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

ДИСЦИПЛИНА: «Защита информации»

Выполнил: студент гр. ИУК4-72Б _____ (Калашников А. С.)
(Подпись) (Ф.И.О.)

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

Дата сдачи (защиты):

Результаты сдачи (защиты):

- Балльная оценка:
- Оценка:

Калуга, 2023

Цель работы*:* познакомиться с методом криптоанализа зашифрованных сообщений, основанного на анализе частотности символов.

Расшифрованный текст

Был прекрасный июльский день, один из тех дней, которые случаются только тогда, когда погода установилась надолго. С самого раннего утра небо ясно; утренняя заря не пылает пожаром: она разливается кротким румянцем. Солнце - не огнистое, не раскаленное, как во время знойной засухи, не тускло-багровое, как перед бурей, но светлое и приветно лучезарное - мирно всплывает под узкой и длинной тучкой, свежо просияет и погрузится в лиловый ее туман. Верхний, тонкий край растянутого облачка засверкает змейками; блеск их подобен блеску кованого серебра... Но вот опять хлынули играющие лучи, - и весело и величаво, словно взлетая, поднимается могучее светило. Около полудня обыкновенно появляется множество круглых высоких облаков, золотисто-серых, с нежными белыми краями. Подобно островам, разбросанным по бесконечно разлившейся реке, обтекающей их глубоко прозрачными рукавами ровной синевы, они почти не трогаются с места; далее, к небосклону, они сдвигаются, теснятся, синевы между ними уже не видать; но сами они так же лазурны, как небо: они все насквозь проникнуты светом и теплотой. Цвет небосклона, легкий, бледно-лиловый, не изменяется во весь день и кругом одинаков; нигде не темнеет, не густеет гроза; разве кое-где протянутся сверху вниз голубоватые полосы: то сеется едва заметный дождь. К вечеру эти облака исчезают; последние из них, черноватые и неопределенные, как дым, ложатся розовыми клубами напротив заходящего солнца; на месте, где оно закатилось так же спокойно, как спокойно взошло на небо, алое сиянье стоит недолгое время над потемневшей землей, и, тихо мигая, как бережно несомая свечка, затеплится на нем вечерняя звезда.

Вариант №6

Задание

Расшифровать зашиврованный текст

Еюфснлм дзосдусеюм гефхулзщ, ф ргжелрцхюп рг ёогкг нзтл, шпцувфя, тсъхл е цтсу еюфхузоло е Ёулёсулв ф нсозрг. Сёсря фелрщг стголо ьзнц. Ёулёсулм тсезо тлнсм, ргхвёлегв лкс ефзм флою тсесжяв... Цжгу ргфхсоянс дюо флозр, ъхс тлнг, тусрлкге ефнсълеызёс рг рсёл гефхулмщг, жс тсоселрю жузенг есыог е рзёс. Ёулёсулм рз цфтзо еюжзурцхя зз л, тсж хвйзфхяб сфзжгеызёс хзог, усрво, ъцефхецв рг рзм хузтзх л фцжсусёл, елжв, нгн гефхулзщ, езфя тзузосплеылфя ргкгж, тзуздлугзх, щгугтгзх фнубъзррюпл тгоящгпл жузенс. Ёулёсулм, фгп рз кргв жов ъзёс, тсезурцо нсрв. Ежсоя йзозкрсм узызхнл фгжг, нгъгвфя, сдзфтгпвхзе, дзйго гефхулзщ дзк елрхсенл, ф нзтл, кгйгхюп е нцогнз. Ёулёсулм ефхузхлофв ф гефхулмщзп екёовжсп. Рг рзёс пзухес ёовжзол кголхюз фпзухрюп цйгфсп ёогкг. Гефхулзщ пзжозррс фёлдго нсозрл, е ёсуоз ц рзёс ёцжзо дцоянгбьлм шулт. Йпцувфя, Ёулёсулм пгшрцо ыгынсм. Цжгу ф жолррюп тсхвёсп угкеголо ъзузт ргжесз. Гефхулзщ цтго, хстюув уцнл, фосерс тсфнсоякрцеылфя; ёоцшс фхцнрцол с нгпзря псфхсесм тсоселрнл ъзузтрсм нсусднл. Нсря туюёрцо, ефшугтрце, еюрзф Ёулёсулв рг фзузжлрц цолщю. Тс цолщгп тзузфхцнлегол узжзбьлз еюфхузою. Ёулёсулм фозк ф нсрв л кгпсхго ёсосесм. Плпс рзёс фнгнгол нгкгнл тсжсфтзеызм хузхязм фсхрл. Ср дусфло тсесжяв л, фгп рз кргв жов ъзёс, тсжсызо н кгуцдозррспц лп гефхулмфнспц фсожгхц. Хсх озйго хгп йз, ц лёулесм хзфяпю узызхъгхсм сёугжю, еюхврце ёувкрцб нсулързецб огжсря, нгн кг тсжгврлзп. Ёулёсулм

ёоврцо зпц е олщс. Срс тснгкгосфя зпц пгозрянлп, ъцхя ол рз жзхфнлп, рзфпсхув рг елфоюз цфю л лкпцъзррюм тснулеозррюм фцусеюм усх.

