**МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ
ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ГОРОДСКОГО ОКРУГА БАЛАШИХА
«ГИМНАЗИЯ №2»**

ПРОЕКТ

на тему «Шифрование и ключи шифрования»

Слободянюк Игоря Сергеевича,
ученика 9 «Г» класса
Руководитель проекта:
Гезик Д. В.
учитель ИКТ и Информатики

2019 г

ЛИСТ №1

Матрица проекта

1. **Проблема:**

Она заключается в том, что многие не шифруют свои личные данные и их легче украсть.

2. **Цель проекта:**

Научиться шифровать свои сообщения, личные данные и важные материалы по работе.

3. **Задачи проекта:**

   1) **Цели шифрования.**

   2) **Узнать, что такое ключи шифрования.**

   3) **Управление ключами.**

   4) **Древние методы шифрования.**

   5) **Современные методы шифрования.**

   6) **Криптостойкость шифра.**

   7) **Получить рецензию учителя информатики.**

4. **Ход работы:**

Данная тема была очень актуальна в то время, когда компьютерных даже не было. Но и в наше время она имеет огромный спрос. Многие сайты и другие сторонние ресурсы используют шифрование для того, чтобы не потерять свои важные данные и сохранить личную информацию пользователей этого ресурса. Я решил разобраться в данной теме и узнать, какие методы шифрования были раньше и есть сейчас (см. Приложение 5)**, узнать зачем оно нужно и какие методы шифрования больше защищены от взлома или от расшифровки важной информации. Также я хотел узнать для чего нужны ключи и как их применяют в шифровании и расшифровке информации в разных методах шифрования. Используя свои знания, я создал программу, которая основана на шифре Цезаря** (см. Приложение 5).

ВЫВОД

Шифрование данных и другой очень важной информации это была, есть и будет очень актуальная тема для всех людей. С каждым днём люди продвигаются к разработке новых шифров, но и к расшифровке тоже. Для шифра и той информации что скрывается под ним очень важна криптостойкость этого шифра и невозможность понять, что там скрыто. Даже в древней эпохе, во времена царей и королей шифры уже пользовались спросом и их очень часто использовали. Люди придумывали различные хорошие и не очень способы скрывать информацию от своих врагов.

Список литературы

1) https://ru.wikipedia.org/wiki/Ключ_(криптография)

2) https://ru.wikipedia.org/wiki/Шифрование#Криптостойкость_шифра

3) https://ru.wikipedia.org/wiki/Управление_ключами

4) https://studwood.ru/1651802/informatika/tseli_shifrovaniya

5) http://info-tehnologii.ru/INF_BEZ/shifr/Cel_shifr/index.html

6) https://pikabu.ru/story/starinnyie_metodyi_shifrovaniya_6108284

7) https://studbooks.net/2034105/informatika/sovremennaya_kriptografiya

8) https://ru.wikipedia.org/wiki/RSA

10) https://ru.wikipedia.org/wiki/MD5

ПРИЛОЖЕНИЕ 5

ЛИСТ№ 4

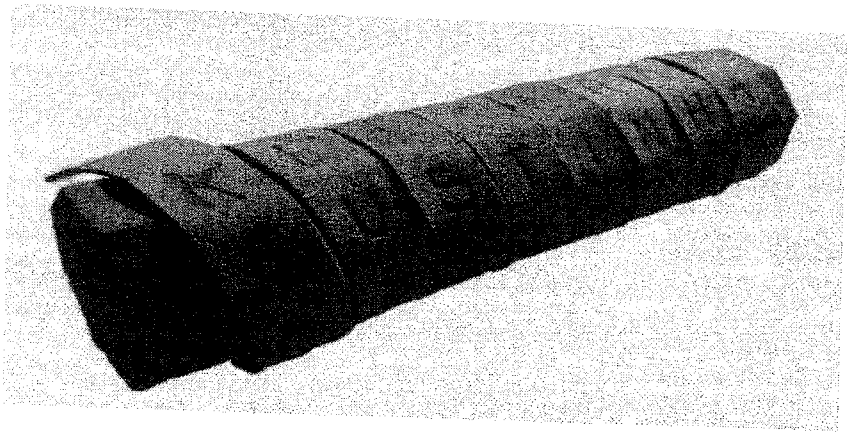
1) Атабаш:

Исходный текст	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Зашифрованный текст	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

