DOI:10.26104/IVK.2019.45.557

ТЕХНИКА ИЛИМДЕРИ

ТЕХНИЧЕСКИЕ НАУКИ

TECHNICAL SCIENCES

Ачекеев К.С., Керимов У.Т., Салижанова А.Б., Салижанова У.Б.

ТЕКСТТИК МААЛЫМАТТЫ ШИФРЛӨӨ ҮЧҮН КОМПЬЮТЕРДИК ПРОГРАММА ТҮЗҮҮ

Ачекеев К.С., Керимов У.Т., Салижанова А.Б., Салижанова У.Б.

СОЗДАНИЕ КОМПЬЮТЕРНОЙ ПРОГРАММЫ ДЛЯ ШИФРОВАНИЯ ТЕКСТОВОЙ ИНФОРМАЦИИ

K. Achekeev, U. Kerimov, A. Salijanova, U. Salijanova

CREATING A COMPUTER PROGRAM FOR ENCRYPTING TEXT INFORMATION

УДК: 004.4

Бул макалада тексттик маалыматты шифрлөө үчүн компьютердик программаны иштеп чыгуунун натыйжалары берилген. Шифрлөөнүн жана чечмелөөнүн негизги түшүнүктөрү, ошондой эле тексттик маалыматты шифрлөө жана дешифрлөө ыкмалары көрсөтүлгөн. Delphi 10 тез өнүктүрүү чөйрөсүн изилдөөдө текстти шифрлөөнүн үч ыкмасы, атап айтканда, Цезарь шифри, Атбаш шифри жана жөнөкөй алмаштыруу шифри ишке ашырылат. Изилдөөнүн максаттары жана милдеттери иштелип чыккан. Тексттик шифрлөө алгоритмдери жана алардын колдонулушу Цезарь шифринин, Атбаш шифринин жана жөнөкөй алмаштыруу шифринин мисалында көрсөтүлгөн. Макала ошондой эле программалык продуктунун өзгөчөлүктөрүн жана көрсөтмөлөрүн сүрөттөйт. Компьютердик тиркемени тестирлөө учурунда максатка - үч шифрлөө ыкмасын ишке ашырган компьютердик программалык продуктуну түзүү - ишке ашкандыгы аныкталды.

Негизги сөздөр: *шифрлөө, дешифрлөө Цезарь шифры, Атбаш шифры, жөнөкөй алмашуу шифры, программалык продукт, Delphi.*

В этой статье представлены результаты разработки компьютерной программы для шифрования текстовой информации. Излагаются основные понятия о шифровании и дешифровании также о методах шифрования и дешифрования текстовой информации. В исследовании средой быстрой разработке приложений Delphi 10 реализуются три метода шифрования текста, а именно шифр Цезаря, шифр Атбаш и шифр простой замены. Были спроектированы целы и задачи исследования. Показаны алгоритмы работы шифрования текста и их применение на примере шифра Цезаря, шифра Атбаш и шифра простой замены. В статье также описываются функции и руководство программным продуктом. В ходе тестирования компьютерного приложение было выявлено, что поставленная цель – создание компьютерного программного продукта, реализующего три метода шифрования было достигнуто.

Ключевые слова: *шифрование, дешифрование, шифр Цезаря, шифр Атбаш, шифр простой замены, программный продукт, Delphi.*

This article presents the results of developing a computer program for encrypting textual information. The basic concepts of encryption and decryption are outlined, as well as the methods of encryption and decryption of textual information. In the Delphi 10 rapid development environment study, three text encryption methods are implemented, namely the Caesar cipher, the Atbash cipher, and the simple substitution cipher. The goals and objectives of the study were designed. The text encryption algorithms and their application are shown on the example of the Caesar cipher, the Atbash cipher and the simple substitution cipher. The article also describes the features and guidance of the software product. During testing of a computer application, it was revealed that the goal - the creation of a computer software product that implements three encryption methods was achieved.

Key words: *encryption, decryption Caesar cipher, Atbash cipher, simple replacement cipher, software product, Delphi.*

Шифрование информации (зашифрование) - процесс применения шифра к защищаемой информации, т.е. преобразование защищаемой информации (открытого текста) в шифрованное сообщение (шифртекст, криптограмму) с помощью определенных правил, содержащихся в шифре [1]. На сегодняшний день существуют множество разнообразных способов шифрования/дешифрования, но секретность данных основана не на тайном алгоритме, а на том, что ключ шифрования (пароль) известен только доверенным лицам.

Шифрование появилось примерно четыре тысячи лет тому назад. Первым известным применением шифра (кода) считается египетский текст, датированный примерно 1900 г. до н.э., автор которого использовал вместо обычных (для египтян) иероглифов не совпадающие с ними знаки [2].

