Криптографический алгоритм замены Юлия Цезаря

Криптография

Классический алгоритм Юлия Цезаря

- Потребность в защите информации существовала издревле. Исторически вплоть до середины XX-го в. все существовавшие алгоритмы можно было разделить на два основных вида сокрытия секретных сообщений: алгоритмы замены, в которых каждый символ секретного сообщения заменялся на другой символ по определенным правилам, известным только посвященным; алгоритмы перестановки, в которых все символы перемешивались по определенным правилам и являлись секретом.

- Так, например, одним из самых известных в истории способов сокрытия важной секретной информации является алгоритм Юлия Цезаря, названный, согласно легендам, в честь его изобретателя.
- В классическом алгоритме Юлия Цезаря каждый символ исходного секретного сообщения заменяется символом из того же алфавита, отстоящим на три позиции далее. Например, для русского алфавита буква А будет заменена на букву Г, Б – на Д и т. д. Данный алгоритм относится к алгоритмам замены.
- Рассмотрим реализацию алгоритма Юлия Цезаря на языке Python:

- Задача. На вход программе подается секретное сообщение, состоящее не более, чем из 200 символов, заканчивающееся точкой (другие точки во входных данных отсутствуют). Необходимо зашифровать его следующим образом: заменить каждую английскую букву на букву, стоящую в английском алфавите на 3 буквы далее (алфавит считается циклическим, т.е., перед буквой A стоит буква Z), оставив другие символы неизменными. Строчные буквы при этом остаются строчными, а прописные – прописными.

- Требуется написать программу, которая будет выводить на экран текст зашифрованного сообщения. Например, если исходный текст был таким:

Zb Ra Cx Dyk.,

- То результат шифровки должен быть следующий:

Ce Ud Fa Gbn.

- Решение:
- Из условия задачи известно, что длина секретного сообщения не превышает 200 символов. Это означает, что для хранения секретного (secret_text) и зашифрованного (cypher_text) сообщений можно использовать строковый тип данных string. Само сообщение может содержать 4 типа символов, каждый из которых необходимо обработать в отдельности: строчные (маленькие) буквы; прописные (большие) буквы; точка; остальные символы. Каждую строчную букву необходимо преобразовать в строчную, отстоящую на три позиции в английском алфавите, каждую прописную – преобразовать в прописную, отстоящую на три позиции в английском алфавите, все остальные символы необходимо оставить без изменений, а если очередным символом оказалась точка, то закончить шифрование и вывести результат:

- Код реализации:

```
secret_text = input("Введите ваше мегасекретное сообщение: ")
cypher_text = "" # зашифрованный текст
for symbol in secret_text:
    if symbol == '.': # очередной символ - точка
        cypher_text += symbol
        break # выход из цикла, т.к сообщение закончилось
    elif ord(symbol) in range(ord('A'), ord('Z') + 1):
        if (ord(symbol) + 3) > ord('Z'):
            cypher_text += chr(ord(symbol) + 3 - 26)
        else:
            cypher_text += chr(ord(symbol)+ 3) # очередной символ - большая буква
    elif ord(symbol) in range (ord('a'), ord('z') + 1):
        if (ord(symbol) + 3) > ord('z'):
            cypher_text += chr(ord(symbol) + 3 - 26)
        else:
            cypher_text += chr(ord(symbol) + 3)
    else:
        cypher_text += symbol # любой другой символ
print(cypher_text)
```

- Разновидности криптографического алгоритма Юлия Цезаря
- Следует отметить, что существует бесконечное множество разновидностей криптографического алгоритма Юлия Цезаря. Приведем некоторые из возможных модификаций условия данного алгоритма:

1. замена каждой буквы алфавита на букву, стоящую в английском алфавите на K букв далее (алфавит считается циклическим, т.е., перед буквой A стоит буква Z), оставив другие символы неизменными. Строчные буквы при этом остаются строчными, а прописные – прописными;

2. замена каждой буквы алфавита на букву, стоящую в английском алфавите на K букв ранее (алфавит считается циклическим, т.е., перед буквой A стоит буква Z), оставив другие символы неизменными. Строчные буквы при этом остаются строчными, а прописные – прописными;
3. Замена каждой буквы алфавита на букву, стоящую в английском алфавите на K букв далее (алфавит считается циклическим, т.е., перед буквой A стоит буква Z), оставив другие символы неизменными. Строчные буквы при этом преобразуются в прописные, а прописные остаются прописными;

4. замена каждой буквы алфавита на букву, стоящую в английском алфавите на K букв ранее, оставив другие символы неизменными. Строчные буквы при этом преобразуются в прописные, прописные остаются прописными, каждая цифра заменяется на следующую за ней, другие символы остаются неизменными (алфавит считается циклическим, т.е., перед буквой A стоит буква Z, перед цифрой 0 – цифра 9).