

## Лабораторная работа №2 “Шифры перестановки”

1. Подготовить открытый текст для шифрования : импортировать файл соответствующий номеру N по списку в группе и содержащий открытый текст (папка Plaintext; . distributions\ импорт открытого текста.nb ), привести размер текста к величине кратной 10, удалить пробелы.

In[1]:= `plaintext =`

```
FromCharacterCode[Import["/Users/milord/Documents/STUDY/8_sem/ZI/LAB2_ZI/work  
task/work task/Text-04.txt", "Byte"], "WindowsCyrillic"]
```

Out[1]= сигарету и закурил хотя больше всего ему сейчас хотелось вскочить в машину и  
гнать гнать гнать поскорее отсюда но гнать было пока нельзя все надо  
было делать медленно и расчетливо что же ты плачущим голосом сказал из  
машины барбридж воду не вылил снасти все сухие чего стоишь прячь хабар

In[2]:= `textnospace = StringReplace[plaintext, " " -> ""]`

Out[2]= сигаретуизакурилхотябольшевсегоемусейчасхотелосьвскочитьвмашинуигнатьгнатьгнать  
ьпоскорееотсюданогнатьбылопоканельзявсенадобылоделатьмедленноирасчетливочто  
оже тыплачущимголосомсказализмашиныбарбриджводу не вылилснастивсесухиечегосто  
ишьпрячьхабар

In[3]:= `text100 = StringTake[textnospace, 230]`

Out[3]= сигаретуизакурилхотябольшевсегоемусейчасхотелосьвскочитьвмашинуигнатьгнатьгнать  
ьпоскорееотсюданогнатьбылопоканельзявсенадобылоделатьмедленноирасчетливочто  
оже тыплачущимголосомсказализмашиныбарбриджводу не вылилснастивсесухиечегосто  
ишьп

2. Определить следующие характеристики текста: энтропию позначной модели, энтропию биграммной модели, частоты чередования гласных и согласных букв (см. distributions\ анализ текста на чередование букв.nb).

In[4]:= `Print["Энтропия позначной модели"]`

```
En = N[Entropy[2, text100]]
```

Энтропия позначной модели

Out[5]= 4.41307

In[6]:= `Print["Энтропия биграммной модели"]`

```
N[Entropy[2, Partition[Characters[text100], 2]]]
```

Энтропия биграммной модели

Out[7]= 6.39528

In[8]:= `gl = {"а", "е", "и", "о", "у", "ы", "э", "ю", "я"}`

Out[8]= {а, е, и, о, у, ы, э, ю, я}

In[9]:= `sl = {"б", "в", "г", "д", "ж", "з", "й", "к", "л", "м",  
"н", "п", "р", "с", "т", "ф", "х", "ц", "ч", "ш", "щ", "ъ", "ь"}`

Out[9]= {б, в, г, д, ж, з, й, к, л, м, н, п, р, с, т, ф, х, ц, ч, ш, щ, ъ, ь}

```

In[10]:= listGL = Table[char = StringTake[text100, {i}];
           StringMatchQ[char, sl], {i, 1, StringLength[text100]}};
summGG = 0;
summGS = 0;
summSG = 0;
summSS = 0;

In[15]:= Do[Which[listGL[[k]] && listGL[[k + 1]], summGG++,
              listGL[[k]] && ! listGL[[k + 1]], summGS++,
              ! listGL[[k]] && listGL[[k + 1]], summSG++,
              ! listGL[[k]] && ! listGL[[k + 1]], summSS++], {k, StringLength[text100] - 1}]

In[16]:= Print["гласная-гласная = ", summGG, "\n",
              "гласная-согласная = ", summGS, "\n",
              "согласная-гласная = ", summSG, "\n",
              "согласная-согласная = ", summSS]

гласная-гласная = 53
гласная-согласная = 84
согласная-гласная = 84
согласная-согласная = 8

```

3. Сформировать матрицу, содержащую 10 столбцов.

