Муниципальное бюджетное общеобразовательное учреждение города Иркутска средняя общеобразовательная школа с углубленным изучением отдельных предметов № 19

**Шифровка Информации при помощи авторского телеграмм бота**

Работа ученика 10 Б класса

Лебедя Дениса Максимовича

Руководитель проекта Рейнгольд Григорий Борисович, педагог ДО МБУДО ЦДТТ

Работа допущена к защите «13» Апреля 2023 г.



Подпись руководителя проекта ( )

Иркутск

2023 г.

**Паспорт проекта**

|  |  |
| --- | --- |
| Название проекта | Шифровка Информации при помощи авторского телеграмм бота |
| Руководитель проекта | Рейнгольд Григорий Борисович, педагог ДО МБУДО ЦДТТ |
| Автор проекта | Лебедь Денис Максимович, ученик 10Б класса МБОУ СОШ №19 |
| Предметная направленность | Математика, информатика |
| Тип проекта | Прикладной |
| Цель работы | Создать телеграмм бота, умеющего шифровать и дешифровывать сообщения, и научить пользователей использовать телеграмм бота правильно |
| Задачи проекта | 1. Изучить разнообразные методы шифровки и дешифровки информации 2. Создать собственный универсальный метод шифровки 3. Изучить язык Python и библиотеку Telebot 4. Создать телеграмм бота 5. Исправлять недоработки и увеличивать функционал |
| Сроки реализации проекта | 10.04.2023 |
| Краткое содержание проекта | Проект заключается в изучении методов шифрования, аналогичных ботов в телеграмме, изучение языка python и библиотеки telebot, и создании телеграмм бота, его отладке и распространению, чтобы пользователи могли защищать информацию |
| Результат проекта  (проектный продукт) | Работающий телеграмм бот |
| Область применения  результата проекта | Создание безопасных заметок, которые сложно перехватить, создание базы данных зашифрованных паролей, заметок и пр конфиденциальной информации |

**Оглавление**

1. Введение
   1. Проблема
   2. Актуальность
   3. Цель
   4. Задачи
2. Теоретическая часть
   1. Шифрование. История шифрования
   2. Методы шифрования, используемые мной в работе
   3. Python как универсальный язык программирования, и библиотека telebot
3. Практическая часть
   1. Создание бота
   2. Испытания и исправления ошибок
   3. Распространение
   4. Памятка по использованию
4. Заключение
5. Список литературы
6. Приложение

**Введение**

У каждого человека есть свои секреты, которые он хотел бы записать куда то, но нет желания утруждаться в поиске способа защиты. И для таких людей я представляю своего бота, способного за короткое время зашифровать достаточно большой объем данных

**Проблема:** порой необходимо найти способ защиты информации для ее сохранности. Но не хватает времени и терпения зашифровать объем большой объем информации, или методы шифрования слишком просты и легко обходятся людьми, которые не должны знать информацию

**Актуальность:** Телеграмм – популярная соцсеть, которая также очень надежная. Помимо всего, телеграмм боты становятся все большей частью жизни пользователей телеграмма, и постепенно появляются все новые и новые возможности ботов.

**Цель:** Создать телеграмм бота, умеющего шифровать и дешифровывать сообщения, и научить пользователей использовать телеграмм бота правильно

**Задачи:**

1. Изучить разнообразные методы шифровки и дешифровки информации
2. Создать собственный универсальный метод шифровки
3. Изучить язык Python и библиотеку Telebot
4. Создать телеграмм бота
5. Исправлять недоработки и увеличивать функционал
6. Составить инструкцию для использования бота правильно, и распространять бота

**Теоретическая часть**

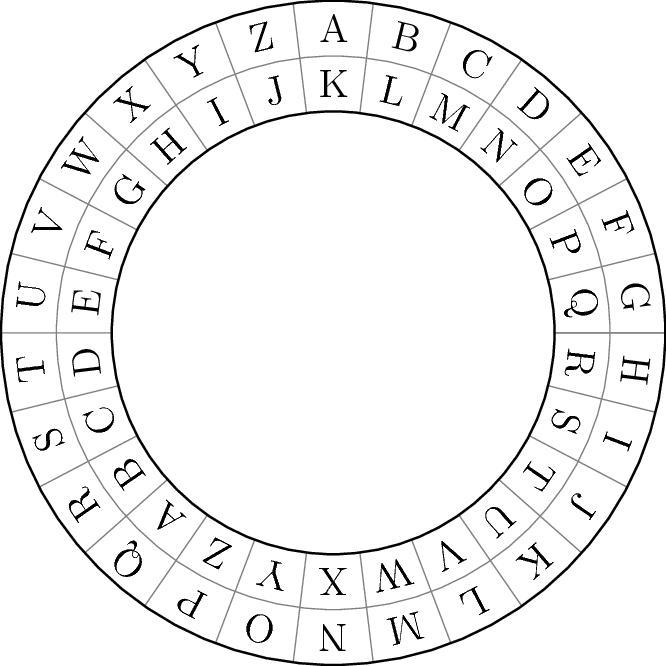
**Шифрование. История шифрования**

Шифрование – обратимое преобразование [информации](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F) в целях сокрытия от [неавторизованных](https://ru.wikipedia.org/wiki/%D0%90%D0%B2%D1%82%D0%BE%D1%80%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F) лиц с предоставлением в это же время [авторизованным](https://ru.wikipedia.org/wiki/%D0%90%D0%B2%D1%82%D0%BE%D1%80%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F) пользователям доступа к ней. Главным образом, шифрование служит для соблюдения [конфиденциальности](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BD%D1%84%D0%B8%D0%B4%D0%B5%D0%BD%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D1%81%D1%82%D1%8C) передаваемой информации. Важной особенностью любого алгоритма шифрования является использование [ключа](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F)), который утверждает выбор конкретного преобразования из совокупности возможных для данного алгоритма.

