УДК 004.413.2

Ключи от тайны

Штепа Михаил Евгеньевич
МБОУ СОШ №1 г. Биробиджана
Учащийся 6 класса

Александрович Дмитрий Александрович
МБОУ СОШ №1 г. Биробиджана
Учащийся 10 класса

Штепа Юлия Петровна
Приамурский государственный университет им. Шолом-Алейхема
кандидат педагогических наук, доцент кафедры информационных систем, математики и методик обучения

Коломеец Светлана Николаевна
МБОУ СОШ №1 г. Биробиджана
Учитель информатики

Аннотация
В статье излагается краткая история шифрования информации и описание наиболее интересных методов криптографии. Описаны три способа шифрования, разработанные авторами, а также их программная реализация в среде программирования Delphi.
Ключевые слова: информатика, шифр, шифрование, криптография.

Keys to the mystery

Shtepa Mihail Evgen'evich
Municipal budget institution of general education "Secondary school of general education №1"
The pupil of the 6-th form

Alexandrovich Dmitriy Alexandrovich
Municipal budget institution of general education "Secondary school of general education №1"
The pupil of the 10-th form

Shtepa Julija Petrovna
Sholom-Aleichem Priamursky State University
Candidate of pedagogical sciences, associate professor of the Department of information systems, mathematics and teaching methods

Kolomeets Svetlana Nikolaevna
Municipal budget institution of general education "Secondary school of general education №1"
Teacher of computer science

Abstract
The article presents a brief history of information encryption and description of the most interesting methods of cryptography. We describe three encryption method developed by the authors and their program implementation in Delphi programming environment.
Keywords: computer science, code, encryption, cryptography.

«… История криптографии…–
это история человечества».
Д.Канн

Недавно мы наткнулись в интернете на такую интересную фотографию. Перед центральным офисом ЦРУ расположена удивительная скульптура, состоящая из беспорядочного, на первый взгляд, набора символов.

Рисунок 1 – Скульптура «Криптос»

Оказалось, что скульптура-загадка «Криптос» является зашифрованным посланием. Она разбита на четыре секции. С 1990 года сообществу удалось разгадать содержимое только трех секций этой скульптуры. Четвертая же до сих пор не разгадана. Эта скульптура и подтолкнула нас к тому, чтобы начать изучать искусство шифрования или криптографию.

Объектом нашего исследования является криптография, а предметом – методы шифрования.

Цель нашей работы – изучить основные способы шифрования и разработать свои шифры.

Мы поставили перед собой следующие задачи:

1. ознакомиться с историей шифров;

2. изучить некоторые способы шифрования;
3. разработать свои шифры;
4. использовать язык программирования для автоматической расшифровки текстов.

Издавна люди изыскивали способы уберечь некоторые важные сообщения от посторонних глаз. Например, один царь обрил голову своего гонца, написал на ней послание и отослал гонца к своему союзнику лишь тогда, когда волосы на его голове отросли. Развитие химии дало толчок развитию тайнописи: симпатические чернила, записи которыми не видны до тех пор, пока бумагу не нагреют или обработают каким-нибудь химикатом. Но чаще стали применять шифры – системы преобразования текста для обеспечения секретности передаваемой информации.

Современные компьютерные системы многократно усложнили дешифровку данных. Часто разработчики известных проектов предлагают желающим попробовать свои силы в дешифровке. Так, например, в 2013 году основатель «ВКонтакте» Павел Дуров предложил всем желающим принять участие в расшифровке его переписки с братом.

Спустя год в качестве вознаграждения победителю сулился приз в 200 тысяч долларов, но никто так и не выполнил эту задачу, а конкурс продолжили, увеличив награду до 300 тысяч. Любопытной была реакция некоторых членов сообщества, которые сожалели о такой строгой формулировке задания и предлагали взломать сам сервер.

Но не стоит думать, что в современных условиях дешифрованием могут заниматься только программисты и хакеры. К счастью, прошлый век оставил нам уйму загадок и полезной пищи для того, чтобы размять наши «серые клеточки».

В Древней Спарте использовали вот такую палицу (рис.2), которая называется скитала (примерно V век до нашей эры).

Рисунок 2 – Скитала

На этот посох наматывалась по спирали полоска пергамента с зашифрованным посланием. Смысл такого «гаджета» был в том, что прочитать эту полоску мог лишь обладатель скиталы аналогичного размера. При правильном размере витка буквы послания совпадали, и получался связный текст. Устройство было очень простым и практичным, хотя не особо надежным.