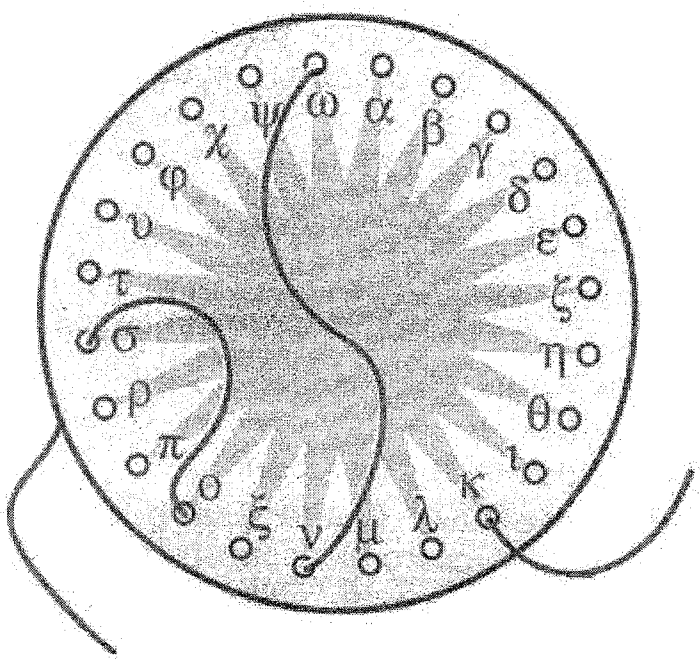
Исходный текст	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Зашифрованный текст	Я	Ю	Э	Ь	Ы	Ъ	Щ	Ш	Ч	Ц	Х	Ф	У	Т	С	Р	П	О	Н	М	Л	К	Й	И	З	Ж	Е	Ё	Д	Г	В	Б	А

Исходный текст	א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת
Зашифрованный текст	ת	ש	ר	ק	צ	פ	ע	ס	נ	מ	ל	כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א

