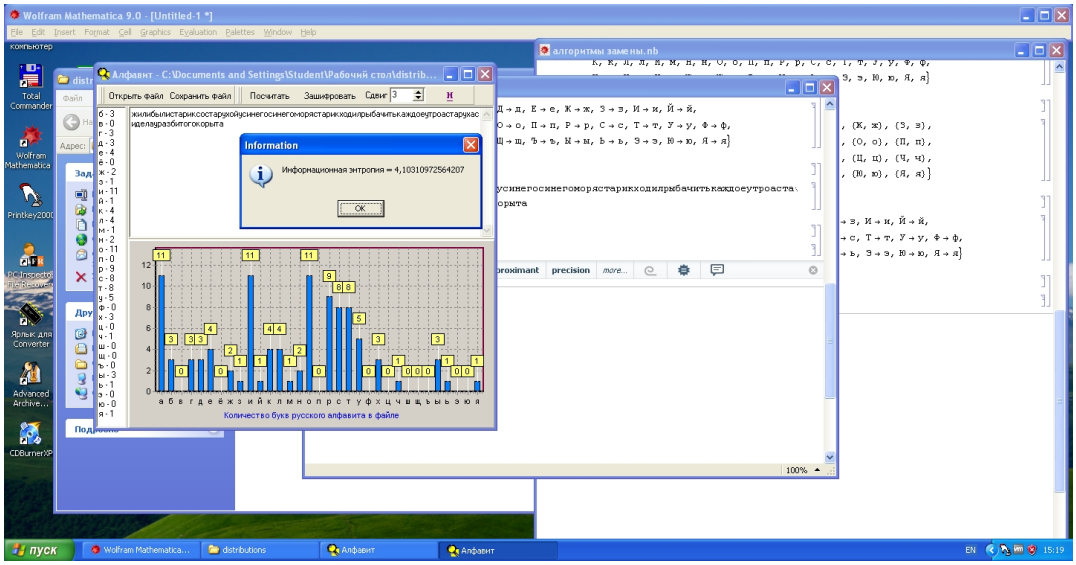
Лабораторная работа №1 “Исследование частотных свойств шифра простой замены”

1. Набрать текст (или ввести в“ALFAVIT” из файла) в “ Блокноте” (порядка 100 букв), исключить пробелы, знаки препинания и заменить заглавные буквы на строчные.

```
In[1]:= text = "Жили были старик со старухой у синего синего моря. Старик
          ходил рыбачить каждое утро, а старуха сидела у разбитого корыта."
Out[1]= Жили были старик со старухой у синего синего моря. Старик
        ходил рыбачить каждое утро, а старуха сидела у разбитого корыта.

In[2]:= text2 = StringReplace[text, " " → ""]
Out[2]= Жилибылистариксостарухойусинегосинегоморя.Старикходилрыбачитькаждоеутро,
        астарухасиделауразбитогокорыта.

In[3]:= text3 = StringReplace[text2, {"." → "", "," → ""}]
Out[3]= ЖилибылистариксостарухойусинегосинегоморяСтарикходилрыбачитькаждоеутроастаруха
          сиделауразбитогокорыта

In[4]:= alfA = CharacterRange["А", "Я"]
Out[4]= {А, Б, В, Г, Д, Е, Ж, З, И, Й, К, Л, М, Н,
         О, П, Р, С, Т, У, Ф, Х, Ц, Ч, Ш, Щ, Ъ, Ы, Ь, Э, Ю, Я}

In[5]:= alfa = CharacterRange["а", "я"]
Out[5]= {а, б, в, г, д, е, ж, з, и, й, к, л, м, н,
         о, п, р, с, т, у, ф, х, ц, ч, ш, щ, ъ, ы, ь, э, ю, я}

In[6]:= temp1 = Partition[Riffle[alfA, alfa], 2]
Out[6]= {{А, а}, {Б, б}, {В, в}, {Г, г}, {Д, д}, {Е, е}, {Ж, ж}, {З, з}, {И, и}, {Й, й}, {К, к},
         {Л, л}, {М, м}, {Н, н}, {О, о}, {П, п}, {Р, р}, {С, с}, {Т, т}, {У, у}, {Ф, ф}, {Х, х},
         {Ц, ц}, {Ч, ч}, {Ш, ш}, {Щ, щ}, {Ъ, ъ}, {Ы, ы}, {Ь, ь}, {Э, э}, {Ю, ю}, {Я, я}}

In[7]:= rl = Apply[Rule, temp1, {1}]
Out[7]= {А → а, Б → б, В → в, Г → г, Д → д, Е → е, Ж → ж, З → з, И → и, Й → й,
         К → к, Л → л, М → м, Н → н, О → о, П → п, Р → р, С → с, Т → т, У → у, Ф → ф,
         Х → х, Ц → ц, Ч → ч, Ш → ш, Щ → щ, Ъ → ъ, Ы → ы, Ь → ь, Э → э, Ю → ю, Я → я}

In[8]:= StringReplace[text3, rl]
Out[8]= жилибылистариксостарухойусинегосинегоморястарикходилрыбачитькаждоеутроастаруха
          сиделауразбитогокорыта
```

