Муниципальное бюджетное общеобразовательное учреждение средняя общеобразовательная школа №28 города Пенза имени Василия Осиповича Ключевского

Исследовательская работа
На тему:

“Криптография как метод кодирования и декодирования информации”

Выполнил:
Кудрявцев Даниил Павлович,
ученик 11 «А» класса
МБОУ СОШ №28 г.Пенза им. В.О.Ключевского
Руководитель:
Смирнова А.Д.,
учитель информатики
МБОУ СОШ №28 г.Пенза имени В.О.Ключевского

Пенза, 2022

Оглавление

Введение

Актуальность: Криптография – наука о методах обеспечения конфиденциальности и аутентичности информации. Криптография включает в себя методы шифрования информации, ассиметричные криптосистемы, системы электронной цифровой подписи, хеш-функции, управление ключами, получение скрытой информации, а также квантовую криптографию.

В современном мире криптография используется во многих отраслях. Примерами могут являться телекоммуникация, электронный документооборот, шифрование сообщений в мессенджерах и др. На широкое распространение криптографии повлияли быстрое развитие технологий и заинтересованность людей в сохранении личной информации. Ежедневно в мире происходит обмен миллионами сообщений, документов, фото и видеофайлами, которые нуждаются в защите от посторонних лиц, злоумышленников.

Этот проект был создан для того, чтобы расширить свои познания в области кодировки и различных шифров. Также, на данный момент, знания о шифрах могут помочь людям, работающим или же заинтересованным в сфере технологий и IT.

Цель исследования: изучить и научиться пользоваться наиболее популярными видами шифрования в криптографии; создание оконного приложения на языке Python.

Объект исследования: криптография

Предмет исследования: методы кодирования и декодирования в криптографии

Гипотеза исследования: криптография как наука нужна, используется в настоящее время и будет нужна в будущем.

Задачи исследования:

Найти и изучить информацию о криптографии.

Изучить виды шифрования

Изучить методы шифрования

Найти информацию о наиболее популярных методах шифрования

Применить полученные знания и закодировать, а после декодировать своё “сообщение”

Методы исследования:

Теоретические – анализ, классификация, формализация, моделирование, обобщение, умозаключение.

Эмпирические – наблюдение, описание, сравнение.

Основная часть

Базовая терминология: Основные алгоритмы шифрования

В криптографической терминологии исходное послание именуют открытым текстом. Шифрование — это процесс изменения данных таким образом, чтобы они стали неузнаваемыми и бесполезными для несанкционированного лица. А дешифрование — процесс превращения данных в их первоначальный вид. Наиболее безопасные виды шифрования используют математические алгоритмы и переменную — «ключ». Выбранный ключ (зачастую любая случайная последовательность) вводится при шифровании и является неотъемлемой частью изменения данных. Тот же самый ключ необходим для дешифровки сообщения.

Наиболее популярным является симметричное шифрование – ключ шифровки есть только у отправителя и получателя, другим лицам он недоступен. Симметричные алгоритмы подразделяют на потоковые шифры и блочные шифры. Потоковые позволяют шифровать информацию побитово, а блочные работают с некоторым набором бит данных (обычно размер блока составляет 64 бита) и шифруют этот набор как единое целое.

Ассиметричные шифры допускают, чтобы открытый ключ находился во всеобщем доступе. Это позволяет любому зашифровать сообщение. Однако расшифровать его сможет только нужный человек - тот, кто владеет ключом дешифровки. Ключ для шифрования называют открытым ключом, а ключ для дешифрования - закрытым ключом или секретным ключом.

Виды современных алгоритмов

К современным алгоритмам шифрования относят DES-шифр, Triple Des-шифр, AES-шифр.

DES-шифр – это шифр-алгоритм, с помощью серии сложных операций преобразует строку битов открытого текста фиксированной длины в другую строку битов зашифрованного текста той же длины. Длина блока составляет 56 бит. Но так как DES был специально разработан для аппаратного обеспечения, то не было предусмотрено, чтобы он эффективно работал в ПО.

Triple DES (3DES) модификация DES, позволяющая увеличить длину ключа до 112 бит. Получившийся шифр намного медленнее других шифров, но время для криптоанализа 3DES во много раз больше, чем время, нужное для вскрытия DES.

В свою очередь AES (Advanced Encryption Standard или Rijndael) поддерживает три длины ключа 128, 192 и 256 бит и использует 128-битный размер блоков. В настоящее время он считается достаточно стойким и используется по всему миру. Архитектура AES основана на принципе, известном как замена и перестановка, и быстро работает как в программном, так и на аппаратном уровнях. В отличие от своего предшественника — DES, AES не использует сеть Фейстеля (один из методов построения блочных шифров).

