

Міністерство освіти і науки України  
Національний технічний університет України  
*“Київський політехнічний інститут”*  
Фізико-технічний інститут

ЛАБОРАТОРНА РОБОТА №1

Експериментальна оцінка ентропії на символ джерела  
відкритого тексту. Криптоаналіз шифру Віженера

Виконав:  
*Грубіян Є.О.*  
Прийняв:  
*Яковлев С.В.*

Київ 2015 р.

# Обчислення $H_1$

Скрипт обчислення  $H_1$  та частотного аналізу для твору 'Ідіот' Достоевського:

```
# -*- coding: utf-8 -*-
import re
import codecs
import operator
from math import *

file = codecs.open("idiot.txt", "r", encoding='utf-8')
file2 = codecs.open("freq.txt", "w", encoding='utf-8')

text = re.sub('\s+', ' ', file.read().lower()).strip()
#text = file.read().lower()
alphabet_ru = (u'a',u'b',u'в',u'г',u'д',u'е',u'ж',u'з',u'и',u'к',u'л',u'м', \
               u'й',u'н',u'о',u'п',u'р',u'с',u'т',u'у',u'ф',u'х',u'ц',u'ч', \
               u'ш',u'щ',u'ъ',u'ы',u'ь',u'э',u'ю',u'я',)

alphabet_ua = (u'a',u'b',u'в',u'г',u'г',u'д',u'е',u'ж',u'з',u'и',u'к',u'л',u'м', \
               u'i',u'ї',u'й',u'н',u'о',u'п',u'р',u'с',u'т',u'у',u'ф',u'х', \
               u'ц',u'ч',u'ш',u'щ',u'ъ',u'є',u'ю',u'я')

alphabet_de = (u'a',u'b',u'c',u'd',u'e',u'f',u'g',u'h',u'i',u'j',u'k',u'l', \
               u'm',u'n',u'o',u'p',u'q',u'r',u's',u't',u'u',u'v',u'w',u'x', \
               u'y',u'z',u'ä',u'ö',u'ü',u'ß',u' ')

alphabet = alphabet_ru

l = 0
freq_table = dict(zip(alphabet, [0]*len(alphabet)))

for char in text:
    if char in alphabet:
        freq_table[char] += 1
        l += 1

file2.write("total "+str(l)+" symbols\n")

for i in sorted(freq_table.items(), key=operator.itemgetter(1), reverse=True):
    file2.write(i[0] + ": {:.2f}".format((i[1]/float(l)) *100) + "%\n")

entropy = 0

for i in freq_table.values():
    p = i/float(l)
    if p != 0:
        entropy += - p*log(p,2)

file2.write("entropy of the text: {:.2f} bit/symbol\n".format(entropy))
```

## Результати для тексту з пробілами:

```
total 1235048 symbols
: 17.03%
о: 9.34%
е: 7.48%
а: 6.60%
н: 5.56%
и: 5.30%
т: 5.23%
с: 4.41%
в: 3.91%
л: 3.85%
р: 3.23%
к: 2.70%
м: 2.59%
д: 2.55%
п: 2.25%
у: 2.18%
я: 1.98%
ь: 1.87%
ч: 1.59%
г: 1.56%
э: 1.44%
ы: 1.44%
б: 1.39%
ж: 0.98%
й: 0.81%
ш: 0.68%
х: 0.60%
ю: 0.50%
э: 0.30%
щ: 0.24%
ц: 0.24%
ф: 0.15%
ъ: 0.02%
entropy of the text: 4.36 bit/symbol
```

## Результати для тексту без пробілів:

```
total 1024691 symbols
о: 11.26%
е: 9.02%
а: 7.96%
н: 6.70%
и: 6.38%
т: 6.31%
с: 5.32%
в: 4.71%
л: 4.64%
р: 3.90%
к: 3.25%
м: 3.12%
д: 3.07%
п: 2.71%
у: 2.63%
я: 2.39%
ь: 2.25%
ч: 1.91%
г: 1.88%
э: 1.74%
ы: 1.73%
б: 1.67%
ж: 1.18%
й: 0.98%
ш: 0.82%
х: 0.73%
ю: 0.60%
э: 0.36%
щ: 0.29%
ц: 0.29%
ф: 0.18%
ъ: 0.02%
entropy of the text: 4.46 bit/symbol
```