Изначально обычная письменность была шифрованием. Ведь во многих странах древнего мира алфавит состоял из очень большого количества символов, и лишь единицы могли записывать их.

В древней Спарте придумали первое шифровальное устройство. Оно называлось скитала, и состояла из пергамента, обвивающего цилиндр, и цилиндра. Текст писали в строку на пергаменте. После разматывания ленты текст превращался в шифр, прочитать который было возможно, только имея цилиндр такого же диаметра

Один из первых сохранившихся шифров считается шифр Цезаря, заключающийся в смещении алфавита на определенное число символов. Разгадать шифр можно узнав это число.



Значительных успехов достигли арабы в шифровке, что придумали множество надежных шифров, благодаря математикам в странах. Из арабских стран эти методы попали в Европу, где криптография считалась темным искусством, как и магия.

В эпоху Возрождения криптография переживает подъем. Начинается период формальной криптографии, связанный с появлением формализованных, более надежных шифров.

Прорывом в криптографии стала книга «Полиграфия» аббата Иоганеса Тритемия 1518 года, рассказывающая в том числе о шифрах с полиалфавитной заменой. Самым известным шифровальщиком XVI века считается дипломат и алхимик из Франции Блез де Виженер, придумавший абсолютно стойкий шифр, в котором использовалось 26 алфавитов, а порядок использования шифра определялся знанием пароля. Можно сказать, что шифр Виженера представлял собой комбинацию нескольких уже упоминавшихся шифров Цезаря.

Промышленная революция не обошла вниманием и криптографию. Около 1790 года один из отцов – основателей США Томас Джефферсон создал дисковый шифр, прозванный позже цилиндром Джефферсона. Этот прибор, основанный на роторной системе, позволил автоматизировать процесс шифрования и стал первым криптоустройством Нового времени.

Большое влияние на шифровальное дело оказало изобретение телеграфа. Прежние шифры вмиг перестали работать, при этом потребность в качественном шифровании только возрастала в связи с чередой крупных военных конфликтов. В XIX-XX веках основные импульсы для развития криптографии давала именно военная сфера. С 1854 года британские военные применяют шифр Плейфера, в основе которого – шифрование биграмм, или пар символов. Этот шифр использовался до начала Второй мировой войны.

Во Второй мировой войне противники уже использовали мобильные электромеханические шифраторы, шифры которых считались нераскрываемыми. Устройства были роторными или на цевочных дисках. К первым относилась знаменитая машина «Энигма», которой пользовались нацисты, ко вторым – американская машина M-209.

Принцип работы «Энигмы» заключался в следующем: при каждом нажатии на клавишу с буквой алфавита в движение приходили один или несколько роторов. Буква изменялась несколько раз по принципу шифра Цезаря, и в окошке выдавался результат. Шифры «Энигмы» считались самыми стойкими для взлома, так как количество ее комбинаций достигало 15 квадриллионов. Однако код «Энигмы» все же был расшифрован, сперва польскими криптографами в 1932 году, а затем английским ученым Аланом Тьюрингом, создавшим машину для расшифровки сообщений «Энигмы» под названием «Бомба». Комплекс из 210 таких машин позволял англичанам расшифровывать до 3 тыс. военных сообщений нацистов в сутки и внес большой вклад в победу союзников.

В 1949 году Клод Шеннон пишет работу «Теория связи в секретных системах», и криптография окончательно переходит в сферу математики. К концу 1960-х роторные шифровальные системы заменяются более совершенными блочными, которые предполагали обязательное применение цифровых электронных устройств. В 1967 году ученый Дэвид Кан издал популярную книгу «Взломщики кодов», которая вызвала большой интерес к криптографии.

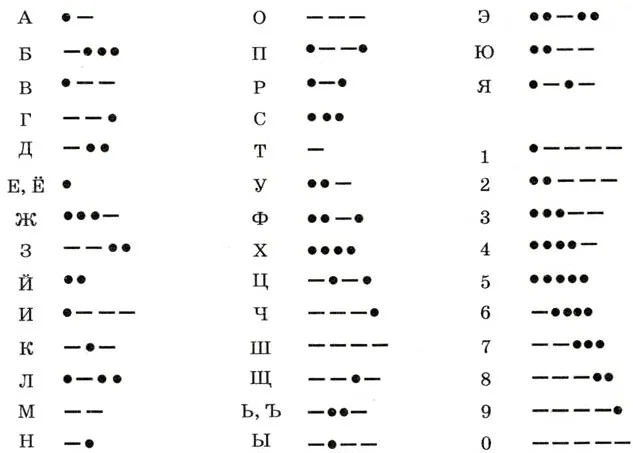
С распространением компьютеров криптография выходит на новый уровень. Мощности новых устройств позволяют создавать на порядки более сложные шифры. Шифр или код становится языком общения между компьютерами, а криптография становится полноценной гражданской отраслью. В 1978 году разрабатывается стандарт шифрования DES, который стал основой для многих современных криптографических алгоритмов.