Роль криптографии в современном мире

Основные причины, по которым криптография так востребована:

Конфиденциальность — когда нужно передать данные так, чтобы человек, перехвативший зашифрованное сообщение, не смог узнать его содержание. То же самое относится и к хранимым данным, которые должны быть защищены на случай несанкционированного доступа к ним.

Аутентификация — это свойство эквивалентно подписи. Получатель сообщения хочет быть уверен, что оно пришло от определённой стороны, а не от кого-либо ещё (даже если позже эта сторона захочет это опровергнуть).

Целостность — получатель сообщения хочет доказательства того, что оно не было изменено третьей стороной.

Отказ от ответственности — предотвратить отказ автора за создание или отправку сообщения.

Современные алгоритмы шифровки/дешифровки достаточно сложны и их невозможно проводить вручную. Настоящие криптографические алгоритмы разработаны для использования компьютерами или специальными аппаратными устройствами. В большинстве приложений криптография производится программным обеспечением и имеется множество доступных криптографических пакетов.

Методы криптографической защиты информации

Наиболее популярными шифрования являются шифр транспонирования, азбука Морзе, шифр Цезаря, моноалфавитная замена, шифр Виженера и многие другие.

Рассмотрим подробнее шифр Виженера. Он состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Для зашифровывания может использоваться таблица алфавитов, называемая квадрат (таблица) Виженера. Применительно к латинскому алфавиту таблица Виженера составляется из строк по 26 символов, причём каждая следующая строка сдвигается на несколько позиций. Таким образом, в таблице получается 26 различных шифров Цезаря. На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова.

Чтобы расшифровать шифр Виженера, для начала угадывают длину кодового слова и применяют частотный анализ к каждой n-ной букве послания.

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

Рис.1. Квадрат (таблица) Виженера

Попробуем применить шифр Виженера вручную.

1. Для того, чтобы зашифровать сообщение «wikiHow is the best» нужно записать его без пробелов – WIKIHOWISTHEBEST.

2. Ключевым словом будет LIME.

3. Ключевое слово записывается под сообщением так, чтобы каждая буква стояла строго под соответствующей буквой сообщения. В нашем примере это выглядит так:

WIKIHOWISTHEBEST

LIMELIMELIMELIME

4. Следует укоротить ключевое слово, чтобы оно помещалось во фразу, если это необходимо. В данном примере, слово LIME подходит по количеству букв для ключевой фразы, поэтому сокращать его не нужно.

5. Надо перейти к ряду первой буквы в ключевом слове в квадрате Виженера и найти колонку с первой буквой изначального сообщения, а затем найти точку пересечения ряда и колонки. В данном примере это ряд, обозначенный L, и колонка, обозначенная W. Буква на их пересечении будет первой буквой вашего зашифрованного сообщения.

6. Пятый шаг повторяется для всех букв фразы по порядку, пока оно не будет зашифровано целиком. Первая буква, полученная в предыдущем шаге —буква H, вторая — Q и так далее. В итоге получилась фраза: HQWMSWIMDBTIMMEX

Теперь попробуем расшифровать сообщение.

1. Для расшифровки сообщения все действия выполняются в обратном порядке.

2. Находим ряд, обозначенный первой буквой ключевого слова. В нем ищем первую букву зашифрованной фразы. Смотрим в какой колонке она находится: буква, которой обозначена эта колонка, и будет первой буквой расшифрованного сообщения.

3. Продолжаем делать то же самое для всех букв фразы по порядку, пока не расшифровываем её целиком, и не получил изначальную фразу - WIKIHOWISTHEBEST.

Но кодирование и декодирование сообщения вручную занимает достаточно времени. И в наше время этот процесс можно ускорить благодаря программированию. Чтобы ускорить процесс была мной была реализована программа на языке программирования Python.