## Обчислення $H_2$

Скрипт обчислення  $H_2$  та частотного аналізу біграм для твору 'Ідіот' До-

```

# -*- coding: utf-8 -*-
import re
import codecs
import operator
import itertools
import string
from math import *
import collections

file = codecs.open("idiot.txt", "r", encoding='utf-8')
file2 = codecs.open("bigram.txt", "w", encoding='utf-8')

punctuation = set(string.punctuation)
text = ''.join(ch for ch in file.read().lower() if ch not in punctuation)
text = re.sub('\s+', '', text.strip())

alphabet_ru = [u'a', u'б', u'в', u'г', u'д', u'е', u'ж', u'з', u'и', u'к', u'л', u'м', \
               u'н', u'о', u'п', u'р', u'с', u'т', u'у', u'ф', u'х', u'ц', u'ч', \
               u'ш', u'щ', u'ъ', u'ы', u'ь', u'э', u'ю', u'я']

alphabet_ua = [u'a', u'б', u'в', u'г', u'д', u'е', u'ж', u'з', u'и', u'к', u'л', \
               u'м', u'н', u'о', u'п', u'р', u'с', u'т', u'у', u'ф', \
               u'х', u'ц', u'ч', u'ш', u'щ', u'ъ', u'е', u'ю', u'я', ]

alphabet_de = [u'a', u'b', u'c', u'd', u'e', u'f', u'g', u'h', u'i', u'j', u'k', u'l', \
               u'm', u'n', u'o', u'p', u'q', u'r', u's', u't', u'u', u'v', u'w', u'x', \
               u'y', u'z', u'ä', u'ö', u'ü', u'ß', u' ']

bi_ua = list(itertools.product(alphabet_ua, alphabet_ua))
bi_ru = list(itertools.product(alphabet_ru, alphabet_ru))
bi_de = list(itertools.product(alphabet_de, alphabet_de))
alphabet = alphabet_ru
bi = bi_ru

l = 0
freq_table = dict(zip(bi, [0]*(len(alphabet)**2)))

for i in range(0, len(text)-1):
    bigram = (text[i], text[i+1])
    if bigram in bi:
        freq_table[bigram] += 1
        l += 1

file2.write("Total {} bigrams\n".format(l))
l=float(l)
max_len = 5

file2.write("Table of frequincies (in percents):\n          "+(" "*(max_len-1)) \
            .join(alphabet) + "\n")

for i in range(0, len(alphabet)):
    file2.write(alphabet[i]+" ")
    for j in range(0, len(alphabet)):
        file2.write(" {:.2f}".format(100*freq_table[(alphabet[i], \
            alphabet[j])]/l))
    file2.write("\n")
entropy = 0

for i in freq_table.values():
    p = i/float(l)

```

```
        if p != 0:
            entropy += - p*log(p,2)
entropy = entropy/2
file2.write("Entropy of the text: {:.02.2f} bit/symbol".format(entropy))
```

# Результати для тексту з пробілами:

Total 1225448 bigrams

Table of frequincies (in percents):

