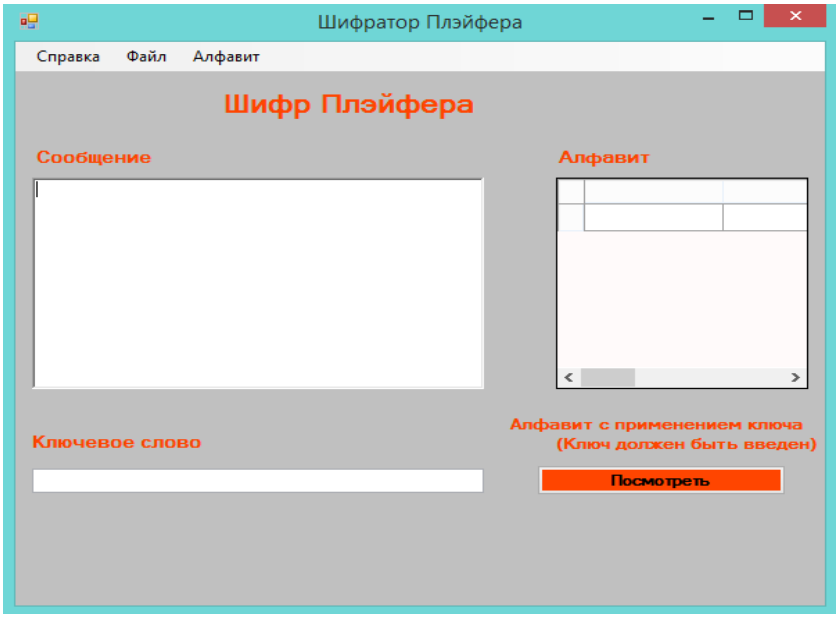

Рисунок 7. Шифратор/дешифратор шифра Плэйфера

Шифр, имеющий многолетнюю историю своего изобретения – шифр Виженера. Впервые метод был описан еще в 1553 году, но свое имя получил лишь в XIX веке в честь французского дипломата Блеза Виженера. Хотя

шифр легко понять и реализовать, на протяжении трех столетий он сопротивлялся всем попыткам его взломать [1].

Блез Виженер представил своё описание простого, но стойкого шифра перед комиссией Генриха III во Франции в 1586 году, и позднее изобретение шифра было присвоено именно ему. Шифр основан на простой формуле, с помощью которой шифруется каждый символ сообщения.

Шифр Виженера достаточно прост для использования в полевых условиях, особенно если применяются шифровальные диски. Например, «конфедераты» использовали медный шифровальный диск для шифра Виженера в ходе Гражданской войны.