Реализация приложения кодирования и декодирования информации

```
from tkinter import *
from tkinter import messagebox

def shifr():
    mode = mode_tf.get()
    message = message_tf.get().replace(' ', '').upper()
    key = key_tf.get().upper()
    key *= len(message) // len(key) + 1
    final_message = ""
    for i, j in enumerate(message):
        if mode == '1':
            temp = ord(j) + ord(key[i])
        if mode == '2':
            temp = ord(j) - ord(key[i])
        final_message += chr(temp % 26 + ord('A'))
    if mode == '1':
        messagebox.showinfo('final_message-pythonguides',
f'Зашифрованное сообщение = {final_message}')
```

```
    elif mode == '2':
        messagebox.showinfo('final_message-pythonguides',
f'Расшифрованное сообщение = {final_message}')
    else:
        messagebox.showinfo('final_message-pythonguides', f'Не
понимаю вас!')


# создаем окно приложения. Добавляем название приложения
window = Tk()
window.title('Кодирование и декодирование сообщений')
window.geometry('400x300')

frame = Frame(
    window,
    padx=10, # отступ по горизонтали
    pady=10 # отступ по вертикали
)
frame.pack(expand=True)

mode_lb = Label(
    frame,
    text="1 - зашифровать \n2 - расшифровать  "
)
mode_lb.grid(row=3, column=1)

message_lb = Label(
    frame,
    text="Введите свой текст  "
)
message_lb.grid(row=4, column=1)

key_lb = Label(
    frame,
    text="Введите ключ шифрования  ",
)
key_lb.grid(row=5, column=1)

mode_tf = Entry(
    frame,
)
mode_tf.grid(row=3, column=2, pady=5)

message_tf = Entry(
    frame,
```

```
)
message_tf.grid(row=4, column=2, pady=5)

key_tf = Entry(
    frame,
)
key_tf.grid(row=5, column=2, pady=5)

cal_btn = Button(
    frame,
    text='Обработать сообщение',
    command=shifr
)
cal_btn.grid(row=6, column=2)

window.mainloop()
```

Пользователь имеет возможность, осуществить ввод сообщения, которое он хочет зашифровать/расшифровать, запустить программу, проанализировать, получить результаты анализа и обработки.

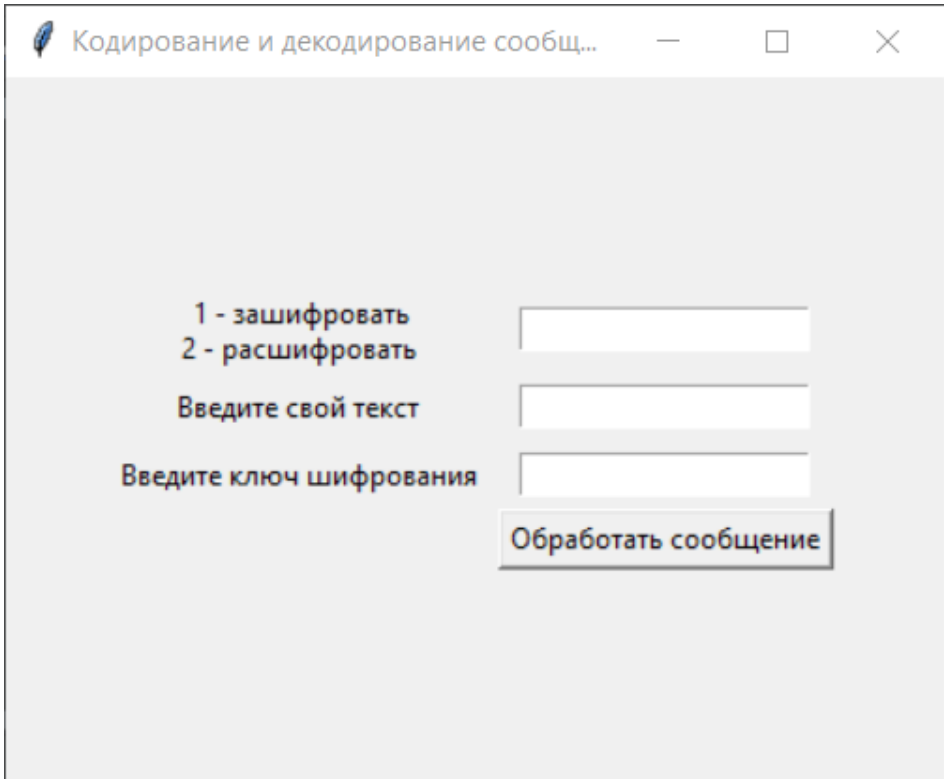

Рис. 2. Меню приложения.