	а	б	в	г	д	е	ж	з	и	к	л	м	й	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	
а	0.00	0.04	0.33	0.10	0.18	0.13	0.18	0.32	0.03	0.54	0.77	0.32	0.08	0.33	0.00	0.07	0.18	0.51	0.38	0.00	0.01	0.08	0.00	0.08	0.09	0.02	0.00	0.00	0.00	0.00	0.09	0.18	1.59
б	0.05	0.00	0.00	0.00	0.00	0.23	0.00	0.00	0.06	0.01	0.06	0.01	0.00	0.02	0.18	0.00	0.09	0.02	0.00	0.12	0.00	0.00	0.00	0.00	0.00	0.02	0.01	0.40	0.00	0.00	0.00	0.05	0.04
в	0.59	0.00	0.00	0.02	0.08	0.54	0.00	0.04	0.31	0.01	0.09	0.01	0.00	0.17	0.61	0.04	0.05	0.37	0.02	0.05	0.00	0.00	0.00	0.01	0.07	0.00	0.00	0.30	0.01	0.00	0.00	0.02	0.52
г	0.11	0.00	0.00	0.00	0.11	0.08	0.00	0.00	0.05	0.00	0.16	0.00	0.00	0.02	0.84	0.00	0.05	0.00	0.00	0.04	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.10	
д	0.53	0.00	0.07	0.00	0.00	0.44	0.00	0.00	0.22	0.02	0.06	0.00	0.00	0.19	0.38	0.01	0.15	0.03	0.02	0.15	0.00	0.01	0.03	0.01	0.01	0.00	0.00	0.05	0.09	0.00	0.00	0.02	0.08
е	0.00	0.14	0.20	0.32	0.29	0.16	0.07	0.13	0.01	0.13	0.53	0.43	0.22	0.76	0.03	0.13	0.59	0.43	0.57	0.01	0.00	0.06	0.04	0.12	0.09	0.08	0.00	0.00	0.00	0.00	0.03	0.03	1.93
ж	0.13	0.00	0.00	0.00	0.08	0.48	0.00	0.00	0.13	0.00	0.00	0.00	0.00	0.07	0.00	0.00	0.00	0.00	0.00	0.02	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.05	
з	0.48	0.01	0.10	0.04	0.06	0.02	0.00	0.00	0.04	0.01	0.02	0.02	0.00	0.19	0.04	0.00	0.02	0.00	0.00	0.03	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.03	0.13	0.00	0.02	0.05	0.12
и	0.01	0.06	0.22	0.04	0.15	0.17	0.02	0.19	0.05	0.14	0.53	0.24	0.10	0.32	0.03	0.07	0.04	0.21	0.42	0.00	0.00	0.13	0.07	0.16	0.06	0.01	0.00	0.00	0.00	0.00	0.03	0.11	1.72
к	0.62	0.00	0.02	0.00	0.00	0.05	0.00	0.00	0.18	0.00	0.04	0.00	0.00	0.23	0.78	0.00	0.15	0.03	0.05	0.10	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.46
л	0.57	0.00	0.00	0.02	0.00	0.37	0.03	0.00	0.65	0.02	0.01	0.00	0.00	0.02	0.51	0.01	0.00	0.15	0.00	0.13	0.00	0.00	0.00	0.02	0.00	0.00	0.00	0.07	0.36	0.00	0.09	0.15	0.68
м	0.22	0.00	0.00	0.01	0.00	0.42	0.00	0.00	0.22	0.01	0.01	0.00	0.00	0.17	0.37	0.01	0.01	0.01	0.01	0.22	0.00	0.00	0.00	0.01	0.00	0.00	0.00	0.08	0.01	0.00	0.00	0.04	0.77
й	0.00	0.00	0.00	0.00	0.02	0.00	0.00	0.00	0.00	0.01	0.00	0.00	0.00	0.05	0.00	0.00	0.00	0.05	0.04	0.00	0.00	0.00	0.01	0.02	0.02	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.60
н	1.00	0.00	0.00	0.00	0.03	1.12	0.00	0.00	0.70	0.03	0.00	0.00	0.00	0.25	1.05	0.00	0.01	0.03	0.03	0.23	0.00	0.00	0.02	0.03	0.00	0.01	0.00	0.25	0.11	0.00	0.02	0.35	0.35
о	0.00	0.32	0.71	0.48	0.43	0.21	0.25	0.09	0.07	0.18	0.51	0.52	0.27	0.55	0.02	0.12	0.47	0.56	0.64	0.01	0.03	0.03	0.01	0.25	0.08	0.02	0.00	0.00	0.00	0.00	0.06	0.06	2.45
п	0.13	0.00	0.00	0.00	0.00	0.21	0.00	0.00	0.08	0.01	0.04	0.00	0.00	0.01	0.89	0.05	0.69	0.00	0.01	0.05	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.02	0.01	0.00	0.00	0.05	0.00
р	0.66	0.01	0.04	0.01	0.07	0.51	0.02	0.00	0.44	0.02	0.01	0.02	0.00	0.06	0.68	0.01	0.01	0.01	0.04	0.23	0.01	0.01	0.00	0.01	0.03	0.00	0.00	0.09	0.09	0.00	0.02	0.10	0.06
с	0.19	0.01	0.12	0.00	0.02	0.44	0.00	0.00	0.13	0.32	0.29	0.12	0.00	0.09	0.25	0.17	0.01	0.07	0.97	0.06	0.00	0.02	0.00	0.04	0.01	0.00	0.00	0.02	0.33	0.00	0.02	0.38	0.36
т	0.59	0.00	0.22	0.00	0.01	0.55	0.00	0.00	0.36	0.03	0.03	0.00	0.00	0.09	1.46	0.01	0.24	0.11	0.01	0.14	0.00	0.00	0.01	0.03	0.00	0.00	0.00	0.12	0.65	0.00	0.00	0.05	0.58
у	0.00	0.05	0.07	0.14	0.16	0.02	0.16	0.03	0.00	0.06	0.10	0.13	0.01	0.02	0.00	0.05	0.05	0.10	0.15	0.00	0.00	0.03	0.00	0.08	0.05	0.02	0.00	0.00	0.00	0.00	0.07	0.00	0.63
ф	0.02	0.00	0.00	0.00	0.00	0.03	0.00	0.00	0.05	0.00	0.00	0.00	0.00	0.00	0.01	0.00	0.01	0.00	0.00	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.02	0.00	0.00	0.00	0.00
х	0.04	0.00	0.02	0.00	0.00	0.01	0.00	0.00	0.01	0.00	0.01	0.01	0.00	0.01	0.22	0.00	0.01	0.00	0.00	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.26
ц	0.06	0.00	0.00	0.00	0.00	0.07	0.00	0.00	0.01	0.01	0.00	0.00	0.00	0.00	0.02	0.00	0.00	0.00	0.00	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.02	0.00	0.00	0.00	0.00	0.04
ч	0.28	0.00	0.00	0.00	0.00	0.40	0.00	0.00	0.16	0.02	0.00	0.00	0.00	0.09	0.01	0.00	0.03	0.00	0.46	0.07	0.00	0.00	0.00	0.00	0.01	0.00	0.00	0.00	0.02	0.00	0.00	0.00	0.05
ш	0.09	0.00	0.01	0.00	0.00	0.21	0.00	0.00	0.14	0.05	0.05	0.00	0.00	0.03	0.02	0.00	0.00	0.00	0.00	0.03	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.04	0.00	0.00	0.00	0.01
щ	0.03	0.00	0.00	0.00	0.00	0.14	0.00	0.00	0.05	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.01	0.01
ъ	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.01	0.00
ы	0.00	0.01	0.08	0.01	0.02	0.06	0.00	0.00	0.00	0.02	0.19	0.09	0.13	0.03	0.00	0.01	0.02	0.07	0.09	0.00	0.00	0.08	0.00	0.03	0.04	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.45
ь	0.00	0.01	0.00	0.01	0.00	0.06	0.00	0.01	0.01	0.12	0.00	0.03	0.00	0.13	0.00	0.00	0.00	0.09	0.02	0.00	0.00	0.01	0.01	0.04	0.00	0.00	0.00	0.00	0.00	0.03	0.04	1.24	
э	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.28	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
ю	0.00	0.04	0.00	0.00	0.03	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.02	0.03	0.00	0.00	0.00	0.01	0.00	0.02	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.32
я	0.00	0.00	0.02	0.00	0.05	0.01	0.01	0.19	0.00	0.02	0.08	0.03	0.00	0.05	0.00	0.00	0.00	0.05	0.15	0.00	0.00	0.01	0.01	0.02	0.00	0.01	0.00	0.00	0.00	0.00	0.01	0.01	1.22
	0.24	0.67	1.67	0.37	0.75	0.40	0.22	0.43	1.16	0.91	0.27	0.61	0.00	1.61	1.03	1.48	0.38	1.52	0.84	0.47	0.08	0.14	0.03	0.66	0.06	0.01	0.00	0.00	0.00	0.28	0.00	0.28	0.00