Целью данного исследования является разработка компьютерного программного продукта, который бы позволял обычным пользователям компьютера зашифровывать и дешифровать необходимый им текст.

Реализация поставленной задачи проводилось в среде быстрой разработке приложений Delphi 10, располагающей широкими возможностями по созданию компьютерных программ.

Для выполнения этой цели были поставлены нижеследующие задачи:

DOI:10.26104/IVK.2019.45.557

- изучить теоретические сведения, необходимые для решения данной задачи;
- с проектировать пользовательский интерфейс;
- разработать компьютерное приложение реализующий три шифра (шифр Цезаря, шифр Атбаш и шифр простой замены).

Шифр Цезаря является историческим примером шифра замены (I век до н.э.), описанным историком Древнего Рима Светонием. Гай Юлий Цезарь использовал в своей переписке шифр собственного изобретения. При этом выписывался алфавит, затем под ним выписывался тот же алфавит, но с циклическим сдвигом на 3 буквы влево.

Шифр Атбаш, использованный для еврейского алфавита и получивший оттуда свое название. Шифрование происходит заменой первой буквы алфавита на последнюю, второй на предпоследнюю и т.д.

При разработке программного продукта требовалось решить следующие задачи:

1. Проектирование интерфейса компьютерной программы.
2. Проектирование процедур, реализующие три метода шифрования.
3. Вывод результата на экран.
4. Остановка и выход из программы.

Руководство для пользователя. При запуске компьютерной программы на экране появляется главная форма, состоящее из предложения выбора шифра и выхода из программы.

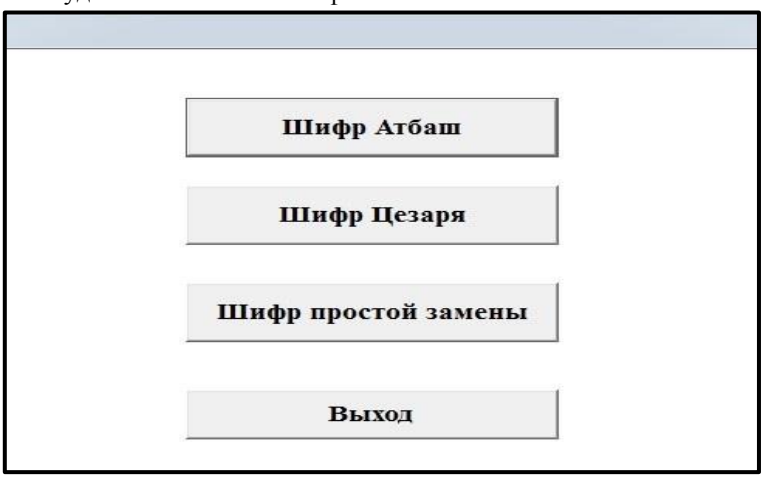

Рис. 1. Запуск программы.

После выбора шифра откроется новое окно программы выбранного алгоритма шифрования.

При выборе из меню шифр «Атбаш» в поле «Ввод текста» вводим текст для шифрования, затем нажимаем на кнопку зашифровать. Результат шифрования выводиться в поле «Вывод»

В программе первая буква алфавита заменяется на последнюю, вторая – на предпоследнюю и т.д.

Пример: Анарбеков = Ятяпюъхсэ (рис. 2).

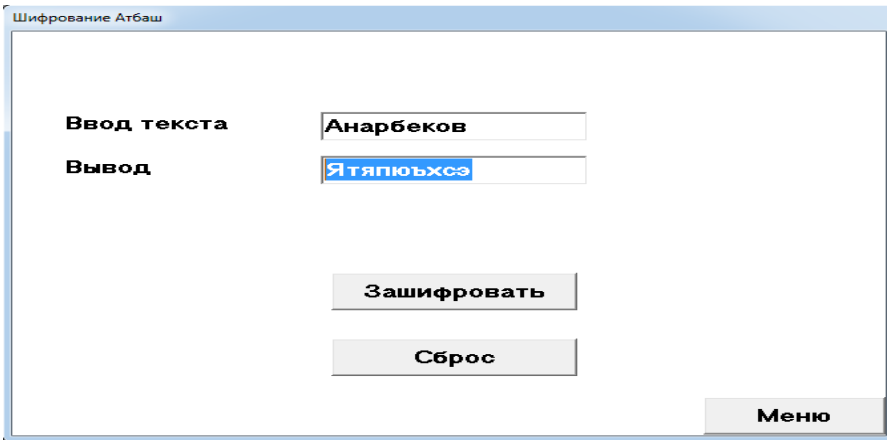

Рис. 2. Шифр Атбаш.

