Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное

учреждение высшего образования

«СибирскИЙ государственнЫЙ Университет

геоСИСТЕМ И ТЕХНОЛОГИЙ»

(СГУГИТ)

ОТЧЕТ

ЛАБОРАТОРНАЯ РАБОТА 1. Разработка технического задания.

Выполнила обучающаяся

группы БИ – 33.1

Тимошенко Д.С.

Проверил

ст. преподаватель кафедры ПИиИС

Шарапов А. А.

Новосибирск – 2022

Цель работы: научиться составлять техническое задание для разработки программного обеспечения.

Выполнение работы:

1. Введение

1.1 Наименование программы

Наименование программы – «Тренажер «Криптограф»».

Краткая характеристика области применения. В школах в рамках предмета Информатика изучается обширный раздел «Криптография». Программа предназначена для исследования и изучения работы нескольких методов шифрования.

2. Основания для разработки

Основанием для разработки является Договор 1 от 03.09.2022. Договор утвержден Директором ООО «SChool» Щевцовым Николаем Сергеевичем, именуемым в дальнейшем Заказчиком, и Тимошенко Дарьи Сергеевны, именуемым в дальнейшем исполнителем, 03.09.2022.

Согласно Договору, Исполнитель обязан разработать приложение «Тренажер» не позднее 20.12.2022, предоставить исходные коды и документацию к разработанной системе не позднее 25.10.2022.

3. Назначение разработки

Программа дает возможность зашифровать слово или фразу, а после попытаться расшифровать получившийся текст.

Программа будет использоваться учениками на уроках или дома для изучения методов шифрования.

4. Требования к программе или к программному изделию

4.1 Требования к функциональным характеристикам

Программа должна читать таблицу Виженера из базы данных.

В программе должно рассматриваться три шифра: шифр Цезаря, шифр Виженера и шифр вертикальной перестановки. Каждым шифром используется три формы: для шифрования; для дешифровки; справка.

Шифрование методом Цезаря должно работать следующим образом:

1. Каждый символ в тексте заменяется символом, находящимся на некотором постоянном числе позиций правее него в алфавите.

Шифрование методом Виженера должно работать следующим образом:

1. Ключевое слово записывается циклически до тех пор, пока его длина не будет соответствовать длине исходного текста;

2. Первый символ исходного текста зашифрован первым символом ключа. Первый символ зашифрованного текста находится на пересечении столбца первого символа ключ и строки первого символа исходного текста в таблице Виженера. Точно так же для второго символа исходного текста используется второй символ ключа. Остальная часть исходного текста шифруется подобным способом.

Шифрование вертикальной перестановкой должно работать следующим образом:

1. Выбирается количество столбцов для таблицы (от 5 до 20);

2. Каждый символ шифруемого текста записывается в ячейку таблицы (запятая заменяется на последовательность букв ЗПТ, а точка - ТЧК;

3. Полученный текст выписывается колонками в порядке, который выбирает пользователь.

Для шифра Цезаря на первой форме должно иметься:

* поле для заполнения числа, для смещения алфавита (натуральное число от 1 до 33 включительно);
* кнопка для шифровки сообщения;
* поле для ввода сообщения для шифрования (сообщение на русском языке, может содержать следующие знаки: «-», «,», «.», «!», «?» и пробел);
* кнопки для перехода на другие шифры, главное меню, справку и кнопка для сброса введенных данных.

На второй форме должно иметься:

* поле с зашифрованными данными;
* поле для ввода расшифрованного сообщения (необходима проверка соответствия количества символом зашифрованного текста и расшифрованного сообщения);
* кнопка, вызывающая справку;
* поле с числом смещения, которое нельзя изменить;
* таймер, которое показывает время, затраченное на расшифровку;
* кнопка, открывающая изображение алфавита;
* кнопка, открывающая подсказку через 1 минуту расшифровки (подсказка должна содержать в себе таблицу с буквами изначального и зашифрованного алфавита);
* кнопка, показывающая зашифрованный текст, открывающаяся через 3 минуты с начала расшифровки;
* кнопка для проверки правильности расшифрованного сообщения (при правильной расшифровке поле меняет цвет на зеленый, при неправильном меняет цвет на красный, показывает сообщение с количеством совершенных ошибок).

На форме «Справка» должна находится справка о шифре Цезаря, о шифровании и дешифровании этого шифра.

Для шифра Виженера на первой форме должно иметься:

* поле для заполнения слова-ключа (одно слово);
* поле для ввода сообщения для шифрования (сообщение на русском языке, может содержать следующие знаки: «-», «,», «.», «!», «?» и пробел);
* кнопки для перехода на другие шифры, главное меню, справку и кнопка для сброса введенных данных;
* кнопка для шифровки сообщения.