Entropy of the text: 3.95 bit/symbol

## Результати для тексту без пробілів:

Total 1019476 bigrams

Table of frequincies (in percents):

	а	б	в	г	д	е	ж	з	и	к	л	м	й	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
а	0.05	0.10	0.59	0.16	0.30	0.22	0.24	0.42	0.16	0.76	0.96	0.46	0.09	0.59	0.11	0.25	0.26	0.77	0.55	0.05	0.02	0.11	0.01	0.16	0.12	0.02	0.00	0.00	0.00	0.03	0.11	0.26
б	0.06	0.00	0.01	0.00	0.00	0.28	0.00	0.00	0.08	0.01	0.08	0.01	0.00	0.03	0.22	0.00	0.11	0.02	0.00	0.15	0.00	0.00	0.00	0.00	0.02	0.02	0.48	0.00	0.01	0.00	0.06	
в	0.71	0.02	0.04	0.05	0.12	0.66	0.01	0.06	0.40	0.06	0.12	0.03	0.00	0.25	0.76	0.12	0.08	0.52	0.07	0.07	0.00	0.01	0.00	0.03	0.09	0.00	0.00	0.37	0.02	0.04	0.00	0.02
г	0.13	0.00	0.01	0.00	0.14	0.10	0.00	0.01	0.07	0.01	0.20	0.01	0.00	0.04	1.02	0.01	0.06	0.01	0.00	0.05	0.00	0.00	0.00	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
д	0.64	0.00	0.09	0.00	0.01	0.53	0.00	0.01	0.27	0.04	0.07	0.01	0.00	0.24	0.46	0.01	0.19	0.04	0.03	0.18	0.00	0.01	0.04	0.01	0.01	0.00	0.00	0.06	0.10	0.00	0.00	0.03
е	0.03	0.27	0.49	0.43	0.45	0.23	0.12	0.24	0.17	0.26	0.67	0.62	0.26	1.10	0.17	0.39	0.77	0.74	0.79	0.09	0.01	0.10	0.05	0.22	0.11	0.10	0.00	0.00	0.00	0.05	0.03	0.06
ж	0.16	0.01	0.00	0.00	0.10	0.58	0.00	0.00	0.17	0.01	0.00	0.00	0.00	0.09	0.01	0.01	0.00	0.01	0.01	0.03	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
з	0.58	0.02	0.13	0.05	0.08	0.03	0.01	0.01	0.05	0.02	0.03	0.04	0.00	0.24	0.06	0.02	0.03	0.02	0.01	0.04	0.00	0.00	0.00	0.01	0.00	0.00	0.00	0.04	0.16	0.00	0.02	0.06
и	0.03	0.16	0.50	0.09	0.30	0.25	0.04	0.29	0.17	0.27	0.67	0.35	0.12	0.60	0.16	0.29	0.09	0.45	0.61	0.06	0.02	0.17	0.09	0.26	0.08	0.02	0.00	0.00	0.00	0.02	0.03	0.17
к	0.75	0.05	0.07	0.01	0.02	0.07	0.01	0.01	0.26	0.03	0.06	0.02	0.00	0.34	0.96	0.04	0.19	0.09	0.09	0.14	0.00	0.00	0.00	0.02	0.00	0.00	0.00	0.00	0.00	0.01	0.00	0.01
л	0.69	0.03	0.08	0.05	0.03	0.49	0.04	0.02	0.85	0.10	0.03	0.02	0.00	0.09	0.68	0.06	0.02	0.24	0.04	0.17	0.00	0.00	0.00	0.07	0.00	0.00	0.00	0.08	0.44	0.01	0.11	0.19
м	0.28	0.03	0.09	0.03	0.05	0.52	0.02	0.02	0.33	0.05	0.03	0.03	0.00	0.30	0.51	0.10	0.03	0.12	0.05	0.30	0.00	0.01	0.00	0.05	0.00	0.00	0.00	0.10	0.01	0.01	0.00	0.06
й	0.01	0.02	0.06	0.02	0.07	0.01	0.02	0.01	0.07	0.05	0.01	0.04	0.00	0.10	0.03	0.07	0.03	0.13	0.07	0.01	0.01	0.00	0.01	0.05	0.03	0.00	0.00	0.00	0.00	0.01	0.00	0.01
н	1.20	0.03	0.04	0.01	0.05	1.35	0.00	0.01	0.87	0.05	0.00	0.01	0.00	0.34	1.28	0.04	0.02	0.07	0.06	0.29	0.01	0.00	0.02	0.05	0.00	0.01	0.00	0.30	0.13	0.00	0.02	0.42
о	0.03	0.54	1.18	0.63	0.63	0.32	0.35	0.18	0.25	0.35	0.65	0.74	0.33	0.92	0.23	0.39	0.63	0.94	0.92	0.11	0.05	0.06	0.02	0.42	0.11	0.02	0.00	0.00	0.00	0.05	0.07	0.14