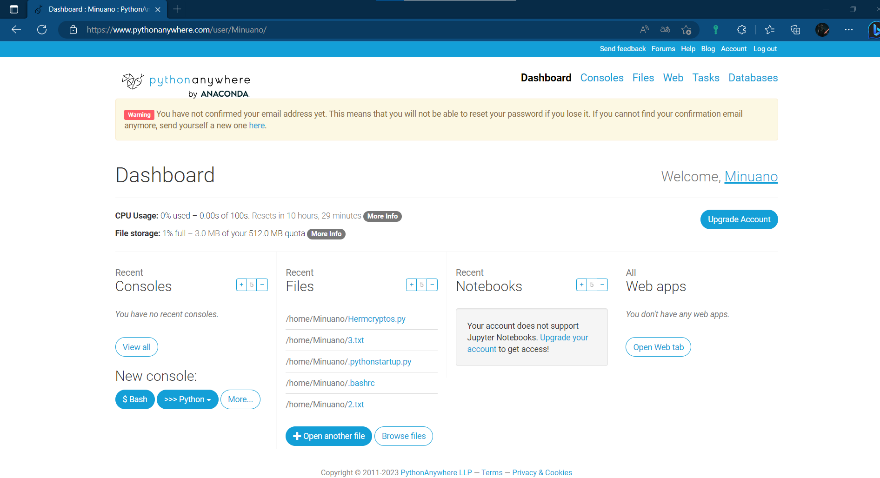
Сфера использования криптографии расширяется, при этом власти различных стран пытаются удержать контроль над использованием шифров. Разработки криптографов засекречиваются, от производителей шифровальных машин требуют оставлять в продуктах «черные ходы» для доступа спецслужб

**Методы шифрования, используемые мной в работе**

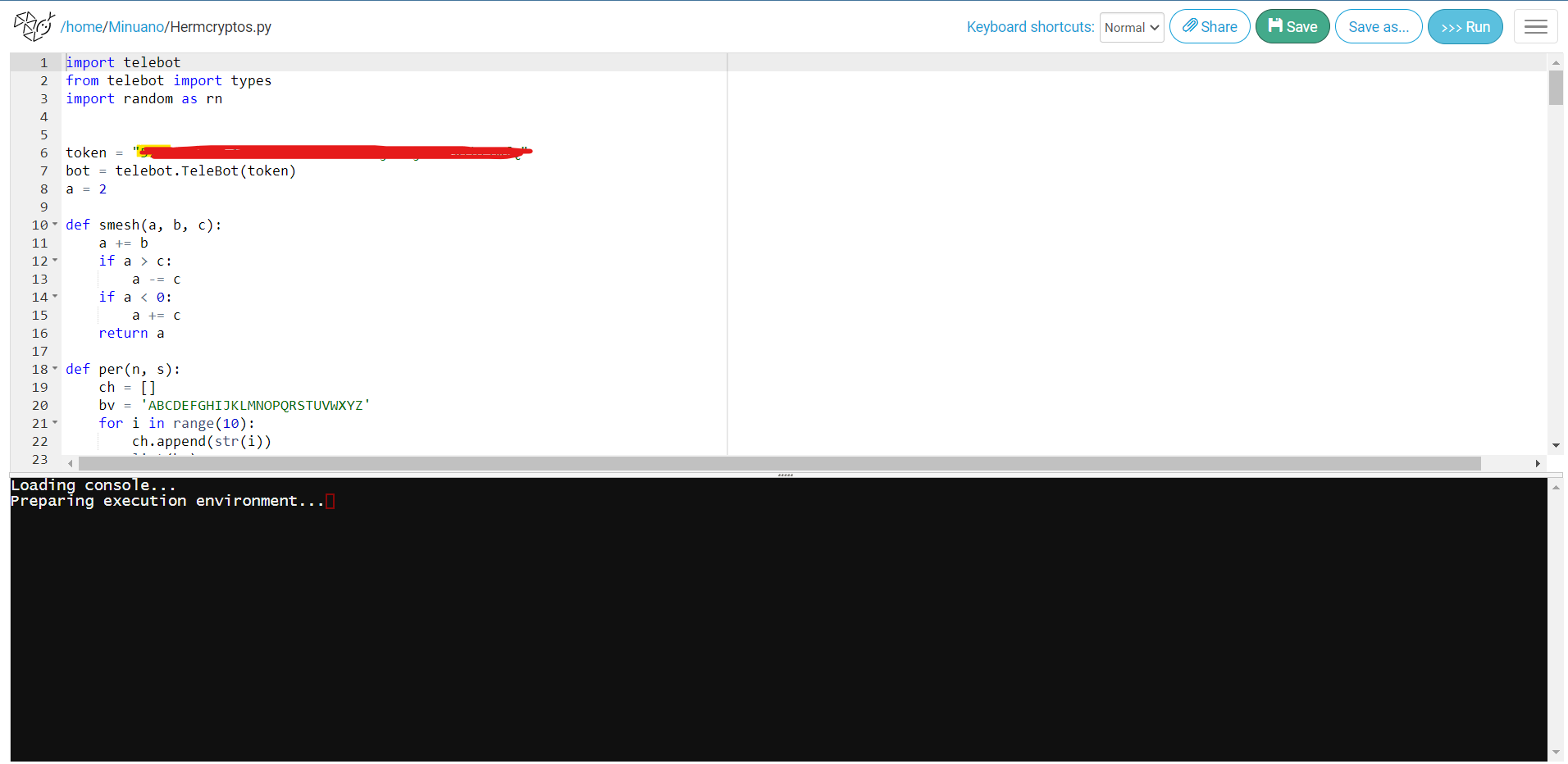
В современном мире сейчас очень много различных вариантов шифровок. Их перечислить будет почти невозможно. Помимо вышеупомянутых шифров в работе я решил использовать некоторые перечисленные ниже шифры, а также простое кодирование – перевод в другие системы счисления