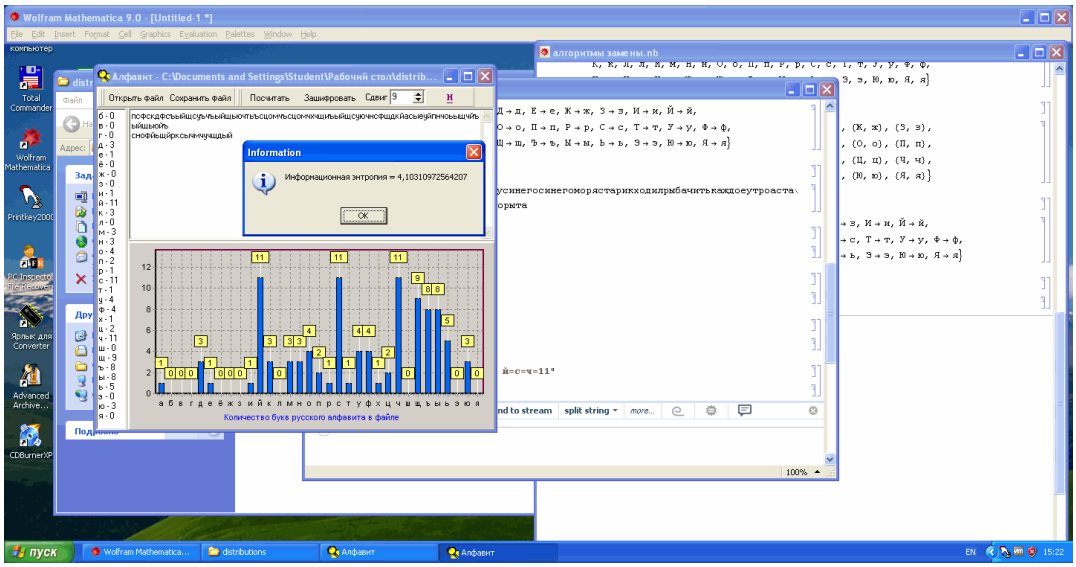
2. Провести анализ текста (опции «Посчитать» и «Н»), выделить и зафиксировать наиболее информативные признаки (3-4 наибольших значения и их положение относительно друг друга) полученного распределения.



H=4.10310972564207, a=и=о=11

3. Для значения КЕ = (N+3)mod11+2, где N - номер по списку в группе, зашифровать текст и вновь провести анализ. Сравнить полученные результаты.