Наряду с линейкой Сен-Сира, большой популярностью пользовались шифровальные круги, идею которых подсказал в своих трудах Леон Баттиста Альберти – итальянский учёный середины XV столетия.

Рисунок 3 – Диск Альберти

Во время войны Севера и Юга в США диск Альберти («колесо Альберти») – кружок диаметром девять с половиной сантиметров – лежал в кармане у разведчиков и связистов. Шифровальный диск состоял из двух концентрических кругов, скрепленных посередине. Внутренний диск содержал буквы и окончания, а внешний включал в себя группу сигнальных цифр. Секретное устройство украшали буквы A.J.M. – инициалы главного начальника связи, генерала Альберта Дж. Майера.

В военной академии Сен-Сир придумали простое и оригинальное устройство, состоящее из двух частей – алфавитной линейки и подвижного бегунка с написанным алфавитом и прорезью. Принцип шифрования этой линейкой был очень простым и основывался на замещении букв алфавита. Но, в отличие от шифра Цезаря, где общий сдвиг букв при письме был одним и тем же (например, вместо А – Б, вместо В – Г и так далее), в линейке Сен-Сира был реализован шифр замещения с переменным сдвигом, так называемый шифр Блеза де Виженера, французского дипломата, жившего в шестнадцатом столетии.

Рисунок 4 – Линейка Сен-Сира

Решётка Кардано – инструмент кодирования и декодирования, представляющий собой специальную прямоугольную таблицу-карточку, часть ячеек которой вырезана. Автором метода является Джироламо Кардано, который в 1550 году предложил простую решетку для шифрования сообщений. Он планировал маскировать сообщения под обычное послание, так что в целом они не были полностью похожи на шифрованные.

Шифры, реализованные с использованием картонных решеток, принято называть решётками Кардано.

Решетка Кардано может быть двух видов – простая и симметрично-поворотная. В первом случае для шифрования применяется трафарет с отверстиями, через которые «фильтруется» полезный текст. Другой вариант решетки, более интересный, состоит в том, чтобы использовать симметричный (квадратный) трафарет, который можно применять несколько раз, просто поворачивая его вокруг центра.

Мы решили сделать сами решётку Кардано. Мы взяли лист А4 и разлиновали квадрат со стороной в восемь клеток.

По центру квадрата провели две перпендикулярные черты, отделив четыре зоны. Затем заполнили каждую из зон номерами клеток. Нумерацию клеток начинали из угла и вели ее так, чтобы направление нумерации каждый раз было по часовой стрелке.

В каждой части квадрата есть набор цифр. В произвольном порядке закрасили цифры от 1 до 16 так, чтобы числа не повторялись в разных частях решетки (например, если в первой зоне закрашена двойка, то в других зонах ее закрашивать уже не нужно).

Закрашенные клетки – это отверстия, которые мы вырезали. Квадратная решетка Кардано готова. С помощью нашей решетки мы решили зашифровать фразу: «Семь раз отмерь, один раз отрежь». Затем приложили ее к листу и вписали текст (рис.5).