Или не теряющий актуальность код Морзе

**Python как универсальный язык программирования, и библиотека telebot**

Python – Один из основных языков программирования, который используется во всех отраслях программирования. Он популярен из-за простоты по сравнению со многими другими языками, и в то же время по функциональности он не уступает им. В качестве среды я использую сайт <https://www.pythonanywhere.com/>



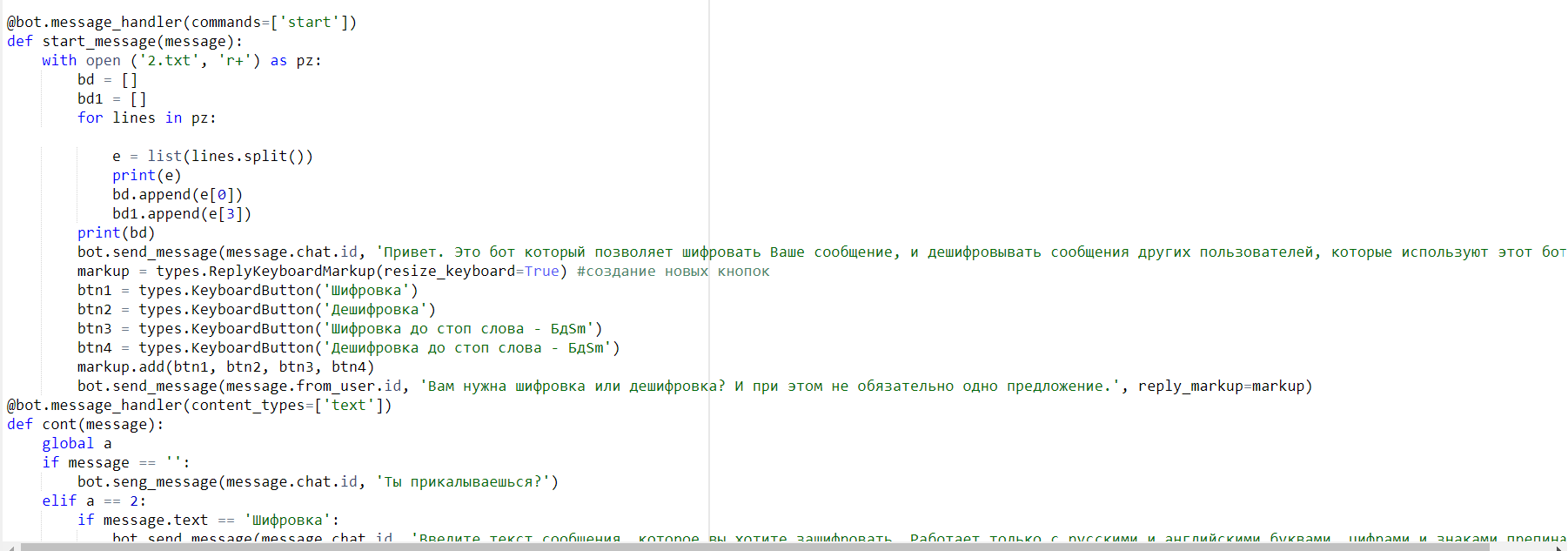
А в качестве библиотеки для создания телеграмм бота я использую библиотеку telebot.

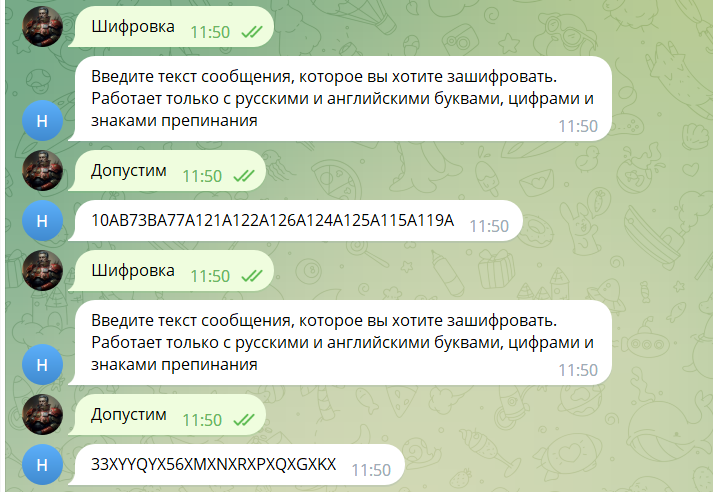
**Практическая часть**

**Создание бота**

Для начала я написал в BotFather, бот для создания других ботов. Я придумал имя бота, и получил токен, для того чтобы связать код и бота. <https://t.me/BotFather> После получения токена я вставил его в переменную в коде. Код я разделил на 2 части – математика, то есть шифровка и дешифровка, и чисто работа с библиотекой telebot. В функциях шифровки и дешифровки я использовал собственный алгоритм. А в функциях взаимодействия с пользователем я прописал порядок использования функций, реакция бота на определенный тип сообщений и т.д. Бот использует такой алгоритм шифровки, что одно и то же слово может быть записано в 5530 различных вариантах.

