Шифрование гаммированием конечной гаммой.

Меньшов Иван Сергеевич

20 ноября, 2021, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

Цель лабораторной работы

Изучение алгоритма гаммированием конечной гаммой.

Выполнение лабораторной работы

Шифр гаммированием конечной гаммой

В методе гаммирования шифрование выполняется путем сложения символов исходного текста и ключа по модулю, равному числу букв в алфавите. Если в исходном алфавите, например, 33 символа, то сложение производится по модулю 33. Такой процесс сложения исходного текста и ключа называется в криптографии наложением гаммы.

Контрольный пример (код)

```python
# Вводим алфавит и ключ
word_to_encode = input("Введите фразу для шифрования: ").upper()
key_word = input("Введите ключ: ").upper()
# Растягиваем ключ на длину слова
if len(key_word) < len(word_to_encode):
    k = (len(word_to_encode) % len(key_word))
    key_word = '' + key_word * (len(word_to_encode) // len(key_word)) + key_word[:k]
# Формируем алфвавит и порядковый словарь
alphabet = 'АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ'
alp_dict = {letter: idx + 1 for idx, letter in enumerate(alphabet)}
# процесс кодировки
encoded_word = ''
for word_letter, key_letter in zip(word_to_encode, key_word):
    encoded_word += list(alp_dict.keys())[(alp_dict[word_letter] + alp_dict[key_letter] % len(alphabet))-1]
print("Зашифрованное сообщение: ", encoded_word)
# процесс декодировки
word_to_decode = input("Введите фразу для дешифрования: ").upper()
decoded_word = ''
for word_letter, key_letter in zip(word_to_decode, key_word):
    decoded_word += list(alp_dict.keys())[(alp_dict[word_letter] - alp_dict[key_letter] % len(alphabet))-1]
print("Расшифрованное сообщение: ", decoded_word)

```

Figure 1: Програмный код

Контрольный пример (алгоритм)

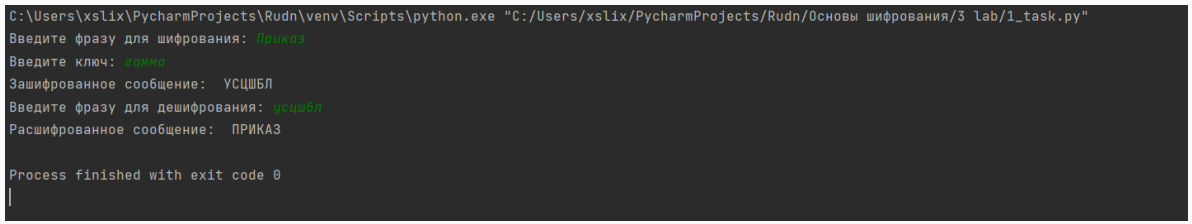

Figure 2: Работа кода

Выводы

Результаты выполнения лабораторной работы

Изучили работу алгоритма гаммированием конечной гаммой.