4. Провести операцию шифрования методом простой маршрутной перестановки: заполнить таблицу открытым текстом последовательно по строкам, а затем считать текст последовательно по столбцам. Определить характеристики зашифрованного текста согласно п.2.

```

In[17]:= listText = Characters[text100]

```

```

Out[17]:= {с, и, г, а, р, е, т, у, и, з, а, к, у, р, и, л, х, о, т, я, б, о, л, ь, ш, е, в, с, е, г, о,
           е, м, у, с, е, й, ч, а, с, х, о, т, е, л, о, с, ь, в, с, к, о, ч, и, т, ь, в, м, а, ш,
           и, н, у, и, г, н, а, т, ь, г, н, а, т, ь, г, н, а, т, ь, п, о, с, к, о, р, е, е, о, т,
           с, ю, д, а, н, о, г, н, а, т, ь, б, ы, л, о, п, о, к, а, н, е, л, ь, з, я, в, с, е, н,
           а, д, о, б, ы, л, о, д, е, л, а, т, ь, м, е, д, л, е, н, н, о, и, р, а, с, ч, е, т,
           л, и, в, о, ч, т, о, ж, е, т, ы, п, л, а, ч, у, щ, и, м, г, о, л, о, с, о, м, с, к,
           а, з, а, л, и, з, м, а, ш, и, н, ы, б, а, р, б, р, и, д, ж, в, о, д, у, н, е, в, ы,
           л, и, л, с, н, а, с, т, и, в, с, е, с, у, х, и, е, ч, е, г, о, с, т, о, и, ш, ь, п}

```

In[18]:= **matrix = Partition[listText, 23]**

Out[18]= { {с, и, г, а, р, е, т, у, и, з, а, к, у, р, и, л, х, о, т, я, б, о, л},  
 {ь, ш, е, в, с, е, г, о, е, м, у, с, е, й, ч, а, с, х, о, т, е, л, о},  
 {с, ь, в, с, к, о, ч, и, т, ь, в, м, а, ш, и, н, у, и, г, н, а, т, ь},  
 {г, н, а, т, ь, г, н, а, т, ь, п, о, с, к, о, р, е, е, о, т, с, ю, д},  
 {а, н, о, г, н, а, т, ь, б, ы, л, о, п, о, к, а, н, е, л, ь, з, я, в},  
 {с, е, н, а, д, о, б, ы, л, о, д, е, л, а, т, ь, м, е, д, л, е, н, н},  
 {о, и, р, а, с, ч, е, т, л, и, в, о, ч, т, о, ж, е, т, ы, п, л, а, ч},  
 {у, щ, и, м, г, о, л, о, с, о, м, с, к, а, з, а, л, и, з, м, а, ш, и},  
 {н, ы, б, а, р, б, р, и, д, ж, в, о, д, у, н, е, в, ы, л, и, л, с, н},  
 {а, с, т, и, в, с, е, с, у, х, и, е, ч, е, г, о, с, т, о, и, ш, ь, п} }

In[19]:= **matrixG = Grid[matrix, Frame → All]**

Out[19]= 

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

In[20]:= **mt = Transpose[matrix]**

Out[20]= { {с, ь, с, г, а, с, о, у, н, а},  
 {и, ш, ь, н, н, е, и, щ, ы, с}, {г, е, в, а, о, н, р, и, б, т},  
 {а, в, с, т, г, а, а, м, а, и}, {р, с, к, ь, н, д, с, г, р, в},  
 {е, е, о, г, а, о, ч, о, б, с}, {т, г, ч, н, т, б, е, л, р, е},  
 {у, о, и, а, ь, ы, т, о, и, с}, {и, е, т, т, б, л, л, с, д, у},  
 {з, м, ь, ь, ы, о, и, о, ж, х}, {а, у, в, п, л, д, в, м, в, и},  
 {к, с, м, о, о, е, о, с, о, е}, {у, е, а, с, п, л, ч, к, д, ч},  
 {р, й, ш, к, о, а, т, а, у, е}, {и, ч, и, о, к, т, о, з, н, г},  
 {л, а, н, р, а, ь, ж, а, е, о}, {х, с, у, е, н, м, е, л, в, с},  
 {о, х, и, е, е, е, т, и, ы, т}, {т, о, г, о, л, д, ы, з, л, о},  
 {я, т, н, т, ь, л, п, м, и, и}, {б, е, а, с, з, е, л, а, л, ш},  
 {о, л, т, ю, я, н, а, ш, с, ь}, {л, о, ь, д, в, н, ч, и, н, п} }