Ke=9



Энтропия та же, й=с=ч=11

Построить вариационный ряд (упорядочить буквы по убыванию вероятности), сравнить с распределением частот русского языка

In[10]:=
```
varr = {{"а", 0.11}, {"и", 0.11}, {"о", 0.11}, {"р", 0.09}, {"с", 0.08},
   {"т", 0.08}, {"у", 0.05}, {"е", 0.04}, {"к", 0.04}, {"л", 0.04},
   {"б", 0.03}, {"г", 0.03}, {"д", 0.03}, {"х", 0.03}, {"ы", 0.03},
   {"ж", 0.02}, {"н", 0.02}, {"з", 0.01}, {"й", 0.01}, {"м", 0.01},
   {"ч", 0.01}, {"ь", 0.01}, {"я", 0.01}, {"в", 0}, {"ё", 0}, {"п", 0},
   {"ф", 0}, {"ц", 0}, {"ш", 0}, {"щ", 0}, {"ъ", 0}, {"э", 0}, {"ю", 0}}
```

Out[10]=
```
{{а, 0.11}, {и, 0.11}, {о, 0.11}, {р, 0.09}, {с, 0.08}, {т, 0.08},
 {у, 0.05}, {е, 0.04}, {к, 0.04}, {л, 0.04}, {б, 0.03}, {г, 0.03},
 {д, 0.03}, {х, 0.03}, {ы, 0.03}, {ж, 0.02}, {н, 0.02}, {з, 0.01},
 {й, 0.01}, {м, 0.01}, {ч, 0.01}, {ь, 0.01}, {я, 0.01}, {в, 0},
 {ё, 0}, {п, 0}, {ф, 0}, {ц, 0}, {ш, 0}, {щ, 0}, {ъ, 0}, {э, 0}, {ю, 0}}
```

In[15]:=
```
alfru = {{" ", 0.175}, {"а", 0.062}, {"б", 0.014},
   {"в", 0.038}, {"г", 0.013}, {"д", 0.025}, {"е", 0.072}, {"ж", 0.007},
   {"з", 0.016}, {"и", 0.062}, {"й", 0.010}, {"к", 0.028}, {"л", 0.035},
   {"м", 0.026}, {"н", 0.053}, {"о", 0.090}, {"п", 0.023}, {"р", 0.040},
   {"с", 0.045}, {"т", 0.053}, {"у", 0.021}, {"ф", 0.002}, {"х", 0.009},
   {"ц", 0.003}, {"ч", 0.012}, {"ш", 0.006}, {"щ", 0.003}, {"ы", 0.016},
   {"ь", 0.014}, {"э", 0.003}, {"ю", 0.006}, {"я", 0.018}}
al = Sort[alfru, #1[[2]] > #2[[2]] &]
```

Out[15]=
```
{{ , 0.175}, {а, 0.062}, {б, 0.014}, {в, 0.038}, {г, 0.013}, {д, 0.025}, {е, 0.072},
 {ж, 0.007}, {з, 0.016}, {и, 0.062}, {й, 0.01}, {к, 0.028}, {л, 0.035},
 {м, 0.026}, {н, 0.053}, {о, 0.09}, {п, 0.023}, {р, 0.04}, {с, 0.045}, {т, 0.053},
 {у, 0.021}, {ф, 0.002}, {х, 0.009}, {ц, 0.003}, {ч, 0.012}, {ш, 0.006},
 {щ, 0.003}, {ы, 0.016}, {ь, 0.014}, {э, 0.003}, {ю, 0.006}, {я, 0.018}}
```

Out[16]=
```
{{ , 0.175}, {о, 0.09}, {е, 0.072}, {и, 0.062}, {а, 0.062}, {т, 0.053}, {н, 0.053},
 {с, 0.045}, {р, 0.04}, {в, 0.038}, {л, 0.035}, {к, 0.028}, {м, 0.026}, {д, 0.025},
 {п, 0.023}, {у, 0.021}, {я, 0.018}, {ы, 0.016}, {з, 0.016}, {ь, 0.014},
 {б, 0.014}, {г, 0.013}, {ч, 0.012}, {й, 0.01}, {х, 0.009}, {ж, 0.007},
 {ю, 0.006}, {ш, 0.006}, {э, 0.003}, {щ, 0.003}, {ц, 0.003}, {ф, 0.002}}
```