п	0.16	0.00	0.00	0.00	0.00	0.25	0.00	0.00	0.10	0.01	0.05	0.00	0.00	0.01	1.07	0.06	0.83	0.00	0.02	0.07	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.02	0.01	0.00	0.00	0.06
р	0.80	0.02	0.05	0.02	0.09	0.61	0.03	0.01	0.54	0.03	0.01	0.03	0.00	0.08	0.82	0.02	0.01	0.02	0.05	0.28	0.01	0.01	0.00	0.01	0.04	0.00	0.00	0.11	0.11	0.00	0.02	0.12
с	0.23	0.02	0.18	0.02	0.04	0.54	0.03	0.01	0.17	0.42	0.36	0.16	0.00	0.17	0.32	0.24	0.02	0.12	1.20	0.09	0.00	0.02	0.01	0.06	0.02	0.00	0.00	0.02	0.39	0.01	0.03	0.45
т	0.72	0.06	0.33	0.01	0.04	0.68	0.01	0.02	0.49	0.08	0.04	0.02	0.00	0.17	1.78	0.06	0.30	0.19	0.05	0.18	0.00	0.00	0.01	0.07	0.00	0.00	0.00	0.14	0.78	0.02	0.00	0.07
у	0.02	0.08	0.15	0.18	0.23	0.03	0.21	0.05	0.06	0.11	0.14	0.19	0.01	0.11	0.04	0.13	0.07	0.17	0.22	0.02	0.00	0.04	0.00	0.15	0.07	0.03	0.00	0.00	0.00	0.01	0.09	0.01
ф	0.03	0.00	0.00	0.00	0.00	0.04	0.00	0.00	0.05	0.00	0.00	0.00	0.00	0.00	0.01	0.00	0.01	0.00	0.00	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.03	0.00	0.00	0.00
х	0.05	0.01	0.05	0.01	0.02	0.01	0.00	0.01	0.04	0.02	0.02	0.02	0.00	0.04	0.28	0.04	0.01	0.04	0.01	0.02	0.00	0.00	0.00	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
ц	0.07	0.00	0.01	0.00	0.00	0.08	0.00	0.00	0.02	0.01	0.00	0.00	0.00	0.00	0.03	0.01	0.00	0.00	0.00	0.02	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.02	0.00	0.00	0.00	0.00
ч	0.34	0.00	0.01	0.00	0.00	0.48	0.00	0.00	0.20	0.03	0.00	0.00	0.00	0.11	0.01	0.01	0.04	0.01	0.56	0.08	0.00	0.00	0.00	0.00	0.02	0.00	0.00	0.00	0.02	0.00	0.00	0.00
ш	0.10	0.00	0.01	0.00	0.00	0.25	0.00	0.00	0.17	0.06	0.06	0.00	0.00	0.04	0.03	0.00	0.00	0.00	0.00	0.03	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.05	0.00	0.00	0.00
щ	0.03	0.00	0.00	0.00	0.00	0.17	0.00	0.00	0.06	0.00	0.00	0.00	0.00	0.01	0.00	0.00	0.00	0.00	0.00	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
ъ	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.02
ы	0.01	0.04	0.15	0.02	0.05	0.08	0.01	0.02	0.04	0.05	0.23	0.14	0.15	0.09	0.03	0.05	0.03	0.13	0.14	0.01	0.00	0.10	0.00	0.06	0.05	0.01	0.00	0.00	0.00	0.01	0.00	0.01
ь	0.02	0.05	0.15	0.03	0.06	0.12	0.01	0.05	0.14	0.23	0.03	0.09	0.00	0.31	0.09	0.12	0.03	0.22	0.09	0.04	0.00	0.02	0.01	0.08	0.05	0.01	0.00	0.00	0.00	0.03	0.04	0.08
э	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.34	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
ю	0.01	0.06	0.03	0.01	0.05	0.01	0.01	0.01	0.03	0.02	0.01	0.02	0.00	0.04	0.02	0.03	0.01	0.06	0.05	0.01	0.01	0.00	0.00	0.04	0.00	0.02	0.00	0.00	0.00	0.00	0.00	0.01
я	0.02	0.06	0.19	0.04	0.12	0.05	0.03	0.27	0.13	0.10	0.11	0.08	0.00	0.23	0.08	0.12	0.03	0.19	0.26	0.04	0.02	0.03	0.01	0.07	0.00	0.02	0.00	0.00	0.00	0.02	0.02	0.02