In[21]:= **mtG = Grid[mt, Frame → All]**

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

Out[21]=

In[22]:= **rotText = Flatten[mt]**

Out[22]= {с, ь, с, г, а, с, о, у, н, а, и, ш, ь, н, н, е, и, щ, ы, с, г, е, в, а, о, н, р, и, б, т, а, в, с, т, г, а, а, м, а, и, р, с, к, ь, н, д, с, г, р, в, е, е, о, г, а, о, ч, о, б, с, т, г, ч, н, т, б, е, л, р, е, у, о, и, а, ь, ы, т, о, и, с, и, е, т, т, б, л, л, с, д, у, з, м, ь, ь, ы, о, и, о, ж, х, а, у, в, п, л, д, в, м, в, и, к, с, м, о, о, е, о, с, о, е, у, е, а, с, п, л, ч, к, д, ч, р, й, ш, к, о, а, т, а, у, е, и, ч, и, о, к, т, о, з, н, г, л, а, н, р, а, ь, ж, а, е, о, х, с, у, е, н, м, е, л, в, с, о, х, и, е, е, е, т, и, ы, т, т, о, г, о, л, д, ы, з, л, о, я, т, н, т, ь, л, п, м, и, и, б, е, а, с, з, е, л, а, л, ш, о, л, т, ю, я, н, а, ш, с, ь, л, о, ь, д, в, н, ч, и, н, п}

In[23]:= **stringRot = StringJoin[rotText]**

Out[23]= сысгасоунаишньннеищысгеваонрибтавстгаамаирскьндсгрвееогаочобстгчнтбелреуоиаьытои сиеттбллсдузмььыоижхаувлдвмвиксмоеоеосоеуеасплчкдчрйшкоатауеичиоктознгла: нраьжаеохсуенмелвсохиееттиыттоголдызлоятнттьлпмиибеасзелалшолтюднчнп

In[24]:= **Print["Энтропия позначной модели"]**

**En = N[Entropy[2, stringRot]]**

Энтропия позначной модели

Out[25]= 4.41307

```
In[26]:= Print["Энтропия биграмной модели"]
N[Entropy[2, Partition[Characters[stringRot], 2]]]
Энтропия биграмной модели
```

```
Out[27]= 6.57149
```

```
In[28]:= listGL2 = Table[char = StringTake[stringRot, {i}];
StringMatchQ[char, sl], {i, 1, StringLength[stringRot]}}];
summGG2 = 0;
summGS2 = 0;
summSG2 = 0;
summSS2 = 0;

In[33]:= Do[Which[listGL2[[k]] && listGL2[[k + 1]], summGG2++,
listGL2[[k]] && ! listGL2[[k + 1]], summGS2++,
! listGL2[[k]] && listGL2[[k + 1]], summSG2++,
! listGL2[[k]] && ! listGL2[[k + 1]], summSS2++], {k, StringLength[stringRot] - 1}]

In[34]:= Print["гласная-гласная = ", summGG2, "\n",
"гласная-согласная = ", summGS2, "\n",
"согласная-гласная = ", summSG2, "\n",
"согласная-согласная = ", summSS2]
```

```
гласная-гласная = 87
гласная-согласная = 50
согласная-гласная = 50
согласная-согласная = 42
```

5. Расшифровать текст соответствующий номеру N (папка Crypttext; . distributions\ импорт зашифрованного текста.nb), который зашифрован методом перестановки столбцов (шифр вертикальной перестановки) с ключом, приведенном в таблице:

