Исследование криптографических шифров на основе подстановки (замены) символов

Выполнил: Макаров Алексей Игоревич, 3 курс 4 группа 2 подгруппа

2024

**Ход работы**

В результате выполнения лабораторной работы было выполнено зашифрование/расшифрование текстового документа, созданного на основе алфавита языка в соответствии с таблицей вариантов задания, а имеено с алфавитом немецкого языка, согласно 4 варианту. Были использованы следующие шифры: на основе следующих соотношений для зашифрования



и расшифрования:

,

где k = 7, а N= 30 для немецкого алфавита.

Так же использовалась таблица Трисемуса, где ключевое слово – enigma.

Сущность подстановочного шифрования состоит в том, что исходный текст (из множества М) и зашифрованный текст (из множества С) основаны на использовании одного и того же или разных алфавитов, а тайной или ключевой информацией является алгоритм подстановки. Первый упомянутый шрифт соответсвует классическому шифру подстановки – шифру Цезаря. Реализация шифра представлена в листинге 1.

|  |
| --- |
| def substitution\_cipher(text, alphabet, k, decrypt=False):  if decrypt:  k = -k  cipher\_text = ''  for char in text:  if char in alphabet:  cipher\_text += alphabet[(alphabet.index(char) + k) % len(alphabet)]  else:  cipher\_text += char  return cipher\_text |

Листинг 1 – Реализация кода зашифрования/расшифрования сообщения

Результатом работы кода должны быть гистограммы частот. По гистограммам частот можно определить, какие символы чем заменены. Выполнение данного кода представлено на рисунке 1.

A graph of different sizes and numbers

Description automatically generated with medium confidence

Рисунок 1 – Гистограммы частот в зашифрованном/расшифрованном сообщении

Таблица Трисемуса. В 1518 г. в развитии криптографии был сделан важный шаг благодаря появлению в Германии первой печатной книги по криптографии. Аббат Иоганнес Трисемус, настоятель монастыря в Вюрцбурге, написал книгу «Полиграфия», в которой он описал ряда шифров, один из которых развивает идею многоалфавитной подстановки. Зашифрование осуществляется так: заготавливается таблица подстановки (так называемая «таблица Трисемуса» – таблица со стороной, равной N, где N – мощность алфавита), где первая строка – это алфавит, вторая – алфавит, сдвинутый на один символ, и т. д. При зашифровании первая буква открытого текста заменяется на букву, стоящую в первой строке, вторая – на букву, стоящую во второй строке, и т. д. После использования последней строки вновь возвращаются к первой.

Реализация шифра таблицы Трисемуса представлен в листинге 2.

|  |
| --- |
| def trisemus\_cipher(text, key, alphabet, k, decrypt=False):  key = ''.join(sorted(set(key), key=key.index)) *# Удаление дубликатов из ключа и сохранение порядка* grid = key + ''.join([char for char in alphabet if char not in key]) *# Создание сетки Трисемуса* if decrypt:  k = -k  cipher\_text = ''  for char in text:  if char in grid:  cipher\_text += grid[(grid.index(char) + k) % len(grid)] *# Шифрование/дешифрование символа* else:  cipher\_text += char return cipher\_text |

Листинг 2 – Реализация шифра таблицы Трисемуса

Результат работы представлен на рисунке 2.

A graph of different sizes and numbers

Description automatically generated with medium confidence

Рисунок 2 – Гистограммы частот

Таким образом, была разработана программа для зашифрования/расшифрования текстового документа, на основе которых были сделаны гистограммы частот