Министерство науки и высшего образования Российской Федерации
Калужский филиал
федерального государственного бюджетного
образовательного учреждения высшего образования
«Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)»
(КФ МГТУ им. Н.Э. Баумана)

ФАКУЛЬТЕТ ***ИУК «Информатика и управление»***

КАФЕДРА ***ИУК4 «Программное обеспечение ЭВМ, информационные технологии»***

ЛАБОРАТОРНАЯ РАБОТА №2

«Элементы криптоанализа. Оценка частотности символов в тексте»

ДИСЦИПЛИНА: «Защита информации»

Выполнил: студент гр. ИУК4-72Б _____ (Карельский М.К.)
(Подпись)

Проверил: _____ (Ерохин И.И.)
(Подпись)

Дата сдачи (защиты):

Результаты сдачи (защиты):

- Балльная оценка:
- Оценка:

Калуга, 2023

Цель: ознакомиться с основными понятиями криптоанализа. Получить практические навыки применения метода криптоанализа зашифрованных сообщений, основанного на анализе частотности символов.

Задачи: изучить предложенный теоретический материал для получения базовой информации об основных понятиях криптоанализа и принципа действия метода криптоанализа зашифрованных сообщений, основанного на анализе частотности символов. Реализовать программу вычисляющею частотность символов в тексте. При помощи разработанной программы исследовать частотность символов зашифрованного текста, взятого согласно варианту. Составить таблицу замен алгоритма шифрования и расшифровать зашифрованный текст. Выполнить эвристический анализ текста, полученного в результате дешифровки. Довести результат дешифровки до приемлемого (удобочитаемого) вида. Подготовить ответы на контрольные вопросы.

Вариант 7

1. Реализовать программу вычисляющею частотность символов в тексте.
2. Используя текстовый файл, содержащий художественный текст на русском языке в открытом виде, исследовать частотность символов с помощью разработанной программы.
3. Исследовать частотность символов зашифрованного текста. Текст взять согласно варианту.
4. Сравнивая частотность символов русского языка, полученную в пункте 2, с частотностью символов зашифрованного текста, составить таблицу замен алгоритма шифрования и расшифровать зашифрованный текст.
5. Выполнить эвристический анализ текста, полученного в результате дешифровки. По смыслу текста выявить те замены, которые оказались неверными, и сформировать верные замены. Доведите результат дешифровки до приемлемого (удобочитаемого) вида.

Листинг:

```
def get_frequency(text: str):
    symbols = {}
    for s in text:
        if not s.isalpha():
            continue

        s = s.lower()
        if s in symbols:
            symbols[s] += 1
        else:
            symbols[s] = 1

    symbols = dict(sorted(symbols.items(), key=lambda item: item[1],
reverse=True))
    length = len(text)
```

```
    for s in symbols:
        symbols[s] /= length
        print(f'{s}: {symbols[s]*100:.4f}%')

    return symbols

source_file = open('source.txt', 'r')
source_text = source_file.read()
source_symbols = get_frequency(source_text)
source_keys = list(source_symbols.keys())

print()

encrypted_file = open('encrypted.txt', 'r')
encrypted_text = encrypted_file.read()
encrypted_symbols = get_frequency(encrypted_text)
encrypted_keys = list(encrypted_symbols.keys())

decrypted_text = ''
for s in encrypted_text:
    if not s.isalpha():
        decrypted_text += s
        continue

    s = s.lower()
    index = encrypted_keys.index(s)
    if index >= len(source_keys):
        decrypted_text += '?'
        continue
    decrypted_text += source_keys[index]

print(decrypted_text)

fixed_text = decrypted_text
def swap_letters(a, b):
    global fixed_text

    fixed_text = fixed_text.replace(a, '#')
    fixed_text = fixed_text.replace(b, a)
    fixed_text = fixed_text.replace('#', b)

swap_letters('л', 'к')
swap_letters('а', 'н')
swap_letters('т', 'с')
swap_letters('т', 'и')
swap_letters('д', 'у')
swap_letters('т', 'л')
swap_letters('к', 'в')
swap_letters('д', 'н')
swap_letters('ч', 'ь')
swap_letters('х', 'ш')
swap_letters('л', 'р')
```

```
swap_letters('б', 'ы')
swap_letters('л', 'к')
swap_letters('л', 'н')
swap_letters('з', 'п')
swap_letters('л', 'з')
swap_letters('т', 'л')
swap_letters('у', 'г')
swap_letters('ч', 'б')
swap_letters('д', 'т')
swap_letters('ж', 'ч')
swap_letters('ж', 'я')
swap_letters('ж', 'д')
swap_letters('у', 'ж')
swap_letters('ц', 'щ')
swap_letters('ю', 'х')
swap_letters('?', 'э')
fixed_text = fixed_text.replace('?', 'ъ')

print(fixed_text)

fixed_symbols = dict.fromkeys(encrypted_keys)

for i in range(len(fixed_text)):
    symbol = encrypted_text[i].lower()
    if not symbol.isalpha():
        continue

    fixed_symbol = fixed_text[i]
    fixed_symbols[symbol] = fixed_symbol

for s in fixed_symbols:
    print(f'{s} = {fixed_symbols[s]}')
```