Entropy of the text: 4.12 bit/symbol

### Визначення умовних ентропій $H^{(10)}$ , $H^{(20)}$ , $H^{(30)}$

[illegible]





# Криптоаналіз шифру Віженера

Скрипт криптоаналізу шифру Віженера:

```
# -*- coding: utf-8 -*-
import math
import codecs

alphabet_ru = (u'a',u'б',u'в',u'г',u'д',u'е',u'ж',u'з',u'и',u'й',u'к',u'л',u'м',\
               u'н',u'о',u'п',u'р',u'с',u'т',u'у',u'ф',u'х',u'ц',u'ч',u'ш',\
               u'щ',u'ъ',u'ы',u'ь',u'э',u'ю',u'я')
alphabet_en = ('a','b','c','d','e','f','g','h','i','j','k','l','m','n','o',\
               'p','q','r','s','t','u','v','w','x','y','z')
file2 = codecs.open("tmp.txt", "w", encoding='utf-8')
def vigenere(text, key, alphabet):
    z = dict(zip(alphabet, range(0, len(alphabet))))
    r = len(key)
    y = ""

    for i in range(0, len(text)):
        y += alphabet[ (z[text[i]] + z[key[i%r]]) % len(alphabet) ]

    return y

def vigenere_d(text, key, alphabet):
    z = dict(zip(alphabet, range(0, len(alphabet))))
    r = len(key)
    y = ""

    for i in range(0, len(text)):
        y += alphabet[ (z[text[i]] - z[key[i%r]]) % len(alphabet) ]

    return y

def attack(text, alphabet):
    n = len(text)
    D = []
    z = dict(zip(alphabet, range(0, len(alphabet))))

    for r in range(1,31):
        D.append(0)
        for i in range(0,n-r):
            D[r-1] += 1 if text[i] == text[i+r] else 0
    #for i in range(0, len(D)):
    #    print str(i+1) + ": " + str(D[i])

    r = D.index(max(D)) + 1
    #print "r = "+str(r)

    freq_table = [dict(zip(alphabet, [0]*len(alphabet))) for e in range(0,r)]
    key = []
    for k in range(0, r):
        #print len(range(k,n,r))
        c=0
        for i in range(k, n, r):

            if text[i] in alphabet:
                freq_table[k][text[i]] += 1
        #for i in range(0, len(alphabet)):
        #    #file2.write(alphabet[i]+": "+"\
        #    #    str(freq_table[k][alphabet[i]])+"; ")
        #file2.write("\n")
        m = max(freq_table[k].values())
        #print m
```

```

a = [i for i,j in freq_table[k].items() if j == m][0]

key.append((z[a]-z[u'o']) % len(alphabet))
for i in range(0,r):
    key[i] = alphabet[key[i]]
return "".join(key)

if __name__ == "__main__":
    file = codecs.open("encrypted5.txt", "r", encoding='utf-8').\
        read().replace('\n','')
    key = attack(file, alphabet_ru)
    actual_key = u"делолисоборотней"
    pre = vigenere_d(file, actual_key, alphabet_ru)
    file2.write("Key: "+key+"\n")
    file2.write("Pre-open-text:\n")
    for i in range(0, len(pre)):
        file2.write(pre[i])
        if i % 100 == 0 and i != 0:
            file2.write("\n")
    file2.write("\n")
    file2.write("actual key: "+actual_key)