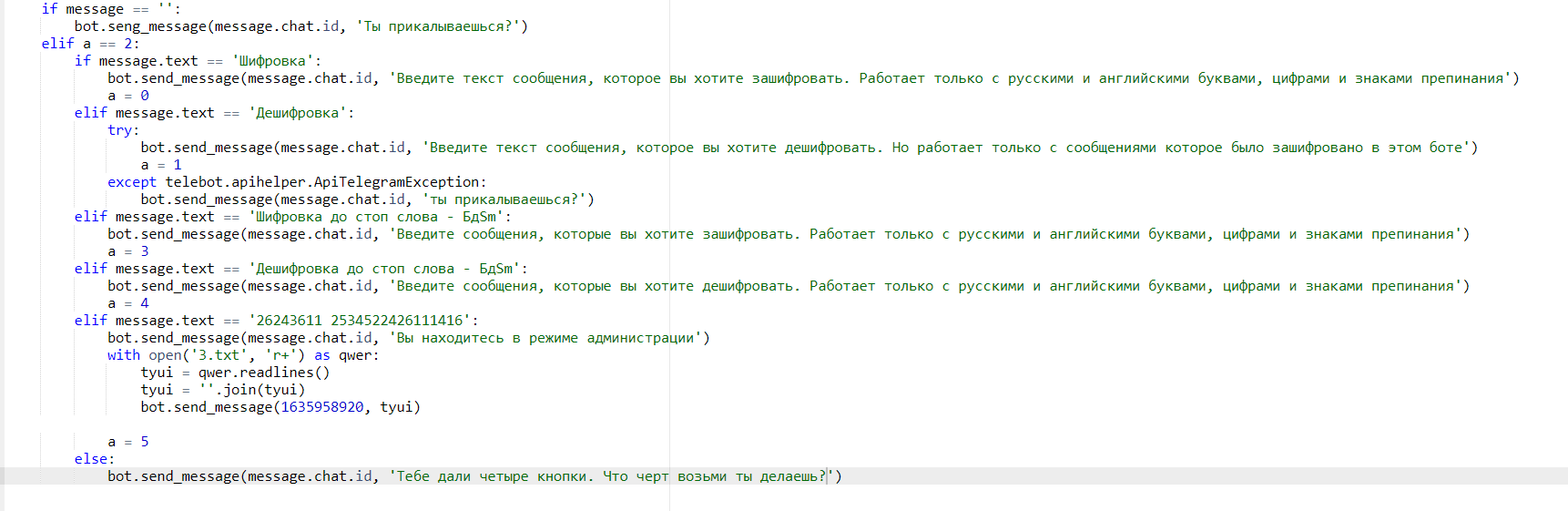




****

**Испытания и исправления ошибок**

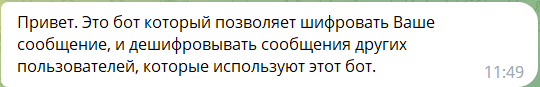
Поначалу испытания альфа-версии проекта меня устроили. Потому что работало так как я и хотел.

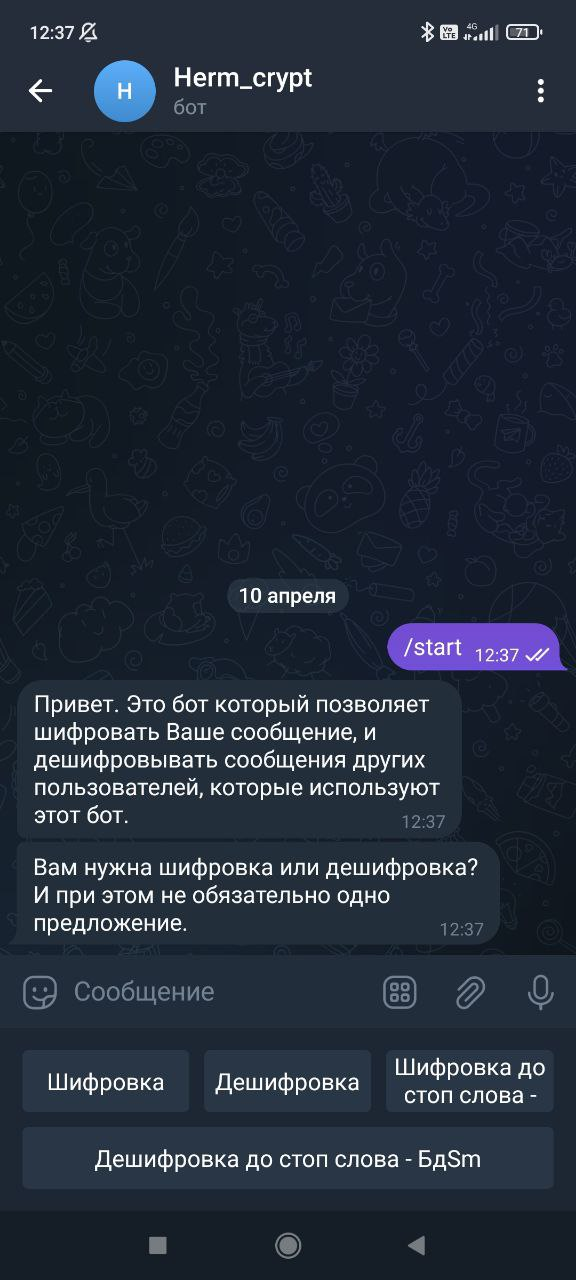
Но, к сожалению, я не видел некоторые ошибки, потому что я знал, что вводить. А пользователи мыслят не так как разработчики проекта. И поэтому они постоянно заставляют бота вылетать, когда вводят не то, что от них требуется. И поэтому пришлось прописывать варианты, которые я изначально не предусмотрел. Собственно, именно пользователи позволяют находить новые ошибки, которые необходимо исправить.

