

# Лабораторная работа №3

## Шифрование гаммированием

---

ВОЛКОВА ДАРЬЯ АЛЕКСАНДРОВНА НПММД-02-21

# Цель работы

---

Изучение алгоритма шифрования гаммированием конечной гаммой.

# Задачи

---

Программная реализация алгоритма шифрования гаммированием конечной гаммой

# Теоретические сведения

---

Частным случаем многоалфавитной подстановки является гаммирование. В этом способе 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.

Гамма шифра – псевдослучайная последовательность, вырабатываемая по определенному алгоритму, используемая для шифровки открытых данных и дешифровки шифротекста.

Обычно разделяют две разновидности гаммирования – с конечной и бесконечной гаммами.

# Результаты

```
: # Шифрование гаммированием конечной гаммой
```

```
: message = input('Введите строку: ').lower()  
: gamma = str(input('Введите гамму: ')).lower()
```

Введите строку: приказ  
Введите гамму: гамма

```
: alphabet = 'абвгдежзийклмнопрстуфхцщъыьэя'
```

```
: n = len(gamma)  
: m=len(message)
```

```
: k = (m % n) # Количество символов которые нужно дополнить  
: gamma_len = '' + gamma * (m // n) + gamma[:k]  
: print(message, gamma_len, sep='\n')
```

приказ  
гаммаг

```
: c=[]
```

```
: for i in range(m):  
:     c.append(alphabet.find(message[i])+(alphabet.find(gamma_len[i])+1)%33)
```

```
: encrypted = ''
```

```
: for i in range(len(c)):  
:     encrypted+=alphabet[c[i]]
```

```
: print('Криптограмма:', encrypted)
```

Криптограмма: усхчбл

Пример работы алгоритма шифрование гаммированием конечной гаммой

# Выводы

---

В ходе выполнения работы удалось изучить алгоритм шифрования гаммированием конечной гаммой, а также реализовать данный алгоритм программно на языке Python.