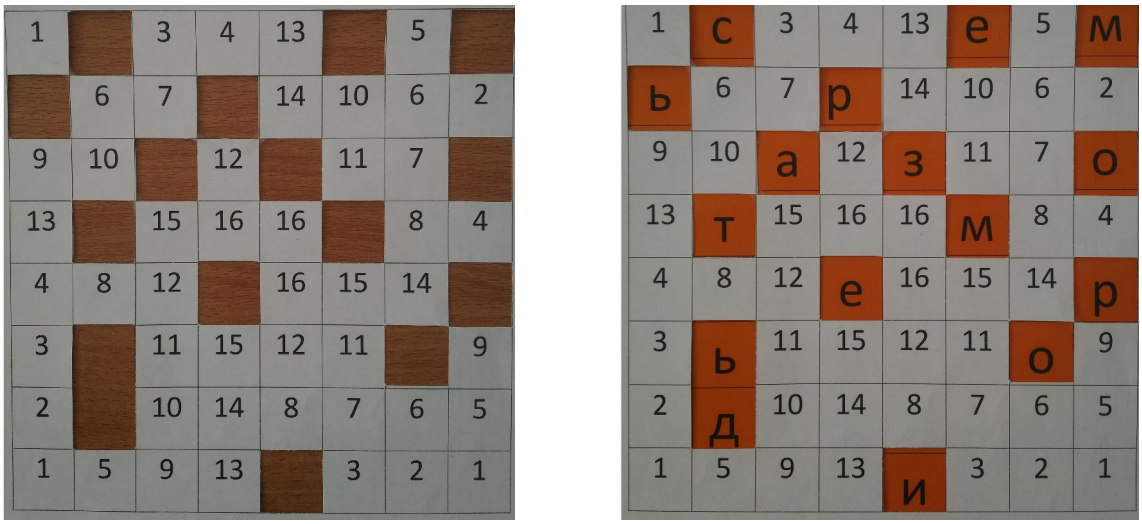

Рисунок 5 – Решетка Кардано

Затем поворачивали лист на 90 градусов и продолжали писать текст, затем снова поворачивали и так до тех пор, пока весь квадрат под решеткой не будет заполнен текстом. Вот что в итоге у нас получилось (рис.6).

Рисунок 6 – Шифрограмма для решетки Кардано

Мы решили попробовать разработать несколько собственных шифров.

Шифр № 1 «Замена»: Записываем 32 буквы русского алфавита (без буквы ё) по 8 букв в ряду. Таким образом, получается 4 ряда. Шифрование происходит путем замены каждой буквы исходного текста другой буквой, находящейся под ней в следующем ряду. Буквы 4 ряда заменяются буквами первого ряда (рис.7).

Рисунок 7 – Пример шифра «Замена»

ПРИМЕР

Слово: шифрование

Шифрограмма: аръщцкихрн

Шифр № 2 «Перестановка». В исходной фразе буквы попарно меняются местами. Если в слове нечетное количество букв, то последняя буква слова остается без изменения.

ПРИМЕР

Слово:

Шифрограмма

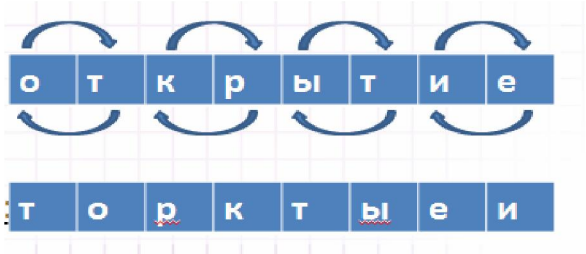

Рисунок 8 – Пример шифра «Перестановка»

Шифр № 3 «С переменным ключом». Из исходной фразы выписываются буквы, номера которых кратны числу, являющемуся ключом.

ПРИМЕР

Шифрограмма:
АБцММСкаФКЧмЪЕЭаДфГ_ТщЧмрФлыхнУлКФЭаПфС_ЮЙчрТрэаЯчфмБИЙуЯБе

ключ: 4

Дешифровка: Мама мыла раму

Однако процесс шифрования и дешифрования оказался очень трудоемким, и мы подумали о том, чтобы этот процесс как-то автоматизировать.

Для разработки программ шифрования и дешифрования мы изучили тему «Работа со строковым типом данных», а также основные возможности среды визуального программирования Delphi.

Для алгоритмизации первого шифра понадобились знания о сопоставлении символов их номерам в кодовой таблице и наоборот.

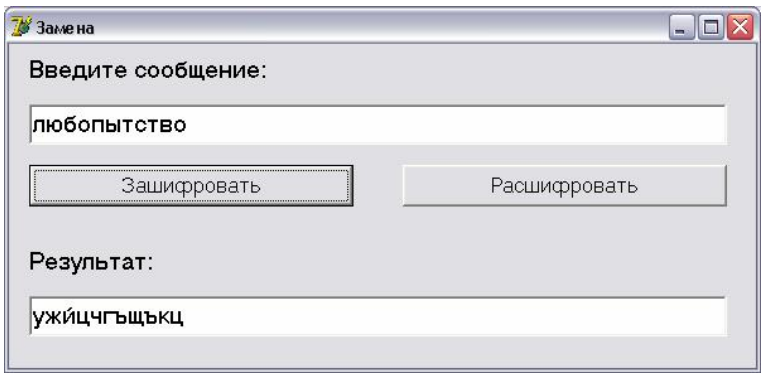

Рисунок 9 – Окно программы «Замена»