1 - барокамера 7 - кавалерист 2 - ватерлиния 8 - легкоатлет 3 - галантерея 9 - магнитофон 4 - двухтомник 10 - нормировка 5 - жилплощадь 11 - радиолампа 6 - заповедник 12 - стекловата

```
In[35]:= te = Import["/Users/milord/Documents/STUDY/8_sem/ZI/LAB2_ZI/work
task/work task/Text-04c.txt"]
```

```
Out[35]= икоееонасдыбматумаиывгсабохкиноюблорччомрвиеитеаваьттнааовлоирнсеьзягсшгпс
ьедтиоасзбетчпхвйсвааенкеенлыоабднхиуосчьмттоаанлнпплауаишелееоьннегосде
ттгзыосуоришслтггропволееманвлстгулмтчуткалзыесошсдлсоарьюеиьноялдчжики
жиес
```

```
In[36]:= tab = {"барокамера", "ватерлиния", "галантерея", "двухтомник",
"жилплощадь", "заповедник", "кавалерист", "легкоатлет",
"магнитофон", "нормировка", "радиолампа", "стекловата"}
```

```
Out[36]= {барокамера, ватерлиния, галантерея, двухтомник, жилплощадь, заповедник,
кавалерист, легкоатлет, магнитофон, нормировка, радиолампа, стекловата}
```

```
In[37]:= ord = Table[0, {12}];
For[i = 0, i ≤ 11, i++;
ord[[i]] = Ordering[Characters[tab[[i]]]]]
```

In[60]:= `Grid[key = {ord[[4]], Range[Length[ord[[12]]]}], Frame → All]`

Out[60]=

2	1	9	10	7	8	6	5	3	4
1	2	3	4	5	6	7	8	9	10

In[59]:= `cryptText = te`

Out[59]= `икоеоонасдыьбматумаиывгсабохкинояблорччомрвиеитеаваьттнаовлоирнсеьзгссшгпс  
ьедтиоасзбетчпхвйсвааенкеенлыоабднхиуосчьмттоаанлнпплауаишелееоьннегосде  
ттгзыосуоришслтггруппволееманвлстгулмтчуткалзыесошсдлсоарьуеииьноялджик  
жис`

In[61]:= `cryptTable = Partition[Characters[cryptText], 23]`

Out[61]=

```
{ {и, к, о, е, о, о, н, а, с, д, ы, ь, б, м, а, т, у, м, а, и, ы, в, г},
  {с, а, б, о, х, к, и, н, о, ю, б, л, о, ь, р, ч, ч, о, м, р, в, и, е},
  {и, т, е, а, в, а, ь, ь, т, т, н, а, а, о, в, л, о, и, р, н, с, е, ь},
  {з, я, г, с, с, ш, г, п, с, ь, е, д, т, и, о, а, с, з, б, е, т, ч, п},
  {т, х, в, й, с, в, а, а, е, н, к, е, е, н, л, ы, о, а, б, д, н, х, и},
  {у, о, с, ч, ь, м, т, т, о, а, а, н, л, н, и, п, л, л, а, у, а, и, ш},
  {е, л, е, е, о, ь, н, н, е, г, о, с, д, е, т, т, г, з, ы, о, с, у, о},
  {р, и, ш, с, л, т, г, г, р, о, п, в, о, л, е, е, м, а, н, в, л, с, т},
  {г, у, л, м, т, ч, у, т, к, а, л, з, ы, е, с, о, щ, с, ш, д, л, с, о},
  {а, р, ь, у, е, и, и, ь, о, н, о, я, л, д, ч, ж, и, к, и, ж, и, е, с} }
```

In[62]:= `cryptTable = Transpose[cryptTable]`

Out[62]=

```
{ {и, с, и, з, т, у, е, р, г, а},
  {к, а, т, я, х, о, л, и, у, р}, {о, б, е, г, в, с, е, ш, л, ь},
  {е, о, а, с, й, ч, е, с, м, у}, {о, х, в, с, с, ь, о, л, т, е},
  {о, к, а, ш, в, м, ь, т, ч, и}, {н, и, ь, г, а, т, н, г, у, и},
  {а, н, ь, п, а, т, н, г, т, ь}, {с, о, т, с, е, о, е, р, к, о},
  {д, ю, т, ь, н, а, г, о, а, н}, {ы, б, н, е, к, а, о, п, л, о},
  {ь, л, а, д, е, н, с, в, з, я}, {б, о, а, т, е, л, д, о, ы, л},
  {м, ь, о, и, н, н, е, л, е, д}, {а, р, в, о, л, и, т, е, с, ч},
  {т, ч, л, а, ы, п, т, е, о, ж}, {у, ч, о, с, о, л, г, м, щ, и},
  {м, о, и, з, а, л, з, а, с, к}, {а, м, р, б, б, а, ы, н, ш, и},
  {и, р, н, е, д, у, о, в, д, ж}, {ы, в, с, т, н, а, с, л, л, и},
  {в, и, е, ч, х, и, у, с, с, е}, {г, е, ь, п, и, ш, о, т, о, с} }
```

```
In[63]:= Grid[cryptTable, Frame → All]
```