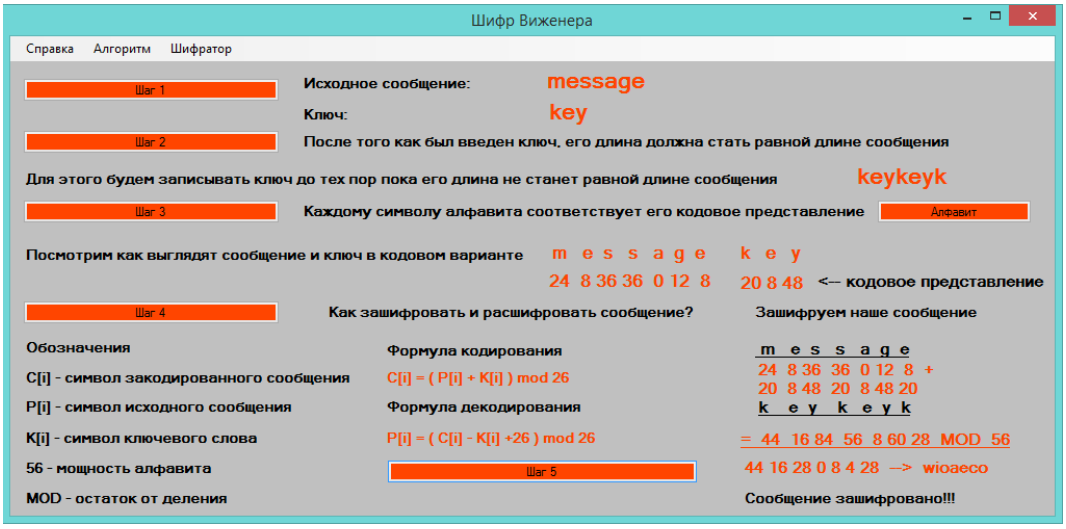

Рисунок 8. Пошаговое изучение шифра Виженера

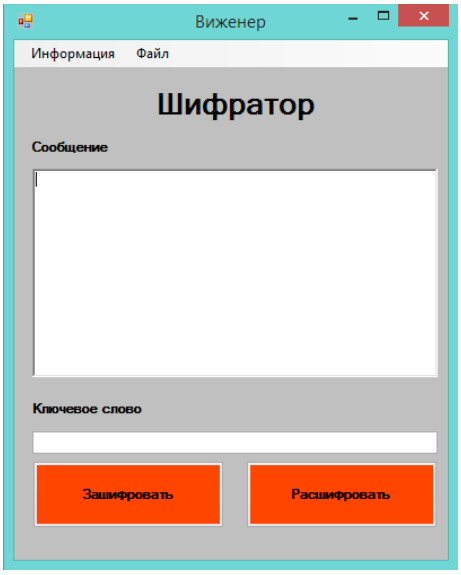

Рисунок 9. Шифратор/дешифратор шифра Виженера

С появлением шифровальных служб развитие криптографии заметно ускорилось. Методы шифрования стали совершенствоваться и усложняться. Так, в 18 веке руководителем первой дешифровальной службы Германии графом Гронсфельдом, был создан одноименный шифр. Шифр Гронсфельда

можно считать усовершенствованием шифра Цезаря и Виженера, который отличался большей надежностью и скоростью шифрования [2].

Рисунок 10. Пошаговое изучение шифра Гронсфельда

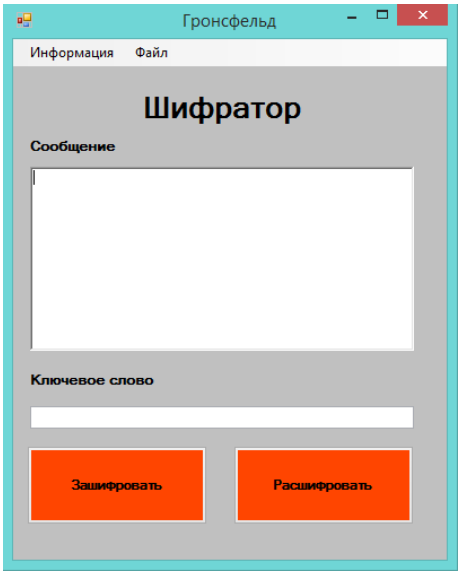

Рисунок 11. Шифратор/дешифратор шифра Гронсфельда

Несмотря на многообразие современных шифровальных систем, простейшие шифры, созданные много веков назад, и сейчас имеют свое применение в шифровании информации. Представленные алгоритмы не рекомендуется использовать при шифровании важной информации, т.к. современные методы взламывают эти шифры в считанные секунды. Целесообразно в этих целях применять современные алгоритмы шифрования. Данную работу полезно использовать при первоначальном знакомстве с криптографией и шифрованием, как в личных, так и общественных целях. Наиболее значимое применение работы раскрывается в школе, на уроках информатики, при изучении шифрования, а так же на уроках программирования.

Библиографический список

1. Алферов А. П., Зубов А. К., Кузьмин А.С., Черемушкин А. В. Основы криптографии: Учебное пособие. М., 2002. 480 с.
2. Криптография. Под редакцией В.П. Шерстюка, Э.А. Применко / А.В. Бабаш, Г.П. Шанкин. М.: СОЛОН-ПРЕСС, 2007 г. 512 с.