Отчёт по лабораторной работе №3. Шифрование гаммированием

Дисциплина: Математические основы защиты информации и информационной безопасности

Студент: Майорова О.А., 1032212322
Группа: НФИмд-02-21
Преподаватель: д.ф.-м.н., Кулябов Д. С.

Москва, 2021

Цель и задачи

Цель: Ознакомиться с шифрованием гаммированием.

Задача: Программно реализовать алгоритм шифрование гаммированием конечной гаммой.

Теоретическое введение

Гаммирование - метод симметричного шифрования, заключающийся в сложении символов исходного текста и ключа (гаммы) по модулю, равному числу букв в алфавите.

Можно записать правило гаммирования следующим образом:

$$z = x + k(mod N),$$

где x - исходный символ, k - символ гаммы, z – закодированный символ, N - количество символов в алфавите.

Если гамма короче, чем сообщение, предназначенное для зашифрования, гамма повторяется требуемое число раз.

Шифрование гаммированием

Исходный текст - “приказ”; гамма - “гамма”.

```
1 gamm('приказ', 'гамма')
```

```
'усхчбл'
```

Исходный текст - “order”; гамма - “gamma”.

```
1 gamm('order', 'gamma')
```

```
'vsqrs'
```

Заключение

Таким образом, была достигнута цель, поставленная в начале лабораторной работы. Было осуществлено знакомство с новым методом шифрования - шифрованием гаммированием. Также была получена реализация алгоритма шифрования гаммированием конечной гаммой для русского и английского алфавита нижних регистров на языке Python.

Спасибо за внимание