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

Out[63]=

```
In[64]:= Grid[decryptTable = Table[0, {23}, {10}], Frame → All]
```

[illegible]

Out[64]=

```
In[65]:= Do[decryptTable[All, key[[1, i]]] = cryptTable[All, key[[2, i]]], {i, 1, 10}]
Row[Grid[cryptTable, Frame → All], Grid[decryptTable, Frame → All]], " "]
plain = StringJoin[decryptTable]
```

Out[66]=

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

```
Out[67]= сигаретуизакурилхотябольшевсегоемусейчасхотелосьвсколотитьмашинуигнатьгнатьгнать
ьпоскорееотсюданогнатьбылопоканельзязвсенадобылоделатъмедленноирасчетливочто
оже тыплачушимголосомсказализмашиныбарббриджводуневылилснастивсесухиечтосто
ишьп
```

```
In[68]:= Print["Энтропия позначной модели"]
```

```
N[Entropy[2, plain]]
```

```
Энтропия позначной модели
```

Out[69]= 4.41307

```
In[70]:= Print["Энтропия биграмной модели"]
```

```
N[Entropy[2, Partition[Characters[plain], 2]]]
```

```
Энтропия биграмной модели
```

Out[71]= 6.39528

```
In[72]:= listGL3 = Table[char = StringTake[stringRot, {i}];
StringMatchQ[char, sl], {i, 1, StringLength[stringRot]}}];
summGG3 = 0;
summGS3 = 0;
summSG3 = 0;
summSS3 = 0;
```



```
In[77]:= Do[Which[listGL3[[k]] && listGL3[[k + 1]], summGG3++,
  listGL3[[k]] && ! listGL3[[k + 1]], summGS3++,
  ! listGL3[[k]] && listGL3[[k + 1]], summSG3++,
  ! listGL3[[k]] && ! listGL3[[k + 1]], summSS3++], {k, StringLength[plain] - 1}]
```

```
In[78]:= Print["гласная-гласная = ", summGG3, "\n",
  "гласная-согласная = ", summGS3, "\n",
  "согласная-гласная = ", summSG3, "\n",
  "согласная-согласная = ", summSS3]
```

