МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ «МИСИС»
ИНСТИТУТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И КОМПЬЮТЕРНЫХ НАУК
КАФЕДРА АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ

Лабораторная работа №3

«Криптоанализ шифра простой замены»

по дисциплине

«Информационная безопасность и кодирование»

Выполнила:
студентка группы БИВТ-21-4
Савенко Е. И.

Проверил:
Гончаренко А. Н.

Москва, 2025

Цель работы: Выполнить криптоанализ текста, зашифрованного шифром простой замены с применением неперебoрного метода вскрытия шифротекста.

Задачи:

- Использовать результаты сравнения статистических характеристик символов шифртекста и русского языка для определения предварительных значений нескольких символов в шифртексте.
    - Выполнить частотный анализ символов зашифрованного текста.
    - Выписать символы из шифртекста с частотой большей 0,04 и произвести ранжирование их в порядке убывания частоты.
    - Сравнить ранги символов шифртекста с рангами символов в рус-
    - ском языке.
    - Выбрать 3–4 наиболее частых символа в шифртексте и русском языке с одинаковыми рангами.
    - Заменить три или четыре символа в шифртексте на символы русского языка с теми же рангами. Проверить совпадение рангов замененных символов в шифртексте и соответствующих символов в русском языке. Например, буква «о» самая частая буква в русском языке – она же должна оказаться самой частой буквой в шифртексте.
- Использовать результаты грамматического анализа шифртекста и на его основе произвести полное дешифрование текста.
    - Выполнить предварительный анализ и расшифровку коротких слов (предлогов, местоимений, союзов междометий и т.п.) с использованием результатов, полученных в п. 1.5.
    - Для идентификации остальных символов шифртекста воспользоваться особенностями русского языка (удвоения букв, окончания слов и т.п.).

Ход работы:

Зашифрованное сообщение:

Ъыщбпьь шпцжтй ъщшйэж, щьшкшщмум пнщ.

Произведем частотный анализ шифрованного текста (таблица 1).

Таблица 1 – Распределение частот шифрованного текста.

Буква	Частота
Щ	0,1613
Ш	0,129
П	0,0968
Ь	0,0968
Ъ	0,0645

Ж	0,0645
Й	0,0645
М	0,0645
Ы	0,0323
Б	0,0323
Ц	0,0323
Т	0,0323
Э	0,0323
К	0,0323
У	0,0323
Н	0,0323

Произведем ранжирование символов с частотой большей 0,04 (таблица 2).

Таблица 2 – Ранжирование символов.

Буква	Ранг
Щ	1
Ш	2
П	3
Ь	3
Ж	4
Й	4
М	4
Ъ	4

Согласно таблице частоты появления символов в среднестатистическом тексте для русского языка:

— “О” – символ первого ранга

— “Е” – символ второго ранга

— “А” и “И” – символы третьего ранга

— “Н” и “Т” – символы четветного ранга

Заменим символы одного ранга в зашифрованном сообщении (таблица 3).

Таблица 3 – Замена символов согласно рангу.

Ранг	Шифр	Замена	Ъыщбпьь шпцжтй ъщшйэж, щьшкшщмум пнщ.
1	Щ	О	Ъыобаьь еацнтй ъоейэн, оьекеомум ано.
2	Ш	Е	
3	П	А	
4	Ж	Н	
1	Щ	О	Ъыобаьь еацттй ъоейэт, оьекеомум ано.
2	Ш	Е	
3	П	А	

4	Ж	Т	
1	Щ	О	Ъыобаьь еацжтн ъоенэж, оьекеомум ано.
2	Ш	Е	
3	П	А	
4	Й	Н	
1	Щ	О	Ъыобаьь еацжтт ъоетэж, оьекеомум ано.
2	Ш	Е	
3	П	А	
4	Й	Т	
1	Щ	О	Ъыобаьь еацжтй ъоейэж, оьекеонун ано.
2	Ш	Е	
3	П	А	
4	М	Н	

К сожалению, высказывать предположения об оригинальном сообщении с подобной дешифрацией невозможно, так как замена символов одного ранга не соответствует действительности.

Попробуем провести расшифровку коротких слов и выявим при каком ключе k все символы могут иметь логическое значение:

k	Расшифровка
1	омш
2	нлч
3	мкц
4	лйх
5	киф
6	йзу
7	ижт
8	зёс
9	жер
10	ёдп
11	его
12	двн
13	гбм
14	вал
15	бяк
16	аюй
17	яэи
18	юьз
19	эыж
20	ьъё
21	ыще
22	ъшд

23	щчг
24	шцв
25	чхб
26	цфа
27	хуя
28	фтю
29	усэ
30	трь
31	спы
32	роъ
33	пнщ

Таким образом из всех комбинаций имеет смысл слово при k=11. Проверяя догадку и дешифруя сообщение, получаем:

“Процесс нельзя понять, оснановив его.”

