Стандарт

Вычислительная практика, 2021

Цели и задачи

Создать стандарт для удобства программиста,который описывает работу алгоритма шифрования и дешифрования Цезаря

Основные задачи, которые нужно реализовать в ходе разработки проекта:

- Описать как будет создаваться алфавиты(русский и английский язык) для шифрования
- При помощи чего будет шифроваться
- Сама шифровка

Код

1. Алфавит
   Создаются 2 списка(заглавных букв и строковых), первоначально состоящих с русского алфавита,далее с английского

```
193
194  # creating alphabets for encrypting and decrypting messages
195  lower_cyrillic = ''.join(map(chr, range(ord('а'), ord('я') + 1)))
196  upper_cyrillic = ''.join(map(chr, range(ord('А'), ord('Я') + 1)))
197  lower_eng = ''.join(map(chr, range(ord('a'), ord('z') + 1)))
198  upper_eng = ''.join(map(chr, range(ord('A'), ord('Z') + 1)))
199  lower_cyrillic = lower_cyrillic + lower_eng
200  upper_cyrillic = upper_cyrillic + upper_eng
201
```

2. Сдвиги алгоритмов для будущей шифровки/дешифровки

Будет использовать в алгоритме шифрования/дешифрования, возвращает значение с определенным сдвигом из списков, разработанных выше(*строчки кода 194-200*)

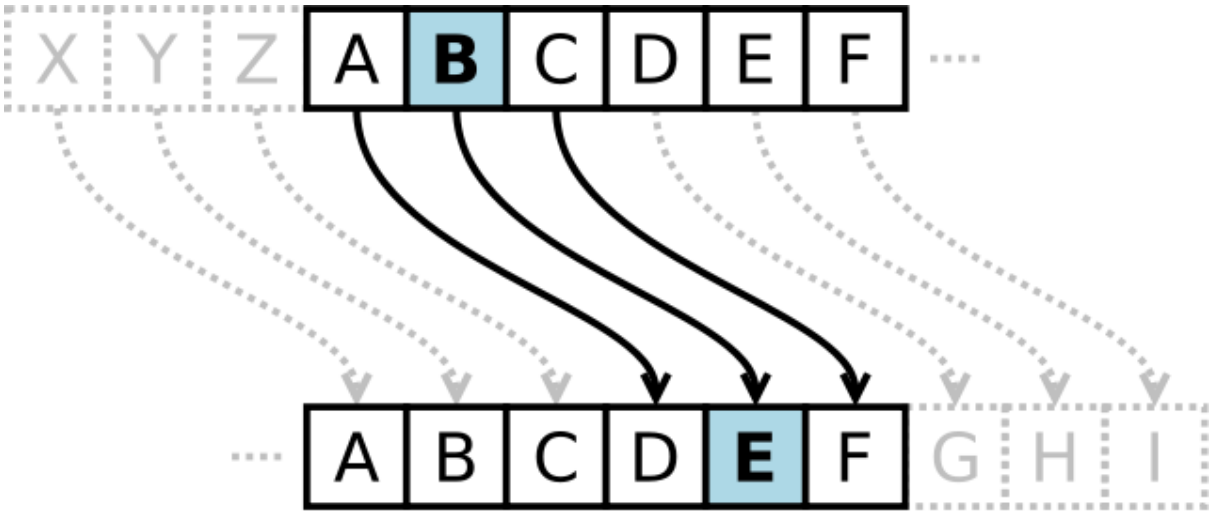
```
202
203   # shifting alphabet on particular number
204   def alphabet(shift):
205       return lower_cyrillic[shift:] + \
206              lower_cyrillic[:shift] + \
207              upper_cyrillic[shift:] + \
208              upper_cyrillic[:shift]
209
```

3. Функция шифрования/дешифрования сообщений

Значение по умолчанию на сдвиг равняется 3. Сначала мы объединяем сдвиги заглавных и строчных букв(строчка кода 213). Мы устанавливаем сдвиг на сколько необходимо произвести(строчка кода 214). Далее просто происходит шифровка/дешифровка.

```
210
211   # function for encrypting\decrypting message
212   def coding(typ="enc", shift=3):
213       a1 = lower_cyrillic + upper_cyrillic
214       a2 = alphabet(shift)
215
216       t = {
217           "enc": str.maketrans(a1, a2),
218           "dec": str.maketrans(a2, a1)
219       }
220
```

Немного о самом алгоритме



Математическая формула:

$$C_i = (a_i + k) \, mod \, n$$

где:

a_i – символ исходного текста;

k – ключ;

n – мощность алфавита.

В методе Цезаря используется k. Развитием этого метода является метод, основанный на свойстве децимации. $C_i = (a_i + k) \, mod \, n$

Децимация– выборка k–тых элементов.Номера символов в шифротексте в k раз больше номеров символов исходного текста, где номер относится к алфавиту, а не исходному тексту.

Время работы шифра Цезаря - это *O(1)*. Так как размер алфавита постоянен.

Но время работы в *худшем состоянии T(n)* .