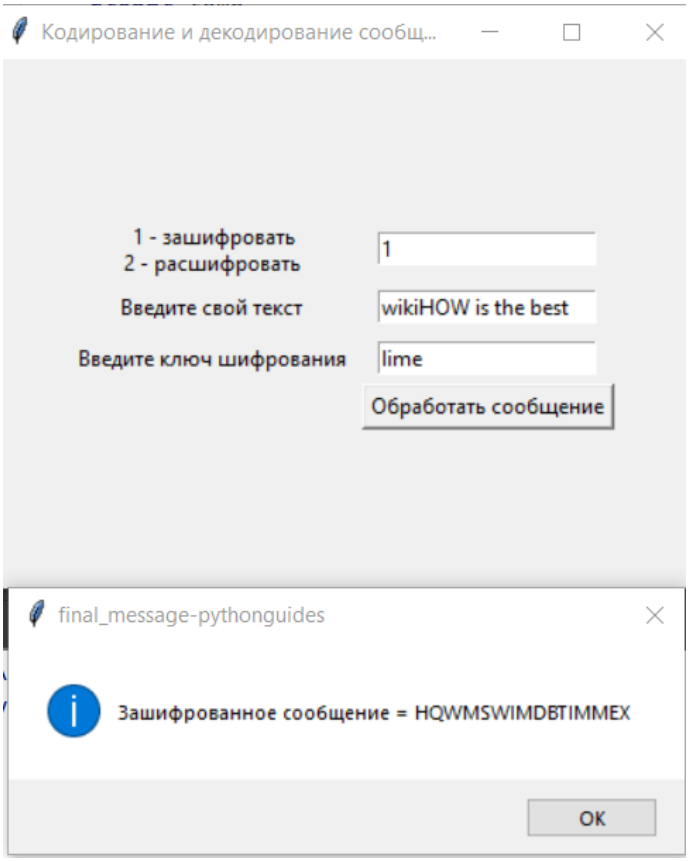

Рис. 3. Кодирование сообщения.

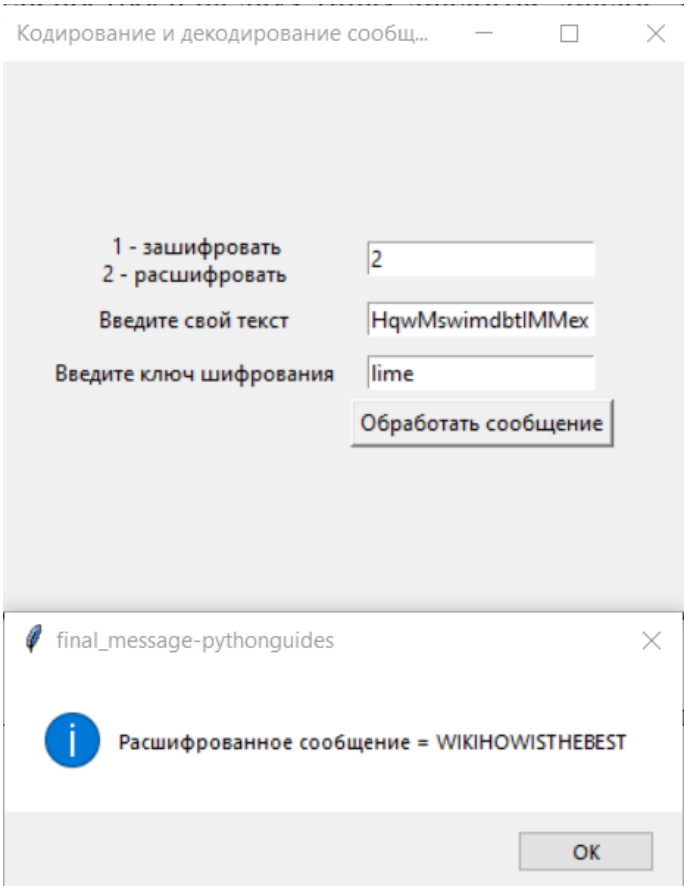

Рис. 4. Декодирование сообщения.

Интерфейсный модуль построен на двух типах диалогов: диалог "вопрос – ответ" и диалог типа "меню".

Программа эксплуатируется на персональном компьютере (ПК). Для работы в диалоговом режиме используется экран дисплея, клавиатура и манипулятор типа "мышь". Входные данные хранятся на гибком и/или жестком дисках. Программа работает под управлением ОС.

На вход подаются команды «1» - зашифровать сообщение; «2» - расшифровать сообщение. Программа не может быть использована при вводе значений, непредусмотренных программой, поэтому эти значения являются недопустимыми, а программа реагирует на них выводом сообщения “Не понимаю вас!”

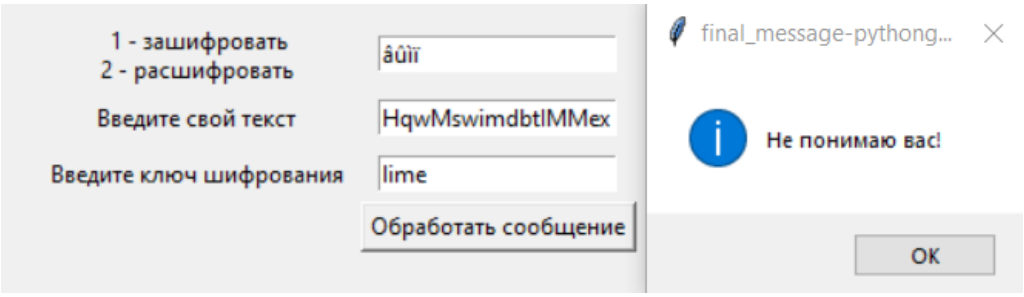

Рис. 5. Работа программы при вводе некорректных данных.