In[21]:=
```
Row[{Grid[varr, Frame → All], Grid[al, Frame → All]}, " "]
```

Out[21]=

а	0.11
и	0.11
о	0.11
р	0.09
с	0.08
т	0.08
у	0.05
е	0.04
к	0.04
л	0.04
б	0.03
г	0.03
д	0.03
х	0.03
ы	0.03
ж	0.02
н	0.02
з	0.01
й	0.01
м	0.01
ч	0.01
ь	0.01
я	0.01
в	0
ё	0
п	0
ф	0
ц	0
ш	0
щ	0
ъ	0
э	0
ю	0

	0.175
о	0.09
е	0.072
и	0.062
а	0.062
т	0.053
н	0.053
с	0.045
р	0.04
в	0.038
л	0.035
к	0.028
м	0.026
д	0.025
п	0.023
у	0.021
я	0.018
ы	0.016
з	0.016
ь	0.014
б	0.014
г	0.013
ч	0.012
й	0.01
х	0.009
ж	0.007
ю	0.006
ш	0.006
э	0.003
щ	0.003
ц	0.003
ф	0.002

5. Расшифровать предлагаемый текст CN (N- номер по списку группы), используя наиболее вероятное распределение частот появления букв в тексте на русском языке (пробел в программе ALFAVIT исключен из анализа).

In[22]:=
```
cipher = "те сеитнчтаъ туцнчкрдъ ъхетнчцд
    тк чурбпу цшишжу путщнйктынербтед нтщухсеынд, ту н
журбэук пурнькцчзу нтщухсеынуттаъ хкцшхцуз, знйкусечкхнеруз, щутуихесс,
ткпутчхурнхшксук хецфхуцчхетктнк пучухаъ фу пепнс-рнжу фхньнтес тклкречкрбту.
сецце чепнъ сечкхнеруз тепефрнзекчцд те чкркцчшйндъ, цчшйндъ мзшпумефнцн,
хейнуцчетындъ, з фхезууъхетнчкрбтаъ ухиетеъ н йхшинъ цчхшпчшхеъ."
```

Out[22]=
```
те сеитнчтаъ туцнчкрдъ ъхетнчцд тк
  чурбпу цшишжу путщнйктынербтед нтщухсеынд, ту н
журбэук пурнькцчзу нтщухсеынуттаъ хкцшхцуз, знйкусечкхнеруз, щутуихесс,
ткпутчхурнхшксук хецфхуцчхетктнк пучухаъ фу пепнс-рнжу фхньнтес тклкречкрбту.
сецце чепнъ сечкхнеруз тепефрнзекчцд те чкркцчшйндъ, цчшйндъ мзшпумефнцн,
хейнуцчетындъ, з фхезууъхетнчкрбтаъ ухиетеъ н йхшинъ цчхшпчшхеъ.
```

In[23]:=
```
calfa = RotateLeft[alfa, 5]
```

Out[23]=
```
{е, ж, з, и, й, к, л, м, н, о, п, р, с, т,
 у, ф, х, ц, ч, ш, щ, ъ, ы, ь, э, ю, я, а, б, в, г, д}
```

In[24]:=
```
temp2 = Partition[Riffle[calfa, alfa], 2]
```

Out[24]=
```
{{е, а}, {ж, б}, {з, в}, {и, г}, {й, д}, {к, е}, {л, ж}, {м, з}, {н, и}, {о, й}, {п, к},
 {р, л}, {с, м}, {т, н}, {у, о}, {ф, п}, {х, р}, {ц, с}, {ч, т}, {ш, у}, {щ, ф}, {ъ, х},
 {ы, ц}, {ь, ч}, {э, ш}, {ю, щ}, {я, ъ}, {а, ы}, {б, ь}, {в, э}, {г, ю}, {д, я}}
```