гласная-гласная = 87

гласная-согласная = 50

согласная-гласная = 50

согласная-согласная = 42

6. Провести процедуру шифрования открытого текста (п. 1) с применением шифра перестановки степени  $n$ , где  $n$  - это длина текста. Для чего сформировать случайную неповторяющуюся последовательность целых чисел из интервала  $[1, n]$  с помощью функции `RandomSample[]`, ключом является начальное состояние генератора случайных чисел, определяемое  $N$ . Провести перестановку символов в списке и получить зашифрованный текст. Определить характеристики зашифрованного текста согласно п.2. Провести расшифрование зашифрованного текста.

```
In[79]:= SeedRandom[4];
```

```
In[80]:= keyR = RandomSample[Range[1, 230]]
```

```
Out[80]:= {80, 183, 89, 91, 46, 82, 90, 15, 227, 54, 116, 161, 142, 65, 177, 223, 67, 18, 171,
  199, 168, 203, 169, 210, 219, 121, 118, 48, 139, 12, 93, 28, 87, 37, 83, 4, 86,
  131, 50, 165, 141, 61, 40, 76, 1, 197, 182, 211, 2, 21, 35, 195, 196, 117, 24,
  170, 113, 215, 176, 13, 163, 228, 99, 145, 3, 221, 179, 129, 36, 200, 64, 157,
  206, 95, 104, 56, 148, 126, 8, 70, 213, 88, 218, 212, 189, 22, 224, 112, 135,
  134, 225, 57, 75, 167, 103, 33, 25, 110, 154, 14, 158, 216, 190, 162, 9, 11,
  187, 127, 186, 30, 77, 68, 205, 38, 137, 209, 202, 108, 96, 180, 151, 166, 63,
  41, 123, 23, 130, 120, 16, 47, 55, 72, 98, 81, 192, 125, 207, 217, 136, 107, 29,
  94, 146, 109, 79, 149, 160, 69, 194, 42, 128, 229, 208, 147, 184, 153, 159, 193,
  101, 71, 31, 214, 124, 222, 138, 105, 100, 45, 51, 106, 201, 59, 58, 49, 175, 5,
  164, 27, 174, 66, 230, 26, 150, 152, 60, 144, 44, 132, 52, 111, 62, 39, 191, 97,
  133, 32, 78, 178, 53, 188, 198, 17, 226, 172, 122, 7, 156, 84, 20, 220, 19, 43,
  143, 73, 114, 173, 85, 92, 34, 155, 119, 102, 74, 185, 181, 204, 6, 10, 140, 115}
```

```
In[82]:= chars = Characters[text100]
```

```
Out[82]:= {с, и, г, а, р, е, т, у, и, з, а, к, у, р, и, л, х, о, т, я, б, о, л, ь, ш, е, в, с, е, г, о,
  е, м, у, с, е, й, ч, а, с, х, о, т, е, л, о, с, ь, в, с, к, о, ч, и, т, ь, в, м, а, ш,
  и, н, у, и, г, н, а, т, ь, г, н, а, т, ь, г, н, а, т, ь, п, о, с, к, о, р, е, е, о, т,
  с, ю, д, а, н, о, г, н, а, т, ь, б, ы, л, о, п, о, к, а, н, е, л, ь, з, я, в, с, е, н,
  а, д, о, б, ы, л, о, д, е, л, а, т, ь, м, е, д, л, е, н, н, о, и, р, а, с, ч, е, т,
  л, и, в, о, ч, т, о, ж, е, т, ы, п, л, а, ч, у, щ, и, м, г, о, л, о, с, о, м, с, к,
  а, з, а, л, и, з, м, а, ш, и, н, ы, б, а, р, б, р, и, д, ж, в, о, д, у, н, е, в, ы,
  л, и, л, с, н, а, с, т, и, в, с, е, с, у, х, и, е, ч, е, г, о, с, т, о, и, ш, ь, п}
```

```
In[86]:= textR = {};
Do[AppendTo[textR, chars[[keyR[[i]]]], {i, 230}]
resR = StringJoin[textR]
```

```
Out[88]= пштюосииисчагаоаоонллотеоньокасейкаеьсмриснсдаиибсвоеьсзсущтегеиаееиысоьид
угсоивросьлдтвголмшежрпубуиабеыгatlчнсаягзчгухылтдлстааоионхекентньваъжоль
алиолдбноелгнпльковамваривкнпешчемолнарнеетлчаухомбттоячттстятсрдудеаььнми
езив
```

```
In[89]:= Print["Энтропия позначной модели"]
N[Entropy[2, resR]]
Энтропия позначной модели
```

```
Out[90]= 4.41307
```

```
In[91]:= Print["Энтропия биграмной модели"]
N[Entropy[2, Partition[Characters[resR], 2]]]
Энтропия биграмной модели
```

```
Out[92]= 6.62367
```

```
In[98]:= listGL4 = Table[char = StringTake[resR, {i}];
StringMatchQ[char, sl], {i, 1, StringLength[resR]}};
summGG4 = 0;
summGS4 = 0;
summSG4 = 0;
summSS4 = 0;
```

```
In[103]:= Do[Which[listGL4[[k]] && listGL4[[k + 1]], summGG4++,
listGL4[[k]] && ! listGL4[[k + 1]], summGS4++,
! listGL4[[k]] && listGL4[[k + 1]], summSG4++,
! listGL4[[k]] && ! listGL4[[k + 1]], summSS4++], {k, StringLength[resR] - 1}]
```

```
In[104]:= Print["гласная-гласная = ", summGG4, "\n",
"гласная-согласная = ", summGS4, "\n",
"согласная-гласная = ", summSG4, "\n",
"согласная-согласная = ", summSS4]
```

```
гласная-гласная = 83
гласная-согласная = 54
согласная-гласная = 54
согласная-согласная = 38
```