2) Скитала



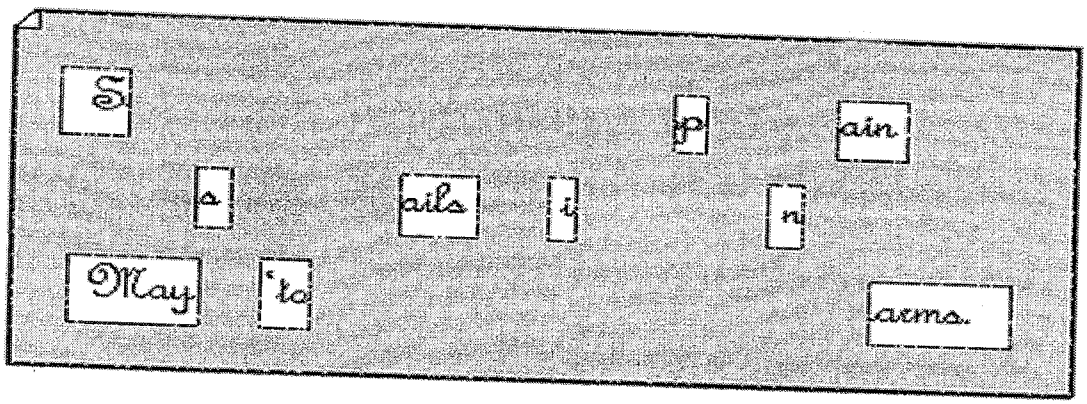
3) Диск Энея



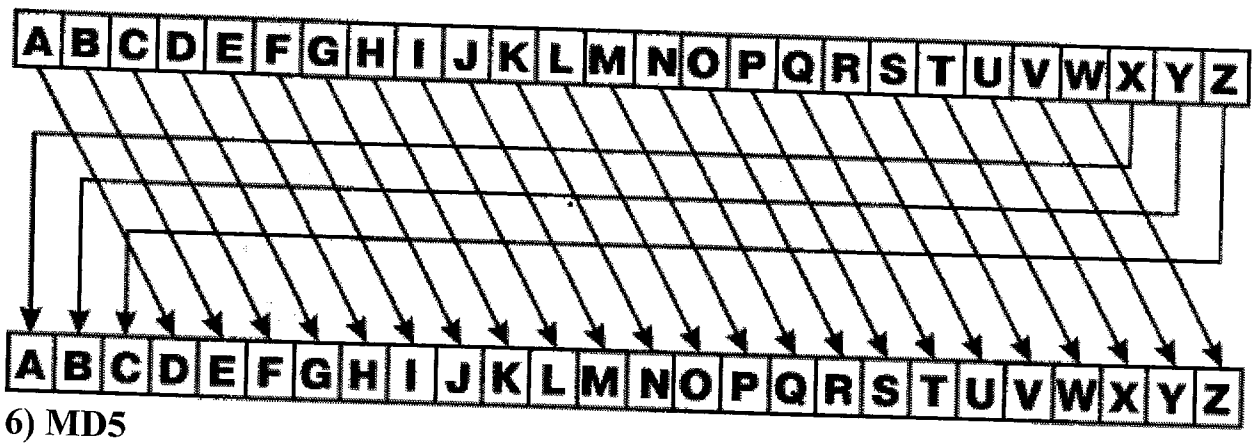
ЛИСТ№ 5

4) Решетка Кардано

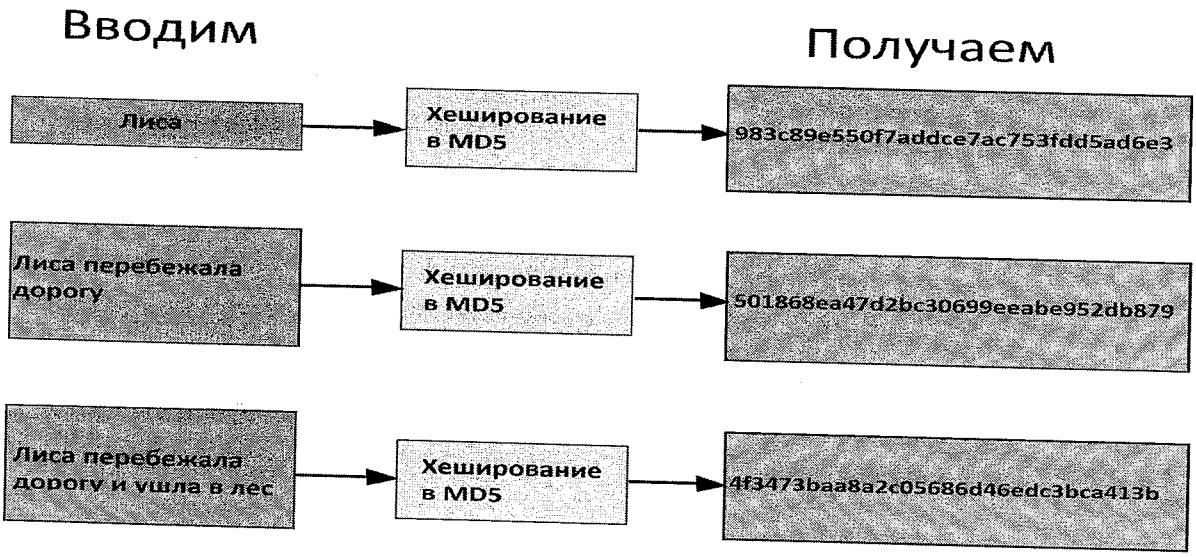
Sir John regards you well and spekes again that
all as rightly 'vails him is yours now and ever.
May he 'tone for past d'lays with many charms.