In[25]:=
```
rule2 = Apply[Rule, temp2, {1}]
StringReplace[cipher, rule2]
```

Out[25]=
```
{е → а, ж → б, з → в, и → г, й → д, к → е, л → ж, м → з, н → и, о → й,
 п → к, р → л, с → м, т → н, у → о, ф → п, х → р, ц → с, ч → т, ш → у, щ → ф,
 ъ → х, ы → ц, ь → ч, э → ш, ю → щ, я → ъ, а → ы, б → ь, в → э, г → ю, д → я}
```

Out[26]=
```
на магнитных носителях хранится не
  только сугубо конфиденциальная информация, но и
большое количество информационных ресурсов, видеоматериалов, фонограмм,
неконтролируемое распространение которых по каким-либо причинам нежелательно.
масса таких материалов накапливается на телестудиях, студиях звукозаписи,
радиостанциях, в правоохранительных органах и других структурах.
```

6. Используя результаты п.5, определить ключ расшифрования KD.

Kd=5

7. Открыть пакет “Математика” и прочитать (ReadList) первые 10 букв из файла п.1.

In[41]:=
```
list =
 ReadList["/Users/milord/Documents/STUDY/8_sem/ZI/LAB1_ZI/text1.txt", Byte, 10]
```

Out[41]=
```
{230, 232, 235, 232, 225, 251, 235, 232, 241, 242}
```

In[28]:=
```
first10 = FromCharacterCode[list]
```

Out[28]=
```
æèëèáûëèñò
```

8. С помощью функции FromCharacterCode перевести коды ASCII в символы.

In[42]:=
```
f10code = ToCharacterCode[first10]
```
Out[42]=
```
{230, 232, 235, 232, 225, 251, 235, 232, 241, 242}
```

9. Создать строку, содержащую первые пять символов русского алфавита и с помощью функции ToCharacterCode определить коды представления русского алфавита.

In[44]:=
```
strA = "абвгд"
```
Out[44]=
```
абвгд
```

In[45]:=
```
ToCharacterCode[strA]
```
Out[45]=
```
{1072, 1073, 1074, 1075, 1076}
```

10. Перевести символы вектора п.7 из кодов ASCII в UNICOD и вновь вывести с помощью FromCharacterCode (см. Character Codes в системе документации Wolfram Mathematica).

In[46]:=
```
FromCharacterCode[f10code + 848]
```
Out[46]=
```
жилибылист
```

11. Используя пример (шаблон) для латинского алфавита сформировать программу, реализующую шифр Цезаря для русского алфавита с вводом данных из файла. С помощью функции ToCharacterCode и FromCharacterCode пакета “Математика”, преобразующих символы в ASCII коды и обратно (код буквы a-97, код буквы b-98 и т.д.), можно задать шифр Цезаря с помощью следующей функции:

```
CaesarCipher[plaintext_, key_]:=
FromCharacterCode[ Mod[ ToCharacterCode[plaintext] - 97 +key, 26] + 97]
```

Пример использования:

```
CaesarCipher[plaintext_, key_]:=  FromCharacterCode[ Mod[ ToCharacterCode[plaintext] - 97 +key, 26] + 97]
plaintext=”typehereyourplaintextinsmallletters”;
key=24;
CaesarCipher[plaintext,key]
rwncfcpcwmspnjyglrcvrglqkyjjjcrrcpq
```

In[47]:=
```
CaesarCipher[plaintext_, key_] :=
 FromCharacterCode[Mod[ToCharacterCode[plaintext] - 1072 + key, 32] + 1072]
```

In[48]:=
```
CaesarCipher["жилибылист", 9]
```
Out[48]=
```
псфскдфсъы
```

12. Реализовать расшифровку заданного в п.5 файла CN методом силовой атаки (использовать первые 40 символов текста).

Пример для латинского алфавита : ciphertext=”yhaklwpnw”;

Table[CaesarCipher[ciphertext,-key],{key,1,26}].