Листинг программы:

```
def sum(text,letter,size):
    count = 0
    for i in range(size):
        if letter == text[i]:
            count += 1
    return count
#Открытый тектс-----------------------------------------
with open("text1.txt", "r", encoding='utf-8') as file:
    content = file.read()

text = list(content)
size_t = len(text)

alphabet = 'абвгдежзийклмнопрстуфхцчшщъыьэюя'
alphabet_size = len(alphabet)

alp = list(alphabet)

Open_text = [0] * alphabet_size
for i in range(alphabet_size):
    Open_text[i] = [0] * 2

for i in range(alphabet_size):
    Open_text[i][0] = alp[i]

for i in range(alphabet_size):
    Open_text[i][1] = sum(text, alp[i], size_t)


Open_text = sorted(Open_text, key=lambda x: x[1], reverse=True)
print("Расшифрованный текст")
print(Open_text)

#Шифрованный текст--------------------------------------------
with open("text2.txt", "r", encoding='utf-8') as file:
    content_cipher = file.read()

text_cipher = list(content_cipher)
text_cipher_final = list(content_cipher)
size = len(text_cipher)

Cipher_text = [0] * alphabet_size
for i in range(alphabet_size):
    Cipher_text[i] = [0] * 2

for i in range(alphabet_size):
    Cipher_text[i][0] = alp[i]

for i in range(alphabet_size):
    Cipher_text[i][1] = sum(text_cipher, alp[i], size)

Cipher_text = sorted(Cipher_text, key=lambda x: x[1], reverse=True)
print("Шифрованный текст")
```

```
print(Cipher_text)

for i, j in zip(Open_text, Cipher_text):
    print(i[0]+"-"+j[0])

filename = "text2.txt"
alphabet_lower = 'абвгдеёжзийклмнопрстуфхцчшщъыьэюя'
alphabet_upper = 'АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ'

with open(filename, 'r', encoding='utf-8') as file:
    ciphertext = file.read()
shift = 3
text = ''
for simbol in ciphertext:
    if simbol in alphabet_lower:
        text += alphabet_lower[(alphabet_lower.index(simbol) - shift) %
len(alphabet_lower)]
    elif simbol in alphabet_upper:
        text += alphabet_upper[(alphabet_upper.index(simbol) - shift) %
len(alphabet_upper)]
    else:
        text += simbol

print("Расшифрованный текст:")
print(text)
```

Результат:

```
Расшифрованный текст
[['о', 156], ['е', 144], ['н', 108], ['а', 91], ['и', 77], ['т', 74], ['с', 73], ['л', 60], ['к', 59], ['в', 57], ['р', 56], ['м', 39], ['я', 38], ['д', 34], ['у', 34], ['з', 32
], ['п', 29], ['г', 28], ['ы', 27], ['б', 25], ['й', 25], ['ч', 15], ['х', 13], ['ь', 12], ['ж', 11], ['ю', 7], ['ц', 3], ['ш', 3], ['щ', 3], ['э', 1], ['ф', 0], ['ъ', 0]]
Шифрованный текст
[['с', 112], ['з', 104], ['л', 97], ['г', 87], ['у', 76], ['р', 73], ['о', 72], ['ф', 66], ['е', 64], ['х', 53], ['н', 45], ['ц', 44], ['п', 38], ['т', 38], ['ж', 33], ['в', 30]
, ['м', 28], ['ю', 27], ['я', 24], ['к', 22], ['ъ', 14], ['щ', 13], ['д', 12], ['ы', 11], ['й', 7], ['б', 6], ['ш', 5], ['ь', 3], ['а', 0], ['и', 0], ['ч', 0], ['э', 0]]
```

Рис.1 Количество букв в тексте

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

Рис.2 Соотношение букв

```
Высокий белобровый австриец, с надвинутым на глаза кепи, хмурясь, почти в упор выстрелил в Григория с колена. Огонь свинца опалил щеку.
Григорий повел пикой, натягивая изо всей силы поводья... Удар настолько был силен, что пика, пронизав вскочившего на ноги австрийца, до
половины древка вошла в него. Григорий не успел выдернуть ее и, под тяжестью оседавшего тела, ронял, чувствуя на ней трепет и судороги,
видя, как австриец, весь переломившись назад, перебирает, царапает скрюченными пальцами древко. Григорий, сам не зная для чего, повернул
коня. Вдоль жел-езной решетки сада, качаясь, обеспамятев, бежал австриец без винтовки, с кепи, зажатым в кулаке. Григорий встретился с
австрийцем взглядом. На него мертво глядели залитые смертным ужасом глаза. Австриец медленно сгибал колени, в горле у него гудел булькающий
хрип. Жмурясь, Григорий махнул шашкой. Удар с длинным потягом развалил череп надвое. Австриец упал, топыря руки, словно поскользнувшись;
глухо стукнули о камень мостовой половинки черепной коробки. Конь прыгнул, всхрапнув, вынес Григория на середину улицы. По улицам
перестукивали редеющие выстр-елы. Григорий слез с коня и замотал головой. Мимо него скакали казаки подоспевшей третьей сотни. Он бросил
поводья и, сам не зная для чего, подошел к зарубленному им австрийскому солдату. Тот лежал там же, у иг-ривой тесьмы решетчатой ограды,
вытянув грязную коричневую ладонь, как за подаянием. Григорий глянул ему в лицо. Оно показалось ему маленьким, чуть ли не детским, несмотря
на вислые усы и измученный покривленный суровый рот.
```

Рис.3 Расшифрованный текст

Выводы: в результате выполнения лабораторной работы познакомился с методом криптоанализа зашифрованных сообщений, основанного на анализе частотности символов.