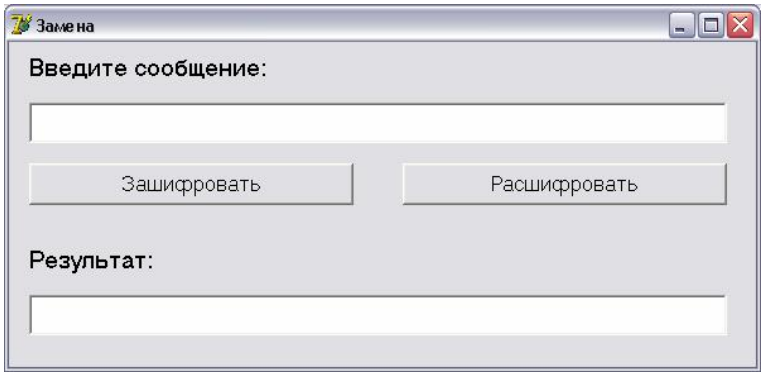

Рисунок 10 – Окно программы «Замена» с результатом работы

Для разработки алгоритма второго шифра мы работали со строками как с массивами данных. Кстати, во втором шифре процессы шифрования и дешифрования идентичны друг другу.

Рисунок 11 – Окно программы «Перестановка»

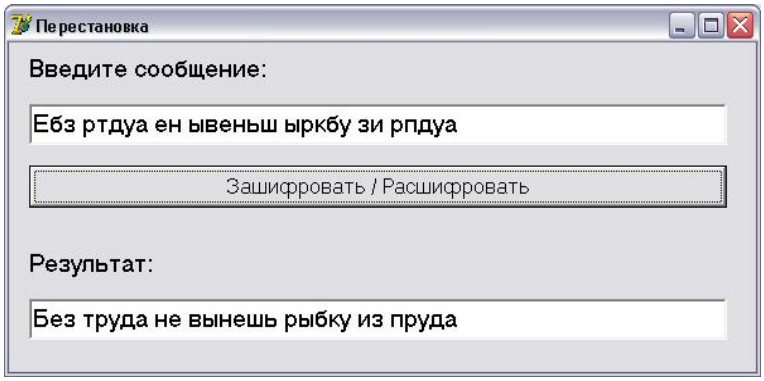

Рисунок 12 – Окно программы «Перестановка» с результатом работы

А при алгоритмизации третьего шифра снова понадобилась работа с массивом символьных переменных с использованием числовой переменной, выполняющей роль ключа.

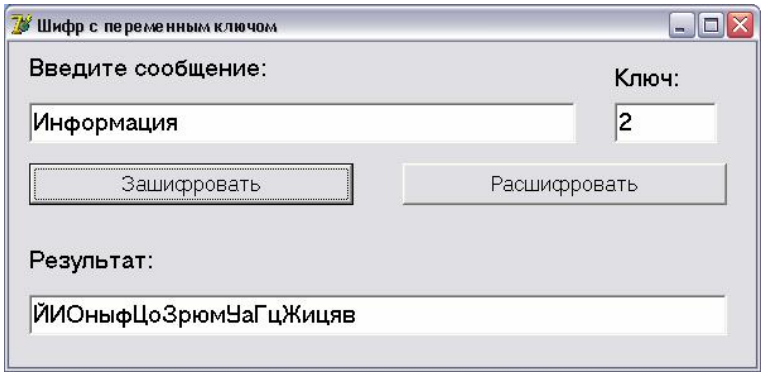

Рисунок 13 – Результат работы программы

Работая над исследованием, мы познакомились с историей криптографии и заметили, что данный вопрос будоражит умы людей уже много столетий. Мы изучили шифры Цезаря, Виженера, Кардано и др.; познакомились с древними устройствами шифрования – скитала, диск Альберти, линейка Сен-Сира. Нам удалось найти примеры использования криптографии в произведениях таких авторов как Эдгар Аллан По, Артур Конан Дойл, Жюль Верн и Кит Уильямс и разработать несколько собственных способов шифрования. Придуманные шифры мы реализовали в виде компьютерных программ.

А еще, мы убедились в том, что криптография лично для нас очень полезная наука, так как требует большой мыслительной активности и способствует развитию творческих и логических способностей. А также служит постоянным источником самообразования.

Библиографический список

1. Бауэр Ф. Расшифрованные секреты. Методы и принципы криптологии. М.: Мир, 2007. 550 с.
2. Владимир Беглецов URL: http://vova-beg.ru/magazin/shifrator-kardano/ (дата обращения: 10.03.2016).
3. Vigenère Cipher - Decoder, encoder, decrypt, encrypt URL: http://www.dcode.fr/vigenere-cipher (дата обращения: 10.03.2016).
4. Сингх С. Книга шифров. Тайная история шифров и их расшифровки. М.: Аст, Астрель, 2006. 447 с.