Входными данными для программы является фраза и ключ

Выходными данными являются:

– выводимая на экран графическая и текстовая информация (результаты анализа системы);

– диагностика состояния системы и сообщения обо всех возникших ошибках.

Заключение и выводы

Криптография прошла гигантский путь от простых шифров древности к сложнейшим криптосистемам. Распространение доступного интернета по всему миру невозможно представить без криптографии. Сегодня мы сталкиваемся с криптографией ежедневно, когда вводим пароль от почтового сервиса, узнаем статус покупки онлайн или делаем денежный перевод через приложение банка. С появлением мессенджеров, социальных сетей, онлайн-магазинов и сайтов государственных услуг передача персональной информации в сети происходит без остановки и в огромных количествах. Пока конфиденциальные данные требуют защиты, криптография будет продолжать развиваться. Криптографические системы, используемые в блокчейне криптовалют сегодня, представляют одну из наиболее продвинутых форм этой науки. Они также являются частью традиционной истории человечества.

Я выбрал науку криптографию для изучения, потому что с детства интересовался кодированием и всем, что с ним связано. В будущем мне бы хотелось связать свою жизнь с информационной безопасностью, и такое подробное изучение столь важной темы не только поможет мне в дальнейшем погружении в тему, но и может предоставить наипростейшие знания заинтересовавшимся новичкам или освежить память хорошо ориентирующимся в шифрах людям.

В процессе изготовления моей исследовательской работы я научился составлять план действий и следовать ему, расставлять приоритеты по степени важности определенных задач, правильно оформлять информационный продукт и самое важное в чем и заключалась цель данного проекта - я научился кодированию и декодированию информации с помощью различных методов шифрования информации.

Список источников и литературы

1. Коллектив Авторов, «Введение в криптографию», 2017
2. Саймон Сингх, «Книга шифров. Тайная история шифров и их расшифровки», издательство Астрель, 2007
3. Нильс Фергюсон, Брюс Шнайер, «Практическая криптография», издательство Вильямс, 2017
4. http://algolist.ru/defence/intro.php
5. https://naked-science.ru/article/sci/ot-manuskriptov-do-shifrovalnyh
6. https://academy.binance.com/ru/articles/history-of-cryptography
7. https://tproger.ru/translations/understanding-cryptography/
8. http://www.realcoding.net/articles/vvedenie-v-kriptografiyu.html-0
9. https://oyla.xyz/article/kod-enigmy
10. https://thecode.media/vernam/
11. https://www.dcode.fr/hill-cipher
12. https://intellect.icu/
13. https://planetcalc.ru/

Рецензия
на работу обучающегося 11 «А» класса
МБОУ СОШ № 28 г. Пензы им. В. О. Ключевского
Кудрявцева Даниила Павловича
«Криптография как метод кодирования и декодирования информации»

Работа «Криптография как метод кодирования и декодирования информации» представляет собой исследование в области информатики. В работе представлено обоснование темы, указана актуальность, практическая значимость, определены цели и задачи, объект и предмет исследования, обозначены особенности анализируемого материала, описаны методы исследования, выдвинута гипотеза по обозначенной проблеме.

В ходе выполнения работы обучающийся рассмотрел теоретические основы данного вопроса, обратился к источникам, освещающим историю криптографии, рассмотрел методы шифрования информации, методы решения вопроса с помощью языка программирования Python, библиотеку TKinter.

В практической части автор создает собственное приложение для кодирования информации.

Практическая значимость исследования определяется тем, что рассмотренные и описанные материалы могут быть использованы на уроках информатики. Материал работы будет полезен любителям информатики для расширения кругозора.

Работа соответствует целям и задачам изучаемой проблемы, в структуре работы просматривается логика изложения, самостоятельность в разработке темы.

Оформление работы соответствует требованиям и критериям, предъявляемым к работам на V открытый региональный конкурс исследовательских и проектных работ школьников «Высший пилотаж - Пенза» 2023.

В представлении результатов работы предполагается использование презентации.

Рецензент  Смирнова Алина Дмитриевна, учитель информатики
МБОУ СОШ № 28
г. Пензы им. В. О. Ключевского