Результат:

Частоты символов текста в открытом виде, частоты символов в закодированном тексте и итоговые замены символов:

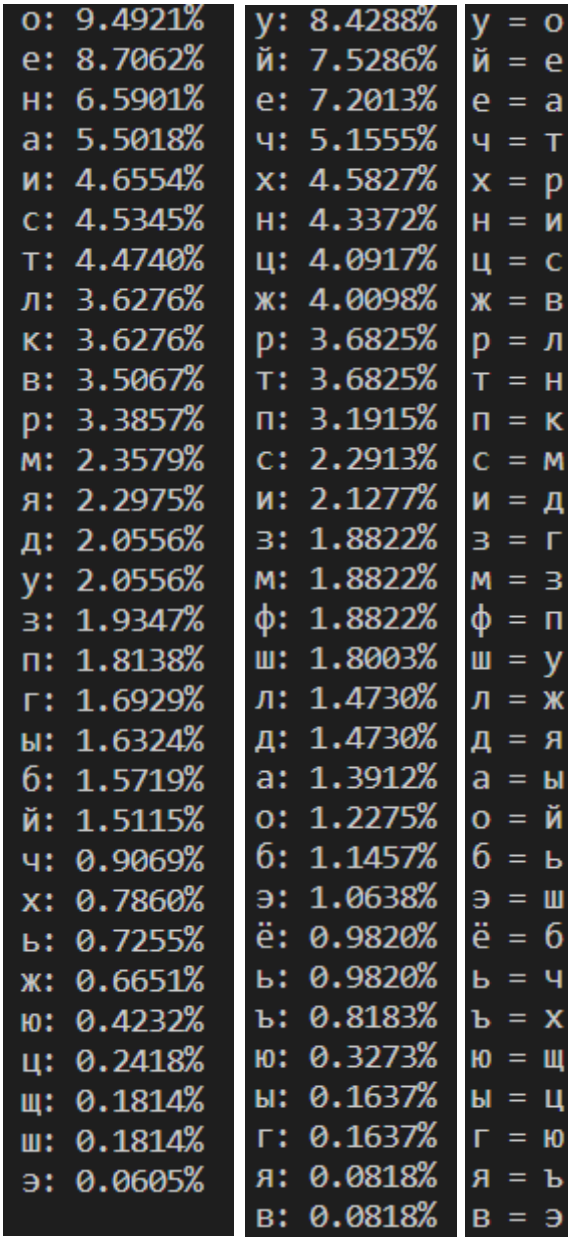

Рис. 1. Вычисленные значения

Зашифрованный текст:

Ж зреме ёбйч мехйжу фулехе ж иерн тефхежу. Чйрйлпе цчунч фхучнж чузу рйцпе, ьчу учпхажерцд фхн мехтныеъ. Рйцуп уч мехйже цчер чйфйхб ьйхтас н жйцб маёпу ихулнч, пеп ихулнч н жцй фурй фйхйи тнс ж цшсхеьту-пхецтус чхйфйчй уч чузу леиту тйцшюйзуцд ж тйёй фресйтн, пучухуй, тйцсучхд те иерб, фураъейч ц ёйзшюнсн ж тйс чйтдсн иасе чуьту ж жйхцчй уч чйрйлпн, хемядхдйчцд жцй лехьй н зхумтйй, уъжечажейч зухнмутч жцй жаэй н энхй, - пелйчцд, ьчу лех йзу шлй иуъуинч иу рные, иу хшп, жнийт иелй теи ьйхтучуо мйсрн пхецтао фйхйфрйч пепуо-чу цзухйжэйо пхаэн. Е фуи цчйтуо рйце цчудч, ёезхужу цйхйд, чхн ёурбэнъ журпе, н ж зремеъ ш тнъ сйрбпейч чу цпжумтуо мйрйтао ёрйцп, чу пхецтао, - фхумхеьтао н дхпно, пеп зухдьно цнхуф жехйтбд нм пхецтуо цсухуинта. Н руэеин, эшсту жцъхефтшж, жихшз инпнс зеруфус шиехдгч жёуп, жрйжу, фу феэтй, серао, те жуллеъ, жернчцд темеи, е чйрйлпе, цу цчшпус н чхйцпус, сучедцб, ёбйчцд фу жмсйчес... Зий-чу теи ужхезус руэеин йюй хем жмсйчтшрнцб, ту уте, жцпуьнж, шцфйре жахжечб

