

Лабораторная работа № 1.

Шифрование данных методами подстановки, перестановки и полиалфавитными шифрами

Карасев Илья Алексеевич, М23-505

Цель работы, постановка задачи

Приобретение навыков шифрования информации с использованием простейших методов шифрования.

Задача лабораторной работы является разработки алгоритм и составить программу, позволяющую закодировать любой текст выбранным методом шифрования и выполнить обратное преобразование

Описание исходных данных

Выбранный вариант: 4

Метод кодирования: Перестановка

Группа перестановки (Вариант 2):

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix}$$

Тестируемое строка: Hello World

Язык программирования: Python

Алгоритм работы программы

1. Программе не вход подается строка и режим работы (кодирование\декодирование), по умолчанию используется режим кодирования
2. Исходя из выбранного режима работы определяется требуемая операция (кодирование\декодирование)
3. Определяется длина поданного текста, если он не кратен количеству символов в группе перестановки, то она дополняется пробелами, что удовлетворить условие кратности
4. Проводится операция кодирования\декодирования в зависимости от выбранного режима
 - а. Исходный текст проходит блоками размера длины группы перестановки (5)
 - б. Символы в блоке переставляются в соответствии с группой перестановки
5. Убираются пробелы с конца результирующего текста
6. Результат выводится в консоль

Текст программы

```
import argparse

class CypherTransposition:
    """
    Предоставляет методы кодирования и декодирования
    """

    # block = [0, 1, 2, 3, 4]
    _trans = [4, 3, 0, 1, 2]
    _block_len = 5

    @classmethod
    def _pad_text(cls, text: str) -> str:
        """Если длина текста не кратна _block_len,
        то добавляет необходимое количество пробелов,
        что бы строка была кратной
        """

        pad = cls._block_len - len(text) % cls._block_len
        text = text if pad == 5 else text + " " * pad
        return text

    @classmethod
    def encode(cls, text: str) -> str:
        """Закодирование текста"""

        text = cls._pad_text(text)
        encrypted = ""
        for i in range(0, len(text), cls._block_len):
            for j in range(0, cls._block_len):
                encrypted += text[i + cls._trans[j]]
        return encrypted.rstrip()

    @classmethod
    def decode(cls, text: str) -> str:
        """Декодирование текста"""

        text = cls._pad_text(text)
        decrypted = ""
        for i in range(0, len(text), cls._block_len):
            block = [""] * 5
            for j in range(0, cls._block_len):
                block[cls._trans[j]] = text[i + j]
            decrypted += "".join(block)
        return decrypted.rstrip()

parser = argparse.ArgumentParser(
    prog="Кодировани и декодирование методом подстановки",
    description="По умолчанию кодирует заданный текст, для декодирования используйте ключ [-d]",
)

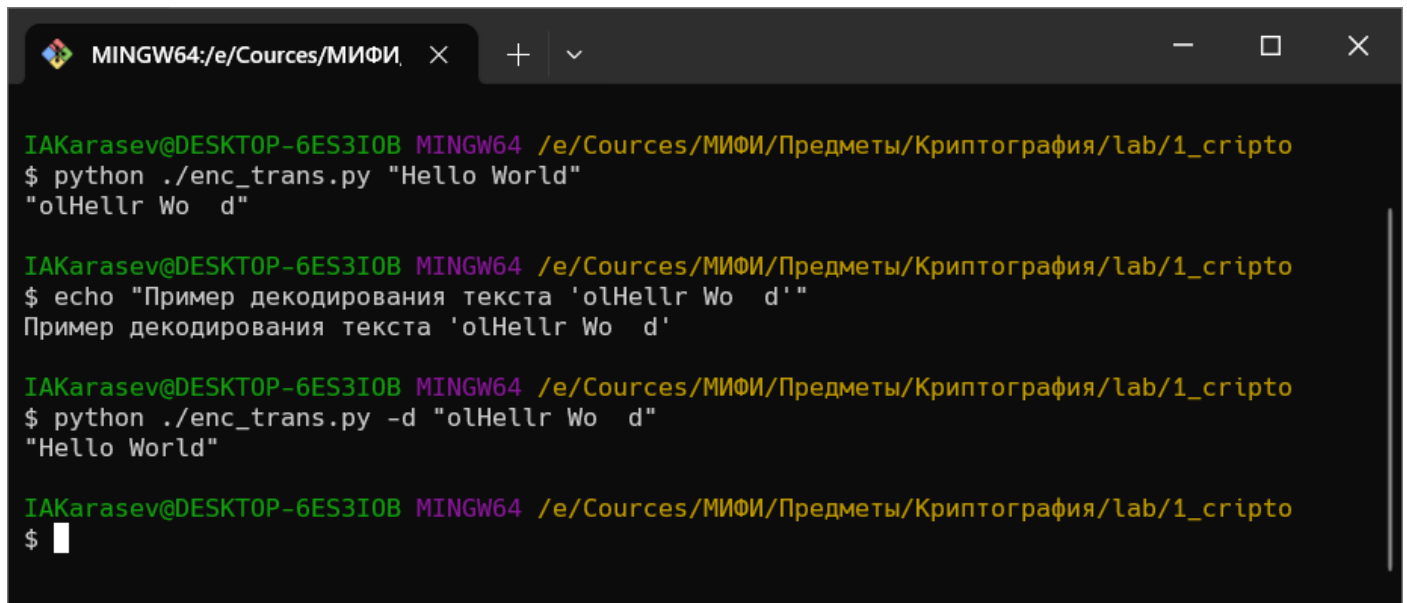
parser.add_argument(
    "text",
    type=str,
    help="Входной текст",
)

parser.add_argument(
    "-d",
    "--decrypt",
    action="store_true",
    default=False,
    help="Декодировать текст",
)

args = parser.parse_args()

if args.decrypt:
    print(f'"{CypherTransposition.decode(args.text)}"')
else:
    print(f'"{CypherTransposition.encode(args.text)}"')
```