**Распространение**

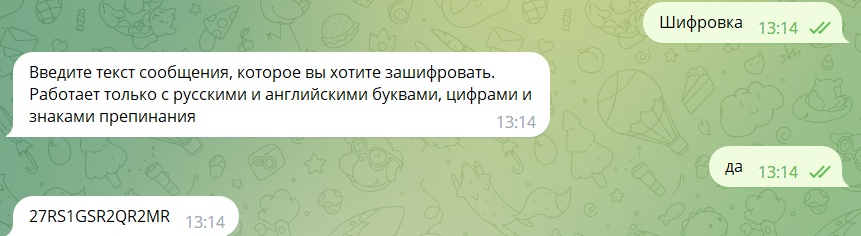
Я решил, что о боте должно знать в первое время не сильно большое число людей. Только люди, которым я доверяю. И пока о боте знает немного людей, я могу спокойно доработать и убрать ошибки. А когда ошибки будут исправлены, я планирую распространять бота при помощи различных методов.

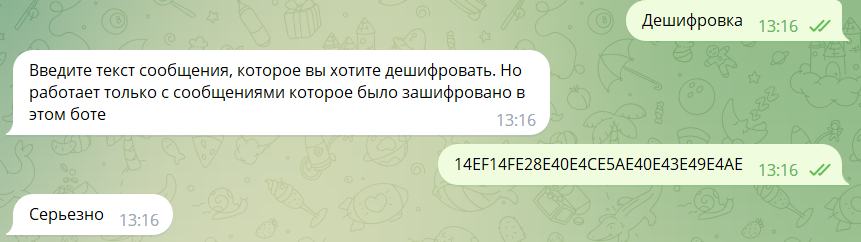
**Памятка по использованию**

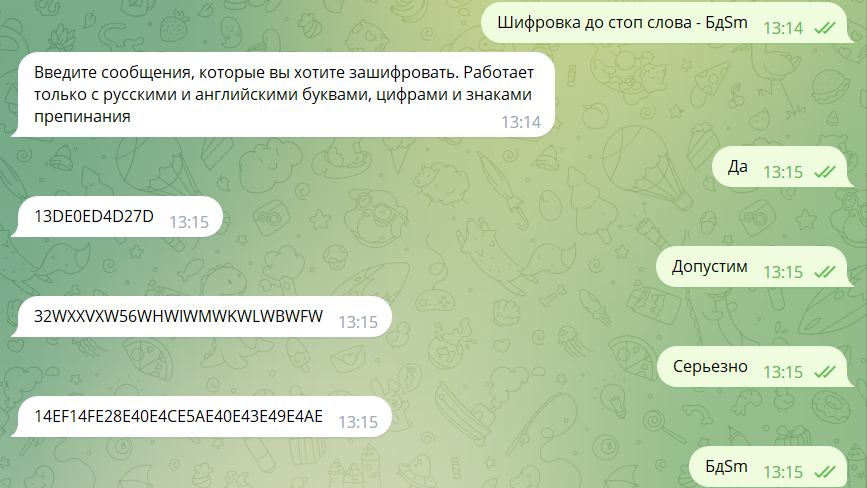
1. Во время запуска работы бота Вам будет выведено приветствие 
2. Далее вам будет показано меню из 4 кнопок.

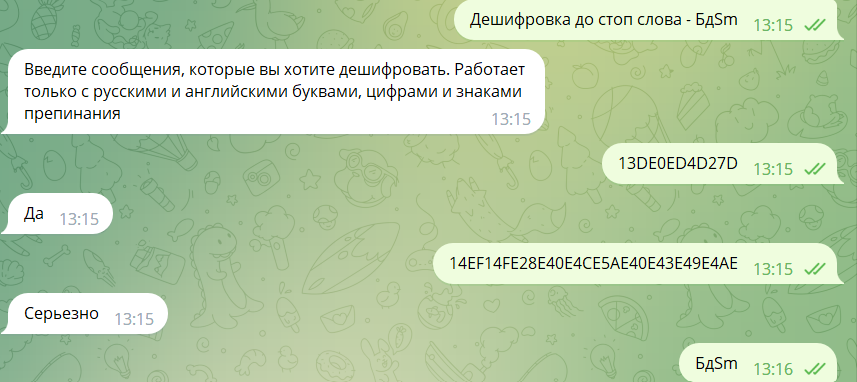


1. Надо выбрать ровно одну. Если это шифровка и дешифровка, то надо будет ввести всего одно слово, а далее в зависимости от выбора. Если выбрать Шифровка до стоп слова или дешифровка до стоп слова, то ты можешь вводить сколько угодно сообщений для шифровки или дешифровки.