Контрольные вопросы

1) Что такое энтропия языка?

Энтропия языка — это мера неопределенности или случайности в тексте на определенном языке. В контексте криптографии энтропия показывает, насколько сложно предсказать следующий символ в тексте на основе предыдущих.

2) Что понимается под избыточностью сообщения?

Избыточность сообщения — это количество лишней информации в сообщении, которая не влияет на его основное содержание, но помогает обеспечить устойчивость к ошибкам или облегчить дешифрование. В контексте языка избыточность связана с повторяющимися элементами, которые помогают восстанавливать информацию при передаче или дешифровке.

3) Что такое шифр простой замены?

Шифр простой замены — это метод шифрования, при котором каждый символ открытого текста заменяется другим символом из алфавита согласно заранее составленной таблице или ключу замены. Это простая форма подстановки, где один символ заменяется на другой без учета других символов.

4) В чем состоит обобщение шифра Цезаря?

Обобщение шифра Цезаря заключается в том, что вместо фиксированного сдвига на определенное количество символов, как в классическом шифре, сдвиг может быть произвольным, т.е. каждый символ может заменяться на другой по разным правилам или сдвигам, в зависимости от его позиции или других факторов.

5) Опишите краткую историю возникновения шифра Цезаря.

Шифр Цезаря был назван в честь Юлия Цезаря, который использовал его для безопасной переписки с генералами. Он использовал сдвиг на три буквы в алфавите, чтобы скрыть содержание сообщений от посторонних. Этот шифр был одним из первых известных методов шифрования.

6) Объясните принцип дешифрования шифра простой замены.

Дешифрование шифра простой замены заключается в том, чтобы по таблице замены восстановить исходные символы. Каждому зашифрованному символу находится соответствующий символ открытого текста, используя обратную таблицу замены или ключ.

7) Объяснить, почему при вскрытии шифра простой замены используется не полное ранжирование по частоте всех символов русского языка, а лишь 3-4 наиболее частых символов, как в п. 1.4?

Использование частотного анализа основано на том, что в любом языке существуют буквы, которые встречаются значительно чаще, чем другие. Вскрытие шифра может начинаться с анализа только этих наиболее частых символов, что сокращает количество возможных вариантов для подбора ключа, ускоряет процесс дешифрования и позволяет избежать ошибок.

8) Какими характеристиками должен обладать шифр, чтобы была возможность применить метод частотного анализа?

Для применения метода частотного анализа шифр должен быть:

- известны алгоритмы шифрования и дешифрования;
- необходимо перебрать небольшое количество вариантов;
- язык открытого текста известен и легко узнаваем.

9) Какие виды криптоанализа Вам известны?

Известны следующие виды криптоанализа:

Частотный анализ — анализирует частоту появления символов в зашифрованном сообщении для выявления паттернов.

Брутфорс — перебор всех возможных ключей для взлома шифра.

Анализ по шаблонам — изучает повторяющиеся фразы или структуры в тексте.

10) Охарактеризуйте базовую модель криптографии.

Базовая модель криптографии включает три основные компонента:

- Открытое сообщение — информация, которая должна быть защищена.
- Шифрование — процесс преобразования открытого сообщения в зашифрованный текст с использованием ключа.
- Ключ — секретная информация, которая используется для шифрования и дешифрования.
- Зашифрованное сообщение — результат шифрования.
- Дешифрование — процесс преобразования зашифрованного текста обратно в исходное сообщение с использованием ключа.

11) Какие основные разновидности шифров простой замены применялись в прошлом?

В прошлом использовались следующие основные виды шифров простой замены:

- Шифр Цезаря (сдвиг каждого символа на фиксированное количество).
- Шифр Атбаш — буквы алфавита заменяются на противоположные (первая — последняя, вторая — предпоследняя и т.д.).

12) Сформулируйте правила шифрования/дешифрования шифра Цезаря.

Шифрование: Каждую букву открытого текста заменяют на букву, которая стоит на фиксированное количество позиций дальше в алфавите.

Дешифрование: Каждую букву зашифрованного текста заменяют на букву, которая находится на фиксированное количество позиций раньше в алфавите, чем в зашифрованном сообщении.

Листинг: https://github.com/darcysoul/caesar