# Шифрование с помощью Python

Проект Брехова Акима

ученика 9 А класса МБОУ Ближнеборисовская СШ

# Актуальность:

- Ещё до нашей эры была большая востребованность людьми спрятать текстовую информацию от посторонних глаз при её передаче или хранении. В нашей эре в течение войн была необходимость защитить информацию во время её передачи от сил противника. Сейчас, когда наш мир полностью пользуется интернетом и повсюду идёт информация, тайно передавать важную информацию и поддерживать конфиденциальность от мошенников встаёт очень острой и важной проблемой.

# Проблемная ситуация:

- Возможно, не каждый встречался с такой проблемой, как “утечка“ личных данных или информации, но случиться такое может с каждым.
- Однажды, установив нелицензированное ПО на свой рабочий компьютер, я установил RAT-вирус и мой файл, в котором хранились все пароли, украли. Избежать этого можно с помощью элементарных знаний личной информационной безопасности и так называемой криптографии – шифрование информации.

# Проблема:

Нехватка знаний о криптографии, о методах и алгоритмах шифрования.

# Цель проекта:

- Узнать, что такое криптография, где и как применяется шифрование. Написать свой шифратор на языке программирования python.

# Задачи:

1. Выяснить откуда взялось понятие “криптография”.
2. Изучить методы и алгоритмы шифрования.
3. На основе полученных знаний создать свой шифратор.

# Что такое криптография?

- Криптография - наука и искусство передачи сообщений в таком виде, чтобы их нельзя было прочитать без специального секретного ключа. Слово «криптограф» происходит от древнегреческих слов kryptos ‘секрет’ и graphos ‘писание’. Исходное сообщение называется в криптографии открытым текстом. Засекреченное (зашифрованное) сообщение называется шифротекстом, или шифрограммой, или криптограммой. Процедура шифрования обычно включает в себя использование определенного алгоритма и ключа.
- 
- Как только возникло письмо, появились и способы его шифрования. В древних цивилизациях мы находим два вида письма: иератическое, или священное письмо, использовавшееся священнослужителями для тайного общения друг с другом, и демотическое письмо, употреблявшееся всеми остальными. И у греков, и у римлян, и у других сопоставимых с ними по историческому значению народов были свои системы тайного письма. Изобретение первой системы скорописи, которая изначально замышлялась как секретное письмо, приписывается Туллиусу Тиро, вольноотпущенному рабу Цицерона (106-43год до н.э.).
- 
- С 1990-х годов страны начали в открытую формировать свои стандарты криптографических протоколов. США, к примеру, приняло в качестве стандарта для криптографии с закрытым ключом шифр Rijndael, более известный, как AES, в Европе приняли шифр NESSIE, в Японии — CRYPTREC.

# Методы и алгоритмы шифрования.

1) Применяются следующие основные методы шифрования:

- - подстановка (простая – одноалфавитная, многоалфавитная однопетлевая, многоалфавитная многопетлевая);
- - гаммирование (смешивание с короткой, длинной или другой маской);
- - перестановка (простая, усложненная).

2)Строгое математическое описание алгоритмов стандартных методов шифрования слишком сложно. Для пользователей важны в первую очередь «потребительские» свойства различных методов (степень устойчивости к дешифрованию, скорость шифрования и дешифрования, порядок и удобство распространения ключей).

При использовании электронной почты в Интернет довольно популярны, несимметричные методы шифрования или системы с открытыми ключами – public-key systems. К таким методам относится, например, PGP (Pretty Good Privacy - достаточно хорошая секретность).

Каждый из пользователей имеет пару ключей (открытый и закрытый). Открытые ключи предназначены для шифрования информации и свободно рассылаются по сети, но не позволяют произвести ее дешифрование. Для этого нужны специальные, секретные (закрытые) ключи. Принцип шифрования в данном случае основывается на применении так называемых односторонних функций.

# Заключение:

- С помощью этого проекта я узнал, что такое криптография, где и как применяется шифрование. И сумел написать свой шифратор на языке программирования python.