На второй форме должно иметься:

* поле с зашифрованными данными;
* поле для ввода расшифрованного сообщения (необходима проверка соответствия количества символом зашифрованного текста и расшифрованного сообщения);
* поле со словом-ключом, которое нельзя изменить;
* таймер, которое показывает время, затраченное на расшифровку;
* кнопка, открывающая таблицу Виженера;
* таблица с данными шифрования (зашифрованный текст и соответствующая буква слова-ключа);
* кнопка, вызывающая справку;
* кнопка для проверки правильности расшифрованного сообщения (при правильной расшифровке поле меняет цвет на зеленый, при неправильном меняет цвет на красный, показывает сообщение с количеством совершенных ошибок).

На форме «Справка» должна находится справка о шифре Виженера, о шифровании и дешифровании этого шифра.

Для шифра вертикальной перестановкой на первой форме должно иметься:

* поле для заполнения количества столбцов таблицы;
* поле для распределения столбцов в желаемом порядке;
* поле для ввода сообщения для шифрования (сообщение на русском языке, может содержать следующие знаки: «,», «.» и пробел. Знаки препинания заменяются: «,» - на ЗПТ, «.» - на ТЧК);
* кнопки для перехода на другие шифры, главное меню, справку и кнопка для сброса введенных данных;
* кнопка для шифровки сообщения.

На второй форме должно иметься:

* таблица с зашифрованными данными;
* поле для ввода расшифрованного сообщения (необходима проверка соответствия количества символом зашифрованного текста и расшифрованного сообщения);
* таймер, которое показывает время, затраченное на расшифровку;
* кнопка, показывающая таблицу с исходным сообщением, открывающаяся через 3 минуты с начала расшифровки;
* кнопка, вызывающая справку;
* кнопка для проверки правильности расшифрованного сообщения (при правильной расшифровке поле меняет цвет на зеленый, при неправильном меняет цвет на красный, показывает сообщение с количеством совершенных ошибок).

На форме «Справка» должна находится справка о шифре вертикальной перестановки, о шифровании и дешифровании этого шифра.

4.2 Требования к надежности

Программа должна:

- проверять входящие данные на корректность;

- функционировать без ошибок, связанных с некорректно введенными данными;

Время восстановления после отказа, вызванного сбоем электропитания технических средств (иными внешними факторами) не должно превышать 10 минут при условии соблюдения условий эксплуатации технических и программных средств.

Время восстановления после отказа, вызванного неисправностью технических средств, сбоем операционной системы, не должно превышать времени, требуемого на устранение неисправностей технических средств и переустановки программных средств.

4.3 Условия эксплуатации

Программа запускается на компьютере в класса или домашнем ПК.

4.3.1 Климатические условия эксплуатации

Специальные условия не требуются.

4.3.2 Требования к видам обслуживания

Программа не требует проведения каких-либо видов обслуживания.

4.3.3 Требования к численности и квалификации персонала

Программа не требует наличие персонала

4.4 Требования к составу и параметрам технических средств

Состав технических средств:

Компьютер, включающий в себя:

* процессор x86 с тактовой частотой, не менее 2 ГГц;
* оперативную память объемом, не менее 4 Гб;
* видеокарту, монитор, мышь, клавиатура.

4.5 Требования к информационной и программной совместимости

Специальных требований не предъявляется.

4.6 Требование к маркировке и упаковке

Специальных требований не предъявляется.

4.7 Требования к транспортированию и хранению

Специальных требований не предъявляется.

5. Требования к программной документации

Предварительный состав программной документации:

* техническое задание (включает описание применения);
* программа и методика испытаний

6. Технико-экономические показатели

Программа «Тренажер» предназначена для изучения школьниками, но может использоваться и другими пользователями. Будет применима малым кругом лиц.

7. Стадии и этапы разработки

Разработка была проведена в два этапа:

1. техническое задание;
2. технический (и рабочий) проекты;

На этапе «Техническое задание» должен быть выполнен этап разработки, согласования и утверждения настоящего технического задания.

На этапе «Технический (и рабочий) проект» должны быть выполнены перечисленные ниже этапы работ:

* разработка программы;
* разработка программной документации;

Содержание работ по этапам:

На этапе разработки технического задания должны быть выполнены перечисленные ниже работы:

* постановка задачи;
* определение и уточнение требований к техническим средствам;
* определение требований к программе;
* определение стадий, этапов и сроков разработки программы и документации на нее;
* согласование и утверждение технического задания.

На этапе разработки программы должна быть выполнена работа по программированию (кодированию) и отладке программы.

8. Порядок контроля и приемки

Приемосдаточные испытания программы должны проводиться согласно разработанной исполнителем и согласованной заказчиком «Программы и методики испытаний».