5) Шифр Цезаря

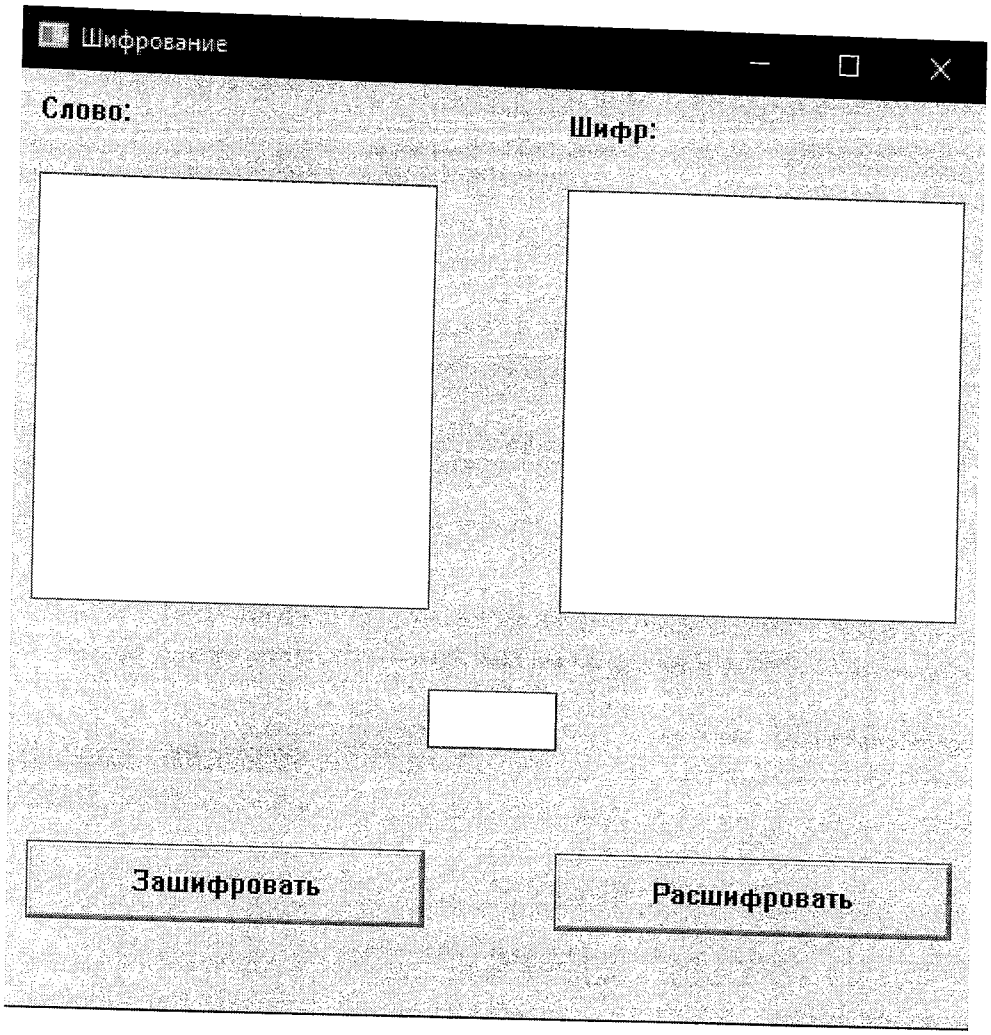


6) MD5



ЛИСТ№ 6

7) Моя программа



РЕЦЕНЗИЯ
на индивидуальный итоговый проект

тема проекта «Шифрование и ключи шифрования»
выпускника 9 г класса МБОУ «Гимназия №2»
Слободянюк Игоря Сергеевича

Данная работа соответствует требованиям ФГОС, предъявляемым к содержанию, оформлению индивидуального итогового проекта.

Тема работы сформулирована грамотно с литературной точки зрения и отражает содержание проекта.

Структура проекта содержит в себе: титульный лист, оглавление, введение, основную часть, заключение, список литературы, приложение (программа). Введение включает в себя ряд следующих положений: актуальность шифрования, применение и значимость шифрования в современном мире.

Проект начинается с обоснования актуальности выбранной темы. Научно-теоретическое и практическое значение темы определяется значимостью процесса шифрования в защите персональных данных в современном цифровом пространстве, способах защиты информации с помощью алгоритмов шифрования, ключей.

Цель сформулирована четко и достигнута в результате выполнения проекта.

Формулируются конкретные задачи, которые необходимо решить.

Выбор средств и методов, адекватных поставленным целям:

- изучены источники с информацией о шифровании, ключах шифрования;

- рассмотрены темы из курса программирования, связанные с шифрованием;

- разработана и реализована с помощью языка программирования программа, работающая по одному из описанных алгоритмов.

Спланирована и определена последовательность работы над проектом.

Основная часть проекта состоит из 4 разделов: цели и ключи шифрования, древние и современные методы шифрования, криптостойкость шрифта, написание программы на языке программирования, реализующей алгоритм шифрования и расшифровки введенного сообщения.

Содержит теоретический материал, содержит практический материал (скомпилированный программный модуль для шифрования и расшифровки сообщения).

Излагая конкретные данные, учащийся приводит доказательства и показывает, как они были получены, проверены, чтобы изложение было достоверным.

Мысли излагаются логично, правильно сформулированы и отражают то, что было открыто и использовано автором исследования.

Перечень использованной литературы оформлен в соответствии с требованиями.

В работе прослеживается научность и литературность языка. Письменная речь орфографически грамотная, пунктуация соответствует правилам, словарный и грамматический строй речи разнообразен, речь выразительна.

Работа аккуратно выполнена, содержит наглядный материал, представлен в виде программы, реализованной посредством языка программирования, и реализует алгоритм шифрования с последующей расшифровкой.

Работа проверена на плагиат (https://text.ru/antiplagiat). Уникальность текста составляет 50,48%.

Руководитель проекта Гезик Д. В.

«22» февраля 2019г.