```

## Результат криптоанализу шифру Виженера:

Key: девелииоборойдей

Pre-open-text:

понятноеделокультурунасилъночеловеканевогткнешъвордусиэтудовольногрустнукистинужналинаверноелучшечем  
 дебытонибыловмирекультуристпреждевсегоусилиеижелиносызмальстваисделалосьчеловекусвечнымдажевнут  
 реннепотребнымоттогоотомногочисленныеподразделенияпалатыцеремонийиуделяютстольковниманиядетямособенно  
 детямтехктонаселяетхутунпотоумужобычаяленоствлюдскаяслужитемупочтинеодолимымпрепятствиемнаеобъятны  
 хпросторахимпериивстречаетсяещенемалолудейкоторымпокакимтолишьбуддазнаеткакимпричинамтакинесталоинте  
 реснымичтоглавноенисветозарныесотыдухавеликихрелигийивечныйпоисксмыслажизниземнойпитающийистинное  
 искусствониголовокружителинебезднынакраюкоихвечнопробываетнастилающаянаднимиобщепроходимыгатинаука  
 ниохотябычистоепросторноеосостоятельноеидобродетельноежитьестольестественноедлябольшинстваордусскихпод  
 данныхчтогрехатаитьхутуннаселеныбыливносновоиаварамииневобычнопониманияизтогоословаисстариобознача  
 вшеголюдейнойнеордусскойкультурынаскореетомегозначениикотороестольжедавносделалосьобычнымевропейц  
 ипочтичуждыевсаякойкультурыневедующиритуаловивозвышенныхзабототсутствиеподлиннойвоспитанностибросает  
 сяздесъглазадаженеинвнимательномунаблюдателючеловексдорогимперстемнапальцеодетыйвпрекрасныйшелковыйс  
 узорочьемхалатможетнапримервприсутствииженщиныпроизнестибранноесловоиливысморгатьсяприлюднопрямвзем  
 люпослечегоспокойнодоставитьзруквадорогойрасшитыйлатокутеретьносежеличеловекпозрелелизаматерельт  
 акомсостоянииудушизменияепокакправилоуженельзязразветчтомудроенебвразумиттакиилиначесмотряпровероиспо  
 веданияюземныластямэтидуховныеобластипутьзаказаннасилиеневместноауещеваниезапоздалокакобыниуроди  
 лсяинисталчеловекнадодатьемупрожитьжизньтаккаконхочетконецноееслионпритомневредитокружающимпоэтомубаг  
 неоченьлюбилрайонхутуновикакправилооказывалсяздесълишьпослужебнойнадобностиоткаксегоднянесмотрянапр  
 отивныйнавевающийхандрудоджикбагылисполненлегкогопьянщегооазартавсегдаспутствовавшегоблизкомуиудач  
 номузавершениючередногоделакакконцуподходилорасследованиеоцелойсетичетырязаведенияединовременноподпол  
 ьныхопиумокурительныхвыявленныхвразудаломпоселкецифрыманилипрасадвернулсъявелександриовдохновленныйоткрыв  
 шимисяперспективамивразудаломпоселкеонужевладелнесколькимихарчевнямиилавкамиисликиприбылямотторговли  
 спиртныхнапиткамудастсдобавитьещейдоходотопиумокурениятоможнобудетподуматьорасширениипредпринима  
 тельствооприобретенииновойнедвижимостииншаллабытьможедажеобустановленииконтролянадвсеххарчевнями  
 лавкамиразудалогопоселкаатамоческорвпринадлежавшиечембольшеохваченозаведенийтемвышеприбытоктаксправедливопола  
 телиоборудовалиспециальныезакутыгдекуслаугамжителейигостейхутуноввыстроилисьудобныележанкикурительны  
 еприборыпрасадпредлагалпосетителямновоесредстворасслабительноеочиститьдушупослетрудовыхбуднейпосетит  
 елизинтересовалисьпотомвошливовкуснопрасадбыладенъмечтахужвозомнивсебякняземразудалогоонзахотелно  
 гоисразунанявсебевпомощьнесколькоджихмолодцовпрасадзабылоглавноиустремилссякнизменномуувязавшисьсилой  
 введятьопиумвхарчевниемунепринадлежавшиечембольшеохваченозаведенийтемвышеприбытоктаксправедливопола  
 галлаагобращатьсяквэйбинамдлярешениявозникающихразногласийбылоневхарактереобитателейхутуновинечестн  
 ыйпрасадбеззастенчивостивмиспользовалсяпопыткиздешнихжителейсовладатьслагашемсвоими силамииувенчалис  
 ьуспехомаспидзаранееподготовилскактычкамитотогооказалсясильнееокончательнонаспоясавшисьонснялсостены  
 двустольноеружьедедаиприлюднопрямопосредипереулкаотпилилстольпослечегосталходитьпохутунамсобреломз  
 апазухойдажепрозвизжалполучилорезагаметныелестилрастерялсяопиумокурительнирассцелилпоселкенеобразн  
 опышнымцветомлагашподсчитывалбарышнивеликийучительвдвадцатьвторойглавебеседисужденийнезрясказалнез  
 наиюногооправлениякотороебылобыбесконечнымсамовольноприсвоенныйпрасадомнебесныймандатместногознач  
 енияужеуплылизегорукхотялагашещенеподозревалообэтомвскоренесколькочеловекпотерялитрудоспособностьинт  
 ерескжизнисамоездоровьеследствиечрезмерногоупотребленияопиуманасонгрядущийавандевятыйпопалвбольшниц  
 уулусноеведомствонародногоздоровьявсестороннеизулопричинузаболеванияиванавскореобрезагасамтогоневе  
 дяяпопалвполезрениуправлениявнешнейохранызаседмицустараниямибагаивзятюгоимвпомощьстаршеговэйбинако  
 важнабагссимпатиейнаблюдалкактогорозовощекийислегкаещеподетскинавзвнймолодецпостепеннопревращается  
 всведущегоипытливогомастерасыскногооделарасположенияневсехзаведенийгдекурилиопиумбылоопределеноснаивозм  
 ожнойточностьтакжебылоставленподробныеспискивсехподданныхимевшихотношениекраспространениюопасног  
 одляздоровьяпорокауправлениевнешнейохранысословочевидцевсоставилочленосборныйпортретчеловекакоторыйп  
 овсемвероятиямвлялсястаршимзаправилойтакчеловеконарушительбылизобличендесятьсамыхспособныхвэйбинов  
 переодевшисьвгражданскоеплатязатроесутонкнепрестанногослужебногообднияустановилигдеобрезагабываетпос  
 воимпротивуправнымделаминчвечеромпристеченииизначительныхсилуправленияидурманиваниеордусскихподдан

