Отчёт по лабораторной работе №1. Шифры простой замены

Дисциплина: Математические основы защиты информации и информационной безопасности

Студент: Аронова Юлия Вадимовна, 1032212303
Группа: НФИмд-01-21
Преподаватель: д-р.ф.-м.н., проф. Кулябов Дмитрий Сергеевич

11 ноября, 2021, Москва

Цели и задачи работы

Цель лабораторной работы

Целью данной лабораторной работы является ознакомление с двумя простейшими методами шифрования: шифром Цезаря и шифром Атбаш, – а так же их реализация на произвольном языке программирования.

Задание

Задание 1
Реализовать шифр Цезаря с произвольным ключом k.

$$y = (x + k)\ mod\ m,$$

где x – символ открытого текста, y – символ шифрованного текста, m – мощность алфавита, k – ключ.

Задание 2
Реализовать шифр Атбаш.

$$y = m - x - 1$$

Ход выполнения и результаты

Шифр Цезаря. Реализация

```
n_eng = 26 # мощность английского алфавита
n_rus = 32 # мощность русского алфавита


lang_dict = {
    "eng" : {"a" : ord('a'), "z" : ord('z'), "m" : n_eng},
    "rus" : {"a" : ord('а'), "z" : ord('я'), "m" : n_rus}
    }
```

Шифр Цезаря. Реализация

```
def shift(letter, k, language):
    a = ord(letter) # Unicode-код символа

    # если этот символ буквенный..
    if lang_dict[language]['a'] <= a <= lang_dict[language]['z']:
        T_new = (a - lang_dict[language]['a'] + k) %
          % lang_dict[language]['m'] +
          + lang_dict[language]['a']

        return chr(T_new) # и возвращаем новую букву
    else: # иначе..
        return letter # возвращаем символ без изменений
```

Шифр Цезаря. Реализация

```
def caesar_encrypt(message, k):
    message_encrypted = []
    caps = [True if letter.isupper() else False for letter in message]
    if lang_dict['eng']['a'] <= ord(message[0].lower())
                                        <= lang_dict['eng']['z']:
        language = "eng" <...>
    for i in range(len(message)):
        message_encrypted.append(shift(message.lower()[i], k, language))
    for i in range(len(caps)):
        if caps[i]:
            message_encrypted[i] = message_encrypted[i].upper()
    return "".join(message_encrypted)
```

Шифр Цезаря. Результаты

```
[3]  print(caesar_encrypt("Veni, vidi, vici", 3))
     print(caesar_encrypt("Festina lente", 1))
     print(caesar_encrypt("Пришёл, увидел, победил", 7))
     ✓ 0.4s

...  Yhql, ylgl, ylfl
     Gftujob mfouf
     Цчпяёт, ъйплмт, цхимлпт
```

Figure 1: Результат шифрования сообщений шифром Цезаря с различным k

Шифр Атбаш. Реализация

```
eng_abc = [chr(code) for code
      in range(lang_dict['eng']['a'], lang_dict['eng']['z'] + 1)]
eng_abc.append(' ')

rus_abc = [chr(code) for code
      in range(lang_dict['rus']['a'], lang_dict['rus']['z'] + 1)]
rus_abc.append(' ')

abc_s = {
    "eng" : eng_abc,
    "rus" : rus_abc
}
```

Шифр Атбаш. Реализация

```
def atbash_encrypt(message):
    message_encrypted = []
    caps = [True if letter.isupper() else False for letter in message]

    if message[0].lower() in eng_abc[:-1]:
        language = "eng"
    <...>

    abc = abc_s[language] # получаем алфавит соответствующего языка
    cba = list(reversed(abc)) # записываем его в обратном порядке

    # приводим сообщение к нижнему регистру
    message_lowered = message.lower()
```

Шифр Атбаш. Реализация

```
for i in range(len(message)): # для каждого символа в сообщении:
    if message_lowered[i] in abc:
        code = abc.index(message_lowered[i])
        message_encrypted.append(cba[code])
    else:
        message_encrypted.append(message_lowered[i])

for i in range(len(caps)):
    if caps[i]:
        message_encrypted[i] = message_encrypted[i].upper()

return "".join(message_encrypted)
```

Шифр Атбаш. Результаты

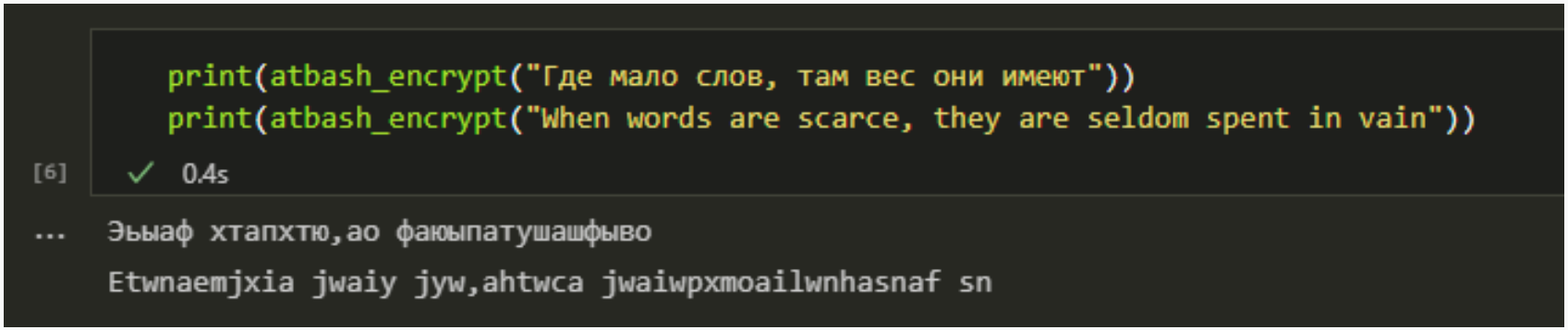

Figure 2: Результат шифрования сообщений шифром Атбаш

Спасибо за внимание