МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
КАФЕДРА КІБЕРБЕЗПЕКИ

ЗВІТ ПРО ВИКОНАННЯ ЛАБОРАТОРНОЇ РОБОТИ №3

із дисципліни

«Алгоритми захисту інформації»

Виконав студент групи КБ-01
Борщ Д.О.

Суми – 2022

ЛАБОРАТОРНА РОБОТА №3

Тема: Використання частотного аналізу для розшифрування тексту..

ХІД РОБОТИ

1. **(5 б.)** Дослідіть два методи криптоаналізу (самостійно обрати):
   1) Частотний аналіз застосовується для класичного шифру,
   2) Метод “грубої сили” застосовується для сучасного шифру.

Наведіть коротку характеристику цих методів криптоаналізу.

1. **Частотний аналіз** у криптографії передбачає, що зашифроване повідомлення зберігає частотне повторення символів вхідної інформації. Частотний аналіз є одним із самих перших і примітивніших способів розшифровки, і у випадку вдалого його застосування, можна з впевненістю сказати, що алгоритм шифрування має вкрай низьку криптостійкість.

2. **Метод «грубої сили»** — метод рішення криптографічної задачі шляхом перебору всіх можливих варіантів ключа. Складність повного перебору залежить від кількості всіх можливих рішень задачі. Якщо простір рішень дуже великий, то повний перебір може не дати результатів протягом декількох років або навіть століть. Будь-яка задача з класу NP може бути вирішена повним перебором. При цьому, навіть якщо обчислення цільової функції від кожного конкретного можливого рішення задачі може бути здійснена за поліноміальний час, в залежності від кількості всіх можливих рішень повний перебір може зажадати експоненціального часу роботи. Даний метод є досить старим та неефективним, але може використовуватися для майже усіх шифрів. Більше того, будь-який шифр можна зламати методом повного перебору, але це буде лише питання часу.

2. **(10 б.)** Використовуючи частотний аналіз, розшифруйте криптограму (російська мова), зашифровану методом одноалфавітної підстановки (заміни).

Варіант 1:

```
Шкцувуп зцпхэыщшшщф буяыщмщф ъщоъуьу ю ощхючпшэк ьмщоуэ шк шпэ ьчёьц пнщ ъщоопцху. Ю зцпхэыщшшщф ъщоъуьу мьпнок чщсшщ юьэкшщмуэж кмэщыьэмщ. Ьщтокмкй зцпхэыщшшюи ъщоъуьж, кмэщы ъщцювкпэ ушящычкбуи щ ткхыёэщч хцивп. Шкцувуп ю кмэщык экхщнщ хцивк пьэж ощхкткэпцжьэмщ эщнщ, вэщ щш мцкопцпб зэщф зцпхэыщшшщф ъщоъуьу.
```

Розраховуємо загальну кількість символів без пунктуаційних знаків та конкретно кожної літери. Також розраховуємо частоту за формулою Частота = Кількість входжень / Загальна кількість.

Загальна кількість	305	
Символ	Кількість входжень	Частота
б	3	0,009836065574
в	6	0,01967213115
ж	4	0,0131147541
з	5	0,01639344262
и	4	0,0131147541
й	1	0,003278688525
к	20	0,06557377049
м	11	0,03606557377
н	4	0,0131147541
о	12	0,0393442623
п	17	0,05573770492
с	1	0,003278688525
т	3	0,009836065574
у	17	0,05573770492
ф	5	0,01639344262
х	11	0,03606557377
ц	14	0,04590163934
ч	5	0,01639344262
ш	17	0,05573770492
щ	38	0,1245901639
ъ	10	0,03278688525
ы	10	0,03278688525
ь	13	0,04262295082
э	22	0,07213114754
ю	7	0,02295081967
я	2	0,006557377049
ё	2	0,006557377049

Рис. 1.1 - Загальна кількість символів та кількість входжень кожної літери.

Встановимо відповідність для всіх символів і заповнимо таблицю відповідності відкритого і закритого алфавіту.

Таблиця підстановок	
б	ц
в	ч
ж	ь
з	э
и	ю
й	я
к	а
м	в
н	г
о	д
п	е
с	ж
т	з
у	и
ф	й
х	к
ц	л
ч	м
ш	н
щ	о
ъ	п
ы	р
ь	с
э	т
ю	у
я	ф
ё	ы

Рис. 1.2 - Таблиця відповідностей.

За порядком літер бачимо, що текст вірогідно був зашифрований за допомогою шифру Цезаря, бо літери йдуть в алфавітному порядку. Залишається розшифрувати текст за допомогою даної таблиці.

Розшифрований текст:

Наличие электронной цифровой подписи у документа сводит на нет смысл его подделки. У электронной подписи всегда можно установить авторство. Создавая электронную подпись, автор получает информацию о закрытом ключе. Наличие у автора такого ключа есть доказательство того, что он владелец этой электронной подписи.

Можемо знайти ключ нашого шифрування.

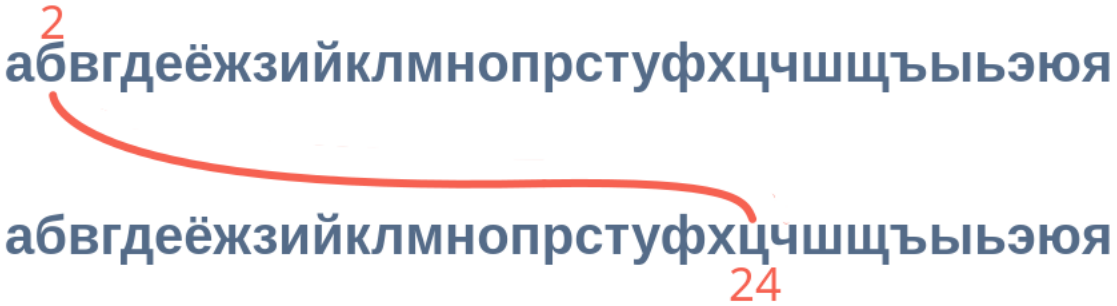

Рис. 1.3 - Зміщення алфавіту відносно таблиці.

За таблицею бачимо, що, при шифруванні літера “ц” була замінена на “б”. тобто можемо сказати, що ключ шифрування К = 11.

ВИСНОВОК

В процесі виконання лабораторної роботи я навчився використовувати метод частотного аналізу для розшифрування простого шифру підстановки.