ныхопиумомрешенобылопресечьпословленномусигналузэйбинынакрываюттсенехорошиезаведениябагсяковомчжаномзадерживаютзаправилиегоближниковкаксталоизвестновечерниечасыпослеобходасвоихвладенийивзиманияежедневнойнеправеднойданилагашсвоимиближникамикороталвносообразномвеселиивхарчевнекунисыновьябагещеразвзглянулначасыираздавилокуроквбронзовойпепельницепораонлегкоподнялсясместаимашинальнопотянулсяпоправитьзапоясоммечномечанебылонапривычномместеродовойклинокбагаканулвнебытиерастворенныйядовитойслюнойзломногоподданногокозюлькаинаэтисобытияописанывделеополкуигоревеановыймечпрославленныйханбалыкскиймастерганьцзянмошубещалотковатьлишьчерезполторагодабагвздохнулнезаметнопроверилскрытыеплотнымхалатомбоевыеножиподхватилзонтипошелквыходуиззалытудагдеседваслышнымшорохомсеялсясквозьгустеющиесумеркибесконечныйдождьпора  
actual key: делолисорботней

## Висновок

В лабораторній роботі було зроблено частотний аналіз різних текстів та визначено ентропії  $H_1$  та  $H_2$ , а також проведено криптоаналіз шифру Віженера та встановлено ключ яким зашифровувався текст.