

# Отчёт по лабораторной работе №3.

## Шифрование гаммированием

---

*Дисциплина: Математические основы защиты информации  
и информационной безопасности*

**Студент:** Агеева Анастасия Сергеевна, 1032212304

**Группа:** НФИмд-02-21

**Преподаватель:** д-р.ф.-м.н., проф. Кулябов Дмитрий Сергеевич

27 ноября, 2021, Москва

# Прагматика

---

## Прагматика данной лабораторной работы

- В рамках дисциплины “Математические основы защиты информации и информационной безопасности” нам необходимо изучить ее разделы. Данная лабораторная работа входит в раздел “Шифрование”.
- Данная работа необходима для более глубоко и детального понимания работы алгоритмов шифрования.

# Цель

---

## Цель выполнения данной лабораторной работы

- Цель данной лабораторной работы изучение реализации алгоритма шифрования гаммированием.

# Задачи

---

# Задачи выполнения данной лабораторной работы

1. Реализовать программно шифрование гаммированием.

# **Результаты выполнения данной лабораторной работы**

---



# Шифрование гаммированием

```
In [3]: def gamming(k, mes, alp):  
    alp = list(alp)  
    k = list(k)  
    mes = list(mes)  
    n = len(alp)  
    while len(k) < len(mes):  
        k += k  
    k = k[:len(mes)]  
    # print(alp, k, mes, n)  
    mes_i = []  
    for i in range(len(mes)):  
        for j in range(n):  
            if mes[i] == alp[j]:  
                mes_i.append(j)  
    k_i = []  
    for i in range(len(k)):  
        for j in range(n):  
            if k[i] == alp[j]:  
                k_i.append(j)  
    # print(mes_i, k_i)  
    new_mes = []  
    for i in range(len(mes_i)):  
        new_mes.append(alp[(mes_i[i]+k_i[i])%n])  
    new_mes = ''.join(new_mes)  
    return new_mes
```

**Figure 1:** Шифрование гаммированием

- Шифрование гаммированием:

```
In [2]: key = 'гамма'  
message = 'приказ'  
alphabet = 'абвгдеёжзийклмнопрстуфхцщъыьэя'
```

**Figure 2:** Входные данные шифрование гаммированием

```
In [4]: new_message = gamming(key, message, alphabet)  
  
In [5]: print(message, "- сообщение")  
        print(new_message, "- зашифрованное сообщение")  
  
приказ - сообщение  
трхчак - зашифрованное сообщение
```

**Figure 3:** Результат программы шифрование гаммированием

- Исходя из теоретических сведений, программы выполнены без ошибок, чему свидетельствуют полученные результаты.
- В ходе выполнения данной работы были выполнены поставленные цели и задачи.