Дисциплина «Информационная безопасность телекоммуникационных систем**»**

Направление - 02.03.03 Математическое обеспечение и администрирование информационных систем

Профиль - Разработка и администрирование информационных систем

Лабораторная работа №1

Простое шифрование и дешифрование - шифр Цезаря

До появления компьютеров криптография состояла из символьных алгоритмов. Криптографические алгоритмы либо заменяли одни символы другими, либо переставляли символы. Лучшие алгоритмы делали и то и другое, причем многократно**.**

Подстановочные шифры

Подстановочным (substitution cipher) называется шифр, который каждый символ открытого текста заменяет другим символом в шифротексте. Получатель выполняет обратную подстановку в шифротексте, восстанавливая открытый текст. В классической криптографии существуют четыре типа подстановочных шифров.

Простой подстановочный шифр (simple substitution cipher), или моноалфавитный шифр (monoalphabetic cipher), - это шифр, который заменяет каждый символ открытого текста соответствующим символом шифротекста. Примером простых подстановочных шифров являются криптограммы в газетах.

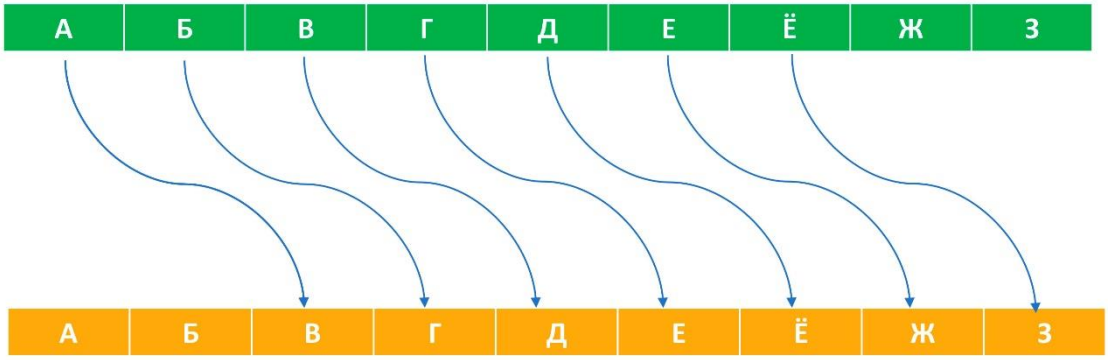
Омофонический подстановочный шифр (homophonic substitution cipher) похож на простую подстановочную криптосистему, за исключением того, что один символ открытого текста заменяется несколькими символами шифротекста. Например, букве A может соответствовать набор чисел 5, 13, 25 или 56, букве B — 7, 19, 31 или 42 и т.д.

Полиграммный подстановочный шифр (polygram substitution cipher) — это шифр, который заменяет одни блоки символов другими. Например, символам ABA могут соответствовать символы RTQ, символам ABB — символы SLL и т.д.

Полиалфавитный подстановочный шифр (polyalphabetic substitution cipher) состоит из нескольких простых подстановочных шифров. Например, можно использовать пять разных простых подстановочных фильтров так, что каждый символ открытого текста заменяется с использованием одного конкретного шифра.

Шифр Цезаря, также известный как **шифр** сдвига, код **Цезаря** или сдвиг **Цезаря** — один из самых простых и наиболее широко известных методов **шифрования**. **Шифр Цезаря** — это вид **шифра** подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него

в алфавите. Например, в **шифре** со сдвигом вправо на 1, А была бы заменена на Б, Б станет Г, и так далее:



Шифр Цезаря представляет собой простой подстановочный фильтр. На самом деле этот алгоритм еще проще, чем подстановочный, потому что алфавит шифротекста представляет собой результат смещения алфавита открытого текста, а не его случайную перестановку.

Лабораторная работа выполняется в среде Visual Studio 2019 с использование языка программирования Python. Начало работы определено в методических указаниях «*Среда Visual Studio 2019 и использование языка программирования Python для проектов дисциплины «Информационная безопасность телекоммуникационных систем*». Доступ в библиотеке сайта http://vikchas.ru

Формирование шифротекста

В начале программы определяем алфавиты русский и английский.

```
alfavit_EU =  'ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ'
alfavit_RU = 'АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ'

Вручную будет определяться шаг сдвига в шифротексте и сообщение для шифровки, переменные
smeshenie и message, а также переменная для шифротекста itog

smeshenie = int(input('Шаг шифровки: '))
message = input("Сообщение для шифровки: ").upper()
itog = ''
```

В программе можно использовать либо русский текст или английский. Вручную вводится тип языка.

```
lang = input('Выберите язык RU/EU: ')   #Добавляем возможность выбора языка
```

Алгоритм формирования шифротекста и его печать будет следующий:

```
if lang == 'RU':
    for i in message:
        mesto = alfavit_RU.find(i)   # Алгоритм для шифрования сообщения на русском
        new_mesto = mesto + smeshenie
        if i in alfavit_RU:
            itog += alfavit_RU[new_mesto]
        else:
            itog += i
else:
    for i in message:
        mesto = alfavit_EU.find(i)              # Алгоритм для шифрования сообщения на
английском
        new_mesto = mesto + smeshenie
        if i in alfavit_EU:
            itog += alfavit_EU[new_mesto]
        else:
            itog += i


print (itog)
```

Дешифровка шифротекста (сообщения)

Алгоритм дешифровки шифротекста вляется обратным шифровке. Изменения произойдут только в части величины шаг, знак должен указываться « - ».

```
alfavit_EU =  'ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ'
alfavit_RU = 'АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ'
smeshenie = int(input('Шаг дешифровки (не забудьте про знак): '))
message = input("Сообщение для Дешифровки: ").upper()
itog = ''
lang = input('Выберите язык RU/EU: ')
if lang == 'RU':
    for i in message:
        mesto = alfavit_RU.find(i)
        new_mesto = mesto + smeshenie
        if i in alfavit_RU:
            itog += alfavit_RU[new_mesto]
        else:
            itog += i
else:
    for i in message:
        mesto = alfavit_EU.find(i)
        new_mesto = mesto + smeshenie
        if i in alfavit_EU:
            itog += alfavit_EU[new_mesto]
        else:
            itog += i


print (itog)
```

ЗАДАНИЯ РАБОТЫ

1. Создать проект в среде Visual Studio 2019 с использование языка программирования Python.

2. Сформировать необходимое окружения языка Python из библиотек, необходимых для выполнения лабораторной работы.
3. Создать два файла-программы в языке python для шифровки и дешифровки.
4. Сформировать тексты программ, в соответствие с методическими указаниями, для шифровки и дешифровки.
5. Подготовить 4 примера – 2 на русском языке и 2 на английском для подготовки шифротекста. Примеры должны содержать правильные тексты (символы алфавита) и ошибочные.
6. Сформировать шифротексты.
7. Выполнить дешифровку шифротекстов.
8. Оформить отчет по работе с указанием описания алгоритма Цезаря, описания программ шифровки и дешифровки, описание примеров и указания недостатков и достоинств алгоритма Цезаря.