1. Когда вводишь дешифровку, то необходимо ввести последовательность цифр и заглавных букв английского алфавита.
2. После ввода строки во время шифровки и дешифровки программа начинает работу с главного меню (пункт 2)

**Заключение**

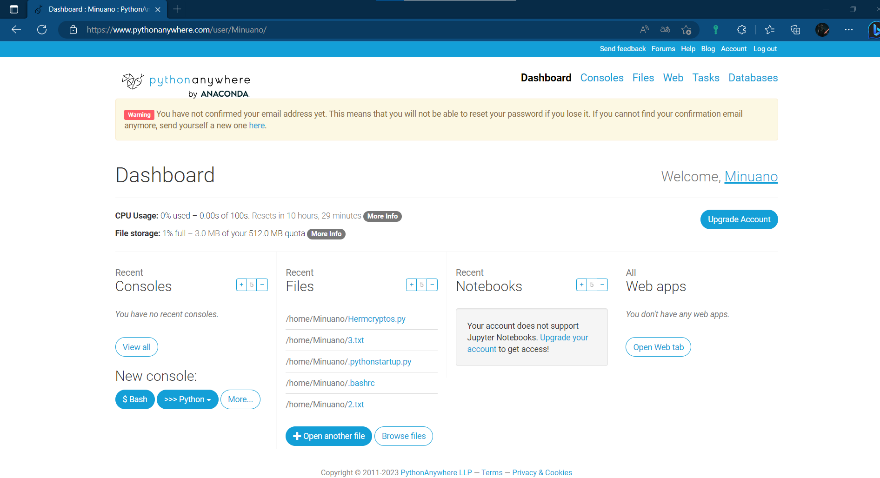
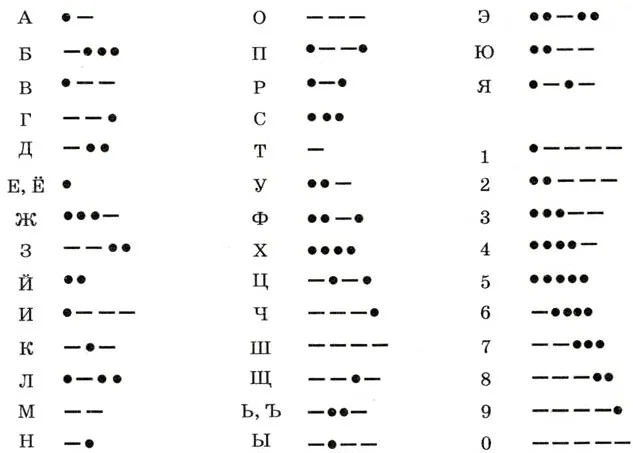
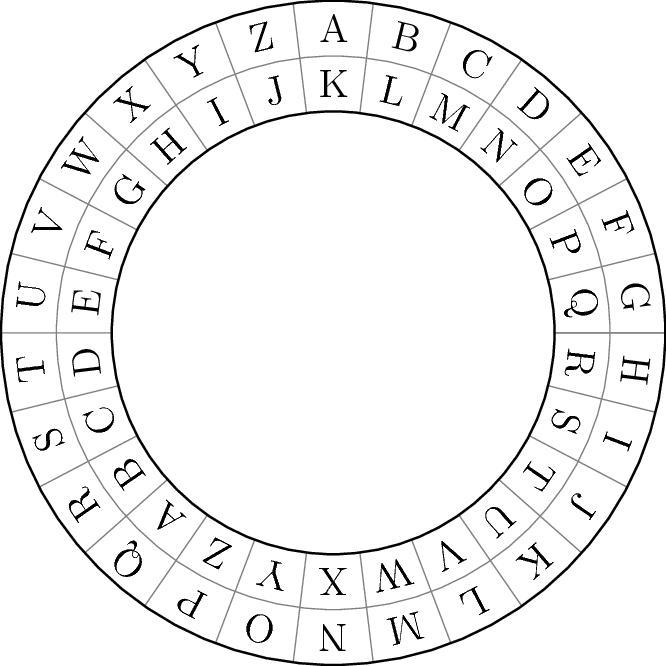
По моему мнению, прогресс по работе есть. Изначально шифр был примитивным, но я значительно улучшил его. Также я сделал памятку для пользователей, чтобы они не путались, и могли вводить то что нужно без ошибок. Мои друзья подтверждают, что над ботом работать нужно, ведь он пока далеко не идеальный.