In[49]:=
```
ciphertext =
 ReadList["/Users/milord/Documents/STUDY/8_sem/ZI/LAB1_ZI/C4.TXT", Byte, 40]
```

Out[49]=
```
{242, 229, 32, 241, 229, 232, 242, 237, 247, 242, 224, 250,
 32, 242, 243, 246, 237, 247, 234, 240, 228, 250, 32, 250, 245, 229,
 242, 237, 247, 246, 228, 32, 242, 234, 32, 247, 243, 240, 225, 239}
```

In[50]:=
```
textToDecipher = ciphertext + 848
```

Out[50]=
```
{1090, 1077, 880, 1089, 1077, 1080, 1090, 1085, 1095, 1090, 1072, 1098, 880, 1090,
 1091, 1094, 1085, 1095, 1082, 1088, 1076, 1098, 880, 1098, 1093, 1077, 1090,
 1085, 1095, 1094, 1076, 880, 1090, 1082, 880, 1095, 1091, 1088, 1073, 1087}
```

In[51]:=
```
newcipher = FromCharacterCode[textToDecipher]
```

Out[51]=
```
теЂсеитнчтаъЂтуцнчкрдъЂъхетнчцдЂткЂчурбп
```

In[52]:=
```
newcipher = StringReplace[newcipher, "Ђ" → ""]
```

Out[52]=
```
тесеитнчтаътуцнчкрдъъхетнчцдткчурбп
```

In[53]:=
```
Table[CaesarCipher[newcipher, -key], {key, 1, 32}]
```

Out[53]=
```
{сдрдзсмцсящстхмцйпгщщфдсмцхгсйцтпао, ргпгжрлхрюшрсфлхиовшшугрлхфврихсоян,
 пвовепкфпэчпрукфзнбччтвпкфубпзфрнюм, обнбдойуоьцоптйужмаццсбойутаожупмэл,
 намагнитныхносителяххранитсянетольк, мялявмзсмъфмнрзсдкюффпямзсрюмдснкый,
 люкюблжрлщулмпжргйэууоюлжрпэлгрмйъи, кэйэакепкштклоепвиьттнэкепоькквплищз,
 йьиьяйдойчсйкндобзыссмьйдоныйбокзшж, иызыюигницриймгнажъррлыигнмъианйжче,
 зъжъэзвмзхпзилвмяещппкъзвмлщзямиецд, жщещьжблжфожзкблюдшоойщжблкшжюлздхг,
 ешдшыеакеунежйакэгчннишеакйчеэкжгфв, дчгчъдяйдтмдеияйьвцммзчдяйицдьйевуб,
 гцвцщгюигслгдзюиыбхллжцгюизхгыидбта, вхбхшвэзврквгжэзъафккехвэзжфвъзгася,
 бфафчбьжбпйбвеьжщяуййдфбьжеубщжвярю, ауяуцаыеаоиабдыешютиигуаыедташебюпэ,
 ятютхяъдянзяагъдчэсззвтяъдгсячдаэоь, юсэсфющгюмжюявщгцьржжбсющгврюцгяьны,
 эрьруэшвэлеэюбшвхыпееарэшвбпэхвюымъ, ьпыптьчбькдьэачбфъоддяпьчбаоьфбэълщ,
 ыоъосыцаыйгыьяцаущнггюоыцаяныуаьщкш, ънщнръхяъивъыюхятшмввэнъхяюмътяышйч,
 щмшмпщфющзбщъэфюсчлббьмщфюэлщсюъчиц, шлчлошуэшжашщьуэрцкааылшуэькшрэщцзх,
 чкцкнчтьчеячшытьпхйяяъкчтыыйчпьшхжф, цйхймцсыцдюцчъсыофиюющйцсыъицоычфеу,
 хифилхръхгэхцщрънузээшихръщзхнъцудт, фзузкфпщфвьфхшпщмтжььчзфпщшжфмщхтгс,
 ужтжйуошубыуфчошлсеыыцжуошчеулшфсвр, тесеитнчтаътуцнчкрдъъхетнчцдткчурбп}
```