DOI:10.26104/IVK.2019.45.557

В шифр Цезаря является шифром перестановки. Как известно, для того чтобы зашифровать сообщение, каждую его букву заменяли на другую букву алфавита, но со сдвигом влево или вправо. Цезарь в своих посланиях к сенату заменял все буквы на три отстоящие слева, Август применял тот же шифр, но со сдвигом в четыре знака. В программе можно зашифровать и дешифровать текст используя кнопки «Зашифровать» и «Дешифровать».

На рисунке 3 приведен пример шифрование и дешифрование текстовой информации на примере шифра Цезаря.

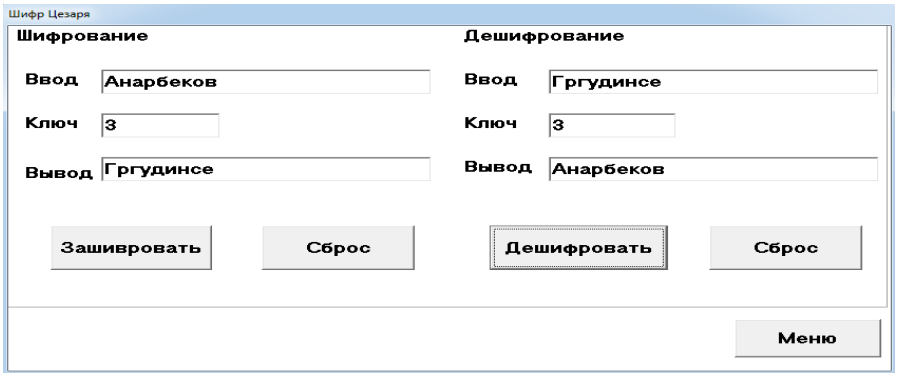

Рис. 3. Шифр Цезаря.

Теперь перейдем к шифру «Простой замены». Она шифрует фразу с помощью шифра простой замены. В программе каждая буква шифруется своим порядковым номером из таблицы кодов. Например: Буква «А» это цифра 192, а буква «Б» - 193 и т.д. На рисунке 4 приведен пример шифрование и дешифрование текстовой информации на примере шифра «Простой замены».

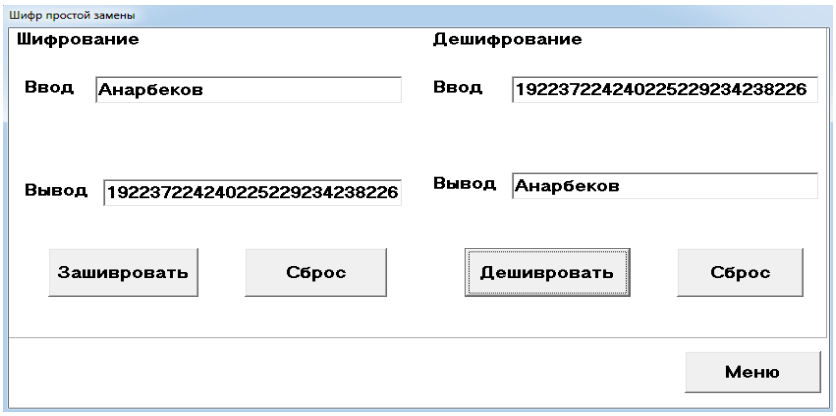

Рис. 4. Шифр Простой замены

Выводы. Таким образом, в ходе тестирования компьютерного приложение было выявлено, что поставленная цель - создание компьютерного программного продукта, реализующего три метода шифрования было достигнуто.

Литература:

1. Жданов О. Н., Золотарев, В. В. Методы и средства криптографической защиты информации: Учебное пособие / О.Н. Жданов, В.В. Золотарев; СибГАУ. – Красноярск, 2007. – 217 с.
2. Жереп Н. С. Методы шифрования информации / Н. С. Жереп, М. В. Двадненко // Студенческий научный форум - 2016: VIII Международная студенческая электронная научная конференция, электронное издание, Саратов, 15 февраля – 31 2016 года. – Саратов: ООО «Научно-издательский центр «Академия Естествознания», 2016.
3. Панасенко С. Алгоритмы шифрования. Специальный справочник. - СПб: БХВ-Петербург, 2009 г., 576 с.
4. Баричев С.Г., Серов Р.Е. Основы современной криптографии. - Горячая Линия - Телеком, 2002 - 153 с.
5. Герасименко В.А. Защита информации в автоматизированных системах обработки данных кн. 1. - М., 2004. – 400 с.
6. Смайылбек К.Ч., Ачекеев К.С. Основные возможности информационной технологии в бизнесе и роль менеджеров в принятии управленческих решений. / Известия ВУЗов Кыргызстана. 2017. №. 5-1. С. 42-44.
7. Бийбосунов Б.И., Байжариков М.А., Ачекеев К.С. разработка сайта и электронных пособий по информатике. / Известия ВУЗов Кыргызстана. 2016. №. 5. С. 94-96.