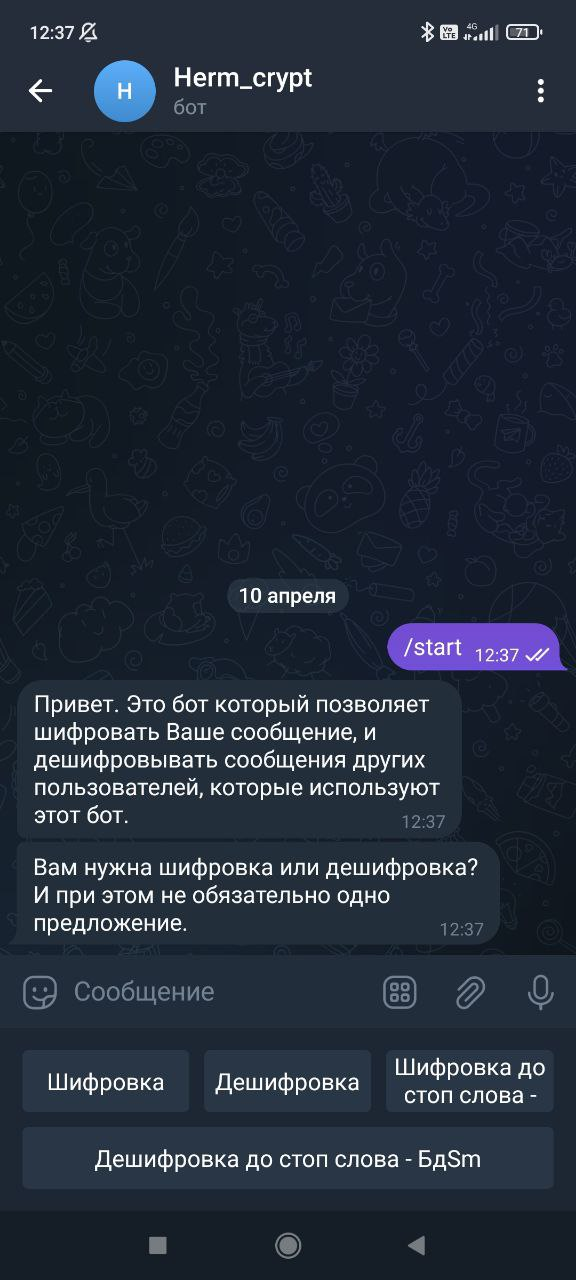
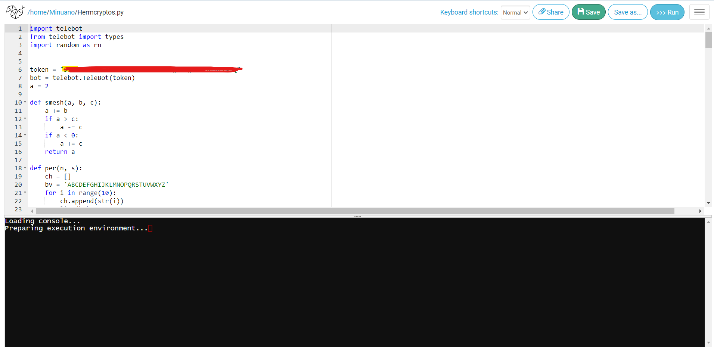
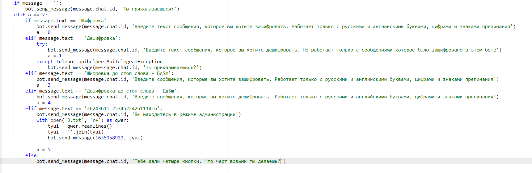
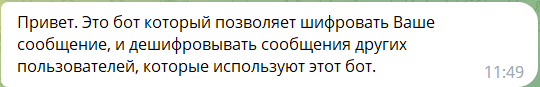
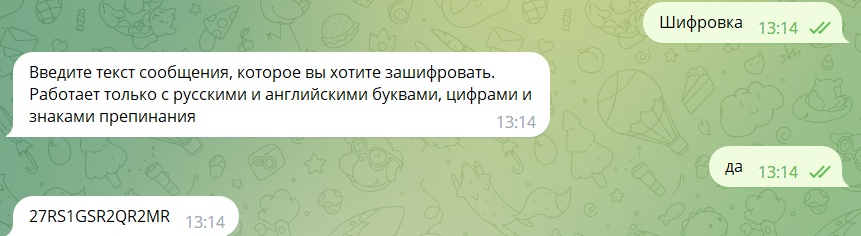
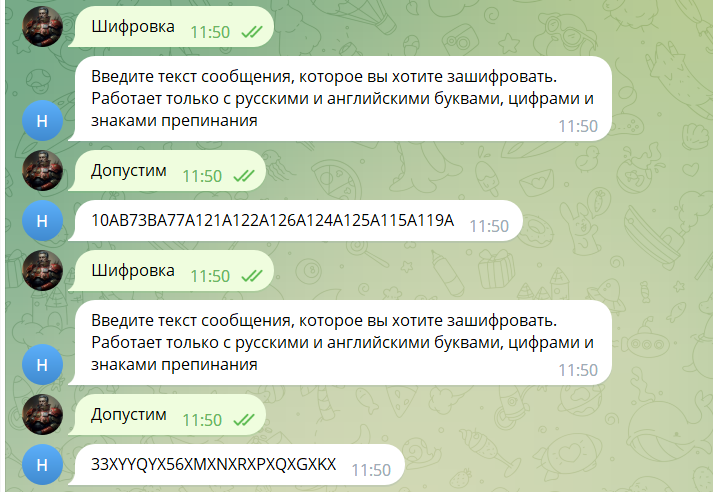
В заключении, могу сказать, что перспектив в этой работе очень много. Помимо исправления ошибок, я планирую усилить систему зашиты, а также добавить заметки. Каждый пользователь вводит заметки, они шифруются, а при необходимости нажимает кодовый символ – и выходят данные, которые нужны пользователю. Считаю, что первый этап работы выполнен на 90%

**Список литературы**

* Криптография. История шифровального дела. Дата обновления – 29.08.2020. [https://rostec.ru/news/kriptografiya-istoriya-shifrovalnogo-dela/#](https://rostec.ru/news/kriptografiya-istoriya-shifrovalnogo-dela/) дата обращения – 01.04.2023
* Telebot. Документация. Дата обновления – 2022. [https://pytba.readthedocs.io/en/latest/index.html дата обращения - 01.04.2023](https://pytba.readthedocs.io/en/latest/index.html%20дата%20обращения%20-%2001.04.2023)
* Python. Работа с файлами. Документация. Дата обновления – 21.05.2015 <http://pythonicway.com/python-fileio?ysclid=lga8m7choh635357296> Дата обращения – 01.04.2023
* Шифрование. Дата обновления – 16.03.2023 <https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5> Дата обращения – 01.04.2023

**Приложение**



****