жуллн нм хшп уэерйжэйзу серузу. Чшч уте ц хемсеъш фурйчйре ж пумра н хеццйпре юйпш уё ьчу-чу лйрймтуй. Чеп н уцчерцд те жцг лнмтб рйзпно эхес ж шзурпй йй зшё, н, пузие ш тйо цфхеэнжерн, учьйзу вчу, уте ц шиужурбцчжнйс шраёерецб.

Расшифрованный текст:

л дкнун ьчеа униело зогнин л янкс внзинло. аекегрн таоса зиоасл аодо кетрн, жао оариблнкты зис унивсщню. кетор оа униелн танк аезеич жеивбм с летч убьро яиогса, рнр яиогса с лте зоке зеиея всм л тпминжво-ринтвом аиезеае оа аодо гняво ветпцедоты л веье зкнмевс, роаоиое, ветмоаиы вн янкч, зокбюнеа т ьедпцсмс л вем аевымс ябмн аожво л леитае оа аекегрс, инуэыиыеаты лте гниже с диоувее, оюлнаблнеа доисуова лте лбхе с хсие, - рнгеаты, жао гни едо пге яоюояса яо ксщн, яо ипр, лсяев янге вня жеивоаой уемкс ринтвбй зеиезкеа рнрой-ао тдоиелхей рибхс. н зоя таевой кетн таоыа, ьндиоло теиеы, аис ьокчхсю локрн, с л дкнуню п всю мекчрнеа ао трлоувой уекевбй ькетр, ао ринтвбй, - зиоуинжвбй с ыирсй, рнр доиыжсй тсиоз лниевчы су ринтвой тмоиоясвб. с кохняс, хпмво лтюинзвпл, ляипд ясрсм днкозом пяниыша льор, лкело, зо знхве, мнкбй, вн логгню, лнксаты внуня, н аекегрн, то тапром с аиетром, моанытч, ьчеаты зо лумеанм... дяе-ао вня олиндом кохняс еце ину лумеавпкстч, во овн, лтрожсл, птзекн лбилнач логгс су ипр охнкелхедо мнкодо. апа овн т инумнюп зокеаекн л роукб с инттеркн церп оь жао-ао гекеувое. анр с отанкты вн лтш гсувч кедрсй хинм л пдокре ее дпь, с, родян п вей тзинхслнкс, оажедо ?ао, овн т пяолокчталсем пкбьнкнтч.

Текст после нахождения замен:

в глаза бьет зарево пожара в дали направо. тележка стоит против того леска, что открывался при зарницах. лесок от зарева стал теперь черным и весь зыбко дрожит, как дрожит и все поле перед ним в сумрачно-красном трепете от того жадно несущегося в небе пламени, которое, несмотря на даль, полыхает с бегущими в нем тенями дыма точно в версте от тележки, разъяряется все жарче и грознее, охватывает горизонт все выше и шире, - кажется, что жар его уже доходит до лица, до рук, виден даже над чернотой земли красный переплет какой-то сгоревшей крыши. а под стеной леса стоят, багрово серея, три больших волка, и в глазах у них мелькает то сквозной зеленый блеск, то красный, - прозрачный и яркий, как горячий сироп варенья из красной смородины. и лошади, шумно всхрапнув, вдруг диким галопом ударяют вбок, влево, по пашне, малый, на вожжах, валится назад, а тележка, со стуком и треском, мотаясь, бьется по взметам... где-то над оврагом лошади еще раз взметнулись, но она, вскочив, успела вырвать вожжи из рук ошалевшего малого. тут она с размаху полетела в козлы и рассекла щеку об что-то железное. так и остался на всю жизнь легкий шрам в уголке ее губ, и, когда у ней спрашивали, отчего это, она с удовольствием улыбалась.

Вывод: в ходе выполнения лабораторной работы были получены практические навыки применения метода криптоанализа зашифрованных сообщений, основанного на анализе частотности символов.