Результаты работы программы



```
IAKarasev@DESKTOP-6ES3IOB MINGW64 /e/Cources/МИФИ \times + \times - \square \times
$ python ./enc_trans.py "Hello World"
"olHellr Wo d"

IAKarasev@DESKTOP-6ES3IOB MINGW64 /e/Cources/МИФИ/Предметы/Криптография/lab/1_cripto
$ echo "Пример декодирования текста 'olHellr Wo d'"
Пример декодирования текста 'olHellr Wo d'

IAKarasev@DESKTOP-6ES3IOB MINGW64 /e/Cources/МИФИ/Предметы/Криптография/lab/1_cripto
$ python ./enc_trans.py -d "olHellr Wo d"
"Hello World"

IAKarasev@DESKTOP-6ES3IOB MINGW64 /e/Cources/МИФИ/Предметы/Криптография/lab/1_cripto
$
```

Анализ результатов

Разработанная программа позволяет закодировать текст используя алгоритм перестановок, а также декодировать шифротекст, закодированный тем же алгоритмом

Выводы

Изучена реализация кодирования\декодирования текста методом перестановок. Так же изучены такие методы простейшего кодирования как метод подстановок и многоалфавитные шифров.

Контрольные вопросы

1. Почему метод подстановки имеет слабую надежность?

Подстановочная криптограмма достаточно легко раскрывается с помощью составления частотных таблиц. Сложность раскрытия может быть повышена при использовании более большого алфавита подстановок, но это сказывается на производительности шифрования.

2. Что такое частотный анализ?

это метод изучения частоты появления определенных элементов в наборе данных или тексте. В основном, это подход используется для определения наиболее часто встречающихся элементов (например, символов, слов или фраз) в тексте или наборе данных. Этот анализ помогает выявить ключевые особенности, например, самые частые слова в тексте или наиболее распространенные символы в зашифрованных сообщениях.

3. Что является криптографическим ключом в методе перестановки?

Правило перестановок позиций символов в блоке символов заданной длины. Это правило определяет порядок, в котором символы в блоке строки должны быть перемещены.

4. Как связаны метод подстановки и многоалфавитные шифры?

Метод подстановки может быть использован при применении многоалфавитного шифра. Символы в исходном тексте могут быть заменены на соответствующие им знаки в подстановочном алфавите метода подстановки. При этом в многоалфавитных шифрах используются несколько подстановочных алфавитов, каждый из которых применяется к символам исходного текста в соответствии с определенными правилами для каждого алфавита.

5. В чем отличие криптографии от криптоанализа?

Криптография занимается созданием безопасных методов обработки информации, в то время как криптоанализ стремится обнаруживать и использовать возможные слабости в этих методах

6. По какому признаку шифры делят на симметричные и асимметричные?

По характеру используемого крипто ключа. В симметричных шифрах для кодирования и декодирования используется один и тот же ключ, в асимметричных же используются пары различных ключей (закрытый для зашифрования, открытый для расшифрования)