

**МИНОБРНАУКИ РОССИИ**

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«МИРЭА – Российский технологический университет»**

|  |
| --- |
| **РТУ МИРЭА** |
|  |
| **Институт кибербезопасности и цифровых технологий (ИКБ)** |
|  |
| КБ-2 «Информационно-аналитические системы кибербезопасности» |

**ОТЧЕТ О ВЫПОЛНЕНИ ЛАБОРАТОРНОЙ РАБОТЫ №9**

**В РАМКАХ ДИСЦИПЛИНЫ «МЕТОДЫ И СРЕДСТВА КРИПТОРГАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ»**

Выполнил:

Студент 3-ого курса

Учебной группы БИСО-02-22

Зубарев В.С.

**1. Одноалфавитная замена**

Ключевое пространство — это количество возможных перестановок алфавита. Если алфавит содержит n символов, то ключевое пространство будет равно числу чимволов:

K=n

В семестре было реализована одноалфавитная замена с мощностью алфавита 256 (ASCII 1251).

К = 256

**2. Перестановка**

Если перестановка меняет местами все n символов в сообщении, то ключевое пространство для перестановки определяется числом возможных перестановок:

K=n!

В семестре была реализована перестановка с длинной ключа 4 и 5

При длине ключа 4, K = 4! = 24  
При длиннее ключа 5, К = 5! = 120

**3. Дополнение до 255 (инверсный метод)**

Для инверсного метода шифрования с таблицей ASCII 1251 ключ не имеет вариаций, так как он всегда один и тот же: для каждого символа выполняется операция Tш= 256 – ​То.

Таким образом, количество возможных ключей для инверсного метода шифрования будет:

K=1

**4. Многоалфавитный метод с ключом произвольной длины**

Для многоалфавитного метода с произвольной длиной ключа, количество возможных ключей будет бесконечным, так как длина ключа может быть произвольной. В этом случае мы можем только рассматривать теоретически возможное количество ключей с условием что ключи не превосходят длину L:

K=, где n – мощность алфавита.

В семестре рассматривалось шифрование с мощностью алфавита 256 и ключом 5.

К = =1 103 823 438 080

**5. Гаммирование**

Метод гаммирования включает использование ключа, который складывается с открытым текстом (например, с помощью XOR). Если длина ключа равна n, то ключевое пространство для гаммирования для алфавита m будет равно количеству возможных битовых последовательностей длины n:

K=mn  
В семестре рассматривалось шифрование с ключом длинны 4  
K = 2564=4 294 967 296  
С точки зрения побитового сложения, каждый символ открытого текста и гаммы преобразовывался в 8 бит (в соответствии с таблицей ASCII 1251). Это позволяет сказать, что K= 2n, где n – длина гаммы в битах. В случае с ключом из 4 значений n = 4\*8 = 32 бит  
K = 232=4 294 967 296

**6. Таблица Виженера**

Таблица Виженера использует повторяющийся ключ для шифрования. Ключевое пространство зависит от длины ключа и размера алфавита. Если алфавит содержит n символов и длина ключа равна k, то ключевое пространство будет равно:

K=nk

В cсеместре рассматривалось шифрование с помощью таблицы ASCII 1251 (256 символов) и ключом длинны 4.

К = 2564= 4 294 967 296

**7. Таблица Плейфера**

Таблица Плейфера использует матрицу MxM, содержащую M2 символов. Матрица выбирается так что M2 >= n, где n – кол-во символов алфавита. Ключевое пространство зависит от того, сколько возможных ключей можно создать, переставляя эти символы. Количество возможных ключей будет равно:

K=M2!

В Семестре рассматривалось шифрование латиницы (мощность алфавита 25, М = 5).  
К = 52! = 15 511 210 043 330 985 984 000 000

**8. Классическая сеть Фейстеля**

Ключевое пространство зависит от длины ключа, который делится на части. Если ключ состоит из n бит и делится на несколько частей, то ключевое пространство будет зависеть от числа возможных вариантов для каждой части.

К =2n

В семестре рассматривался 64-битный исходный ключ

K=264=18 446 744 073 709 551 616