

# Отчёт по лабораторной работе № 3

---

Нирдоши Всеволод Раджендер

12 Октября 2024

РУДН, Москва, Россия

## Лабораторная работа № 3

---

1. Для шифрования была использована гамма, сгенерированная на основе рекуррентного соотношения  $\gamma_i = a \cdot \gamma_{i+1} + b \bmod m$ , где параметры  $a$ ,  $b$  и  $m$  заданы согласно условиям задачи.

```
def encrypt(letters_pair: tuple): idx = (letters_pair[0] + letters_pair[1]) % m return idx
```

2. Операция модульного сложения была применена к каждому символу сообщения и соответствующему символу гаммы для получения зашифрованного текста. Формула шифрования:  $c_i = (p_i + k_i) \bmod N$ , где  $p_i$  – это  $i$ -й символ исходного сообщения,  $k_i$  –  $i$ -й символ гаммы,  $N$  – количество символов в алфавите.

```
for i in range(len(message_ind) - len (gamma_ind)):
    gamma_ind.append(gamma_ind[i % len(gamma_ind)])

print(f'{message.upper()} -> {message_ind}')
print(f'{gamma.upper()} -> {gamma_ind}')

encrypted_ind = list(map(lambda s: encrypt(s), zip(message_ind, gamma_ind

print(f'ENCRYPITION FORM: {encrypted_ind}\n')

return ''.join(list(map(lambda s: alphabet[s],encrypted_ind))).upper()
```

3. В ходе работы были проведены эксперименты с различными значениями параметров гаммы для проверки влияния длины и равномерности гаммы на стойкость шифра.

```
def test_encryption(message: str, gamma: str):  
    print(f'ENCRYPTION RESULT: {gamma_encryption(message, gamma)}')
```

  

```
def main():  
    message = "приказ"  
    gamma = "гамма"  
    print("TEST 1")  
    test_encryption(message, gamma)  
  
    message = "здравствуйте"  
    gamma = "привет"  
    print("TEST 2")  
    test_encryption(message, gamma)
```

```
if __name__ == "__main__":  
    main()
```

TEST 1

ПРИКАЗ -> [15, 16, 8, 10, 0, 7]

ГАММА -> [3, 0, 12, 12, 0, 3]

ENCRYPTION FORM: [18, 16, 20, 22, 0, 10]

ENCRYPTION RESULT: ТРФЦАК

TEST 2

ЗДРАВСТВУЙТЕ -> [7, 4, 16, 0, 2, 17, 18, 2, 19, 9, 18, 5]

ПРИВЕТ -> [15, 16, 8, 2, 5, 18, 15, 16, 8, 2, 5, 18]

ENCRYPTION FORM: [22, 20, 24, 2, 7, 3, 1, 18, 27, 11, 23, 23]

ENCRYPTION RESULT: ЦФШВЗГБТЫЛЧЧ



В ходе лабораторной работы были изучены принципы шифрования методом гаммирования. Полученные результаты показали, что стойкость шифра напрямую зависит от длины гаммы и её равномерности. При использовании псевдослучайной последовательности генератора гаммы шифр становится устойчивым к криптоанализу, но в случае периодичности гаммы возможно упрощение расшифровки. Таким образом, для достижения максимальной стойкости шифрования необходимо выбирать параметры генерации гаммы так, чтобы она была как можно более случайной и непредсказуемой.

Спасибо за внимание!